Sicherheit der Xanadu-Plattform

Zuletzt aktualisiert: 07.11.2024

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

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

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

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

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

Automatische Übersetzung

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

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Inhaltsverzeichnis

Instanz sichern ... 9
ServiceNow Vault ... 11
Platform-Sicherheit ... 14
Security Center ... 16
Übersicht ... 18
Sicherheitshärtung ... 19
Sicherheitsscanner ... 25
Sicherheitsmetriken ... 31
Kundenaktionen ... 37
Best Practices für Sicherheit ... 41
Security Learning ... 48
Bannerankündigungen zur Sicherheit ... 48
Dashboards zur Sicherheitslage ... 49
Benachrichtigungen zu Sicherheitsereignissen ... 51
Instanz-Sicherheitszentrum ... 57
Migration des Instanz-Sicherheitszentrums zu ServiceNow Security Center ... 67
Sicherheitsereignisse überwachen ... 69
Überprüfen Sie die tägliche Compliance-Punktzahl, und konfigurieren Sie die Einstellungen für Sicherheitseigenschaften ... 76
Suchen Sie nach falschen Sicherheitsdefinitionen ... 86
Überwachen Sie Instanzmetriken ... 87
Aktivieren Sie die ISC-Schnittstelle Virtual Agent ... 101
Härtungseinstellungen für die Instanzsicherheit ... 102
Härtungseinstellungen ... 208
Baseline der Härtungseinstellungen ... 209
Zugriffssteuerung ... 230
API und Webservice ... 282
Architektur, Design und Bedrohungsmodellierung ... 298
Authentifizierung ... 308
Geschäftslogik ... 338
Kommunikation ... 341
Konfiguration ... 346
Datenschutz ... 358
Fehlerbehandlung und -protokollierung ... 361
Datei und Ressourcen ... 369
Böswilliger Code ... 377
Management von Anwendersitzungen ... 378
Gespeicherte Kryptografie ... 394
Validierung, Bereinigung und Codierung ... 395
Log Export Service (LES) ... 429

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Log Export Service Rollen 431
Protokollquellen 433
Erstellen Sie eine Protokollquellenkonfiguration 433
Kafka-Verbraucher 435
MID-Server-Verbraucher 440
Überprüfen Sie den Protokollbericht 445
Protokolle 447
Systemprotokolle 448
Protokollierung, Audits und Fehler 463
Geheimnisverwaltung 464
Geheimnisverwaltung erkunden 465
Für den Client zugängliche Geheimnisse konfigurieren 470
Dashboard für die Geheimnisverwaltung 488
Codesignatur 500
Codesignatur erkunden 503
Codesignatur konfigurieren 505
Codesignatur verwenden 528
Codesignaturreferenz 543
Antivirus-Scanning 550
Antivirus-Scanning erkunden 551
Antivirus-Scanning konfigurieren 553
Dateien in Quarantäne werden überprüft 554
Kenntnisse über Wörterbuchattribute für Antivirus-Scanning 555
HTML-Bereinigung 556
HTML-Bereinigung erkunden 558
Konfigurieren der HTML-Bereinigung 561
HTML-Bereinigung aktivieren 562
Auditing 563
Auditing erkunden 565
Auditing für eine Tabelle konfigurieren 567
Sys-Audit- und Audit-Beziehungsänderungstabellen anzeigen 570
Wissen über Verlaufssätze 571
Strenge Sicherheitseinstellungen 582
Strenge Sicherheitseinstellungen erkunden 584
Sandbox-Eigenschaft für Skript konfigurieren 596
Einstellungen für hohe Sicherheit werden aktiviert 600
Virtuelles privates Netzwerk (VPN) 602
Virtual Private Network (VPN) erkunden 603
Aktivieren eines VPN-Service 606
Konfigurieren einer Adresse für die VPN-Kommunikation 606
Plattform-Datenschutz 608
Datenschutz 609

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenschutz erkunden....610
Domain Separation und Datenschutz....611
Unterstützte Feldtypen für die Anonymisierung....612
Datenschutzrollen....613
Datenschutz (klassisch)....614
Datenschutz....626
Datenerkennung....631
Datenerkennung erkunden....633
Datenerkennung aktivieren....634
Klassifizieren Sie Daten auf der Seite Datenerkennung „ Ergebnisse“....635
Datenerkennung Aufträge....635
Datenerkennung Rollen....644
Datenerkennung Auftragsergebnisse....646
Datenerkennung unterstützte Datentypen....647
Scannen mit granularer Konfiguration....649
Data Classification....651
Datenklassifizierung erkunden....653
Demodaten des Plugins Data Classification werden installiert....654
Datenklassifizierungen werden erstellt....656
Datenklassifizierungen werden Wörterbucheinträgen zugewiesen....657
Datenklassifizierungen werden mit dem Übersichts-Dashboard analysiert....657
Domänentrennung und Data Classification....660
Anonymisierung von Daten....660
Anonymisierungstechniken erstellen....661
Erstellen Sie Anonymisierungsrichtlinien....664
Erstellen Sie einen Anonymisierungsauftrag....668
Aktivieren Sie parallele Aufgaben für die Datenanonymisierung....672
Verschlüsselung....674
Key Management Framework....675
Abonnementpaket für Verschlüsselung und Schlüsselverwaltung....676
Key Management Framework....677
Aktionen der Schlüsselverwaltung....710
Importieren Sie einen Schlüssel aus einem Webservice....713
Key Management Framework Gesundheit....717
Bereiten Sie Ihre -Instanz auf die Einstellung von GlideEncrypter vor....719
GlideEncrypter-Nutzung von 3DES für Passwort2-Felder einstellen....720
Key Management Framework Resource Exchange....723
Infrastruktursicherheit....731
Password2-Verschlüsselung mit dem Key Management Framework (KMF)....733
Zertifikate....736
Zertifikate erkunden....738
Generieren eines LDAP-Client-Zertifikats....739

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein Zertifikat wird in eine Instanz hochgeladen....741
Verschlüsselung auf Spaltenebene....743
Verschlüsselung auf Spaltenebene erkunden....744
Verschlüsselung auf Spaltenebene konfigurieren....747
Mithilfe der Verschlüsselung auf Spaltenebene....751
Column Level Encryption Enterprise....782
Cloud-Verschlüsselung mit Schlüsselverwaltung....786
Schlüsselverwaltungsvorgänge....788
Quorum-Steuerungsrichtlinie....797
Transaktionen der Schlüsselverwaltung....802
Protokollierung für die Cloud-Verschlüsselung....804
Manipulationserkennung....807
Vollständige Datenträgerverschlüsselung....810
Edge Encryption....810
Edge Encryption erkunden....812
Die Edge Encryption planen....825
Edge Encryption wird installiert....834
Upgrade von Edge Encryption....889
Konfigurieren von Edge Encryption....897
Datenbankverschlüsselung....956
Datenbankverschlüsselung erkunden....957
Datenbankschlüsselrotation wird angefordert....959
Datenbankverschlüsselung mit kundengesteuertem Switch....960
Zugriffsverwaltung....962
Zero Trust-Zugriff....963
Zero Trust-Zugriff erkunden....965
Zero Trust-Zugriff wird aktiviert....967
Konfigurieren der Rolle für den Sitzungszugriff....967
Systemeigenschaften für Zero Trust-Zugriff....969
Lernprogramm: Verwenden Sie Zero Trust-Zugriff....972
Zero Trust-Zugriff für Mobilgeräte....976
Domänentrennung für Service Provider....977
Domain Separation erkunden....979
Anwendungssupport für die Domänentrennung....999
Empfohlene Domain Separation-Verfahren für Service Provider....1008
Domain Separation – Hilfe....1049
Einrichtung und Verwaltung der Domänentrennung....1051
Domain Separation Center....1085
Authentifizierung....1092
Adaptive Authentifizierung....1095
API-Authentifizierung....1155
API-Zugriffsrichtlinie....1167

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zertifikatbasierte Authentifizierung ... 1194
Zuordnung von anwenderdefinierten URLs zu Ihrer Instanz ... 1202
Installations-Exits ... 1210
Authentifizierung mit IP-Adressbereich ... 1213
LDAP-Integration ... 1216
Begrenzen Sie gleichzeitige Sitzungen ... 1286
Lokale Authentifizierung ... 1290
Multifaktor-Authentifizierung (MFA) ... 1318
Single Sign-on (SSO) für mehrere Anbieter ... 1372
Eingehende und ausgehende OAuth-Authentifizierung ... 1464
Selbstregistrierung bei Instanz ServiceNow ... 1506
Tokenbasierte Authentifizierung (Anwenderanmeldungen) ... 1517
Webservice – Sicherheit ... 1532
Regeln für Zugriffssteuerungsliste ... 1538
Zugriffssteuerungslisten erkunden ... 1539
Konfigurieren einer ACL-Regel ... 1559
Contextual Security Manager ... 1564
Erweiterte ACL-Konfiguration ... 1570
Sicherheitsattribute ... 1582
Sicherheitsattribute – Grundlagen ... 1583
Erstellen Sie Sicherheitsattribute ... 1584
Sicherheitsattribut , Umfang ... 1586
Feldabfragerollen und -einschränkungen ... 1587
Konfigurieren Sie eine Feldabfragerolle ... 1587
Konfigurieren Sie Einschränkungen für Feldabfragen ... 1588
Datenfilterung ... 1588
Datenfilterung erkunden ... 1589
Datenfilterung wird aktiviert ... 1592
Erstellen von Datenfilterungsregeln ... 1592
Betreffkriterien werden erstellt ... 1595
Debugging der Datenfilterung ... 1599
Sicherheitsrollen ... 1601
Explizite Rollen ... 1601
Rollen mit erhöhten Rechten ... 1609
Verbindung und Anmeldeinformationen ... 1611
Anmeldeinformationen, Verbindungen und Aliasse erkunden ... 1613
Erste Schritte mit Verbindungen ... 1629
Erste Schritte mit Anmeldeinformationen ... 1642
Authentifizierungsalgorithmen ... 1738
ServiceNow®-Zugriffssteuerung ... 1749
Zugriffssteuerung ServiceNow® erkunden ... 1750

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

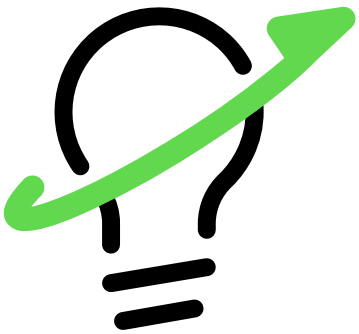
Die Zugriffssteuerung ServiceNow® wird aktiviert....1753
Die Zugriffssteuerung für ServiceNow® wird konfiguriert....1755
Audit-Protokollierung....1757
Identität....1758
Zugriffsanalyse....1759
Zugriffsanalyse erkunden....1760
Mithilfe der Zugriffsanalyse....1761
Berechtigungsauswertung....1782
Häufige Fragen....1784
Zugriffssimulator....1790
Globale Identität....1804
Föderierte ID erkunden....1806
Zugriff auf föderierte ID-Kriterien....1807
ID-Felder werden aktualisiert....1808
Identity Center....1809
Identity Center erkunden....1810
Identity Center wird aktiviert....1810
Identity Center für Benutzer....1811
Identitätsmetriken für Administratoren....1814
System für domänenübergreifendes Identitätsmanagement (SCIM)....1815
SCIM-Anbieter....1816
SCIM-Client....1834
Identitäts- und Zugriffsaudit....1852
Identitäts- und Zugriffsaudit erkunden....1854
Ergebnisse des Identitätsaudits....1855
Prüfbare Felder für Sicherheit....1859
Für Identitätszugriff und Audit unterstützte und nicht unterstützte Felder....1863

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Instanz sichern

Die Plattformsicherheit bietet Funktionen zum Schützen der Instanz.

ServiceNow Vault



Verwenden Sie die

ServiceNow Vault

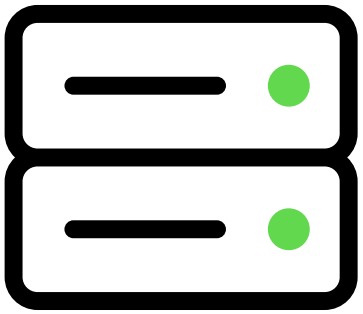
-Produktreihe von Datensicherheitstools, um vertrauliche Daten während ihres gesamten Lebenszyklus vor unbefugtem Zugriff, Beschädigung oder Diebstahl zu schützen.

Platform-Sicherheit



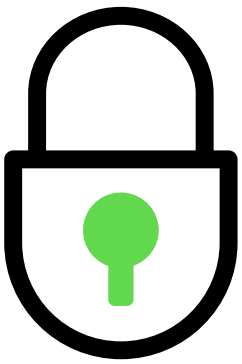
Die Plattformsicherheit bietet Funktionen zum Schützen der Instanz.

Plattform-Datenschutz



Mit Plattformdatenschutz können Sie das vertrauliche Datum in der Instanz maskieren.

Verschlüsselung



Schützen Sie Ihre vertraulichen Daten, und halten Sie die gesetzlichen Anforderungen und Standards ein.

Zugriffsverwaltung



Die Zugriffsverwaltung ermöglicht Ihnen einen sicheren Zugriff auf die Instanz

ServiceNow®

.

Identität



Erfahren Sie mehr über die Identitäten in der Instanz.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Codesignatur  Die Codesignatur erstellt digitale Signaturen für die Daten, die später überprüft werden, um die Authentizität und Integrität der Daten zu bestätigen.		

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ServiceNow Vault

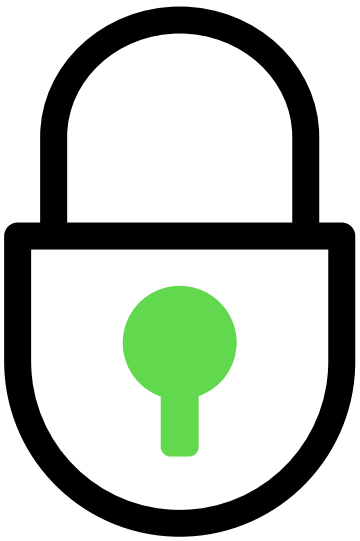
Verwenden Sie die ServiceNow Vault-Produktreihe von Datensicherheitstools, um vertrauliche Daten während ihres gesamten Lebenszyklus vor unbefugtem Zugriff, Beschädigung oder Diebstahl zu schützen. Wenden Sie Schutzmaßnahmen wie Verschlüsselung, Geheimnisverwaltung und Datenschutz zur Schwärzung und Prüfung vertraulicher Informationen an. Die Homepage von ServiceNow Vault stellt einen zentralen, gut erreichbaren Ausgangspunkt dar, um nach ServiceNow Vault-Datensicherheitsprodukten zu suchen und zu ihnen navigieren.

ServiceNow Vault ist ein kostenpflichtiges Plugin, das von ServiceNow-Mitarbeitern in Ihrer Produktionsinstanz aktiviert werden muss. ServiceNow Vault enthält die nachfolgend aufgelisteten Komponenten.

Wenden Sie sich an Ihren ServiceNow-Kundenbetreuer, um ein Abonnement zu erwerben. Wenn Sie ein Abonnement erwerben, werden bestimmte Plugins automatisch aktiviert. Wenn ein kostenpflichtiges Plugin nicht automatisch aktiviert wird, können Sie es manuell in der Liste **Alle Anwendungen** in Ihrer Instanz aktivieren.

Komponenten von ServiceNow Vault

Verschlüsselung



Schlüsselverwaltung und Verschlüsselung auf Spaltenebene sind eine Suite hochgradig konfigurierbarer Verschlüsselungsmodule

Geheimnisverwaltung

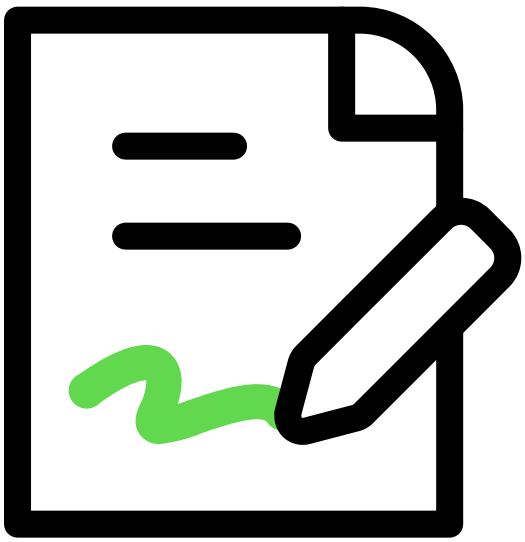


Lösung zum Ersetzen von hartcodierten Geheimnissen wie Passwörtern, Zertifikaten und API-Schlüsseln auf der -Plattform durch die Verwahrung von Geheimnissen durch den Kunden.

Automatische Übersetzung

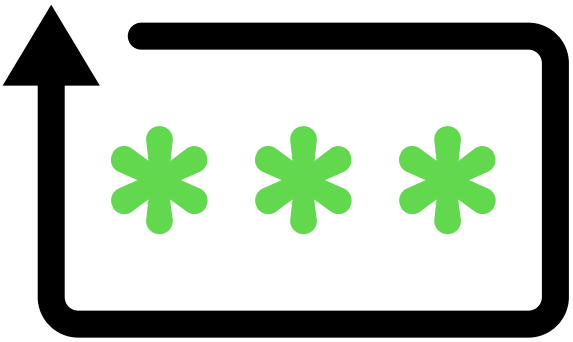
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Codesignatur



Tragen Sie zur Erhöhung der Sicherheit bei, indem Sie sensible Anwendungskonfigurationsdaten und Skripts validieren, bevor sie verwendet werden.

Datenschutz



Verwenden Sie das Plugin „Datenschutz“, um personenbezogene Daten aus Benutzerdaten zu entfernen, wenn diese von einer Produktionsinstanz zu einer Instanz außerhalb der Produktion migriert werden.

Daten-Discovery



Protokolle



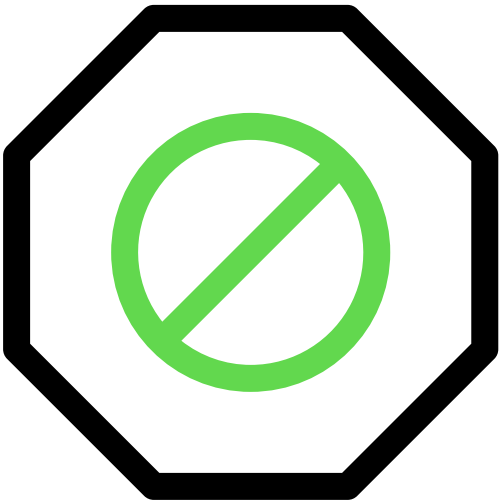
Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit dem Plugin „Data Discovery“ können Sie personenbezogene Daten aus Benutzerdaten finden. Die Daten können dann für weitere Sicherheitsmaßnahmen klassifiziert werden.

Verbessern Sie die Sicherheit, Leistung und Anwender-Experience, indem Sie Protokolldaten von ServiceNow mithilfe des Protokollexportservice in Enterprise Log Analytics importieren.

Zero Trust-Zugriff



Mit dem ServiceNow-Sitzungszugriff können Organisationen die Anwenderberechtigung in einer Websitzung dynamisch reduzieren

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Platform-Sicherheit

Die Plattformsicherheit bietet Funktionen zum Schützen der Instanz.

Sicherheitscenter



Ermöglichen Sie Administratoren, kontinuierlich das höchste Sicherheitsniveau aufrechtzuerhalten und auf einfache Weise unsichere Ereignisse und Verhaltensweisen zu überwachen.

Härtungseinstellungen



Der Inhalt

ServiceNow, Inc.

Security Center-Härtungseinstellungen enthält detaillierte Beschreibungen und Compliance-Werte für die sicherheitsbezogenen Systemeigenschaften und Plugins im

Now Platform

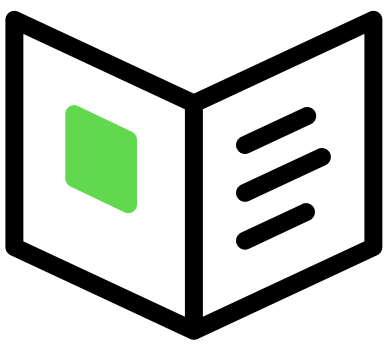
. Sie können diese Eigenschaften mit der App für die Härtungseinstellungen im Security Center festlegen.

Protokollexportservice

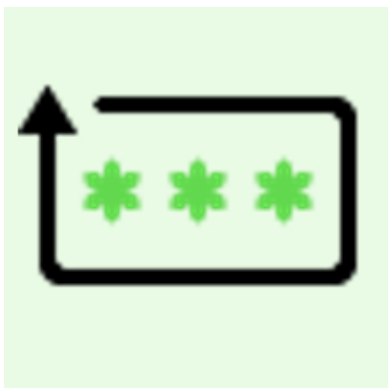


Mit dem Log Export Service (LES) können Sie Ihre Instanzsystem- und Anwendungsprotokolle nahtlos in Ihre Analysetools für Unternehmenssicherheit exportieren. Der Service bietet eine hoch skalierbare Integration mit Analysetools nahezu in Echtzeit, die einfach einzurichten und zu warten ist.

Protokolle



Geheimnisverwaltung



Codesignatur



Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Modul „Protokolle“ bietet eine Vielzahl von Protokollen, mit denen Sie bei Transaktionen und Ereignissen, die innerhalb der Instanz stattfinden, Probleme beheben und Debuggen können.

Verwenden Sie ServiceNow Geheimnisverwaltung für eine granulare Verwaltung des Zugriffs auf Ihre Passwörter entsprechend Ihren Geschäftsanforderungen.

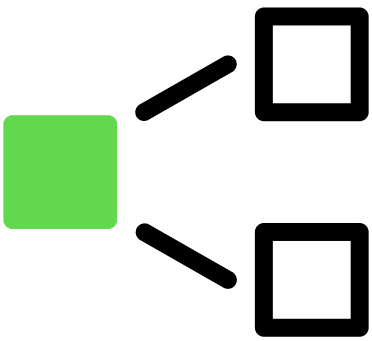
Die Codesignatur erstellt digitale Signaturen für die Daten, die später überprüft werden, um die Authentizität und Integrität der Daten zu bestätigen.

Antivirus-Scanfunktionen



Verwenden Sie Antivirus-Scanning, um Ihre Instanz vor Virusinfektionen zu schützen, die durch Dateianhänge zu Ihren Systemdatensätzen (z. B. Incidents, Probleme und Stories) eingeführt werden können.

HTML-Bereinigung



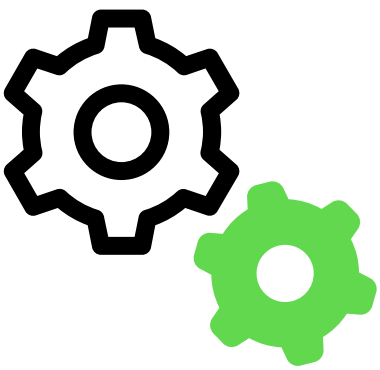
Entfernen Sie unerwünschten Code, und schützen Sie sich vor Sicherheitsbedrohungen wie Angriffen mit websiteübergreifendem Skripting, indem Sie HTML-Markup in HTML-Feldern und übersetzten HTML-Feldern bereinigen.

Auditing



Verfolgen Sie Datensatzänderungen in für Auditing aktivierten Tabellen. Standardmäßig verfolgt das System unter anderem Änderungen an den Incident-, Change- und Problem-Tabellen nach.

Strenge Sicherheitseinstellungen



Virtuelles privates Netzwerk (VPN)



Andere Einstellungen und Sicherheitsressourcen



Legen Sie Sicherheitseigenschaften außerhalb von Instance Security Center fest, das auch andere

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Strenge Sicherheitseinstellungen schließen mehrere Sicherheitsoptionen ein, die in Ihrer Instanz verfügbar sind.	Verwenden Sie ein virtuelles privates Netzwerk (VPN), um Ihre Instanz mit externen Datenquellen über das Internet zu integrieren.	sicherheitsbezogene Ressourcen enthält.

Security Center

ServiceNow Security Center ist eine Anwendung, die aus einer Reihe von Tools besteht, die Ihre Organisation dabei unterstützen sollen, die Sicherheit Ihrer ServiceNow-Bereitstellungen aufrechtzuerhalten. Mit Security Center können Sie den Sicherheitsstatus verbessern und die Compliance-Stufen mit einer nahtlosen Anwender-Experience stärken.

Security Center ist eine kostenlose Anwendung, die Systemadministratoren aus dem ServiceNow Store herunterladen können. Es wird standardmäßig ab dem Vancouver-Release installiert. Außerdem wird es zwischen Familien-Releases vierteljährlich im ServiceNow Store verfügbar gemacht, um die Einführung neuer Funktionen zu beschleunigen.

Wichtig: Das Instanz-Sicherheitszentrum (ISC) erreicht das Ende des Verkaufs im September 2024. ServiceNow Security Center (SSC) ist die empfohlene Lösung für die Zukunft. Weitere Informationen finden Sie unter Migration des Instanz-Sicherheitszentrums zu ServiceNow Security Center ..

Homepage	Sicherheitshärtung	Sicherheitsscanner
		
Zeigen Sie Ihre Compliance-Bewertung für Härtung als Prozentsatz an, analysieren Sie die häufigsten nicht konformen Härtungseinstellungen, die korrigiert werden müssen, und sehen Sie sich die Ergebnisse Ihrer Sicherheitsscans an.	Erfahren Sie, wie Härtungskonfigurationen den Sicherheitsempfehlungen von ServiceNow entsprechen	Scannen Sie eine Reihe von Sicherheitsprüfungen, um Fehlkonfigurationen und unsicheres Verhalten zu identifizieren

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitsmetriken	Virenschutz	Security Learning
		
Überwachen Sie über 50 verschiedene Metriken, um potenzielle Sicherheitsbedrohungen zu identifizieren.	Zeigt den Trend an, wann Ereignisse für potenziell infizierte Dateien auftreten.	Ein zentrales Repository für Sicherheitsressourcen, das Zugriff auf Sicherheits- und Compliance-Dokumente von ServiceNow bietet.

Anwenderrollen

Zur Verwendung des Sicherheitscenters benötigen Sie die Rolle admin oder sn_vsc.security_center_viewer.

Erforderliche Rolle	Anwender	Vorteile
Administrator	Diese Rolle gewährt Zugriff auf alle Features, Funktionen und Daten des Systems, da Administratoren die Möglichkeit haben, Regeln für Zugriffssteuerungslisten (Access Control List, ACL) zu überschreiben und alle Rollenprüfungen zu umgehen. Vermeiden Sie es, Ihren Anwendern diese Rolle zuzuweisen, wenn spezifischere Rollen verfügbar sind.	Verwenden Sie Security Center-Tools, um den Sicherheitsstatus von Instanzen zu verbessern und sicherheitsbezogenes Verhalten zu überwachen.
sn_vsc.security_center_viewer	Diese Rolle ermöglicht Benutzern ohne Administratorrechte den Zugriff auf Informationen in Security Center, verhindert jedoch, dass sie Security Center-Tools ändern oder Änderungen an der Instanzkonfiguration vornehmen.	Verschaffen Sie sich Einblick in Security Center-Tools, um den Sicherheitsstatus von Instanzen und das Sicherheitsverhalten zu überwachen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle	Anwender	Vorteile
	Beispielsweise benötigen Plattformbesitzer, Security Operations-Analysten oder Compliance-Stakeholder möglicherweise Zugriff auf bestimmte Sicherheits-KPIs (Key Performance Indicators, Leistungskennzahlen), Sicherheitseinblicke und Sicherheits-Lernmaterialien, die im Security Center verfügbar sind.	

Erste Schritte

- Security Center ist in allen Familienreleases ab Vancouver enthalten.
- Lesen Sie die Produktdokumentation, beginnend mit Übersicht.
- Schließen Sie den Kurs „ Technische Schulung und Zertifizierung “ (TACO) für Security Center ab.

Übersicht

Verschaffen Sie sich auf der Übersichtsseite einen schnellen Überblick über die Sicherheitslage Ihrer Instanz. Zeigen Sie Ihre Compliance-Punktzahl für Härtung als Prozentsatz an, erkennen Sie grafische Trends Ihrer Compliance-Punktzahl, analysieren Sie die häufigsten nicht konformen Härtungseinstellungen, die korrigiert werden müssen, und sehen Sie sich die Ergebnisse Ihrer Sicherheitsscans an.

Die Compliance-Punktzahl für Härtung ist ein Prozentsatz, der anzeigt, wie genau Ihre Sicherheitseinstellungen mit den empfohlenen Einstellungen übereinstimmen. Die Zusammenfassung der Compliance-Punktzahl für Härtung zeigt diesen Prozentsatz und Daten im Zusammenhang mit den letzten Änderungen der Punktzahl an. Verwenden Sie das Trenddiagramm für die Compliance-Punktzahl für Härtung, um zu sehen, wie sich Ihre Compliance-Punktzahl im Laufe der Zeit geändert hat.

Verbessern Sie Ihre Compliance-Punktzahl, indem Sie die häufigsten nicht konformen Härtungseinstellungen verwenden. In dieser Liste werden die 10 Sicherheitshärtungseinstellungen angezeigt, die sich am negativsten auf Ihre Compliance-Bewertung für Härtung auswirken. Diese Transparenz hilft Ihnen, zu priorisieren, welche Härtungseinstellungen zu korrigieren sind.

Im Abschnitt „Zusammenfassung der Sicherheitsprüfung“ werden Balkendiagramme angezeigt, die die Anzahl der Ergebnisse im Zeitverlauf für jeden Ihrer Sicherheitsscans widerspiegeln.

1. Greifen Sie auf das Trenddiagramm der Compliance-Punktzahl für Härtung über die Übersichtsseite zu, oder navigieren Sie zu **Härtung** > **Punktzahltrend**an.
2. Wählen Sie **Punktzahltrend überprüfen** aus, um den Zeitraum anzupassen und Punkte auf der Trendlinie zur Analyse auszuwählen.
3. Wählen Sie im Abschnitt „Zusammenfassung des Sicherheitsscans“ eine Leiste aus, um zur Seite mit den Scan-Ergebnissen für diese Scan-Suite zu navigieren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitshärtung

Verwenden Sie das Härtungstool von Security Center, um Ihre Compliance-Punktzahl für Härtung anzuzeigen, mit vorherigen Punktzahlen zu vergleichen und die Einstellungen zu ändern, um Ihre Compliance-Punktzahl und den Sicherheitsstatus zu verbessern.

Die Härtungseinstellungen geben empfohlene Werte für die sicherheitsbezogenen Eigenschaften und Plugins in der NOW Platform an. Das Härtungstool berechnet die Compliance-Punktzahl der Härtungseinstellung als Prozentsatz. Diese Zahl gibt an, wie konform Ihre Instanz mit den Härtungseinstellungen von Security Center ist.

Die Formel zur Berechnung der Compliance-Punktzahl für Härtung:

- Jede Härtungseinstellung hat eine Risikopunktzahl zwischen 0 und 10.
- Die Punktzahl entspricht der Summe aller konformen Risikopunktzahlen geteilt durch die Summe aller Risikopunktzahlen.

Wenn beispielsweise die Summe aller konformen Risikopunktzahlen 25,4 beträgt und die Summe aller Risikopunktzahlen 34,9 beträgt, beträgt die Compliance-Punktzahl (25,4/34,9) mal 100, was 72,7 entspricht. Diese Dezimalzahl wird auf die nächste ganze Zahl gerundet und ergibt daher 73.

Diese Berechnung wird automatisch am ersten des Monats oder nach einer Installation oder Neuinstallation von ServiceNow Security Center durchgeführt.

Vergleich der Härtungspunktzahl

Verschaffen Sie sich einen Überblick über die Integrität Ihrer Härtungseinstellungen, und verwenden Sie diese Daten, um den Sicherheitsstatus Ihrer Instanz zu verbessern.

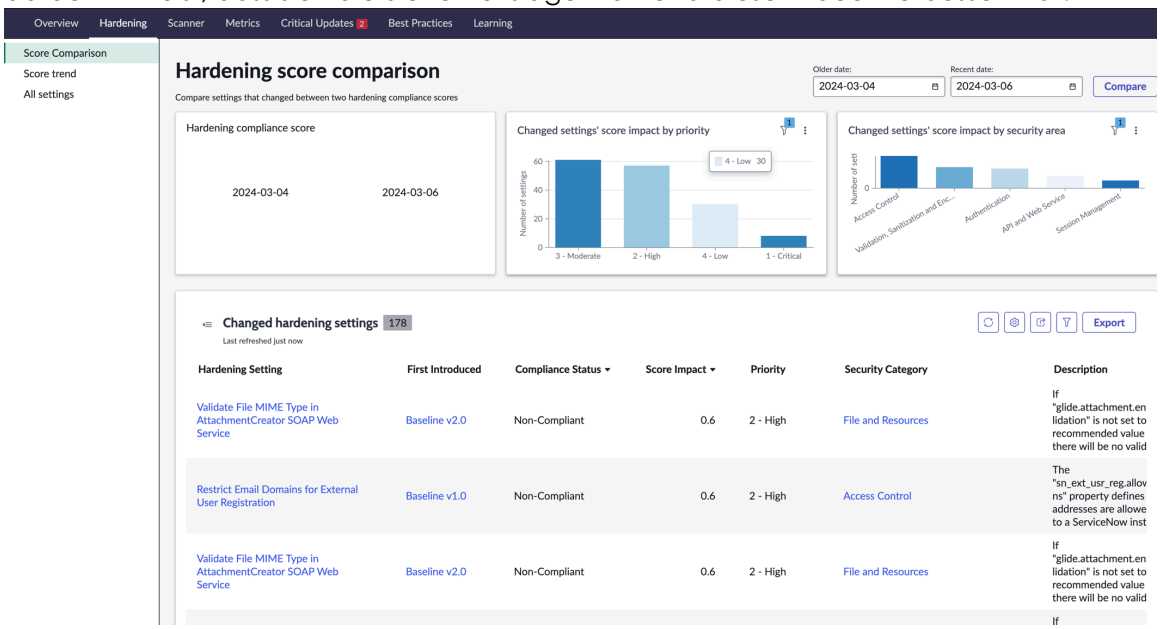
Auf der Seite zum Vergleichen der Härtungspunktzahl werden alle Härtungseinstellungen mit Änderungen des Compliance-Status zwischen dem ersten und zweiten Datum und deren Auswirkungen auf die Compliance-Punktzahl für Härtung angezeigt. Wenn beispielsweise eine Einstellung von „Konform“ in „Nicht konform“ geändert wurde, würde die Punktzahl verringert.

Um die Ergebnisse dieser Änderungen anzuzeigen, geben Sie in der Datumsauswahl oben rechts auf der Seite ein Älteres Datum und ein Letztes Datum ein, und wählen Sie dann Vergleichen aus. Im Folgenden finden Sie eine Erklärung zu jeder Karte:

- Compliance-Punktzahl für Härtung: Zeigt die Compliance-Punktzahl Ihrer Instanz als Prozentsatz für das erste und zweite Datum an, das Sie ausgewählt haben.
- Impact auf die Punktzahl der geänderten Einstellungen nach Priorität: Zeigt die Anzahl der Härtungseinstellungen an, die ihren Compliance-Status zwischen den beiden Datumsangaben geändert haben, sortiert nach Prioritätswert.
- Impact auf die Punktzahl der geänderten Einstellungen nach Sicherheitsbereich: Zeigt die Anzahl der Härtungseinstellungen an, die den Compliance-Status zwischen den beiden Daten geändert haben, organisiert nach Sicherheitsbereich.
- Geänderte Härtungseinstellungen: Zeigt die Liste der Härtungseinstellungen an, die die Compliance-Statuten zwischen den beiden Datumsangaben geändert haben. Sie können Einstellungen, die nicht mehr konform wurden und Ihre Härtungsvergleichspunktzahl verringert haben, auf Möglichkeiten überprüfen, um sie konform zu machen, um Ihre Punktzahl zu erhöhen. Weitere Informationen finden Sie unter Compliance-Punktzahl für Härtung erhöhen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

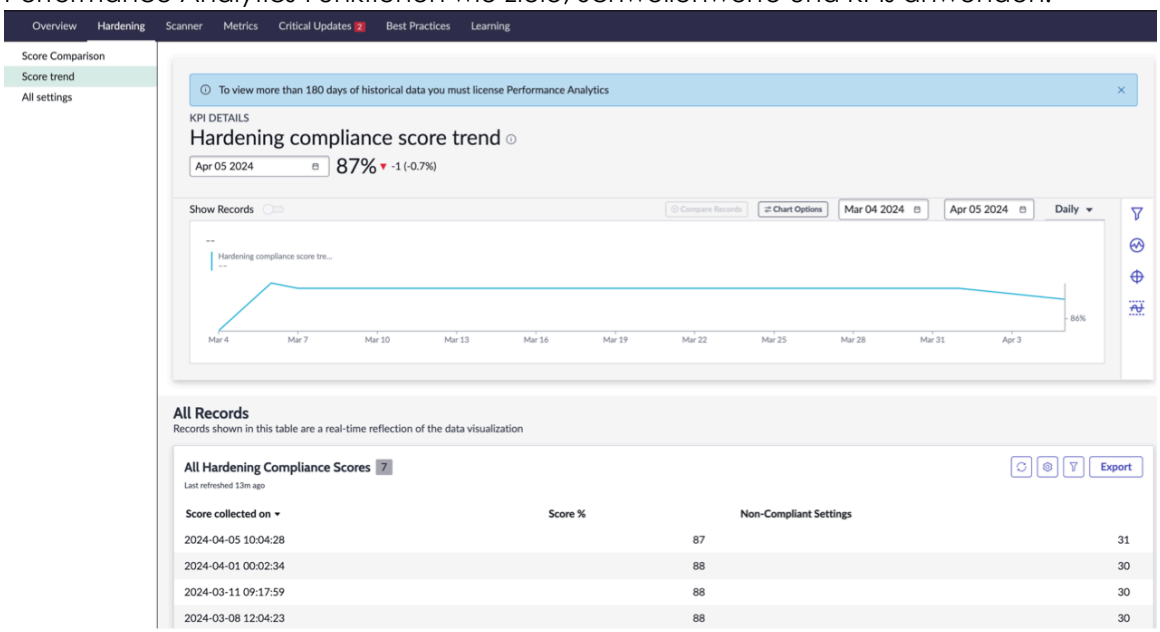
Im folgenden Screenshot wurde beispielsweise die Compliance-Punktzahl erhöht, was darauf hinweist, dass sich die Sicherheitslage während dieser Dauer verbessert hat.



Compliance-Punktzahltrend für Härtung

Zeigen Sie die Trends der Compliance-Punktzahl für Härtung über einen Zeitraum in einem Diagramm oder einer Tabelle an.

Zeigen Sie Trends in Ihrer Compliance-Punktzahl über einen bestimmten Zeitraum an. Verwenden Sie die Datumsauswahl, um einen Zeitraum für die Analyse auszuwählen, und gewinnen Sie dann tiefere Einblicke in die Daten, indem Sie Performance Analytics-Funktionen wie Ziele, Schwellenwerte und KPIs anwenden.



Diagrammoptionen: Wählen Sie **Diagrammoptionen** aus, um Analysen durchzuführen, die Zeitreihen anzuzeigen und die Daten in verschiedenen Diagrammtypen anzuzeigen.

Analyse

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ziel: Ziele, die Ihre Organisation erreichen möchte. Weitere Informationen finden Sie unter Performance Analytics Ziele .
- Schwellenwert: Definiert einen normalen Punktzahlbereich für einen Indikator und benachrichtigt Sie, wenn bestimmte Ereignisse auftreten. Weitere Informationen finden Sie unter Performance Analytics Schwellenwerte .
- Prognose: Beschreibt die Möglichkeit, zukünftige Punktzahlen basierend auf dem vergangenen Verhalten vorherzusagen. Weitere Informationen finden Sie unter Performance Analytics – Prognosen zu Punktzahlen .
- Trend: Zeigt an, wie sich der Wert eines oder mehrerer Elemente im Laufe der Zeit ändert.
- Kommentare: Zeigt Anmerkungen zu einzelnen Datenpunkten an.
- Bezeichnungen: Zeigt Punktzahlen im Zusammenhang mit Visualisierungen an.
- Statistiken: Zeigt Statistiken zu Ihrer Compliance-Bewertung an.

Zeitreihen

- Punktzahl: Punktzahl für den KPI.
- Change: Änderung der Punktzahl für diesen Indikator.
- Change-Prozentsatz: Change-Prozentsatz der Punktzahlen.

Diagrammtypen: Siehe Anwendungsfälle für Zeitreihenvisualisierungstypen .

Tabelle „Alle Datensätze“.

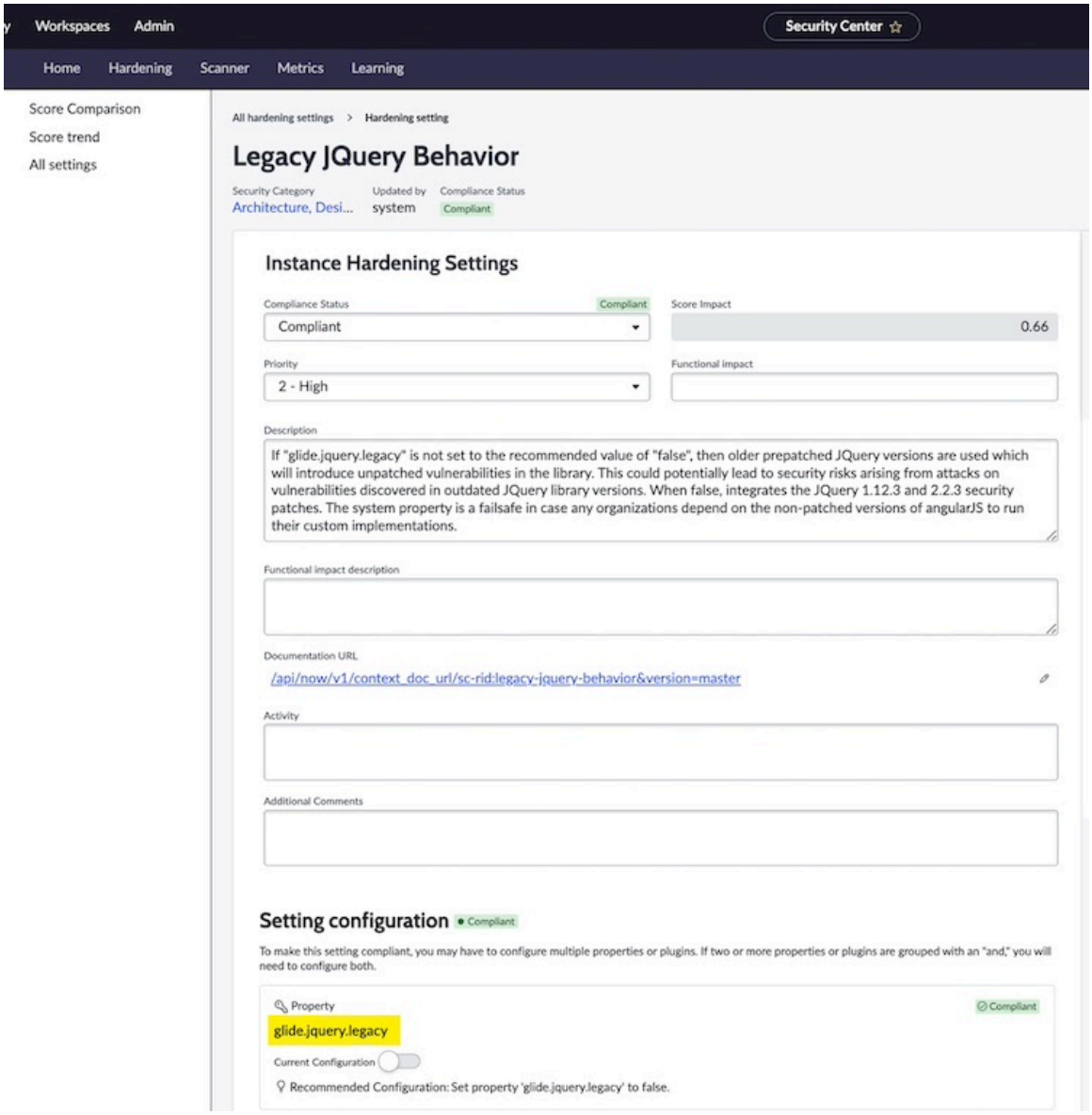
Die Tabelle „Alle Datensätze“ zeigt das Datum an, an dem die Compliance-Punktzahlen gesammelt wurden, die Prozentsätze der Punktzahlen und die Anzahl der nicht konformen Einstellungen. Sie können diese Tabelle als weitere Option verwenden, um die Sicherheitslage Ihrer Instanz im Laufe der Zeit zu analysieren.

Details zu den Härtungseinstellungen

Analysieren Sie die Details einer Härtungseinstellung, indem Sie den entsprechenden Link in der App „Security Center“ auswählen.

Navigieren zu **Härtung** > **Alle Einstellungen**, und wählen Sie dann eine Härtungseinstellung aus, die zu einer Seite im Härtungseinstellungstool umgeleitet werden soll, auf der die sicherheitsbezogenen Informationen angezeigt werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Konfigurationsdetails für Härtungseinstellungen

Konfigurationsattribut	Beschreibung
Compliance-Status	Gibt an, ob die Härtungseinstellung konform ist oder nicht.
Auswirkung auf die Punktzahl	Ein Prozentsatz, der angibt, inwieweit sich diese Härtungseinstellung auf Ihre Sicherheitslage auswirkt.
Priorität	Eine Zahl im Bereich von 1 bis 4, wobei 1 die meiste Gewichtung hat, die die Stärke der Auswirkung dieser Härtungseinstellung auf Ihren Sicherheitsstatus angibt.
Funktionale Auswirkung	Die Auswirkungen, die diese Härtungseinstellung auf den Betrieb Ihrer Instanz hat.
Beschreibung	Eine allgemeine Übersicht über die Härtungseinstellung.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationsdetails für Härtungseinstellungen (Fortsetzung)

Konfigurationsattribut	Beschreibung
Dokumentations-URL	Link zur Dokumentation für die Härtungseinstellung.
Aktivität	Benachrichtigungen über Updates im Zusammenhang mit der Härtungseinstellung.
Einstellungskonfiguration	Details zum Compliance-Status Ihrer Härtungseinstellungen zusammen mit Anweisungen, wie Sie sie konform machen können. **Hinweis:** Für einige Härtungseinstellungen müssen Sie möglicherweise mehrere Eigenschaften und Plugins konfigurieren, um sie konform zu machen.

Compliance-Punktzahl für Härtung erhöhen

Erhöhen Sie Ihre Compliance-Punktzahl für Härtung, indem Sie sicherstellen, dass die Härtungseinstellungen den Empfehlungen des Systems entsprechen.

Vorbereitungen

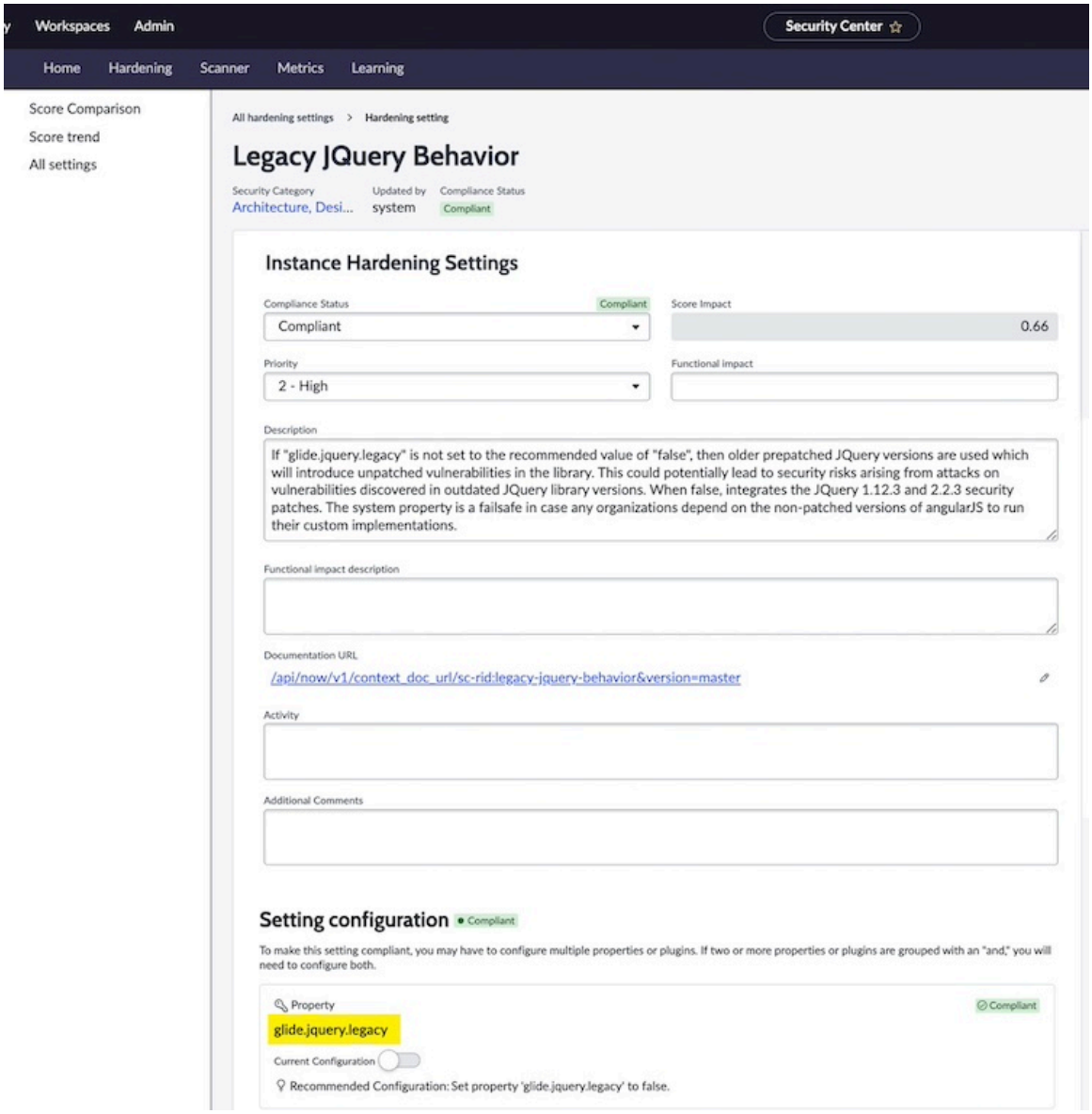
Erforderliche Rolle: admin

Identifizieren Sie nicht konforme Härtungseinstellungen mit der höchsten Auswirkung auf Ihre Instanz. Überprüfen Sie sie, um zu sehen, ob Sie die Systemempfehlungen einhalten können, um Ihre Compliance-Gesamtpunktzahl zu erhöhen.

Prozedur

1. Navigieren zu **Härtung** > **Alle Einstellungen**an.
2. Filtern Sie die Spalte „Compliance-Status“, um nur nicht konforme Härtungseinstellungen anzuzeigen.
3. Wählen Sie **Punktzahlauswirkung** aus, um vom größten zum kleinsten zu sortieren.
4. Wählen Sie Einstellungen aus, und überprüfen Sie die Einstellungsdetails, um zu entscheiden, ob Sie die Empfehlungen einhalten möchten.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Machen Sie die Härtungseinstellung konform.
6. Wenn Sie eine nicht konforme Härtungspunktzahl aktualisieren, um sie konform zu machen, rufen Sie die Homepage auf, und wählen Sie **Punktzahl** aktualisieren, um die aktuelle Punktzahl anzuzeigen.
   Die Härtungspunktzahl wird aufgerundet. Eine Punktzahl von 86,75 % wird auf 87 aufgerundet.

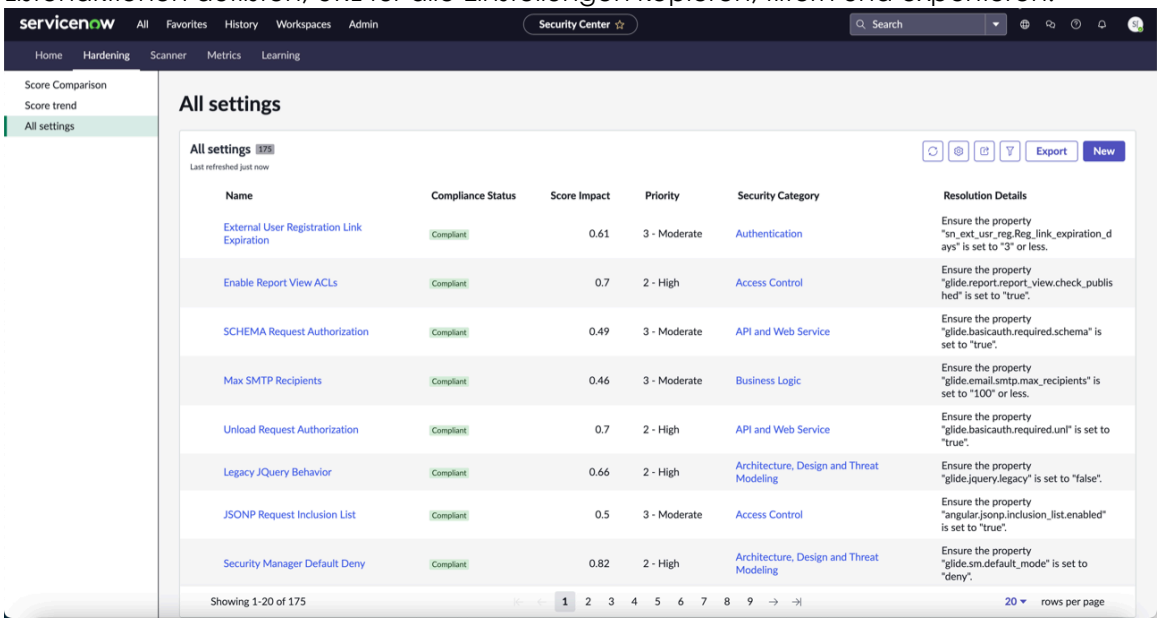
Alle Einstellungen

Zeigen Sie alle in Ihrer Instanz verfügbaren Härtungseinstellungen auf einer einzigen Seite an.

Eine Tabelle, die alle in Ihrer Instanz verfügbaren Härtungseinstellungen anzeigt. Sie können die allgemeinen Vorgänge für eine Tabelle anwenden, indem Sie Symbole oben rechts in der Tabelle auswählen: Liste aktualisieren,

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listenaktionen auflisten, URL für alle Einstellungen kopieren, filtern und exportieren.



- **Name**: Der Name der Einstellung für die Eigenschaftshärtung.
- **Compliance-Status**: **„Konform“** gibt an, dass die Härtungseinstellung ordnungsgemäß konfiguriert ist. „ **Nicht konform** “ gibt an, dass die Einstellung zur Härtung der Eigenschaft nicht gemäß der Systemempfehlung konfiguriert ist.
- **Auswirkung auf die Punktzahl**: Ein Prozentwert der Auswirkung dieser Härtungseinstellung auf Ihren Sicherheitsstatus. Alle Auswirkungen auf die Punktzahl ergeben zusammen 100 %.
- **Priorität**: Ein Wert, der die Relevanz der Einstellung darstellt: Kritisch, Hoch, Mittel und Niedrig. Die Beziehung zwischen Auswirkung auf die Punktzahl und Priorität besteht darin, dass eine Auswirkung auf die Punktzahl eine höhere Relevanz anzeigt.
- **Sicherheitskategorie**: Die Sicherheitskategorie der Eigenschaft.
- **Lösungsdetails**: Schritte, die Sie ausführen sollten, um die Sicherheitsschwachstelle der Härtungseinstellung zu beheben.

Informationen zum Konfigurieren einer Einstellung für die Eigenschafthärtung finden Sie unter Compliance-Punktzahl für Härtung erhöhen.

Sicherheitsscanner

Verwenden Sie das Scanner-Tool, um Ihre Instanz anhand einer Reihe von Sicherheitsprüfungen zu scannen und Fehlkonfigurationen zu identifizieren. Das Tool vereinfacht das Erstellen verschiedener Prüfungssuites für verschiedene Anwendungsfälle, sodass Sie die Ergebnisse im Zeitverlauf analysieren können.

Das Sicherheitsscannen ist eine Methode, um Ihre Instanz auf Konfigurationen zu untersuchen, die auf Sicherheitsprobleme hinweisen. Auf diese Weise können Sie Möglichkeiten zur Implementierung von Sicherheitsempfehlungen für Ihre Organisation identifizieren.

Beim Zugriff auf das Scanner-Tool ist kein Vergleich verfügbar, bis Sie die zu vergleichende Suite mit mindestens zwei Scan-Ergebnissen der Suite auswählen. Sie können die Standard-Suite und -Prüfungen verwenden oder eigene anwenderdefinierte Prüfungen und Suiten erstellen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vergleich der Härtungspunktzahl

Verschaffen Sie sich einen Überblick über die Integrität Ihrer Härtungseinstellungen, und verwenden Sie diese Daten, um Sicherheitsbedrohungen zu beheben und den Sicherheitsstatus Ihrer Instanz zu verbessern.

Auf der Vergleichsseite der Härtungspunktzahl werden die Sicherheitsänderungen in Ihren Härtungseinstellungen zwischen dem ersten und zweiten Datum angezeigt. Um Visualisierungen dieser Änderungen anzuzeigen, geben Sie in der **Datumsauswahl** oben rechts auf der Seite ein **älteres Datum** und ein aktuelles Datum ein, und klicken Sie dann auf **Vergleichen**. Nachfolgend finden Sie eine Erklärung zu jeder Karte:

- **Compliance-Punktzahl für Härtung**: Zeigt die Compliance-Punktzahl Ihrer Instanz am ersten und zweiten Datum als Prozentsatz an.
- **Impact auf die Punktzahl der geänderten Einstellungen nach Priorität**: Zeigt die Anzahl der Einstellungen an, deren Priorität geändert wurde.
- **Impact auf die Punktzahl der geänderten Einstellungen nach Sicherheitsbereich**: Zeigt die Anzahl der Einstellungen an, die Kategorien geändert haben. Beispiel: Wechsel von **Zugriffssteuerung** zu **Datenschutz**.
- **Geänderte Härtungseinstellungen**: Zeigt eine konsolidierte Ansicht der geänderten Einstellungen zusammen mit den zugehörigen Sicherheitsdaten in der Liste an. Darüber hinaus kann allgemeine Funktionen im Zusammenhang mit Listen wie Aktualisierung, Listen-UI-Aktionen, Kopier-URL, Filter und Export anwenden.

Im folgenden Screenshot wurde beispielsweise die Compliance-Punktzahl von 71 % in 73 % geändert, was darauf hinweist, dass die Sicherheitslage in dieser Zeit verbessert wurde.

Die Anzahl der Einstellungen, deren Priorität geändert wurde, beträgt insgesamt vier: zwei hoch und zwei mittel. Darüber hinaus betragen die Anzahl der Einstellungen, die die Sicherheit geändert haben, insgesamt vier: zwei Zugriffssteuerungen, eine Authentifizierung und eine Geschäftslogik. Die Sicherheitsdetails dieser vier Einstellungen werden auch in der Liste Geänderte Härtungseinstellungen angezeigt. Sie können die nicht konformen Einstellungen anzeigen und korrigieren, wodurch die Compliance-Punktzahl für Härtung neu berechnet wird.

Sicherheitsscanner prüft

Prüfungen sind Regeln zur Erkennung von Anomalien innerhalb einer Instanz. Sie werden für Tabellen, Datensätze oder Metadaten ausgeführt.

Sie können mit dem Scanner-Tool vier Arten von Prüfungen verwenden, um Probleme zu identifizieren und Sicherheitsempfehlungen für Ihre Organisation zu implementieren: Tabellenprüfungen, Spaltentypprüfungen, Nur-Skript-Prüfungen und Linter-Prüfungen.

Arten von Prüfungen

Name überprüfen	Beschreibung
Tabellenprüfungen	Verwenden Sie diese Option, wenn Sie die spezifischen Tabellen und Prüfungen kennen, die Sie testen möchten.
Spaltenprüfungen	Implementieren Sie hiermit die von Ihnen erstellte Regel zum Iterieren aller Datensätze, die dem Feldtyp der Zielspalte entsprechen.
Skriptprüfungen	Verwenden Sie diese Option, um Metadaten und Konfigurationen zu überprüfen und

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Arten von Prüfungen (Fortsetzung)

Name überprüfen	Beschreibung
	komplexe Prüfungen auszuführen, indem Sie Ihre eigenen Prüfungen ausstellen.
Linter-Prüfungen	Verwenden Sie diese Option, um Probleme in einem Skript zu identifizieren. Wenn eine Linter-Prüfung für einen Datensatz ausgeführt wird, wird eine abstrakte Syntaxstruktur für den Code generiert, die zur Analyse von Problemen mit dem Code verwendet werden kann.

Erstellen Sie eine neue Suite

Erstellen Sie eine anwenderdefinierte Suite, und planen Sie sie, damit Sie die Sicherheit Ihrer -Instanz für Ihr Unternehmen analysieren können.

Vorbereitungen

Erforderliche Rolle: admin oder sn_vsc.security_center_viewer.

Eine Suite ist eine Sammlung von Prüfungen, die für einen Scan verwendet werden können. Zeigen Sie eine Liste der in Ihrer Instanz verfügbaren Scan-Suites in einer Tabelle an, indem Sie zu navigieren **Scanner** > **Suites**an. Sie haben die Möglichkeit, eigene Suites zu erstellen oder die Standardsuite Auditor zu verwenden: Dies ist eine sofort einsatzbereite Suite, die Prüfungen auf Best Practices für Sicherheit enthält. Diese Prüfungen bestehen aus Systemeigenschaften, Plugins und Tabellen, die sich auf die Sicherheitslage Ihrer Instanz auswirken können. Die folgenden Schritte zeigen, wie Sie eine Suite erstellen und welche Optionen für ihre Konfiguration verfügbar sind.

Prozedur

1. Navigieren zu **Suites** > **Neu**an.
2. Geben Sie einen **Suitenamen** und eine **Beschreibung**ein, und wählen **Sie Speichern**.
3. **Prüfungen**
   Hier fügen Sie Ihrer Suite Schecks hinzu.
   a. Wählen Sie **Bearbeiten**.
   b. Wählen Sie die Schecks aus, die Sie hinzufügen möchten, und wählen Sie dann Hinzufügen (**>**), um sie in Ihrer Suite zu platzieren.
   c. **Speichern**.
4. **Untergeordnete Suites**
   Hier fügen Sie untergeordnete Suites oder die Suites hinzu, die unter den übergeordneten Suites platziert sind.
   a. Wählen Sie **Bearbeiten**.
   b. Wählen Sie die untergeordneten Suites aus, die Sie hinzufügen möchten, und wählen Sie dann Hinzufügen (**>**), um sie in Ihrer untergeordneten Suite zu platzieren.
   c. **Speichern**.
5. **Übergeordnete Suites**
   Hier fügen Sie übergeordnete Suiten hinzu. Alle untergeordneten Suites werden ausgeführt, wenn eine übergeordnete Suite in einem Scan verwendet wird.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie **Bearbeiten**.

b. Wählen Sie die untergeordneten Suites aus, die Sie hinzufügen möchten, und wählen Sie dann Hinzufügen (**>**), um sie in der übergeordneten Suite zu platzieren.

c. Speichern.

6. Zeitplan
Legen Sie eine Ausführungszeit für Ihre Suite fest.

a. Wählen Sie **Neu**.

b. Geben Sie die Details des geplanten Scans ein.
Die Zeitfelder haben das folgende Format: Stunde:Minuten:Sekunden.

c. Speichern.

Klonen Sie die Auditor-Suite für Zugriffssteuerungen

Klonen Sie die Auditor-Suite für standardmäßige Zugriffssteuerungen in Ihrer Instanz, und passen Sie sie an, um eine neue Suite zu erstellen, die auf die Sicherheitspraktiken Ihrer Organisation zugeschnitten ist.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Die mit Ihrer Instanz bereitgestellte Audit-Suite für standardmäßige Zugriffssteuerungen kann nicht geändert werden. Wenn Sie jedoch Prüfungen hinzufügen, entfernen oder bearbeiten möchten, um sie an die Sicherheitspraktiken Ihrer Organisation anzupassen, können Sie die Auditor-Suites für Zugriffssteuerungen duplizieren. Durch das Kopieren der Audit-Steuerungssuites können Sie sie anpassen und eine neue Suite basierend auf der Standardsuite erstellen. Die Auditor-Suites für Zugriffssteuerungen enthalten Prüfungen im Zusammenhang mit Best Practices für Sicherheit und decken Systemeigenschaften, Plugins und Tabellen ab, die sich auf den Sicherheitsstatus der Instanz auswirken. Die folgenden Schritte zeigen, wie Sie die Auditor-Suites für standardmäßige Zugriffssteuerungen duplizieren, um sie an die Anforderungen Ihrer Organisation anzupassen.

Prozedur

1. Navigieren zu **Alle** > **Instanz-Scan** > **Suites**an.

2. Wählen Sie **Neu** aus, und geben Sie einen Namen für Ihre Suite zusammen mit einer optionalen Beschreibung ein.

3. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.

4. Fügen Sie die für Ihren Scan erforderlichen Überprüfungen hinzu.

a. Wählen Sie auf der Registerkarte **Prüfungen** die Option **Bearbeiten**aus.

b. Fügen Sie die Bedingungen hinzu.
Um beispielsweise Scanprüfungen hinzuzufügen, wenden Sie die folgenden Felder, Operatoren, Werte und Bedingungen an:

[Feld][ist][Sicherheit] UND [Anwendung][ist][Global]

Es sollte beispielsweise wie folgt aussehen: „`Kategorie" ist „Sicherheit" und „Anwendung" ist „Global"`.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie **Ausführungsfilter aus**.
6. Wählen Sie die Scanprüfungen, die Sie hinzufügen möchten, aus der Sammlungsliste zur Prüfliste aus, und wählen Sie dann die Schaltfläche Hinzufügen (>).
7. Wählen Sie **Speichern**aus.
   Die Suite mit Ihren hinzugefügten anwenderdefinierten Prüfungen wurde erstellt.
8. Wählen Sie **Suite-Scan ausführen aus**.

Zeigen Sie die Auditor Suite für Zugriffssteuerungen an

Zeigen Sie die Prüfungen an, die in den standardmäßigen Auditor-Suites für Zugriffssteuerungen verfügbar sind, um zu verstehen, welche Prüfungen bei der Ausführung dieser Suite ausgeführt werden.

Warum und wann dieser Vorgang ausgeführt wird

Die Schritte, die Sie ausführen müssen, um auf die Auditor-Suites für standardmäßige Zugriffssteuerungen in Ihrer ServiceNow-Instanz zuzugreifen.

Prozedur

1. Navigieren Sie zu Auditor Suite für Zugriffssteuerung, indem Sie auswählen **Scanner** > **Suites** > **Auditor für Zugriffssteuerungen** Suite. Um die Suite-Prüfungen zu überprüfen, wählen Sie die Registerkarte **Prüfungen**.
   Sie sollten die Liste mit 8 für die Suite verfügbaren Prüfungen anzeigen.
2. Wählen Sie den Namen des Schecks aus, den Sie analysieren möchten.
3. Analysieren Sie die mit dem Scheck verknüpften Felder.

Name	Beschreibung
Name	Name des Schecks
Anwendung	Die Anwendung, zu der der Scheck gehört (Security Center)
Kategorie	Kategorie, die dem Scheck zugeordnet ist.
Priorität	Die Dringlichkeitsstufe.
Version	Versionsnummer des Schecks.
Aktiv	Der Status des Schecks, z. B. aktiv oder inaktiv
Kurzbeschreibung	Eine kurze Zusammenfassung des Schecks.
Beschreibung	Eine umfassendere Zusammenfassung des Schecks.
Lösungsdetails	Potenzielle Security Incidents gemindert.
Dokumentations-URL	Links zu zugehöriger Dokumentation in der Produktdokumentation oder in Knowledge Base-Artikeln (KB).
Ausführungsbedingung	Bedingungen, die den Start der Prüfungen auslösen.
Tabelle	Die Tabelle, zu der der Scheck gehört.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
Bedingungen	Bedingte Logik, die auf die Prüfungen angewendet wird.
Erweitert	Erweiterte Konfigurationsoptionen.

Scan-Ergebnisse

Zeigen Sie Daten im Zusammenhang mit Ihren Scan-Ergebnissen in einer einzigen Ansicht an.

Ein Scan-Ergebnis meldet den Status und den Typ des Scans. Sie können auch alle Prüfungen anzeigen, die als Teil der Prüfung ausgeführt wurden, und alle anderen Informationen im Zusammenhang mit der Prüfung, z. B. Fehler und Prüfungsprotokolle. Wählen Sie Ergebnisse, um zum Dashboard**Scan-Ergebnissezu** navigieren. Die Scan-Ergebnisse werden in der Spalte **Ergebnis** aufgelistet. Klicken Sie auf ein Ergebnis, um die Detailinformationen anzuzeigen und anzuzeigen:

- **Scan-Funde**: Zeigt alle Ergebnisse an, die während der Ausführung der Prüfungen gefunden wurden.
- **Suites**: Zeigt alle Suites an, die als Teil der Prüfung ausgeführt wurden.
- **Prüfungen**: Zeigt alle Prüfungen an, die als Teil der Prüfung ausgeführt wurden.
- **Fehler:** Zeigt alle Prüfungen an, die während der Ausführung des Scans fehlgeschlagen sind. Außerdem wird der Grund für den Fehler in Form einer Fehlermeldung angezeigt.
- **Scanprotokoll**: Zeigt Nachrichten an, die während des gesamten Scans gefunden wurden.
- **Scan-Statistiken**: Zeigt Statistiken zum Scan an.
- **Ziel**: Zeigt alle Ziele an, für die die Prüfungen ausgeführt wurden.

Scanfunde

Ein Ergebnis ist ein Verweis auf einen Datensatz, der gegen eine Regel verstoßen hat, die aus einem Scheck in der Instanz stammt. Sie können den Quelldatensatz und die Häufigkeit finden, mit der der Datensatz Regeln einer bestimmten Prüfung ausgelöst hat.

Navigieren Sie zu Ergebnisse, um eine Liste der **Scanfunde** für Ihre Instanz anzuzeigen. Wählen Sie einen Link unter der Spalte **Erstellt** aus, um Detailinformationen zu einem Ergebnis anzuzeigen:

- **Scheck**: Die Liste der dem Scan zugeordneten Schecks.
- **Kategorie**: Die Sicherheitskategorie, die dem Scan zugeordnet ist. Zum Beispiel Zugriffssteuerung oder böswilliger Code.
- Anzahl: Wie oft der Datensatz gegen**Prüfregeln**verstoßen hat.
- **Priorität**: Der Schweregrad des Sicherheitsrisikos: 1 ist die höchste Priorität, 4 die niedrigste Priorität.
- **Ergebnis**: Der Status und Typ des Scans.
- Scheckversion: Die Change**-Version**des Schecks.
- **Quelltabelle**: Der Datensatz, bei dem ein Verstoß gegen eine Regel des Schecks vorliegt.
- **Stummschaltgrund**: Der Grund für das Stummschalten des Ergebnisses.
- **Quelle**: Das Datum, an dem das Ergebnis erstellt wurde.
- **Aufgabe**: Wird verwendet, um Aufgabenzuweisungen anhand der Suche nach einem Datensatz zu erleichtern.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Domäne**: Definiert, auf was Sie zugreifen können und was nicht.
- **Kurzbeschreibung**: Eine kurze Erklärung der Prüfung.
- **Lösungsdetails**: Anweisungen zur Lösung der Scan-Probleme.

Sicherheitsmetriken

Verwenden Sie das Tool Metriken, um über 50 verschiedene Sicherheitsmetriken zu überwachen und potenzielle Sicherheitsbedrohungen oder unsicheres Verhalten zu identifizieren. Sie können Schwellenwerte für E-Mail-Benachrichtigungen festlegen, die Daten auf verschiedene Arten visualisieren und analysieren, die Daten exportieren oder Dashboards mit den Metriken erstellen, die für Ihre Organisation am wichtigsten sind.

Metriken werden als Analytics Hub-Visualisierungen implementiert, die eine Vielzahl von Funktionen ermöglichen, unter anderem das Senden von E-Mail-Warnungen bei Überschreitung von Schwellenwerten, die Visualisierung von Zielen sowie das Anzeigen und Filtern von zugrunde liegenden Ereignissen.

Meine Sicherheitsmetriken – Dashboard

Zeigen Sie die Sicherheitsmetriken in Ihrer Instanz über ein einziges Dashboard an.

Um zur Seite „Metriken“ zu navigieren, wählen Sie **Meine Metriken**aus. Auf dieser Seite wird das Standard-Dashboard angezeigt. Sie können jedoch auch ein eigenes Dashboard erstellen, indem Sie **Bearbeiten**auswählen.

Sie können Ihr eigenes Dashboard anpassen, indem Sie Visualisierungen, Filter, Überschriften, Bilder, Rich-Text und Listen hinzufügen. Weitere Informationen zu den verschiedenen Möglichkeiten zur Anpassung Ihres Dashboards finden Sie unter Dashboards in Platform Analytics .

Konfigurieren Sie Sicherheitsmetriken, um E-Mails zu senden, wenn Schwellenwerte ausgelöst werden

Erfahren Sie, wie Sie Sicherheitsmetriken so konfigurieren, dass Ihre Instanz eine E-Mail-Benachrichtigung generiert, wenn ein Schwellenwert ausgelöst wird.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Navigieren Sie in Security Center zu **Metriken**.
2. Wählen Sie eine Metrik aus, für die Sie einen Schwellenwert in Ihrer Organisation festlegen möchten.

   Example
   Wenn Sie fehlgeschlagene Anmeldungen verwalten möchten, können Sie einen Schwellenwert festlegen, damit die Administratoren oder Sicherheitsexperten in Ihrer Organisation benachrichtigt werden, wenn fehlgeschlagene Anmeldungen eine bestimmte Anzahl erreichen. Die entsprechende Sicherheitsmetrik für das Ziel lautet in diesem Fall **users** > **fehlgeschlagene Anmeldungen**an.
3. Wählen Sie das Symbol **Schwellenwerte**.
4. Wählen Sie im Schwellenwertbereich das **Plussymbol (+)**, um das Formular zu konfigurieren. Die verfügbaren Optionen dienen zum Festlegen der Sichtbarkeit, des Schwellenwerttyps und des Schwellenwerts.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie aus Sichtbarkeit **für alle** aus, wenn jeder die Benachrichtigung erhalten soll, oder **für mich,** wenn Sie nur eine Benachrichtigung erhalten möchten.

b. Wählen Sie als Schwellenwerttyp „ **Allzeithoch**“ aus.
Dies ist das Feld, das die Schwellenwertbenachrichtigung auslöst.

> **Hinweis:** Ein Schwellenwert muss nur eingegeben werden, wenn der **Schwellenwerttyp** auf **Weniger als** oder **Mehr als**festgelegt ist.

5. Wählen Sie „ **Speichern** “, um den Schwellenwert zu erstellen.
Als Nächstes muss die Benachrichtigung eingerichtet werden.
6. Wählen Sie **alle**aus, und geben Sie **Systembenachrichtigung ein**.
7. Navigieren zu **E-Mail** > **Benachrichtigungen**an.
8. Geben Sie in der **Namensspalte**`*pa thre ein`.
Die Schwellenwertbenachrichtigungen sind ereignisbasiert und werden in der PA-Schwellenwertbenachrichtigungstabelle eingerichtet.
9. Wählen Sie **PA Schwellenwert-Benachrichtigung** aus.
Die Ergebnisse enthalten drei Registerkarten:
   - Sendezeitpunkt: Gibt an, was passieren muss, um die E-Mail-Benachrichtigung zu senden. In diesem Beispiel wird die E-Mail ausgelöst, sobald der zuvor festgelegte Schwellenwert erreicht ist.
   - Empfänger: Gibt an, welche Benutzer die Benachrichtigung erhalten. Sie können Benutzer und Gruppen hinzufügen.
   - Was darin enthalten sein wird: Gibt die Skriptaktion an, die ein Benutzer ändern kann, um die Nachricht anzupassen, die Benutzer und Gruppe erhalten. Weitere Informationen zum Erstellen von Skriptaktionen finden Sie unter Skriptaktionen .

Passen Sie das Dashboard für Sicherheitsmetriken an

Entdecken Sie die Flexibilität des Dashboards für Sicherheitsmetriken, das mit Metriken aus verschiedenen Quellen wie Grafiken und Diagrammen angepasst werden kann. Passen Sie das Dashboard an die spezifischen Anforderungen Ihrer Organisation an.

Vorbereitungen

Um das Dashboard für Sicherheitsmetriken anzupassen, vergewissern Sie sich, dass Sie sich im Anwendungsbereich von Security Center befinden. Um zu diesem Bereich zu wechseln, wählen Sie **Anwendungsauswahl** > **Anwendungsbereich**, und geben Sie Security Center ein.

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Implementieren und passen Sie Sicherheitsmetriken mit dem Security Center-Dashboard an. Fügen Sie Ihrem Dashboard Metriken und Inhalte aus verschiedenen Quellen hinzu, z. B. aus einem Bericht generierte Grafiken und Diagramme. Lernen Sie, wie Sie Ihrem Dashboard für Sicherheitsmetriken eine Registerkarte hinzufügen, damit Sie es an die Anforderungen Ihres Unternehmens anpassen können.

Prozedur

1. Navigieren Sie in der App „Security Center“ zum Dashboard für Sicherheitsmetriken, indem Sie **Metriken**auswählen.
2. Wechseln Sie in den Bearbeitungsmodus, indem Sie **Bearbeiten**wählen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Erstellen Sie eine Registerkarte, indem Sie **+Registerkarte**hinzufügen wählen.

   Hinweis: Sie können auch eine neue Registerkarte hinzufügen, indem Sie das **Pluszeichen (+)** neben einer vorhandenen Registerkarte wählen.

4. Bearbeiten Sie den Titel der neu erstellten Registerkarte, indem Sie das Bleistiftsymbol auswählen und einen Namen eingeben.
5. Fügen Sie Ihrer Registerkarte ein Element hinzu, indem **Sie Neues Element hinzufügen**auswählen.
6. Wählen Sie **Speichern**.
7. Wahlweise: Um das Dashboard für Benutzer, Gruppen und Rollen in Ihrer Organisation freizugeben, wählen Sie **Menü „Weitere Aktionen“** > **Freigeben**an.
   a. Geben Sie den Namen eines Anwenders ein, dem Zugriff gewährt werden soll.
   b. Wählen Sie zum **Bestätigen**aus.

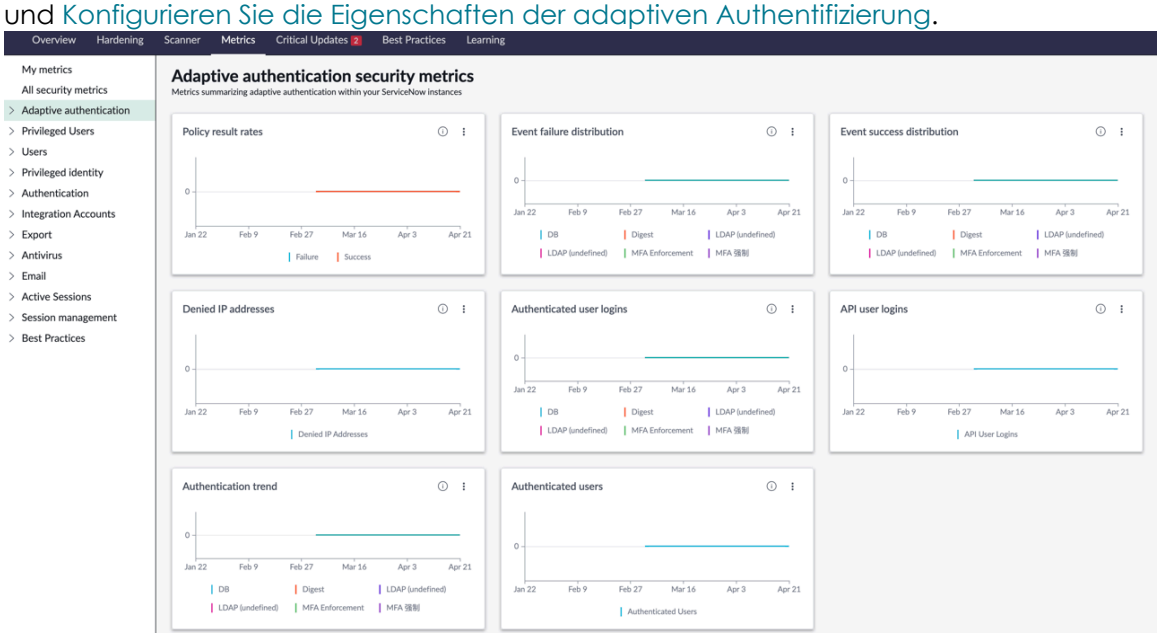
Alle Sicherheitsmetriken

Navigieren Sie zu **Alle Sicherheitsmetriken**, um eine Tabelle mit den Daten anzuzeigen, die sich auf die Sicherheitsmetriken Ihrer Instanz beziehen.

Sicherheitsmetriken der adaptiven Authentifizierung

Verwenden Sie Authentifizierungsrichtlinien, um Authentifizierungsanforderungen auszuwerten und den Zugriff auf Ihre Instanz basierend auf den angegebenen Richtlinienbedingungen zu verweigern oder zuzulassen.

Mit Metriken der adaptiven Authentifizierung können Sie überwachen, wie die adaptive Authentifizierung in Ihrer Instanz verwendet wird. Sie haben die Möglichkeit, eine Zusammenfassung aller Ihrer Metriken zur adaptiven Authentifizierung anzuzeigen, oder Sie können Detailinformationen anzeigen und einzelne Metriken anzeigen, z. B. Richtlinienergebnisraten oder abgelehnte IP-Adressen. Diese Seite erfordert das Plugin „Adaptive Authentifizierung“ (`com.snc.adaptive_authentication`), damit die adaptive Authentifizierung in Ihrer Instanz verfügbar ist. Sie müssen auch die Authentifizierungsrichtlinie aktivieren, um die Metriken anzuzeigen. Weitere Informationen finden Sie unter Aktivieren Sie die adaptive Authentifizierung und Konfigurieren Sie die Eigenschaften der adaptiven Authentifizierung.



Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Diese Funktion wurde mit Version 1.2 veröffentlicht.

- Richtlinienergebnisraten: Alle erfolgreichen und fehlgeschlagenen adaptiven Authentifizierungsereignisse.
- Ereignisfehler-Verteilung: Alle fehlgeschlagenen Ereignisse für jeden Ereignistyp.
- Ereigniserfolgsverteilung: Die erfolgreichen Ereignisse, die jedem Ereignistyp zugeordnet sind.
- Abgelehnete IP-Adressen: Die Anzahl der von der Instanz blockierten IP-Adressen zusammen mit den zugehörigen Daten.
- Authentifizierte Benutzeranmeldungen: Die Anzahl der Ereignisse, die für jeden Ereignistyp gezählt werden, ausschließlich des Ereignisses vor der Anmeldung.
- API-Anwenderanmeldungen: Die Anzahl der Ereignisse, die API-Authentifizierungsrichtlinien für jeden Ereignistyp zugeordnet sind.
- Authentication Trend (Authentifizierungstrend): Gesamtzahl der aufgezeichneten Ereignisse.
- Authentifizierte Benutzer: Die Anzahl der Benutzer, die für jeden Ereignistyp gezählt wurden, ausschließlich des Ereignisses vor der Anmeldung.

Privilegierte Anwender

Zeigen Sie die Trendlinie für die (aktiven und inaktiven) privilegierten Benutzer und ihre Aktivitäten für Now Platforman.

Im Abschnitt Übersicht über privilegierte Benutzer werden die Trendlinie für (aktive und inaktive) privilegierte Benutzer und ihre Aktivitäten für Now Platformangezeigt. Privilegierte Benutzer sind Benutzer, denen von Administratoren zusätzliche Rollen zugewiesen werden, um auf bestimmte Funktionen zuzugreifen, z. B. „Strenge Sicherheitseinstellungen“, „Import“ und „Portalbenutzer“.

Nachfolgend finden Sie eine Erklärung der privilegierten Benutzer:

- Anwender gesamt: Gesamtanzahl der Anwender in Ihrer Instanz.
- Aktive Benutzer: Gesamtzahl der Benutzer, die Sitzungen in Ihrer Instanz initiiert haben.
- Inaktive Benutzer: Benutzer, die sich nicht kürzlich bei Ihrer -Instanz angemeldet haben.
- Inaktive Anwender, die nicht ausgesperrt sind: Anwender, die sich nicht kürzlich angemeldet haben, aber weiterhin Zugriff auf ihren Account haben.
- Gesperrte Anwender: Anwender, die sich nicht bei ihrem Account authentifizieren dürfen.
- Neue Benutzer: Benutzer, die Ihrer Instanz kürzlich hinzugefügt wurden.
- Erfolgreiche Anmeldungen: Anwender, die sich erfolgreich angemeldet haben.
- Fehlgeschlagene Anmeldungen: Nicht erfolgreiche Anmeldungsversuche.
- Lokale Anmeldungen, die nicht durch MFA geschützt sind: Anwender, die sich ohne MFA angemeldet haben.
- Nie angemeldete Benutzer: Benutzer, die sich nie bei Ihrer Instanz angemeldet haben.
- Anwender, die sich im letzten Monat nicht angemeldet haben: Anwender, die sich in den letzten 30 Tagen nicht angemeldet haben.
- Anwender, die sich in den letzten 6 Monaten nicht angemeldet haben: Anwender, die sich in den letzten 6 Monaten nicht angemeldet haben.
- Anwender, die sich im letzten Jahr nicht angemeldet haben: Anwender, die sich im letzten Jahr nicht angemeldet haben.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Muss Passwort zurücksetzen: Anwender, die ihr Passwort zurücksetzen müssen.
- Passwortzurücksetzungs-Fehler der Anwender: Anzahl der Passwortfehler pro Anwender.

Anwender

Zeigen Sie die Trendlinie für die Gesamtzahl der (aktiven und inaktiven) Anwender und ihre Aktivitäten für Now Platforman.

Im Abschnitt „Benutzerübersicht“ werden die Trendlinie für die Gesamtzahl der (aktiven und inaktiven) Benutzer und ihre Aktivitäten im Now Platformangezeigt.

Nachfolgend finden Sie eine Erklärung der Anwendertypen:

- Anwender gesamt: Gesamtanzahl der Anwender in Ihrer Instanz.
- Aktive Benutzer: Gesamtzahl der Benutzer, die Sitzungen in Ihrer Instanz initiiert haben.
- Inaktive Benutzer: Benutzer, die sich nicht kürzlich bei Ihrer -Instanz angemeldet haben.
- Inaktive Anwender, die nicht ausgesperrt sind: Anwender, die sich nicht kürzlich angemeldet haben, aber weiterhin Zugriff auf ihren Account haben.
- Neue Benutzer: Benutzer, die Ihrer Instanz kürzlich hinzugefügt wurden.
- Erfolgreiche Anmeldungen: Anwender, die sich erfolgreich angemeldet haben.
- Fehlgeschlagene Anmeldungen: Nicht erfolgreiche Anmeldungsversuche.
- Externe Anmeldungen: Authentifizierungen, die eine Drittpartei verwenden.
- Nicht durch MFA geschützte lokale Anmeldungen: Anmeldungen, die MFA nicht verwenden.
- Anwender, die sich im letzten Monat nicht angemeldet haben: Anwender, die sich in den letzten 30 Tagen nicht angemeldet haben.
- Anwender, die sich in den letzten 6 Monaten nicht angemeldet haben: Anwender, die sich in den letzten 6 Monaten nicht angemeldet haben.
- Anwender, die sich im letzten Jahr nicht angemeldet haben: Anwender, die sich im letzten Jahr nicht angemeldet haben.
- Muss Passwort zurücksetzen: Anwender, die ihr Passwort zurücksetzen müssen.
- Passwortzurücksetzungs-Fehler der Anwender: Anzahl der Passwortfehler pro Anwender.

Privilegierte Identität

Analysieren Sie Daten im Zusammenhang mit Metriken für Benutzer mit privilegierter Identität.

Dieses Dashboard zeigt Daten zu privilegierten Identitätsbenutzern und ihrer Aktivität in Ihrer Instanz an.

- Administratoranmeldungen: Gesamtanzahl der Anmeldungen mit Anwendern der Administratorrolle.
- Identitätswechsel: Gesamtanzahl der Identitätswechsel, die von Anwendern mit der Rolle „Identitätswechsel“ durchgeführt wurden.
- Erhöhung: Gesamtanzahl der von Benutzern mit der Rolle „security_admin“ vorgenommenen Sicherheitserhöhungen.
- ServiceNow-Anmeldungen: Gesamtanzahl der Anmeldungen von ServiceNow-Mitarbeitern.
- Administratorbenutzer hinzugefügt: Gesamtzahl der Benutzer, denen die Administratorrolle zugewiesen wurde.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Authentifizierungsmetriken

Zeigen Sie in einem -Dashboard Metriken im Zusammenhang mit der Authentifizierung in Ihrer Instanz an.

Zeigt Daten für Metriken im Zusammenhang mit Authentifizierungsschemas wie MFA-Nutzung, Webservicekonten und Nutzung des biometrischen Scanners an.

- Für MFA registrierte Anwender: Gesamtanzahl der Anwender, die für MFA registriert sind.
- Anwender mit MFA-Umgehung: Gesamtanzahl der Anwender, die die Multifaktor-Authentifizierung umgehen.
- Nicht-MFA-Anwender mit hohen Berechtigungen: Gesamtanzahl der Anwender mit hohen Berechtigungen, die keine MFA verwenden.
- Aktive MFA-Benutzer: Gesamtanzahl der MFA-Benutzer, die in Ihrer Instanz aktiv sind.
- Gesperrte MFA-Benutzer: Gesamtanzahl der MFA-Benutzer, die in Ihrer Instanz gesperrt sind.
- Webservice-Account-Anwender: Gesamtanzahl der Anwender, die nur über einen Webservice-Account verfügen.
- Ablaufende X509-Zertifikate: Gesamtanzahl der X509-Zertifikate, die in den nächsten 30 Tagen ablaufen.

Integrations-Accounts

Zeigen Sie die Trends zu den Integrationsaccounts an, die im Now Platformerstellt wurden.

Das Dashboard für Integrationsaccounts zeigt Trends zu den Integrationsaccounts an, die unter Now Platformerstellt wurden.

Nachfolgend finden Sie Erklärungen zu den Metriken der Integrationsaccounts:

- Integrationsaccounts insgesamt: Trends im Zusammenhang mit Integrationsaccounts in Ihrer Instanz.
- Aktive Integrationsaccounts: Trends im Zusammenhang mit aktiven Integrationsaccounts in Ihrer Instanz.
- Inaktive Integrationsaccounts: Trends für die Gesamtanzahl der Integrationsaccounts, die in Ihrer Instanz inaktiv sind.

Exportieren

Ermitteln Sie die Daten, die häufig exportiert werden und welche Anwender exportieren.

- Exporte gesamt: Gesamtanzahl der vom Anwender exportierten Tabellendatensätze.
- Klassifizierte Exporte: Gesamtanzahl der exportierten Tabellendatensätze, zusammengefasst nach der ihnen zugewiesenen Datenklassifizierung.

Virenschutz

Zeigt den Trend an, wann Ereignisse für potenziell infizierte Dateien auftreten. Sehen Sie, wenn sie erkannt, in Quarantäne gestellt, wiederhergestellt oder gelöscht werden.

- Dateien in Quarantäne: Die Anzahl der Dateien, die potenziell Malware enthalten.
- Heruntergeladene Dateien: Die Anzahl der heruntergeladenen Dateien.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wiederhergestellte Dateien: Anzahl der wiederhergestellten Dateien.
- Gelöschte Dateien: Die Anzahl der gelöschten Dateien.

E-Mail

Zeigt Daten zu Spam-E-Mails an, die extern empfangen werden.

Spam-E-Mails geben die Anzahl der pro Tag empfangenen Junk-E-Mails an.

Aktive Sitzungen

Zeigen Sie die Trendlinie der aktiven Benutzer in Now Platforman.

Die Trendlinie kann für die folgenden Metriken angezeigt werden:

- Benutzersitzungen: Metriken im Zusammenhang mit aktiven Benutzersitzungen in Ihrer Instanz.
- Sitzungen privilegierter Benutzer: Metriken, die sich auf privilegierte Benutzer oder Benutzer beziehen, denen zusätzliche Rollen zugewiesen wurden.

Management von Anwendersitzungen

Zeigen Sie Metriken in Bezug auf Benutzersitzungen und die Häufigkeit der Sperrungen der Sitzungen an.

Datenklassifizierung

Greifen Sie auf die Sicherheitsmetriken für die Datenklassifizierung in Ihrer ServiceNow-Instanz zu.

Mit der Datenklassifizierung können Sie Datenklassifizierungsbezeichnungen auf vorhandene Wörterbucheinträge in jeder Tabelle anwenden, um Einblick in die in Ihren Instanzen gehosteten Datentypen zu erhalten und um Datenschutzgesetze und Branchenvorschriften einzuhalten.

Weitere Informationen finden Sie unter Datenklassifizierung .

- **Klassifizierbare Daten**: Tabellen oder Spalten, die klassifiziert werden können.
- **Klassifizierte Daten**: Wörterbucheinträge, Tabellen oder Spalten, die klassifiziert sind.

Die Daten werden in einem anpassbaren Diagramm grafisch angezeigt, das detaillierte Analysen wie das Festlegen von Zielen, Schwellenwerten, Trends, Statistiken oder Prognosen ermöglicht. Die Daten werden auch als Datensätze in einer Tabelle organisiert. Weitere Informationen finden Sie unter Analytics Hub .

Kundenaktionen

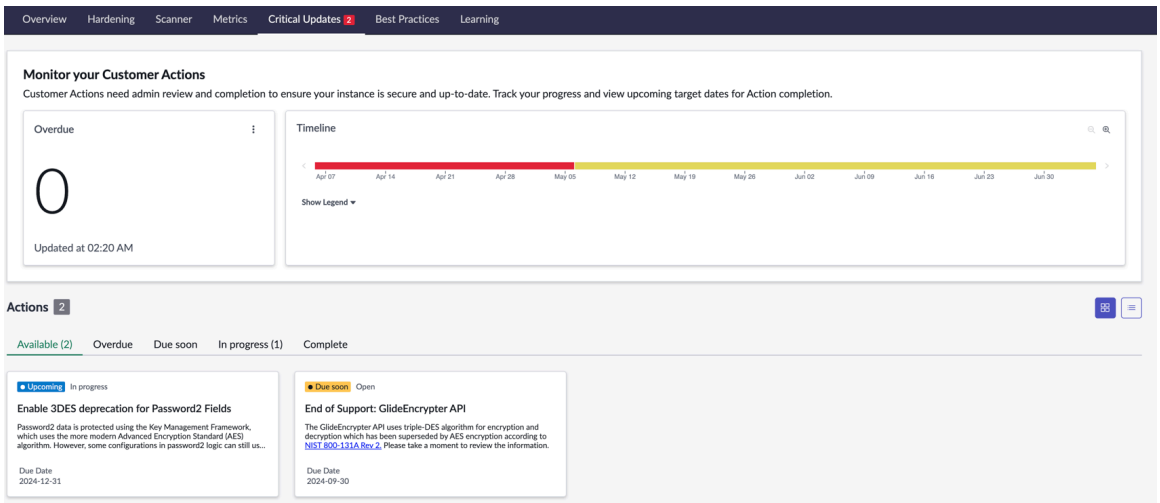
Erhöhen Sie den Sicherheitsstatus Ihrer Instanz, indem Sie sicherstellen, dass die vom System empfohlenen Kundenaktionen rechtzeitig implementiert werden.

Kundenaktionen sind ein Tool, das Administratoren bei der Implementierung wichtiger Sicherheitsupdates basierend auf ihrer Instanz und der Konfiguration von Plugins hilft. Eine Kundenaktion ist eine empfohlene Änderung an einer Instanz, die Ihnen dabei helfen soll, die Bedeutung von sicherheitsbezogenen Änderungen zu verstehen. Kundenaktionen unterstützen Sie bei der Implementierung der Schritte zum Scannen, Aktualisieren und Testen der Sicherheitsupdates in Ihrer Instanz. Implementieren Sie eine Kundenaktion, um zu verhindern, dass die Anpassung Ihrer Instanz beeinträchtigt wird. Manuell implementierte

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kundenaktionen unterscheiden sich von den automatischen Updates, die in Ihrer Instanz an ServiceNow-Code oder -Funktionen mit Familienreleases oder Patches gerendert werden.

Auf der Homepage von „Kundenaktionen“ wird die Zeitleiste der Kundenaktionen angezeigt, um zu priorisieren, wann die Schritte implementiert werden sollen. Die Zeitleiste im Screenshot zeigt die Kundenaktionen, die überfällig sind, und diejenigen, die bald fällig sind. Darüber hinaus können Sie den Fortschritt Ihrer Kundenaktionen unter der Bezeichnung Updates nachverfolgen. Wählen Sie die Registerkarten aus, um die Kundenaktionen als verfügbar, überfällig, bald fällig, in Bearbeitung oder abgeschlossen anzuzeigen.



Erste Schritte:

- Greifen Sie auf dieses Tool zu, indem Sie in Security Center zu **Kundenaktionen** navigieren.
- Kundenaktionen sind ab Washington DC in der Security Center-App enthalten.

Implementieren Sie Schritte für Kundenaktionen

Erfahren Sie, wie Sie Kundenaktionen in Ihrer Instanz implementieren, um den Sicherheitsstatus zu erhöhen.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

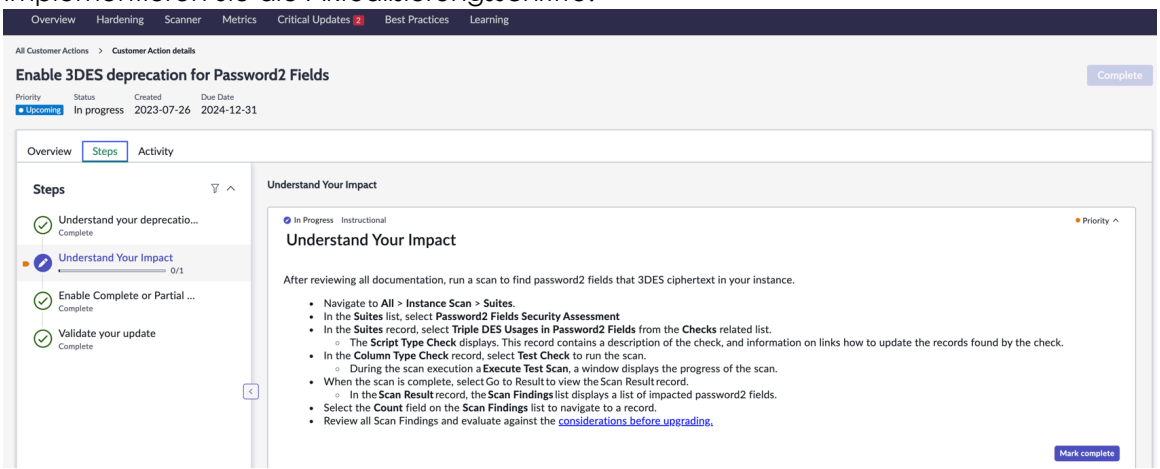
Kundenaktionen (CA) enthält Schritt-für-Schritt-Anweisungen, wie Sie die Changes in Ihrer Instanz implementieren, um Ihren Sicherheitsstatus zu erhöhen. CA ruft relevante Inhalte aus der Produktdokumentation ab, um Sie durch die einzelnen Schritte des Implementierungsprozesses zu führen. Führen Sie die folgenden Schritte aus, um zu erfahren, wie Sie eine Kundenaktion implementieren.

Prozedur

1. Navigieren Sie zur App **Kundenaktionen**.
2. Klicken Sie auf, um eine Kundenaktion zu implementieren.
   Im Abschnitt „ **Updates** “ listet die Registerkarte Verfügbar alle Kundenaktionen in Ihrer Instanz auf. Klicken Sie unter dieser Registerkarte auf eine Kundenaktion, um die Anweisungen anzuzeigen.
3. Lesen Sie die Übersicht, um zu erfahren, warum die Kundenaktion erforderlich ist, und um die Implementierung der Schritte vorzubereiten.
   Klicken Sie auf **„Zum nächsten Schritt** wechseln“, um mit den Implementierungsdetails fortzufahren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Implementieren Sie die Aktualisierungsschritte.



   a. Lesen Sie jede Gruppe von Anweisungen, und implementieren Sie sie in Ihrer Instanz.

   b. Klicken Sie auf Als **abgeschlossen** markieren, wenn Sie mit einer Reihe von Anweisungen fertig sind.

   c. Wiederholen Sie die Schritte ab, bis Sie alle Aktualisierungsschritte abgeschlossen haben.

   d. Klicken Sie auf **Abschließen**.
   Die Kundenaktion sollte nicht mehr verfügbar sein im Abschnitt „Updates“ der Homepage „Kundenaktionen“.

Zeigen Sie die Aktivität von Kundenaktionen an

Zeigen Sie Details zu allen Aktivitäten im Zusammenhang mit Ihren Kundenaktionen an.

Vorbereitungen
Erforderliche Rolle: admin

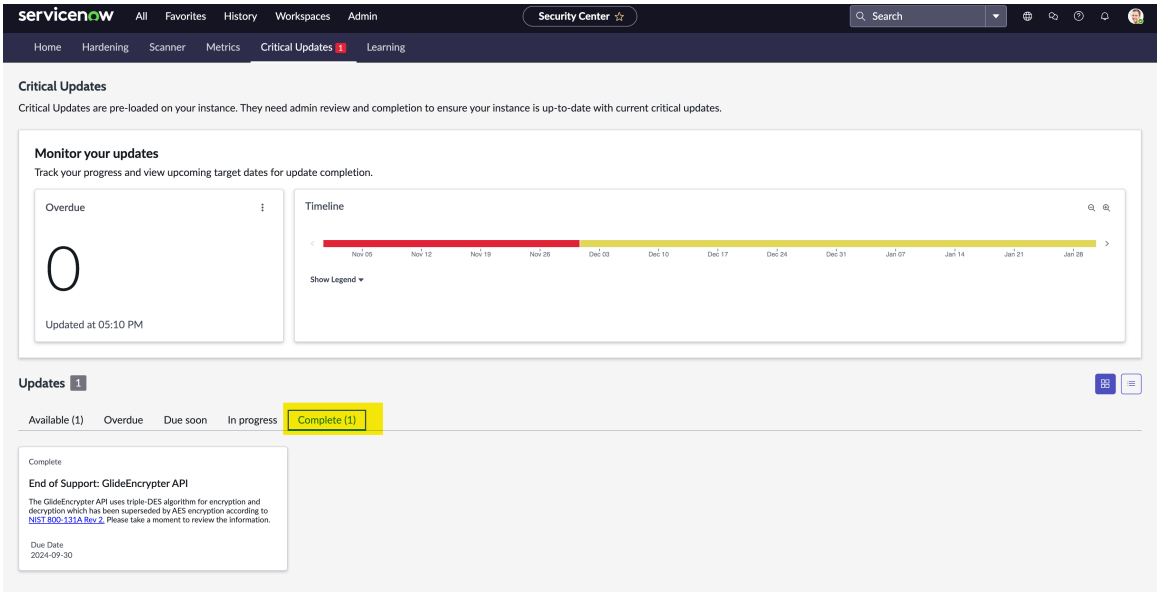
Warum und wann dieser Vorgang ausgeführt wird
Die Aktivitäten werden von den neuesten bis zu den ältesten aufgelistet, sodass Sie die neueste Aktivität zuerst analysieren können. Jede Aktualisierung einer Aktivität wird mit einem Zeitstempel versehen, und Sie können die Suche und den Filter verwenden, um bestimmte Informationen abzufragen.

Prozedur

1. Navigieren Sie in Security Center zur App **Kundenaktionen**.
2. Navigieren Sie zu der Bezeichnung **Updates** von Kundenaktionen.
3. Klicken Sie auf einen Status, und wählen Sie dann eine Kundenaktion aus diesem Status aus.

   Im folgenden Beispiel wird der Status **Abgeschlossen** und dann die Kundenaktion für **Ende des Supports: GlideEncrypter API** ausgewählt.

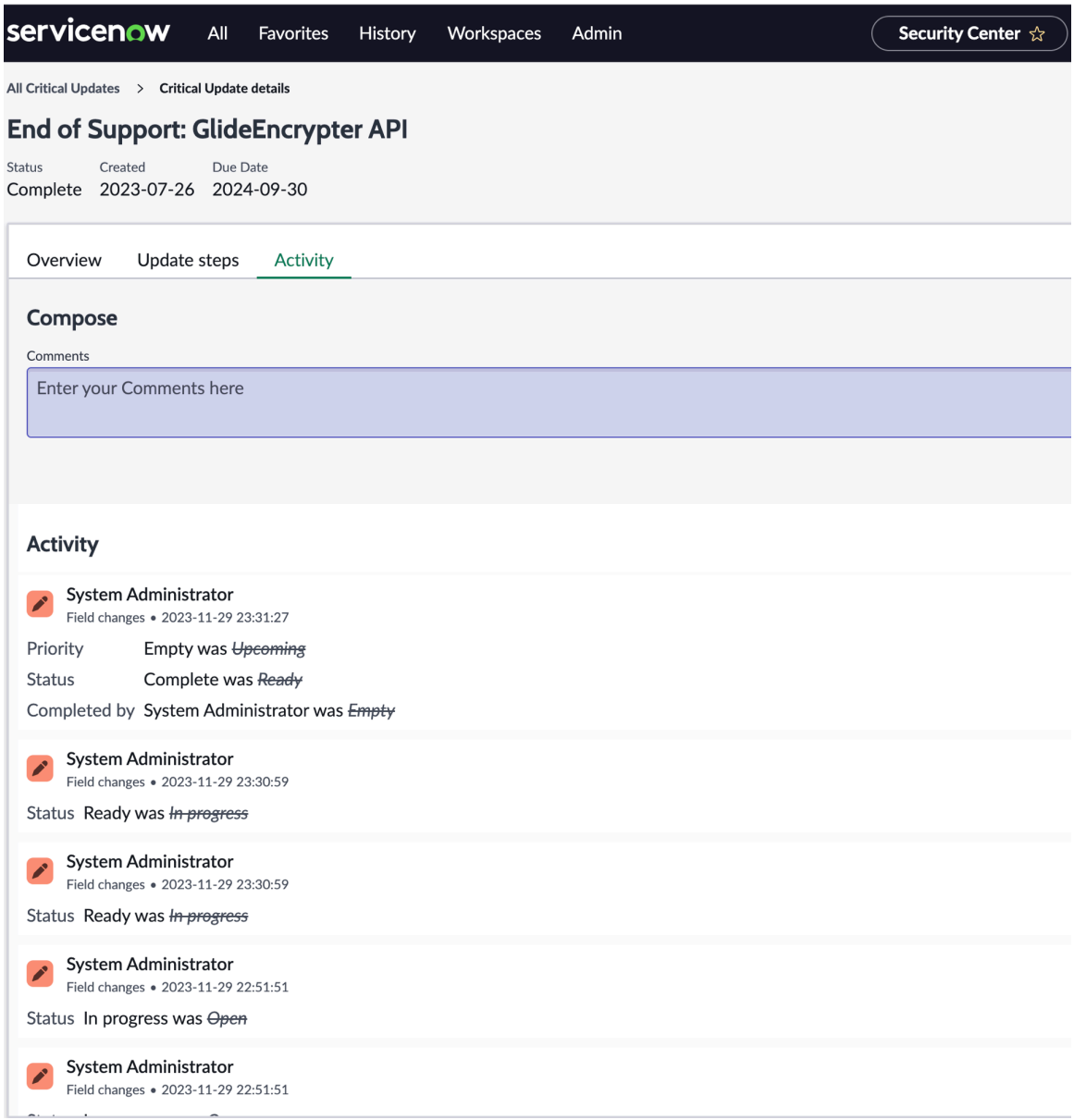
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Zeigen Sie die Aktivität Ihrer Kundenaktion an.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Alle mit einer Kundenaktion verbundenen Aktivitäten werden automatisch aufgezeichnet. Darüber hinaus können Sie Aktivitäten zusätzliche Kommentare hinzufügen.

Best Practices für Sicherheit

Verwenden Sie Best Practices für Sicherheit, um Datenschutz- und Sicherheitskonfigurationsaufgaben in Ihrer ServiceNow-Instanz zu implementieren.

Verwenden Sie Best Practices für Sicherheit, um Sicherheitsvorschläge von ServiceNow zu überprüfen, diejenigen zu identifizieren, die Ihren Sicherheitsstatus am meisten verbessern, und Schritt-für-Schritt-Anweisungen zu ihrer Implementierung zu befolgen.

Die Best Practices für Sicherheit bieten Folgendes:

- Die Homepage von zeigt eine Übersicht über Ihren Fortschritt bei der Implementierung von Best Practices für Sicherheit. Sie können auch Listen mit Best Practices für die Sicherheit entsprechend den Zielen Ihrer Organisation organisieren und verwalten.
- Die Übersichtsseite enthält Details zu den einzelnen Best Practices für Sicherheit, die Schritte zu ihrer Implementierung sowie einen Datensatz aller Aktivitäten und Kommentare.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Auf der Seite mit den Aufgabenschritten finden Sie Anweisungen zur Implementierung von Best Practices für Sicherheit.
- Die Aktivitätsseite verfolgt den Verlauf der Benutzer- und Systemaktionen im Zusammenhang mit Ihren Best Practices für Sicherheit.

Security Best Practices – Homepage

Die Homepage enthält Diagramme, die die Gesamtzahl der abgeschlossenen Best Practices für die Sicherheit insgesamt, die Anzahl der abgeschlossenen Best Practices nach Reifegrad und eine Tabelle mit allen verfügbaren Best Practices für die Sicherheit darstellen.

In der Tabelle können Sie Filter anwenden, um gefilterte Listen zu sortieren und zu speichern, die Sie als Arbeitslisten für verschiedene Anwendungsfälle oder Rollen verwenden können. Weitere Informationen finden Sie unter Gefilterte Liste speichern.

Im Folgenden finden Sie Erklärungen zu den Feldern im Zusammenhang mit der Tabelle mit den Best Practices für Sicherheit.

Zusammenfassung der Felder, die in der Tabelle mit Best Practices für Sicherheit verwendet werden

Name	Beschreibung
Name	Wort, das zur Identifizierung einer Best Practice für Sicherheit verwendet wird.
Reifegrad	Anwendungen und Funktionen, die in der Reihenfolge ihrer Auswirkung angeordnet wurden, um messbare Ergebnisse zu liefern. Die Werte für Reifegrade sind: • Grundlage schaffen • Experience erweitern • Funktionalität optimieren • Erweiterte Funktionen hinzufügen Man kann sie auch als Kriech-, Geh-, Lauf- und Flugphasen betrachten.
Status	Aktueller Status einer Best Practice für Sicherheit: • Offen • In Bearbeitung • Abgeschlossen
Priorität	Reihenfolge der Wichtigkeit für die Implementierung einer Best Practice für Sicherheit in Ihrer Organisation: • Sofort • Später • Nicht zutreffend

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusammenfassung der Felder, die in der Tabelle mit Best Practices für Sicherheit verwendet werden (Fortsetzung)

Name	Beschreibung
Ziele	Sicherheitskategorie, die von einer Best Practice für Sicherheit behandelt wird: • Anfängliche Sicherheitskonfigurationen behandeln • Sichere E-Mails • Überwachungsprotokolle • Zugriffssteuerungen verwalten • Mit Verschlüsselung schützen • Halten Sie Instanzen auf dem neuesten Stand
Zuerst eingeführt	Security Center-Version, in der die Best Practice für Sicherheit eingeführt wurde.
Geändert	Security Center-Version, in der die Best Practice für Sicherheit zuletzt geändert wurde.
Entfernt	Security Center-Version, in der die Best Practice für Sicherheit entfernt wurde.

Übersichtsseite für Best Practices für Sicherheit

Wenn Sie in der Tabelle mit den Best Practices für Sicherheit eine Best Practice für Sicherheit auswählen, gelangen Sie zu einer Seite mit den folgenden Unterregisterkarten: Übersicht, Aufgabenschritte und Aktivität.

Oben auf der Übersichtsseite können Sie allgemeine Informationen über die Best Practice für Sicherheit anzeigen, einschließlich Priorität, Reifegrad und Status.

Im Dropdown-Menü **Priorität** können Sie die Best Practices für die Sicherheit angeben, die für Sie zu diesem Zeitpunkt wichtig sind und die nicht anwendbar sind.

Der Detailabschnitt enthält Inhalte zu den Funktionen, die der Best Practice für Sicherheit zugeordnet sind, und der Dokumentationsabschnitt enthält einen oder mehrere Links, unter denen Sie zusätzliche Informationen finden können.

Die Karte **„Fortschritt** " rechts zeigt die Anzahl der abgeschlossenen Schritte vs. die Gesamtzahl der enthaltenen Schritte. Wählen **Sie „Zum nächsten Schritt** wechseln", um zum nächsten unvollständigen Schritt zu navigieren.

Die Karte mit dem **Best Practice-Aktualisierungsverlauf** bietet einen Snapshot der Release-Informationen für die Best Practice. Sie können nachverfolgen, in welcher ServiceNow Security Center-Version die Best Practice für Sicherheit veröffentlicht wurde und in welchen Versionen sie anschließend zuletzt aktualisiert wurde.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Seite mit Best Practices-Aufgabenschritten für Sicherheit

Wenn Sie die Unterregisterkarte **Aufgabenschritte**auswählen, gelangen Sie zu einer Seite mit schrittweisen Anleitungen zur Implementierung der Best Practice für Sicherheit. Weitere Informationen finden Sie unter Eine Best Practice für Sicherheit abschließen.

Aktivitätsseite „Best Practices für Sicherheit“.

Die Aktivitäten werden von den neuesten bis zu den ältesten aufgelistet, sodass Sie die neueste Aktivität zuerst analysieren können. Jede Aktualisierung einer Aktivität wird mit einem Zeitstempel versehen, und Sie können Suchen und Filter verwenden, um Informationen abzufragen. Weitere Informationen finden Sie unter Filter auf die Tabelle mit Best Practices für Sicherheit anwenden.

Absolvieren Sie eine Best Practice für Sicherheit

Erfahren Sie, wie Sie eine Best Practice für Sicherheit in Ihrer ServiceNow-Instanz durchführen.

Warum und wann dieser Vorgang ausgeführt wird

Führen Sie die folgenden Schritte aus, um Best Practices für die Sicherheit in Ihrer ServiceNow-Instanz zu implementieren.

Prozedur

1. Greifen Sie auf Best Practices für Sicherheit zu, indem Sie in Ihrer ServiceNow-Instanz **Alle** auswählen und dann **Best**Practice eingeben.
2. Wenden Sie einen Filter an, um zu implementierende Sicherheits-Best Practices anzuzeigen.
   a. Navigieren Sie in der Anwenderoberfläche zur Tabelle „ **Best Practices** “.
   b. Wählen Sie das Kebab-Menü oder das Element mit den drei vertikalen Punkten (⋮) in der Spalte **Status** aus.
   c. Wählen Sie die Optionen **Öffnen** und **In Bearbeitung** und anschließend **Übernehmen**aus.
3. Wählen Sie den Namen einer zu implementierenden Sicherheits-Best Practice aus.
4. Wählen **Sie Zum nächsten Schritt wechseln**.
5. Wählen Sie einen Aufgabenschritt aus der Liste der **Aufgabenschritte** aus.
6. Wählen Sie das Caret-Symbol (v), um die Implementierungsanweisungen für diesen Schritt anzuzeigen.
7. Lesen Sie die Anweisungen, und implementieren Sie sie dann in Ihrer ServiceNow-Instanz.
8. Wählen Sie **Schritt als abgeschlossen** markieren aus, wenn Sie mit der Aufgabe fertig sind.

   Hinweis: Sie können die Aufgabe überspringen, wenn Sie später darauf zurückkommen möchten oder wenn sie nicht auf die Ziele Ihrer Organisation zutrifft. Darüber hinaus können Sie einen abgeschlossenen Aufgabenschritt erneut öffnen, indem Sie den Aufgabenschritt auswählen und dann **Schritt**neu starten auswählen.

9. Wählen Sie **Best Practice abschließen aus**.

   Sie können eine Best Practice für Sicherheit jederzeit abschließen. Sie müssen nicht alle Schritte ausführen und können sie auch überspringen. Sie sollten jedoch einen Kommentar auf der Unterregisterkarte Aktivität einfügen, wenn Sie eine Best Practice für Sicherheit anwenden und nicht alle Schritte für eine Audit-Referenz abgeschlossen haben.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie die Aktivität einer Best Practice an

Verfolgen Sie den chronologischen Verlauf und Zeitstempel im Zusammenhang mit einer Best Practice für Sicherheit, die Sie in Ihrer ServiceNow-Instanz durchführen, zusammen mit dem Anwender, der die Aktivität initiiert hat.

Prozedur

1. Greifen Sie auf den Security Best Practices Manager zu, indem Sie in Ihrer ServiceNow-Instanz **Alle** auswählen, und geben Sie dann Best Practice ein.
2. Wählen Sie in der Tabelle „Best Practices“ in der Spalte „ **Name** “ eine Best Practice für Sicherheit aus, deren Aktivität Sie anzeigen möchten.
3. Wählen Sie die Registerkarte **Aktivität**.

   Beispiele für Aktivitäten, die Sie anzeigen können, umfassen Feldänderungen, z. B. wenn sich der Status einer Sicherheits-Best Practice von Offen in Abgeschlossen geändert hat oder wenn ein Aufgabenschritt abgeschlossen oder übersprungen wird. Darüber hinaus können Sie zusätzliche Informationen im Zusammenhang mit einer Aktivität eingeben, indem Sie in das Textfeld einen Kommentar eingeben.

Zeigen Sie Daten abgeschlossener Best Practices an

Sehen Sie sich visuelle Darstellungen der Gesamtmenge der abgeschlossenen Best Practices an, segmentiert nach Reifegrad.

Warum und wann dieser Vorgang ausgeführt wird

Führen Sie die Aktionen aus, um Diagramme anzuzeigen, die visuelle Trends der abgeschlossenen Sicherheits-Best Practices insgesamt und nach Reifegrad zeigen.

Prozedur

1. Greifen Sie auf die App „Security Center“ zu, und navigieren Sie zur Registerkarte **Best Practices**.
2. Wählen Sie unter der Karte **Manage your Best Practices** (Best Practices verwalten) das **Gesamtdiagramm Abgeschlossen** aus.
3. Zeigen Sie das Diagramm an, um Trends zu abgeschlossenen Konfigurationen von Best Practices für die Sicherheit anzuzeigen.
4. Wählen Sie **Abgeschlossen nach Reifegrad aus**, um ein Diagramm anzuzeigen, das Trends für abgeschlossene Best Practices nach Reifegrad anzeigt.

Wenden Sie Filter auf die Tabelle mit Best Practices für Sicherheit an

Wenden Sie Filter an, um relevantere Ergebnisse für Ihre Best Practices für Sicherheit zurückzugeben.

Prozedur

1. Greifen Sie auf den Security Best Practices Manager zu, indem Sie in Ihrer ServiceNow-Instanz **Alle** auswählen und Best Practice eingeben.
2. Navigieren Sie zur Tabelle „ **Best Practices** “, und wählen Sie ein Feld aus, auf das Sie einen Filter anwenden möchten, indem Sie das entsprechende Kebab-Menü oder das Feld mit den drei vertikalen Punkten (⋮) auswählen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder	Filter
Name	Kombinieren Sie einen bedingten Operator mit einer Textzeichenfolge, um Best Practices für die Sicherheit zurückzugeben, die dem eingegebenen Namen entsprechen.
Reifegrad	Wenden Sie einen Filter an, um Best Practices für die Sicherheit zurückzugeben, die einem oder mehreren der folgenden Reifegrade entsprechen: ◦ Grundlage schaffen ◦ Experience erweitern ◦ Funktionalität optimieren ◦ Erweiterte Funktionen hinzufügen
Status	Wenden Sie einen Filter an, um Best Practices für die Sicherheit zurückzugeben, die einem oder mehreren der folgenden Status entsprechen: ◦ Leer ◦ Offen ◦ In Bearbeitung ◦ Abgeschlossen
Priorität	Wenden Sie einen Filter an, um Best Practices für die Sicherheit zurückzugeben, die den folgenden Prioritäten entsprechen: ◦ Leer ◦ Sofort ◦ Später ◦ Nicht zutreffend
Ziele	Wenden Sie einen Filter an, um Best Practices für die Sicherheit zurückzugeben, die einem oder mehreren der folgenden Ziele entsprechen: ◦ Anfängliche Sicherheitskonfigurationen behandeln ◦ Halten Sie Instanzen auf dem neuesten Stand ◦ Zugriffssteuerungen verwalten ◦ Überwachungsprotokolle ◦ Mit Verschlüsselung schützen ◦ Sichere E-Mails

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder	Filter
	Hinweis: Erweiterte Filter werden standardmäßig auf Ziele angewendet. Um sie zu ändern, wählen Sie **Änderungen vornehmen** > **Erweiterte Ansicht** > **Wählen Sie Feldziele aus** Erstellen Sie dann die restlichen Bedingungen, und wählen Sie **Aktualisieren**aus.
Zuerst eingeführt	Kombinieren Sie einen bedingten Operator mit einer Textzeichenfolge, um Best Practices zurückzugeben, die mit der von Ihnen eingegebenen Version erstmals eingeführt wurden.
Geändert	Kombinieren Sie einen bedingten Operator mit einer Textzeichenfolge, um Best Practices für die Sicherheit zurückzugeben, die sich in der von Ihnen eingegebenen Version geändert haben.
Entfernt	Kombinieren Sie einen bedingten Operator mit einer Textzeichenfolge, um Best Practices für die Sicherheit zurückzugeben, die in der von Ihnen eingegebenen Version entfernt wurden.

Speichern Sie einen Filter zur späteren Verwendung

Entdecken Sie die Schritte zum Speichern von Filtern in Ihren Best Practices für Sicherheit zur späteren Wiederverwendung.

Warum und wann dieser Vorgang ausgeführt wird

Nachdem Sie Filter in der Tabelle mit den empfohlenen Sicherheitspraktiken erstellt haben, können Sie sie speichern, um sie bei der nächsten Authentifizierung bei Ihrer Instanz zu verwenden. Wenn Sie mehr Flexibilität bei der Art der Filter wünschen, die Sie erstellen können, können Sie einen erweiterten Filter anwenden.

Prozedur

1. Wählen Sie das Symbol Filter anzeigen ( ).
2. Scrollen Sie im Dialogfeld „ **Filter** “ nach unten, und wählen Sie **Erweiterte Ansicht aus**.
3. Erstellen Sie einen Filter, indem Sie Bedingungen hinzufügen, die ein Feld, einen Operator und Werte enthalten.
4. Wählen **Sie Filter speichern**
5. Geben Sie den Filternamen ein.
6. Wählen Sie eine Berechtigung aus.
7. Wählen Sie **Speichern**.
8. Wählen Sie **Aktualisieren** aus, um den gespeicherten Filter auf die Tabelle mit Best Practices für Sicherheit anzuwenden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie einen gespeicherten Filter

Entdecken Sie die Schritte zur Verwendung der Filter, die Sie für Ihre Best Practices für Sicherheit gespeichert haben.

Warum und wann dieser Vorgang ausgeführt wird
Nachdem Sie sich von Ihrer -Instanz abgemeldet haben, werden Ihre Filter auf die Standardeinstellungen zurückgesetzt. Die folgenden Schritte zeigen, wie Sie einen gespeicherten Filter abrufen, um ihn erneut auf die Tabelle mit Best Practices für Sicherheit anzuwenden.

Prozedur

1. Wählen Sie das Symbol Filterbereich anzeigen ( ) aus.
2. Scrollen Sie im Dialogfeld Filter nach unten, und wählen Sie **Erweiterte Ansicht aus**.
3. Wählen **Sie Vorhandenen Filter verwenden**und anschließend einen gespeicherten Filter aus der Dropdown-Liste aus.
4. Wählen Sie **Aktualisieren** aus, um den gespeicherten Filter anzuwenden.

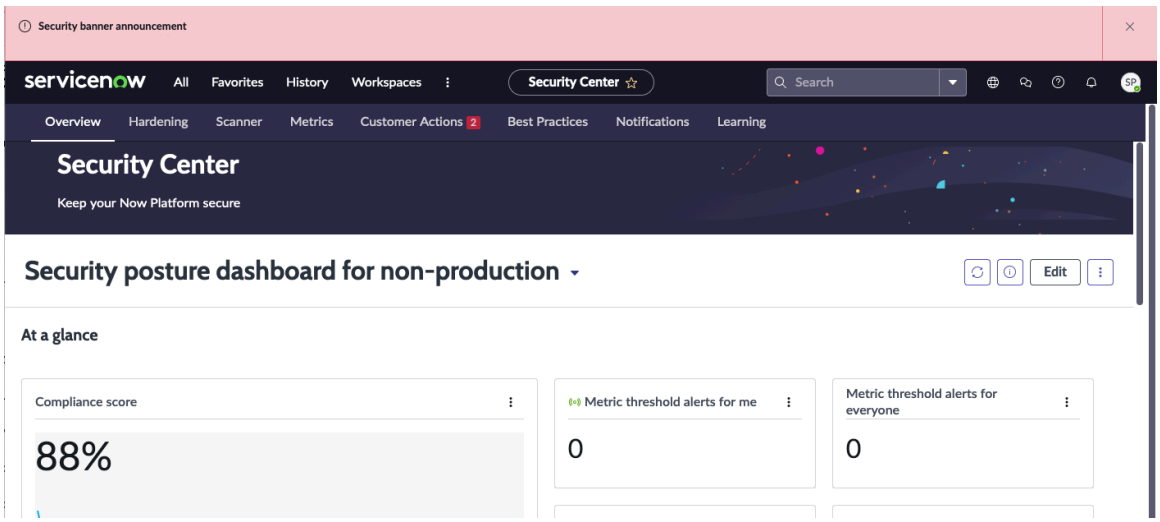
Security Learning

Greifen Sie über eine zentrale Seite auf Lernmaterialien für Sicherheit zu.

Lesen Sie Sicherheitsdokumente, E-Books, Knowledge Base-Artikel (KB), Produktdokumentation und Community-Diskussionen aus einer konsolidierten Ansicht, indem Sie zu **Lernen**navigieren. Der Inhalt ist nach Überschriften und beschreibenden UI-Karten organisiert, damit Sie schnell die richtige Ressource finden können.

Bannerankündigungen zur Sicherheit

Aktivieren Sie Sicherheitsbanner-Ankündigungen, um über dringende und kritische Sicherheitswarnungen informiert zu bleiben, indem Sie Warnbanner verwenden, die für Administratoren in der Instanz-UI sichtbar sind.

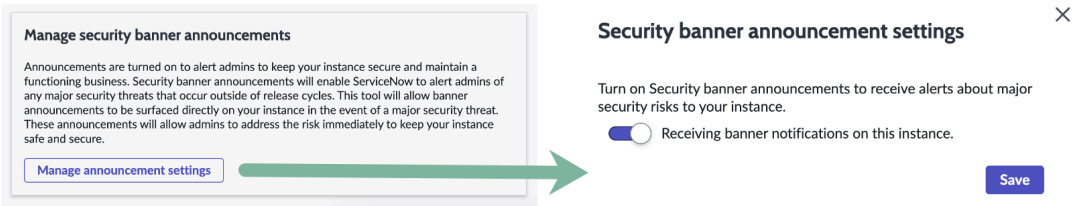


Sicherheitsbannankündigungen sind Ankündigungen, die Kundenadministratoren angezeigt werden und von ServiceNowgesendet werden, um Sie über Korrekturen für potenzielle Sicherheitsbedrohungen zu informieren, die kürzlich erkannt wurden. Diese Warnungen enthalten eine Zusammenfassung des Sicherheitsrisikos und einen Link, über den Sie mehr erfahren und Maßnahmen ergreifen können, um Ihre Instanz zu sichern.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktivieren oder deaktivieren Sie Sicherheitsbannankündigungen

Die Sicherheitsbanner-Funktion ist standardmäßig aktiviert. Um Sicherheitsbannankündigungen zu aktivieren oder zu deaktivieren, navigieren Sie zu **Systemsicherheit** > **Sicherheitscenter** > **Benachrichtigungen**an. Wählen Sie auf dieser Seite die Schaltfläche **Ankündigungseinstellungen verwalten**.



Dashboards zur Sicherheitslage

Überwachen Sie Ihre Sicherheits-KPIs mit den anpassbaren Einzel- und Mehrinstanz-Sicherheitslagen-Dashboards. Diese Dashboards fassen die wichtigen Informationen zur Sicherheit Ihrer Instanzen an einem zentralen Ort zusammen und enthalten eine Reihe von Basissystem-Dashboard-Widgets.

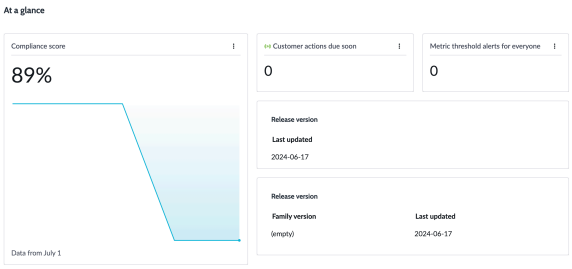
Zugriff auf die Sicherheitslage-Dashboards

Greifen Sie auf das Sicherheitslagen-Dashboard zu, indem Sie zu navigieren **Alle** > **Sicherheitscenter**an. Der Inhalt des Sicherheitslagen-Dashboards befindet sich auf der Registerkarte **Übersicht**.

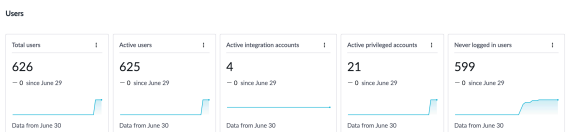
Dashboard-Komponenten

Das Dashboard ist in mehrere Abschnitte unterteilt, die Widgets enthalten, die sich auf einen Aspekt der Instanzsicherheit beziehen. Wählen Sie ein beliebiges Widget im Dashboard aus, um weitere Details zu diesem Aspekt der Sicherheit Ihrer Instanz anzuzeigen.

Der Abschnitt **Auf einen Blick** zeigt eine Übersicht über die Sicherheit in einer Instanz, z. B. eine Compliance-Bewertung, fällige Kundenaktionen sowie Update- und Release-Informationen für die Instanz.

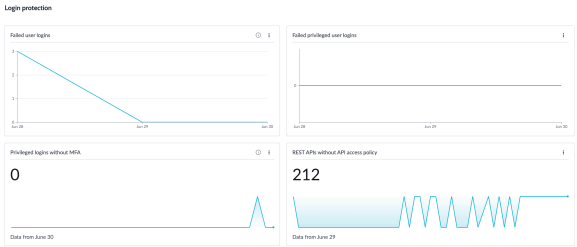


Der Abschnitt „ **Benutzer** “ enthält Informationen zu den Benutzern in Ihrer Instanz. Die Widgets in diesem Abschnitt zeigen Anwenderinformationen und ein Liniendiagramm, das die Änderungen an diesen Informationen im Laufe der Zeit zeigt. Wählen Sie ein Widget aus, um weitere Details anzuzeigen

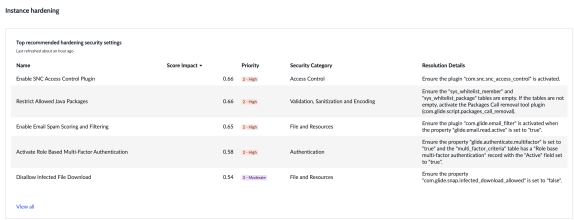


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

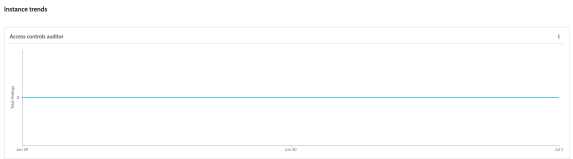
Der Abschnitt „Anmeldeschutz“ enthält Informationen zu fehlgeschlagenen Anmeldungen, einschließlich fehlgeschlagener **Anmeldeversuche** privilegierter Benutzer.



Der Abschnitt „Härtung der **Instanz** “ enthält empfohlene Sicherheitseinstellungen für die Härtung, die Sie ändern können, um die Instanzsicherheit zu verbessern. Verwenden Sie diesen Abschnitt, um die Priorität und die potenziellen Auswirkungen dieser Changes anzuzeigen.



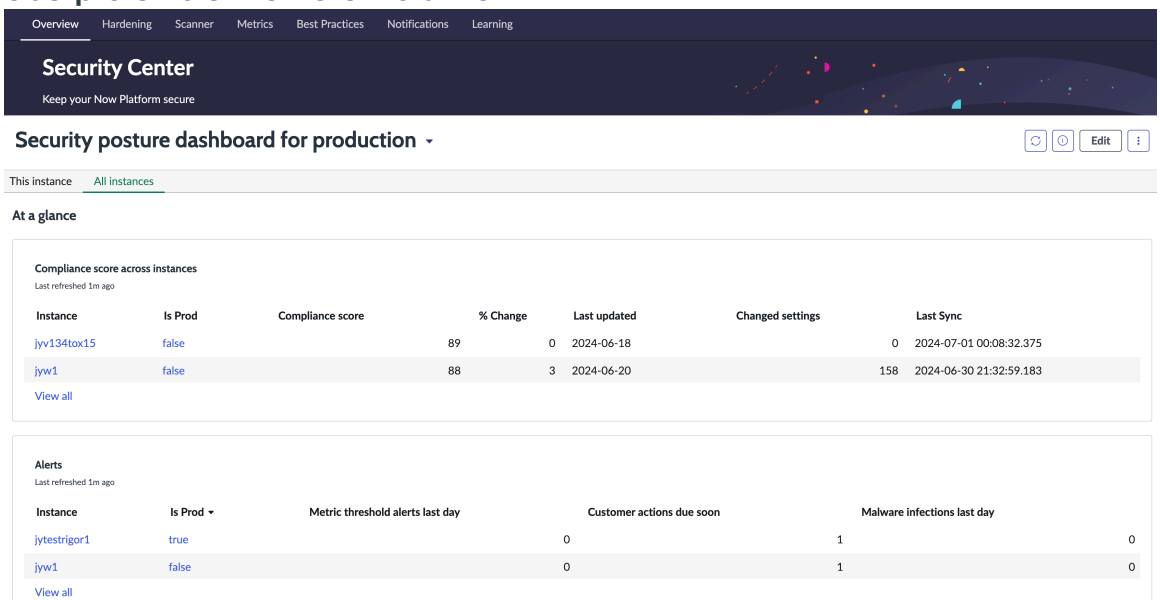
Das Dashboard **Instanztrends** zeigt die Ergebnisse der Audit-Suite für Zugriffssteuerungen an.



Verwenden Sie den Abschnitt „ **Datenschutz** “, um eine Übersicht über klassifizierte Daten anzuzeigen, z. B. personenbezogene Daten. Das Dashboard verfolgt auch Exporte von klassifizierten Daten.



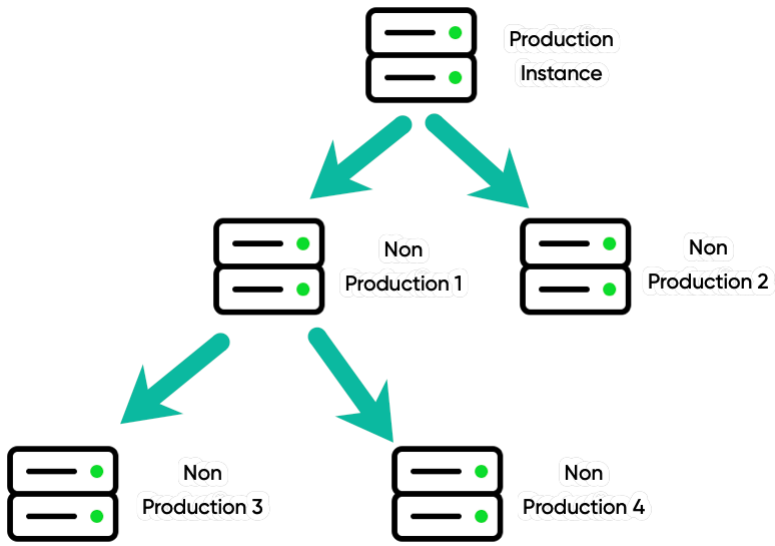
Überprüfen Sie mehrere Instanzen



Zeigen Sie die Sicherheitslage Ihrer Instanzen außerhalb der Produktion an, ohne Ihre Produktionsinstanz zu verlassen, indem Sie die Registerkarte **Alle Instanzen** oben im Dashboard verwenden. Auf der Registerkarte **Alle Instanzen** wird eine komprimierte Version der gleichen Informationen angezeigt wie auf der Registerkarte **Diese Instanz**, zusätzlich werden Daten aus allen Instanzen außerhalb der Produktion angezeigt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardmäßig werden auf der Registerkarte **Alle Instanzen** Informationen zur Produktionsinstanz, zu allen aus der Produktion geklonten Instanzen und zu allen aus den geklonten Instanzen geklonten Instanzen angezeigt. In diesem Beispiel werden zwei Instanzen aus der Produktion geklont, und von einem dieser Klone werden zwei zusätzliche Instanzen geklont. Alle fünf Instanzen werden auf der Registerkarte **Alle Instanzen** angezeigt.



Dashboard-Anpassung

Das Sicherheitsstatus-Dashboard der Instanz kann nicht angepasst werden. Sie können das Dashboard jedoch duplizieren, indem Sie das Symbol **Weitere Aktionen** (⋮) wählen und **Duplizieren**auswählen. Sie können das duplizierte Dashboard ändern.

Benachrichtigungen zu Sicherheitsereignissen

Sie können die standardmäßigen Benachrichtigungsrichtlinien für Sicherheitsereignisse in Ihrer ServiceNow-Instanz anzeigen, verwalten und analysieren und auf die Funktionen zugreifen, um neue anwenderdefinierte Richtlinien zu erstellen.

Sie können ganz einfach Benachrichtigungsrichtlinien anpassen und erstellen, die E-Mail-Benachrichtigungen auslösen, wenn Anwender in der Now Platform Aktionen ausführen, die möglicherweise unsicher sind oder die Überwachung durch einen Administrator erfordern.

Benachrichtigungen über Sicherheits-Ereignisse bestehen aus zwei Teilen: Sicherheitsrichtlinienkonfiguration und Benachrichtigungskonfiguration. Über die Richtlinienkonfiguration können Sie eine Kombination aus Ereignissen und Aktionen angeben, die Benachrichtigungen auslöst. In der Benachrichtigungskonfiguration können Sie die E-Mail-Empfänger und das E-Mail-Format für die E-Mails angeben.

Administratoren können die Werte für die Standardrichtlinien anpassen, Standardrichtlinien klonen und bearbeiten oder eigene anwenderdefinierte Richtlinien erstellen.

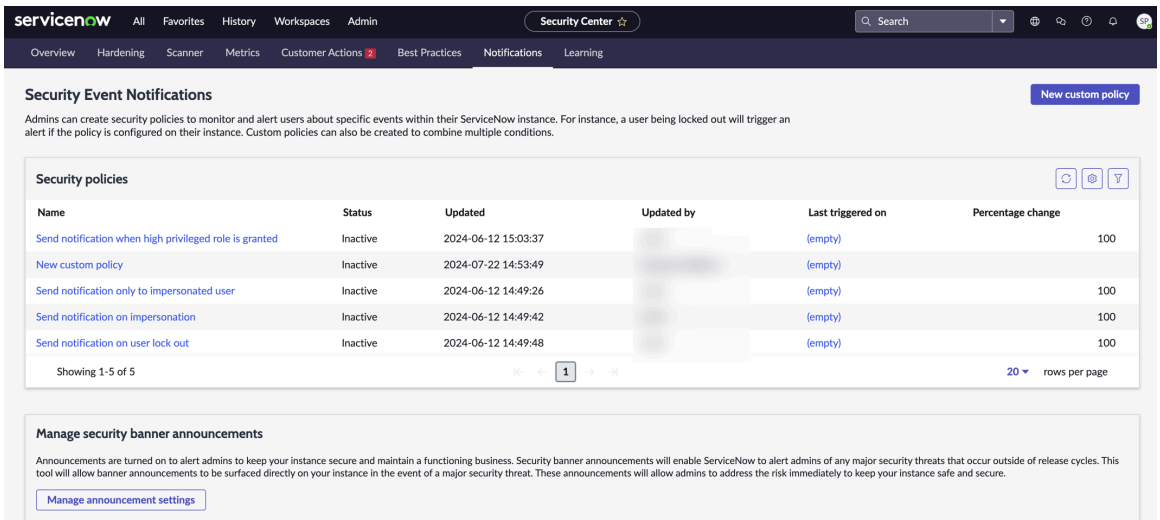
Sicherheitsereignis-Benachrichtigungen – Übersicht

In der Übersicht Security Event Notifications (Benachrichtigungen zu Sicherheitsereignis) sehen Sie eine Tabelle, die alle verfügbaren Sicherheitsrichtlinien für Ihre Instanz organisiert.

Diese Tabelle enthält Spalten, die den Richtliniennamen, den Status (aktiv oder inaktiv), das Datum und die Uhrzeit der letzten Aktualisierung, den aktualisierenden Anwender, das Datum und die Uhrzeit des letzten Auslösers und die prozentuale Änderung oder die

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

wöchentliche Änderungsrate anzeigen Auslöser berechnet als Prozentsatz. Wenn diese Richtlinie beispielsweise durchschnittlich 5 Benachrichtigungen pro Woche auslöst und letzte Woche 10 Mal ausgelöst wurde, entspricht dies einer prozentualen Erhöhung um 100 %.



Darüber hinaus können Sie die Schaltfläche **Neue anwenderdefinierte Richtlinie** wählen, um eine neue anwenderdefinierte Richtlinie zu erstellen, die auf die Anwendungsfälle Ihrer Organisation zugeschnitten ist.

Übersichtsseite über Security Ereignis-Benachrichtigungen

Navigieren Sie zur Homepage Security Event Notifications (Sicherheitsereignis-Benachrichtigungen), und wählen Sie dann eine der Richtlinien aus, die Sie überprüfen oder anpassen möchten. Die Registerkarte „Übersicht“ bietet einen schnellen Überblick über die Richtlinie. Um die Richtlinie anzupassen, wählen Sie die Registerkarte **Richtlinieneinstellungen**.

Für Standardrichtlinien können Sie den Auslöser oder die Bedingungslogik nicht ändern. Wenn Sie solche Änderungen vornehmen möchten, müssen Sie die Richtlinie zuerst duplizieren, indem Sie oben rechts auf der Seite auf die Schaltfläche Duplizieren klicken.

Hinweis: Um die Schaltfläche „Duplizieren“ anzuzeigen, müssen Sie das Kebab-Menüsymbol (Menü mit drei Punkten) rechts neben der Schaltfläche „Aktualisieren“ oben rechts auswählen.

Denken Sie daran, die Schaltfläche Aktualisieren zu wählen, wenn Sie mit den Änderungen fertig sind. Und denken Sie daran, die Richtlinie zu deaktivieren, bis Sie bereit sind, Benachrichtigungen auszulösen. Sie können die Richtlinie mit der Schaltfläche oben rechts neben der Schaltfläche Aktualisieren aktivieren und deaktivieren.

Greifen Sie auf einen Snapshot der Richtlinien für Benachrichtigungen über Sicherheitsereignisse in Ihrer Instanz zu, in der Daten in UI-Karten organisiert sind. Analysieren Sie Details und Aktivitätsabschnitte, und verwenden Sie die Funktionen, um Sicherheitsrichtlinien zusätzliche Informationen hinzuzufügen, z. B. durch Kommentare.

Übersichtstabellenfelder und -funktionen

Bezeichnung	Beschreibung
Name	Der Name der Richtlinie für Benachrichtigungen über Sicherheitsereignisse.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übersichtstabellenfelder und -funktionen (Fortsetzung)

Bezeichnung	Beschreibung
Status	Der Status einer Richtlinie kann entweder „Aktiv“ oder „Inaktiv“ sein.
Aktualisiert	Datum und Uhrzeit der letzten Aktualisierung der Richtlinie.
Aktualisiert von	Der Anwender, der eine Richtlinie aktualisiert hat.
Zuletzt ausgelöst am	Datum und Uhrzeit der letzten Ausführung der Richtlinie.
Ausgelöst-Anzahl letzte Woche	Die Anzahl der Auslöser, die eine Richtlinie in den letzten 7 Tagen generiert hat.
Change in Prozent	Die Änderungsrate für wöchentliche Auslöser, berechnet als Prozentsatz.

Erstellen Sie anwenderdefinierte Richtlinien für Benachrichtigungen über Sicherheitsereignisse

Erfahren Sie, wie Sie anwenderdefinierte Benachrichtigungen über Sicherheitsereignisse erstellen, die speziell auf die Anforderungen Ihrer Organisation zugeschnitten sind. Auf diese Weise können Sie Aktionen von Benutzern und Gruppen in Ihrer Instanz überwachen und Benachrichtigungen für potenzielle Sicherheitsrisiken generieren.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren Sie zur Security Center-App, und wählen Sie **Benachrichtigungen**an.
2. Wählen Sie **Neue anwenderdefinierte Richtlinie aus**.
3. Wählen Sie einen der drei Ereignistypen aus, der den Start der Richtlinie auslöst, und wählen **Sie Erstellen**aus.
4. Konfigurieren Sie die Richtlinie.
   Unter Konfigurieren Sie Voreinstellungen für Benachrichtigungsrichtlinien für Sicherheits-Ereignisse erfahren Sie, wie Sie Ihre neue anwenderdefinierte Richtlinie für Benachrichtigungen über Sicherheitsereignisse konfigurieren.

Ändern Sie Richtlinien für Benachrichtigungen über Sicherheits-Ereignisse

Erfahren Sie, wie Sie die Einstellungen Ihrer Richtlinien für Benachrichtigungen zu Sicherheitsereignissen ändern.

Vorbereitungen

Erforderliche Rolle: admin

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie zur Homepage Security Event **Notification** (Benachrichtigung über Sicherheitsereignis), und wählen Sie die Richtlinien aus, die Sie ändern möchten.

   Hinweis: Sie können die Auslöser- oder Bedingungslogik für Standardrichtlinien nicht ändern. Um diese Einstellungen zu ändern, müssen Sie die Richtlinie zuerst duplizieren. Wählen Sie dazu den Abwärtspfeil neben **Aktualisieren**und dann **Duplizieren**aus.

2. Wählen Sie **Richtlinieneinstellungen aus, um die Einstellungen** zu ändern.
3. Wählen Sie **Aktualisieren** aus, um Ihre Änderungen zu speichern.
4. Wahlweise: Wählen Sie „ **Deaktivieren** “, bis Sie bereit sind, mit der Auslösung von Benachrichtigungen zu beginnen.
5. Wahlweise: Beginnen Sie mit der Auslösung von Benachrichtigungen, indem Sie **Aktivieren**wählen.
   Unter Konfigurieren Sie Voreinstellungen für Benachrichtigungsrichtlinien für Sicherheits-Ereignisse erfahren Sie, wie Sie Ihre neue anwenderdefinierte Richtlinie für Benachrichtigungen über Sicherheitsereignisse konfigurieren.

Konfigurieren Sie Voreinstellungen für Benachrichtigungsrichtlinien für Sicherheits-Ereignisse

Erfahren Sie, wie Sie in Security Center Benachrichtigungsrichtlinien für Sicherheitsereignisse an die spezifischen Anforderungen Ihrer Organisation anpassen können.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Auf der Seite **Richtlinieneinstellungen können** Sie die Einstellungen für eine Richtlinie für Benachrichtigungen über Sicherheitsereignisse anpassen. Hier können Sie Optionen anpassen, die sich darauf beziehen, wann die Richtlinie ausgeführt wird, die bedingte Logik und die gesendeten Benachrichtigungen.

Prozedur

1. Wählen Sie in Security Center **Benachrichtigungen**aus.
2. Wählen Sie in der Tabelle „Sicherheitsrichtlinien“ eine Benachrichtigungsrichtlinie für Sicherheitsereignisse aus, die Sie konfigurieren möchten.
   Beispiel: **Benachrichtigung senden, wenn eine Rolle mit hohen Berechtigungen gewährt wird**.
3. Wählen Sie **Richtlinieneinstellungen aus**.
4. Konfigurieren Sie die Richtlinieneinstellungen.

Konfigurationsoptionen für Richtlinieneinstellungen

Bezeichnung	Zu konfigurieren
Zeitpunkt für Ausführung	**Auslöser**: Das Ereignis, das die Richtlinie startet.
Bedingungen	Bedingungslogik und Bedingungen, die auf Ihre Richtlinien angewendet werden sollen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bezeichnung	Zu konfigurieren
	◦ **Bedingungslogik**: zwei Optionen ▪ **Alle Bedingungen müssen erfüllt sein, um diese Richtlinie auszulösen**: Alle Bedingungen müssen gültig sein, damit die Richtlinie Benachrichtigungen senden kann. ▪ **Zum Auslösen dieser Richtlinie müssen beliebige Bedingungen erfüllt sein**: Benachrichtigungen werden gesendet, wenn eine der Bedingungen gültig ist. ◦ **Bedingung hinzufügen**: Wählen Sie „Bedingung hinzufügen“ aus, und geben Sie die entsprechenden Werte an. Sie können eine Bedingung entfernen, indem **Sie Bedingung entfernen**auswählen.
Benachrichtigungen	Der E-Mail-Text und die E-Mail-Empfänger: ◦ **Benachrichtigung**: Wählen Sie eine der vordefinierten Benachrichtigungsvorlagen aus. Weitere Informationen finden Sie unter Erstellen Sie eine anwenderdefinierte E-Mail für Benachrichtigungen über Sicherheitsereignisse. ◦ **Benachrichtigung hinzufügen**: Wählen Sie Benachrichtigung hinzufügen. ◦ **Gruppen**: Wählen Sie die Gruppe aus, die die Benachrichtigung erhalten soll. ◦ **Anwender**: Wählen Sie die Anwender aus, die die Benachrichtigung erhalten sollen. Sie können eine Benachrichtigung entfernen, indem **Sie Benachrichtigung entfernen**auswählen.

Hinweis: Wenn Sie eine Richtlinie deaktivieren möchten, wählen Sie **Deaktivieren**aus. Wenn Sie eine Richtlinie replizieren möchten, wählen Sie den Abwärtspfeil neben der Schaltfläche **Aktualisieren** (

).

5. Wählen Sie **Aktualisieren** aus, um Ihre Einstellungen zu speichern.

Erstellen Sie eine anwenderdefinierte E-Mail für Benachrichtigungen über Sicherheitsereignisse

Erfahren Sie, wie Sie eine anwenderdefinierte E-Mail für Benachrichtigungen über Sicherheitsereignisse erstellen, indem Sie neue Benachrichtigungen konfigurieren, Auslöser festlegen, Empfänger definieren und E-Mail-Inhalte mit dynamischen Ereignisfeldern erstellen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Auswahlvorgang **-Systembenachrichtigungen** > **Benachrichtigung**an.
2. Wählen Sie **neu**aus.
3. Geben Sie einen **Namen** für das Benachrichtigungsfeld ein.
4. Wählen Sie das Feld neben der **Tabelle** aus, und geben Sie die Sicherheitsrichtlinienbenachrichtigung (*sn_vsc_security_policy*) ein.
5. Konfigurieren Sie den neuen Datensatz.
   Es gibt drei Registerkarten im -Datensatz, die konfiguriert werden müssen: Zeitpunkt **zum Senden**, **Empfänger der Nachricht**und **Was wird enthalten?**

Registerkarte	Beschreibung
Absendezeitpunkt	Wählen Sie das Feld neben **Senden wenn** Bezeichnung und dann **Ausgelöst**aus.
Empfänger	◦ Wählen Sie das lokale Symbol neben **Anwender/Gruppen in Feldern**und anschließend **Anwender** und **Gruppen**aus. Wählen Sie das Symbol **Element hinzufügen** (>), um die Felder in das Textfeld **Ausgewählt** zu verschieben. ◦ Klicken Sie mit der rechten Maustaste auf das Header-Banner des Datensatzes, und wählen **Sie Speichern**.)

Darin enthalten	Erstellen Sie eine E-Mail-Vorlage.
	
	Weitere Informationen finden Sie unter Erstellen einer E-Mail-Vorlage .
	
	Geben Sie Felder des Ereignisses in **Nachrichten-HTML ein**. Dies kann mithilfe von `${event_id.FIELD_NAME}`erfolgen. Hier ist ein Beispiel:
	`Role: ${event_id.role.URI_REF}`
	`Granted to:`
	`${event_id.granted_to.URI_REF}`
	`Granted by:`
	`${event_id.user.URI_REF}`
	`Logged at:`
	`${event_id.sys_created_on}`
	`Security Center Notification:`
	`${execution.policy.name}`

6. Wählen Sie **Absenden**.
7. Fügen Sie der E-Mail-Vorlage in Benachrichtigungen zu Sicherheitsereignissen eine anwenderdefinierte Benachrichtigung hinzu.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie in Security Center **Benachrichtigungen** > **Richtlinieneinstellungen**an.

b. Navigieren Sie zur Bezeichnung **Benachrichtigungen**.

c. Geben Sie im Feld **Benachrichtigung** den Namen der anwenderdefinierten Benachrichtigung ein, die Sie erstellt haben.

Verlauf von Security Event-Benachrichtigungen

Erkunden Sie den vollständigen Verlauf der Benachrichtigungen zu Sicherheitsereignissen in Ihrer Instanz.

Die Seite „ **Benachrichtigungen** “ bietet eine Übersicht über den Benachrichtigungsverlauf für alle Benachrichtigungsrichtlinien für Sicherheitsereignisse in Ihrer Instanz. Sie können die Daten in Diagrammen anzeigen, grafisch darstellen und Performance Analytics-Funktionen wie Ziele, Schwellenwerte und KPI-Signale anwenden. Alternativ können Sie die Daten in einem Tabellenformat anzeigen und so Standardfunktionen wie Suchen, Sortieren, Filtern und Abfragen verwenden.

Instanz-Sicherheitszentrum

Über das Instanz-Sicherheitszentrum können Sie die Compliance-Stufe von Instanzsicherheitskontrollen überwachen, Überwachungsmetriken für Sicherheits-Ereignisse anzeigen und die Sicherheitseinstellungen für Instanzen konfigurieren und verwalten. Das Instanz-Sicherheitszentrum fasst mehrere wichtige Sicherheitskomponenten in einer zentralen Steuerungskonsole zusammen, mit der Sie instanzbasierte Sicherheitsereignisse erkennen, schützen und darauf reagieren können.

Übersicht über das Instanz-Sicherheitszentrum

Wichtig:

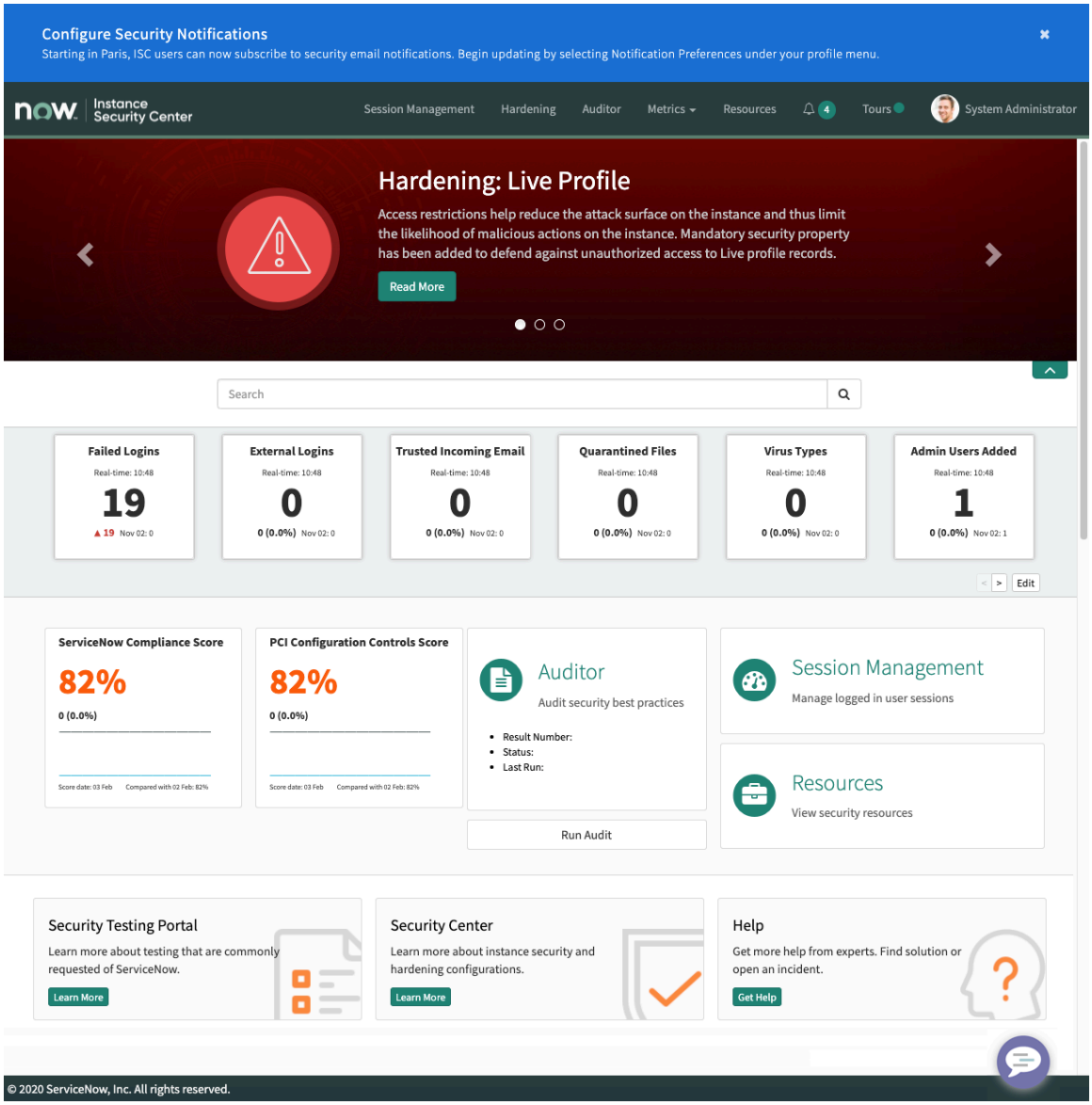
Das Instanz-Sicherheitszentrum (ISC) hat seit September 2024 das Ende des Verkaufs erreicht und wird nicht mehr unterstützt und ist nicht mehr für eine erneute Aktivierung verfügbar.

ServiceNow Security Center (SSC) ist die empfohlene Lösung für die Zukunft. Weitere Informationen finden Sie unter Migration des Instanz-Sicherheitszentrums zu ServiceNow Security Center ..

Komponenten des Instanz-Sicherheitszentrums

Um auf das Instanz-Sicherheitszentrum zuzugreifen, navigieren Sie zu **Systemsicherheit** > **Instanz-Sicherheitszentrum** oder die Homepage für Systemadministration.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die Homepage des Instanz-Sicherheitszentrums enthält die folgenden Sicherheitskomponenten:

- Administratornachrichten
- Rotierendes Sicherheitsbanner
- Suchen
- Sicherheitsereignis-Menüband
- Tägliche Compliance-Punktzahl
- Punktzahl der PCI-Konfigurationssteuerungen
- Management von Anwendersitzungen
- Härtung
- Auditor
- Metriken (Benutzer, E-Mail und Virenschutz)
- Ressourcen
- Sicherheitsbenachrichtigungen
- Touren

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Portal für Sicherheitstests
- Security Center
- Hilfe
- Virtual Agent-Zugriff

Auf der Homepage des Instanz-Sicherheitszentrums können Sie die Punktzahl für Sicherheits-Compliance für Ihre Instanz anzeigen und den allgemeinen Sicherheitszustand überwachen. Anschließend können Sie Systemeigenschaften, die sich auf die Sicherheit Ihrer Instanz beziehen, so konfigurieren oder aktualisieren, dass sie den Sicherheitsanforderungen entsprechen.

Hinweis: Das Instanz-Sicherheitszentrum unterstützt keine Domänentrennung.

Anwenderrollen

Zur Verwendung des Instanz-Sicherheitszentrums benötigen Sie die Rolle admin oder security_dashboard_user.

Weitere Informationen zum Verwalten von Abonnements pro Benutzer finden Sie unter Verwalten von Abonnements pro Benutzer in Abonnement-Management , und wenden Sie sich an Ihren -Kundenbetreuer.

Rollen

Erforderliche Rolle	Anwender	Vorteile
Administrator	Diese Rolle hat Zugriff auf alle Features, Funktionen und Daten des Systems, da Administratoren Regeln für Zugriffssteuerungslisten (Access Control List, ACL) überschreiben und alle Rollenprüfungen übergeben können. Vermeiden Sie es, Ihren Anwendern diese Rolle zuzuweisen, wenn gezieltere Rollen verfügbar sind.	Nutzen Sie die Tools Security Center, um den Sicherheitsstatus von Instanzen zu verbessern und sicherheitsbezogenes Verhalten zu überwachen.
sn_vsc.security_center_viewer	Mit dieser Rolle können Anwender, die keine Administratoren sind, die Informationen in Security Center anzeigen, aber keine Änderungen an den Security Center -Tools vornehmen oder Instanzkonfigurationen mit den Security Center -Tools ändern. Beispielsweise möchten oder müssen Plattformbesitzer, Security Operations-Analysten oder Compliance-Stakeholder möglicherweise	Verschaffen Sie sich Einblick in die Tools Security Center, um den Sicherheitsstatus und das Sicherheitsverhalten von Instanzen zu überwachen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollen (Fortsetzung)

Erforderliche Rolle	Anwender	Vorteile
	einige der in Security Centerverfügbaren Sicherheits-KPIs, Sicherheitseinblicke und Sicherheits-Lernmaterialien anzeigen.	

Warnung: Passen Sie dieses Modul nicht an, um sicherzustellen, dass das Instanz-Sicherheitszentrum bei jedem Upgrade aktuelle Sicherheitsinformationen erhält. Wenn Sie Sicherheitseinstellungen in Ihrer Instanz ändern, testen Sie sie zuerst in einer Umgebung außerhalb der Produktion.

Administratornachrichten

Nachrichten und Erinnerungen, die hauptsächlich für Administratoren gedacht sind, werden über dem rotierenden Sicherheitsbanner angezeigt.

Beispielsweise wird die Meldung `Sicherheitsbenachrichtigungen` konfigurieren angezeigt, um Administratoren daran zu erinnern, Einstellungen für Sicherheitsbenachrichtigungen zu konfigurieren, wenn sie dies noch nicht getan haben. Außerdem wird auf die dafür vorgesehene Seite verwiesen.

Hinweis: Das Banner für Administratornachrichten wird für Nicht-Administratoren oder wenn es keine umsetzbaren Elemente für Administratorbenutzer gibt, nicht angezeigt.

Rotierendes Sicherheitsbanner

Um Sie bei der Überwachung der Sicherheitsintegrität Ihrer Instanz zu unterstützen, werden im rotierenden Banner kritische Nachrichten zur Instanzsicherheit angezeigt.

- Normalerweise wechseln sich zwei bis drei Sicherheitsnachrichten in regelmäßigen Abständen ab.
- Die Punkte am unteren Rand des Banners zeigen die Gesamtzahl der aktuellen Sicherheitsnachrichten an.
- Um darin zu navigieren, wählen Sie die Punkte oder die Pfeile, die auf beiden Seiten der Nachrichten angezeigt werden.

Die Hintergrundfarben des Banners geben den relativen Schweregrad der Nachrichten an.

Farbe	Beschreibung
Rot	Kritische Sicherheitssituation, die eine rechtzeitige Reaktion oder eine Empfehlung zum Schutz vor oder zur Reaktion auf kritische Sicherheitsereignisse erfordert.
Dunkelgrau	Nicht kritische Warnmeldung.
Blau	Allgemeine Informationsnachricht.

Um den Textinhalt im Banner zu reduzieren oder zu minimieren, wählen Sie Banner reduzieren . Um den Textinhalt zu maximieren, wählen Sie ihn erneut aus.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn Sie das Instanz-Sicherheitszentrum erneut verwenden, wird der Textinhalt reduziert oder erweitert angezeigt, je nachdem, wie Sie ihn in der vorherigen Sitzung verwendet haben.
- Wenn sich der Textinhalt selbst ändert, wird er für alle Anwender als maximiert angezeigt.

Suchen

Verwenden Sie die Suchleiste, um das gesamte Instanz-Sicherheitszentrum nach Sicherheitsressourcen zu durchsuchen, die Sie beim Verständnis und der Lösung von Sicherheitsproblemen unterstützen. Sie können die folgenden sicherheitsbezogenen Ressourcen durchsuchen:

- Now Support Knowledge Base Artikel
- Seiten des Instanz-Sicherheitszentrums
- Externe Now Support Links
- PA-Sicherheits-Widgets, z. B. Tägliche Compliance-Punktzahl und Externe eingehende E-Mails
- Banner-Inhalt

Ereignismenüband

Verwenden Sie das Ereignis-Menüband, um wichtige Überwachungsmetriken für Sicherheits-Ereignisse für die aktuelle Instanz anzuzeigen.

- Um manuell durch die Metriken zu scrollen, wählen Sie die Pfeiltasten nach rechts oder nach links.
- Um das Ereignismenüband zu konfigurieren, wählen Sie **Bearbeiten**aus.

Weitere Informationen zum Ereignismenüband und zu seiner Konfiguration finden Sie unter Sicherheitsereignisse überwachen und Konfigurieren Sie das Sicherheitsereignis-Menüband.

Tägliche Compliance-Punktzahl

Der Abschnitt „Tägliche Compliance-Punktzahl“ enthält die Kacheln **Tägliche Compliance-Punktzahl**, **Management**von Anwendersitzungen, **Härtung**, **Auditor**und **Ressourcen**.

Sie verwenden die tägliche Compliance-Punktzahl, um zu messen, wie fehlerfrei Ihre Instanz unter Sicherheitsaspekten ist.

Die Tägliche Compliance-Punktzahl ist eine prozentuale Punktzahl. Sie hängt davon ab, wie konform die aktuellen Einstellungen der Instanzsicherheitseigenschaften mit den im Härtungseinstellungen für die Instanzsicherheitveröffentlichten Compliance-Werten sind.

- Weitere Informationen zur Berechnung der täglichen Compliance-Punktzahl und dazu, wie sich Härtungseinstellungen darauf auswirken, finden Sie unter Überprüfen Sie die tägliche Compliance-Punktzahl, und konfigurieren Sie die Einstellungen für Sicherheitseigenschaften.
- Über die **Schaltfläche Aktualisieren** kann ein Administrator die tägliche Compliance-Punktzahl sofort neu berechnen. Weitere Informationen finden Sie unter Wie tägliche Compliance-Punktzahlen, Trends und Diagrammdaten aktualisiert werden.

Härtung

Verwenden Sie diesen Prozess, um die spezifischen Sicherheitskonfigurationseigenschaften anzupassen, die sich auf die tägliche Compliance-Punktzahl auswirken:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Um auf die Seite „Härtungs-Compliance-Konfigurationen“ zuzugreifen und die Härtung der Instanzsicherheit durchzuführen, wählen Sie die Kachel **Tägliche Compliance-Punktzahl** oder den Link **Härtung**.
2. Geben Sie an, ob alle oder nur die empfohlenen Sicherheitskontrollen angezeigt werden sollen. Wählen Sie dann die Kategorie aus, in der Sie arbeiten möchten.
3. Legen Sie alle Sicherheitskonfigurationseigenschaften in der ausgewählten Kategorie fest. Klicken Sie auf **Weitere** Informationen, um detaillierte Informationen für eine Eigenschaft anzuzeigen.

Weitere Informationen zum Sichern und Optimieren von Sicherheitskonfigurationseigenschaften zur weiteren Verbesserung der Compliance finden Sie unter Passen Sie die Sicherheitseinstellungen der Instanz an, um die Compliance zu erhöhen.

Weitere Informationen zum Aktualisieren von Trend- und Diagrammdaten finden Sie unter Wie tägliche Compliance-Punktzahlen, Trends und Diagrammdaten aktualisiert werden.

Auditor

Führen Sie den Auditor aus, um Ihre Instanz zu scannen und falsche Sicherheitsdefinitionen zu finden. Er liefert Ergebnisse, die Sie korrigieren können, um die Sicherheitslage Ihrer Instanz zu verbessern.

Um auf die Seite „Auditor“ zuzugreifen, wählen Sie die Kachel „ **Auditor** “ oder den Link „ **Auditor** “. Weitere Informationen finden Sie unter Suchen Sie nach falschen Sicherheitsdefinitionen.

Management von Anwendersitzungen

Verwenden Sie das Management von Anwendersitzungen für:

- Zeigen Sie Benutzeranmeldungssitzungen an, und verwalten Sie sie.
- Sehen Sie sich die Benutzeranmeldungssitzung des aktuellen Knotens an, mit dem Sie verbunden sind.
- Zeigen Sie detaillierte Informationen zu jeder Sitzung an, z. B. Anwendername und IP-Adresse.
- Sie können bestimmte Anwendersitzungen, die Sicherheitsrisiken darstellen, isolieren und sperren.

Um auf die Seite „Sitzungsverwaltung“ zuzugreifen, wählen Sie die Kachel **„Sitzungsmanagement“** oder den Link „Sitzungsmanagement“.

Feld	Beschreibung
Anwender	Name des Anwenders, der dieser Anmeldesitzung zugeordnet ist.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	• Um eine bestimmte Benutzersitzung zu finden, wählen Sie das Spotlight-Suchsymbol (), um die Suche nach Anwender, Benutzeragent-Stichwort oder IP-Adresse durchzuführen. Wenn Sie beispielsweise alle aktuellen Anmeldungen über einen bestimmten Browsertyp suchen möchten, geben Sie den Browsernamen als Stichwort in das Feld **Benutzeragent** ein. • Klicken Sie auf einen Anwendernamen, um auf den Anwenderprofildatensatz zuzugreifen. Sie können das Anwenderprofil nur ändern, wenn Ihnen eine Administratorrolle zugewiesen ist. **Hinweis:** Weitere Informationen zu Anwenderprofilen finden Sie unter Anwender erstellen .
MFA	Checkbox, die angibt, ob die Multifaktor-Authentifizierung (MFA) für den angemeldeten Anwender aktiviert ist. Weitere Informationen zu MFA finden Sie unter Multifaktor-Authentifizierung (MFA).
Aktiv	Checkbox, die angibt, ob der angemeldete Anwender aktiv oder inaktiv ist.
Anwenderagent	Browsertyp und Betriebssystem des Geräts für die Benutzeranmeldung.
IP-Adresse	IP-Adresse des angemeldeten Anwenders.
Letzter Zugriff	Datum und Uhrzeit des letzten Zugriffs dieser Anwendersitzung auf die Instanz. **Hinweis:** Um detaillierte Informationen für eine bestimmte Anmeldesitzung anzuzeigen oder die Sitzung selbst zu sperren, wählen Sie die Felder **Anwenderagent**, **IP-Adresse**oder **Letzter Zugriff** aus.

Metriken

Zeigen Sie Details für die folgenden Metriktypen an:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typ der Metrik	Beschreibung
Benutzer	Sicherheitsmetriken, die der Benutzeraktivität in der Instanz zugeordnet sind. Um auf die Seite „Benutzermetriken“ zuzugreifen, wählen Sie den Link **Metriken** und dann **Benutzermetriken aus**.
Exportieren	Sicherheitsmetriken, die aus der Instanz exportierten Daten zugeordnet sind. Um auf die Seite „Exportmetriken“ zuzugreifen, wählen Sie den Link **Metriken** und dann **Exportmetriken aus**.
Authentifizierung	Sicherheitsmetriken, die mit der Authentifizierung verknüpft sind, z. B. selten verwendete IP-Adressen, fehlgeschlagene Anmeldungen und Arten von Authentifizierungsschemata, die von Ihren Benutzern verwendet werden. Um auf die Seite „Exportmetriken“ zuzugreifen, wählen Sie den Link **Metriken** und dann **Authentifizierungsmetriken aus**.
E-Mail	Sicherheitsmetriken, die anomalen Verhaltensweisen im Zusammenhang mit den eingehenden E-Mails an Ihre Instanz zugeordnet sind. Um auf die Seite „E-Mail-Metriken“ zuzugreifen, wählen Sie den Link **Metriken** und dann E- **Mail-Metriken**aus.
Virenschutz	Sicherheitsmetriken, die der Antivirus-Ereignisaktivität in der Instanz zugeordnet sind. Um auf die Seite „Antivirus-Metriken“ zuzugreifen, wählen Sie die **Antivirus** -Kachel, oder wählen Sie den Link **Metriken**, und wählen Sie dann **Antivirus**aus.

Hinweis: Weitere Informationen zum Überwachen der einzelnen Metriktypen finden Sie unter Überwachen Sie Instanzmetriken.

Ressourcen

Greifen Sie auf Artikel, Ressourcen und Blogs von Now Support Knowledge Base zu, die sich auf die Instanzsicherheit beziehen. Diese Ressourcen umfassen Sicherheitseinstellungen, Codierung, Compliance, Korrekturen und verwandte Themen. So greifen Sie auf die Seite „Ressourcen“ zu:

1. Klicken Sie auf die Kachel **Ressourcen** oder den Link Ressourcen.
2. Wählen Sie auf der Seite „Ressourcen“ eine Kategorie aus:

Kategorie	Beschreibung
Empfohlene Richtlinien	Greifen Sie auf empfohlene Sicherheitsrichtlinien zu, einschließlich der Artikel Härtungseinstellungen für die Instanzsicherheit und Leitfaden für sichere Codierung [KB0623354].

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kategorie	Beschreibung
Sicherheitsressourcen	Zugriff auf sicherheitsbezogene Ressourcen in Knowledge Base, einschließlich: ◦ Sicherheitstest der Kundeninstanz ◦ KB-Artikel zum Cloud-Sicherheits-, Trust- und Compliance-Center

Sicherheitsbenachrichtigungen

Im Instanz-Sicherheitszentrum wird ein Benachrichtigungs-Glockensymbol () mit einer Gesamtanzahl ungelesener Sicherheitsbenachrichtigungen angezeigt. Benachrichtigungen bleiben bestehen und werden in dieser Anzahl berücksichtigt, bis Sie sie als gelesen markieren.

1. Klicken Sie auf das Glockensymbol, um die ersten fünf ungelesenen Sicherheitsbenachrichtigungen anzuzeigen.

   Es wird eine Benachrichtigung angezeigt, wenn in Ihrer Instanz die Ereignisse **Administratoranmeldung**, **Administrator entsperrt**, **Fehlgeschlagene**Anmeldung, **Rolle mit hohen Berechtigungen**, **Identitätswechsel**, **Erhöhung der Sicherheit**und **Wöchentliche Zusammenfassung** stattfinden. Weitere Informationen zu diesen Sicherheitsereignissen finden Sie unter Sicherheitsereignisse überwachen.

2. Um detaillierte Informationen für ein bestimmtes Sicherheitsereignis anzuzeigen, wählen Sie die Benachrichtigung aus.

   Wenn Sie beispielsweise eine Benachrichtigung für eine Rolle mit hohen Berechtigungen auswählen, können Sie die Tabelle „Rollen“ (sys_user_role) anzeigen. Verwenden Sie diese Tabelle, um zu sehen, welchen Anwendern während des Kalendertags privilegierte Rollen zugewiesen wurden. Anhand dieses Verlaufs können Sie feststellen, ob die Rollen ordnungsgemäß zugewiesen wurden.

3. Wenn mehr als fünf ungelesene Benachrichtigungen vorhanden sind, wählen Sie **Alle Benachrichtigungen** anzeigen aus, um auf die Seite Alle Benachrichtigungen mit einer Liste aller ungelesenen Benachrichtigungen zuzugreifen.
   - Um detaillierte Informationen für ein bestimmtes Sicherheitsereignis anzuzeigen, wählen Sie die Benachrichtigung aus.
   - Um alle aufgelisteten Benachrichtigungen als gelesen zu markieren, wählen Sie **Alle als gelesen**markieren aus.

Hinweis: Als Administrator können Sie auch Voreinstellungen für das Senden bestimmter Arten von Benachrichtigungen für jeden Typ von Sicherheitsereignis konfigurieren. Weitere Informationen finden Sie unter Legen Sie Voreinstellungen für Benachrichtigungen über Sicherheits-Ereignisse fest.

Touren

Klicken Sie auf den Link **Touren**, um eine geführte visuelle Tour durch das Instanz-Sicherheitszentrum anzuzeigen.

- Die geführte Tour umfasst nur die Sicherheitsüberwachungsfunktionen, die auf der Homepage aufgeführt sind.
- Sie enthält nicht die Sicherheitsfunktionen, auf die Sie zugreifen, wenn Sie die Kacheln oder Links auf der Homepage auswählen.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Portal für Sicherheitstests, Sicherheitscenter und Hilfe

Now Support Serviceportal ist eine zentrale Ressource, mit der Sie Instanzen, Aufgaben und Accounts verwalten. Sie können auch auf nützliche Ressourcen zugreifen, mit denen Sie Sicherheitsprobleme und technische Probleme in Ihrer Instanz diagnostizieren und beheben können.

Um auf diese Ressourcen zuzugreifen, wählen Sie auf den folgenden Kacheln **Weitere Informationen** oder **Hilfe** erhalten:

Kachel	Beschreibung
Portal für Sicherheitstests	Zugriff auf das Sicherheits-Dashboard im Now Support Sicherheitstestportal.
Sicherheitscenter	Zugriff auf Security Compliance im Sicherheitsportal Now Support.
Hilfe	Zugriff auf die folgenden Hilferessourcen im Sicherheitsportal Now Support : • Fragen Sie einen Experten, um Antworten auf häufige Fragen zu erhalten. • Melden Sie dem globalen technischen Support von ServiceNow ein Problem oder einen Ausfall, indem Sie einen Fall öffnen. • Selfservice-Supportressourcen, einschließlich: ◦ Videos ◦ Dokumentation ◦ ServiceNow Community ◦ Wissensdatenbank ◦ Known Error-Portal ◦ Sicherheits-RFX-Datenbank • ServiceNow Community Fragen, die für Sie empfohlen werden.

Virtual Agent-Zugriff

Virtual Agent ist eine Plattform für die Bereitstellung von Anwenderunterstützung durch Konversationen innerhalb einer Messaging-Schnittstelle.

Wenn die zugehörigen Plugins installiert sind, können Administratoren auf die Funktionen Virtual Agent und Natural Language Understanding (NLU) zugreifen, indem sie das Virtual Agent-Symbol wählen:



Sie können damit folgende Aufgaben ausführen:

- Stellen Sie sicherheitsbezogene Fragen, und erhalten Sie dann Antworten in einer Schnellzusammenfassung sowie Referenzlinks, um mehr zu erfahren.
- Erhalten Sie Antworten im Zusammenhang mit Prozessen wie:

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Instanz-Sicherheitszentrum
- Platform-Sicherheit
- ServiceNow Sicherheitsrichtlinien
- Vertrauen, Governance und Risiko

- Suchen Sie nach sicherheitsbezogenen Ressourcen, z. B. nach Knowledge Base -Themen im Now Support -Sicherheitsportal.

Hinweis: Weitere Informationen zur Verwendung und Aktivierung von Virtual Agentfinden Sie unter:

- Virtual Agent
- Aktivieren Sie die ISC-Schnittstelle Virtual Agent

Migration des Instanz-Sicherheitszentrums zu ServiceNow Security Center .

Lernen Sie die wichtigsten Unterschiede bei der Migration vom Instance Security Center (ISC) zu ServiceNow Security Center (SSC) kennen.

Wichtig:

Das Instanz-Sicherheitszentrum ist ein Legacy-Produkt, das im September 2024 das Ende des Verkaufs erreicht. ServiceNow Security Center ist die empfohlene Lösung für Kunden, die in Zukunft eingesetzt werden sollen. Weitere Informationen finden Sie im Artikel über den Abkündigungsprozess (KB0867184) in der Now Support Knowledge Base.

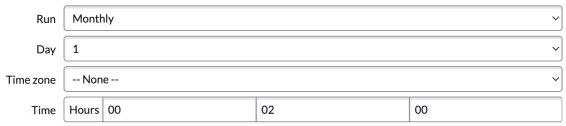
ServiceNow Security Center (SSC) ist eine Sicherheitsanwendung, die aus einer Reihe von speziell entwickelten Tools besteht, die Unternehmen dabei unterstützen sollen, die Sicherheit ihrer ServiceNow -Bereitstellungen aufrechtzuerhalten. Mit SSC können Unternehmen ihren Sicherheitsstatus verbessern und ihre Compliance-Stufen stärken – und das mit einer nahtlosen Anwender-Experience.

Verwenden Sie dieses Dokument, um mehr über die Erweiterungen der SSC-Funktionalität und die Ausführung von Aufgaben in SSC zu erfahren, die zuvor in ISC ausgeführt wurden.

Sicherheitshärtung

Funktionserweiterungen	ISC im Vergleich zu SSC
Aktualisierungen der Benutzerinteraktion	• Überprüfen Sie die neueste Punktzahl, indem Sie zur Übersichts- oder Härtungsvergleichsseite navigieren. • Aktualisieren Sie die neueste Punktzahl manuell, indem Sie zu Übersicht navigieren und Punktzahl aktualisieren auswählen. • Ändern Sie die Konfiguration der Einstellungen, indem Sie auf einer dieser Seiten den Link für einen Einstellungsnamen auswählen, und nehmen Sie dann Änderungen auf der Detailseite für **Einstellungen** vor:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Funktionserweiterungen	ISC im Vergleich zu SSC
	◦ Übersicht ◦ **Härtung** > **Alle Einstellungen** ◦ **Härtung** > **Vergleich**
Legen Sie einen Zeitplan für fest, um Ihre Compliance-Bewertung neu zu berechnen	Mit SSC können Sie festlegen, wann das System eine Aktualisierung Ihrer Compliance-Punktzahl auslöst. **1.** Navigieren Sie zur Tabelle „Geplante Skriptausführungen“ [sysauto_script]. **2.** Suchen und öffnen Sie den Datensatz `SC - Compliance monatlich berechnen`. **3.** Verwenden Sie die Felder **Ausführen**, **Tag**, **Zeitzone**und **Zeit**, um Ihren bevorzugten Zeitplan festzulegen.  **4.** Wählen Sie **Aktualisieren** aus, um Ihre Änderungen zu speichern.

Sicherheits-KPIs und -Metriken

Funktionserweiterungen	ISC im Vergleich zu SSC
Erweiterungen von KPIs	Mit SCC können Sie: • Zeigen Sie den Trend der Punktzahl im Zeitverlauf an. • Überwachen Sie alle KPIs und Metriken über dieselbe Schnittstelle und dieselben Analysefunktionen.
Erweiterungen von Metriken	SCC enthält die folgenden Metrikerweiterungen: • Über 65 Metriken wurden hinzugefügt. • Überwachen und analysieren Sie KPIs und Metriken über eine zentrale Anwenderoberfläche. • Erstellen Sie Ziele und Schwellenwerte für Metriken.
Aktualisierungen der Benutzerinteraktion	Greifen Sie auf Metriken in SSC zu, indem Sie zu navigieren **Übersicht** > **Metriken**, und wählen Sie dann Metrik aus dem Navigationsmenü aus. Alternativ können Sie zu **Alle Metriken**navigieren.

Sicherheitsscanner

Funktionserweiterungen	ISC im Vergleich zu SSC
Neue Funktionalität	SCC enthält diese Funktionen:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Funktionserweiterungen	ISC im Vergleich zu SSC
	• Führen Sie Scans manuell aus, oder planen Sie sie für bestimmte Zeiten. • Erstellen Sie Ihre eigenen Scanprüfungen. • Erstellen Sie Ihre eigene Scan-Suite. • Vergleichen Sie die Ergebnisse von zwei Scans.
Erweiterte E-Mail-Funktionalität	Richten Sie E-Mail-Benachrichtigungen ein, um über Sicherheitsereignisse in Ihrer Instanz informiert zu werden.
Aktualisierungen der Benutzerinteraktion	• Führen Sie die Auditorprüfung aus, indem Sie zu navigieren **Übersicht** > **Scan** > **Suites** und in der Liste **Auditor-Suite** auswählen. • Sehen Sie sich die Scan-Ergebnisse an, indem Sie zu navigieren **Übersicht** > **Scan** > **Ergebnisse**an.

Zusätzliche Sicherheitsfunktionen

Funktionserweiterungen	ISC im Vergleich zu SSC
Überwachen Sie die Sitzungsfunktionalität	• Visualisieren Sie Sitzungsaktivitäten mit Analytics Hub . • Überwachen Sie die Sitzungsaktivität, indem Sie zu navigieren **Metriken** > **Sitzungen**an.
Ressourcen finden	Greifen Sie auf alle Lernressourcen auf einer einzigen Seite unter zu **Übersicht** > **Lernen**an.

Sicherheitsereignisse überwachen

Analysieren Sie die Ereignismetriken in Ihrer Instanz, um potenzielle Sicherheitsereignisse zu erkennen und zu verhindern.

Wichtig:

Das Instanz-Sicherheitszentrum (ISC) hat seit September 2024 das Ende des Verkaufs erreicht und wird nicht mehr unterstützt und ist nicht mehr für eine erneute Aktivierung verfügbar.

ServiceNow Security Center (SSC) ist die empfohlene Lösung für die Zukunft. Weitere Informationen finden Sie unter Migration des Instanz-Sicherheitszentrums zu ServiceNow Security Center ..

Im Ereignis-Menüband auf der Homepage für Instanzsicherheit können Sie diese Metriken und die zugehörigen Details analysieren, um potenzielle Sicherheitsereignisse in der Instanz zu identifizieren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Für jede Ereignismetrik wird in Echtzeit eine einzelne Punktzahl angezeigt, die angibt, wie oft das Ereignis im Laufe des Tages in dieser Instanz aufgetreten ist. Diese Einzel-Punktzahl-Berichte werden automatisch aktualisiert, wenn die entsprechenden Ereignisse stattfinden.
- Jede Ereignismetrik enthält auch Compliance-Trends und Diagramminformationen für einen bestimmten Datumsbereich. Diese Informationen werden täglich aktualisiert, wenn Sie den Performance Analytics-Auftrag ausführen. Weitere Informationen finden Sie im Abschnitt **Ereignis-Trenddetails analysieren**.

Ereignistypen

Sie können mindestens sechs der folgenden Ereignistypen überwachen. Bei mehr als sechs Ereignissen verwenden Sie die Pfeiltasten nach links oder rechts unter dem Ereignismenüband, um durch sie zu scrollen. Informationen zum Konfigurieren des Ereignismenübands finden Sie unter Konfigurieren Sie das Sicherheitsereignis-Menüband.

Benachrichtigungseinstellung	Beschreibung
Administratoranmeldungen	Anzahl der Anmeldeversuche in dieser Instanz während des Kalendertags durch Anwender, denen eine Administratorrolle zugewiesen ist.
Administratoranwender hinzugefügt	Anzahl der Anwender mit einer Administratorrolle, die während des Kalendertags in dieser Instanz hinzugefügt wurden. Angenommen, Ihre Instanz weist möglicherweise ein Sicherheitsproblem auf, wenn die Anzahl 10 beträgt, aber bekanntermaßen 4 Anwender über eine zugewiesene Administratorrolle verfügen.
Externe eingehende E-Mail	Weitere Informationen finden Sie unter E-Mail-Metriken.
Externe Anmeldungen	Anzahl der Anwender mit zugewiesener Rolle „snc_external“, die sich während des Kalendertags bei dieser Instanz angemeldet haben. Diese Anmeldungen erfolgen normalerweise zu Wartungs-, Support-, Beratungs- oder Audit-Zwecken. Durch die Überwachung dieser Metrik können Sie überprüfen, ob die externen Anmeldeversuche legitim sind und keine potenziellen Sicherheitsprobleme darstellen. Weitere Informationen zum Zuweisen externer Anwenderrollen finden Sie unter Explizite Rollen.
Fehlgeschlagene Anmeldungen	Anzahl der Anmeldungen, die in dieser Instanz während des Kalendertags fehlgeschlagen sind. Diese Metrik kann darauf hinweisen, dass versucht wird, sich anzumelden und die Sicherheit Ihrer Instanz zu gefährden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benachrichtigungseinstellung	Beschreibung
Identitätswechsel	Anzahl der Anmeldungen mit Identitätswechsel in dieser Instanz während des Kalendertags. Weitere Informationen dazu, wie Sie die Identität eines Benutzers annehmen, finden Sie unter Identität eines Benutzers annehmen .
Dateien in Quarantäne	Anzahl der Dateien, die unter Quarantäne gestellt wurden, als Sie Antivirus-Scanning in dieser Instanz während des Kalendertags ausgeführt haben. Weitere Informationen zu Dateien in Quarantäne und Antivirus-Scanningfinden Sie unter Antivirus-Metriken und Antivirus-Scanning.
Erhöhungen der Sicherheit	Anzahl der Fälle, in denen ein Sicherheitsadministrator die Sicherheit für Standardbenutzer erhöht hat, indem er die zugewiesene Benutzerrolle während des Kalendertags zu einer Sicherheitsrolle mit hohen Berechtigungen geändert hat. Zu diesen Sicherheitsrollen mit hohen Berechtigungen gehören „oauth_admin“, „admin“, „security_admin“ und „impersonator“. • Diese Metrik gibt an, dass jemand möglicherweise versucht hat, die Sicherheit eines nicht autorisierten Anwenders zu erhöhen. Verwenden Sie diese Metrik nicht allein, um eine bestimmte Sicherheitskompromittierung zu erkennen. Behandeln Sie diese Metrik stattdessen als Hinweis, dass Sie eine andere Metrik überprüfen sollten, um zu sehen, ob eine Sicherheitskompromittierung aufgetreten ist. • Weitere Informationen zum Erhöhen der Benutzersicherheit finden Sie unter Auf eine privilegierte Rolle hochstufen und Rollen mit erhöhten Rechten.
SNC-Anmeldungen	Anzahl von Kundenservice und Support Mitarbeitern, die sich an diesem Kalendertag mithilfe der Hi-Hopping-Technik bei dieser Instanz angemeldet haben. Diese Anmeldungen erfolgen normalerweise zu Wartungs-, Support-, Beratungs- oder Audit-Zwecken. Informationen zur Steuerung des Zugriffs von ServiceNow Unternehmensmitarbeitern

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benachrichtigungseinstellung	Beschreibung
	finden Sie unter ServiceNow-Zugriffssteuerung.
Spam	Weitere Informationen finden Sie unter E-Mail-Metriken.
Vertrauenswürdige eingehende E-Mail	Weitere Informationen finden Sie unter E-Mail-Metriken.
Nicht vertrauenswürdige eingehende E-Mail	Weitere Informationen finden Sie unter E-Mail-Metriken.
Virustypen	Anzahl der verschiedenen Typen von Antivirus-Ereignissen, die in dieser Instanz während des Kalendertags aufgetreten sind. Weitere Informationen zu Antivirus-Ereignistypen finden Sie unter Antivirus-Metriken.

Ereignis-Trenddetails werden analysiert

Klicken Sie zum Anzeigen von Trenddetails für eine Ereignismetrik auf die Ereignisanzahl, um auf die Seite „Analytics Hub“ zuzugreifen. Die Details, die für die Instanz angezeigt werden, hängen vom Typ der Metrik ab.

So zeigen Sie beispielsweise auf der Seite mit den Ereignisprotokollen des Sicherheits-Dashboards eine Liste aller Fehlversuche an:

- Wählen Sie die Metrik **Fehlgeschlagene Anmeldungen** aus.
- Klicken Sie auf der Seite Analytics Hub auf **Datensätze**anzeigen .
- Klicken Sie auf einen der fehlgeschlagenen Anmeldungsversuche.
- Die Details umfassen den Namen des Benutzers, der versucht hat, sich anzumelden, seine IP-Adresse und den Namen der Tabelle, auf die er zugreifen möchte.

Sie können in Analytics Hub Ereignisschwellenwertauslöser einrichten, um Warnungen bereitzustellen, wenn ein bestimmtes Ereignis innerhalb eines bestimmten Punktzahlbereichs für einen Indikator auftritt. Sie können auch Ziele festlegen, um den Unterschied zwischen der gewünschten Punktzahl und der tatsächlichen Punktzahl eines Ereignisse darzustellen.

Sie können beispielsweise einen Schwellenwert von `10` für die Metrik „ **Fehlgeschlagene Anmeldungen** “ festlegen. Wenn an einem Tag zehn oder mehr fehlgeschlagene Anmeldeversuche auftreten, wird eine Warnung an bestimmte Sicherheitsmitarbeiter gesendet. Sie können auch ein ähnliches Ziel festlegen, das eine visuelle Hervorhebung in Analytics Hub bietet, wenn an einem Tag 10 fehlgeschlagene Anmeldungen auftreten.

Die Trenddaten und -diagramme, die in der Kachel des Menübands „Ereignis“ und in Analytics Hub angezeigt werden, werden aktualisiert, nachdem der Performance Analytics-Auftrag um 02:00 Uhr (Ortszeit) ausgeführt wurde. Weitere Informationen finden Sie unter Wie tägliche Compliance-Punktzahlen, Trends und Diagrammdaten aktualisiert werden.

Zugehörige Informationen

Instanz-Sicherheitszentrum

Now Intelligence

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Analytics Hub

Performance Analytics-Zielvorgaben und -Schwellenwerte

Konfigurieren Sie das Sicherheitsereignis-Menüband

Konfigurieren Sie das Sicherheitsereignis-Menüband auf der Homepage des Instanz-Sicherheitszentrums so, dass nur die Ereignisse einbezogen werden, die für die Nachverfolgung der Instanzsicherheit in Ihren Vorgängen relevant sind. Sie können auch die Reihenfolge ändern, in der die Sicherheitsereigniskacheln im Menüband angezeigt werden.

Vorbereitungen

Erforderliche Rolle: security_dashboard_user oder admin

Warum und wann dieser Vorgang ausgeführt wird

Das Menüband für Sicherheitsereignisse wird zunächst mit einem vollständigen Satz standardmäßiger Sicherheitsereignisse gefüllt. Sie können ihn anpassen, indem Sie die Ereignisse entfernen, die für Ihre Organisation nicht relevant sind.

- Wenn Sie beispielsweise vermuten, dass Sicherheitsprobleme auf die Aktionen interner Mitarbeiter zurückzuführen sind, beziehen Sie die Ereignisindikatoren „Administratoranmeldungen“, „Administratoranwender hinzugefügt“ und „Erhöhungen“.
- Diese Indikatoren überwachen, wie oft Benutzer mit Administratorrollen versucht haben, sich anzumelden, und, wenn Administratorbenutzer hinzugefügt wurden, welche Versuche unternommen wurden, die Sicherheitsrollen zu erhöhen.

Hinweis: Weitere Informationen zu den Typen von Sicherheitsereignissen, die im Ereignismenüband angezeigt werden, finden Sie unter Sicherheitsereignisse überwachen.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Instanz-Sicherheitszentrum**an.
2. Klicken Sie im Ereignismenüband auf **Bearbeiten** (< > Edit Bearbeiten des Ereignismenübands).
   Im Formular „Ereignisse bearbeiten“ enthält die Spalte **Ausgewählt** die bereits aufgelisteten Ereignisse.
3. Um dem Ereignismenüband Sicherheitsereignisse hinzuzufügen, verschieben Sie sie aus der Spalte **Verfügbar** in die Spalte **Ausgewählt**.
   Um die Reihenfolge zu ändern, in der die Ereignisse im Menüband angezeigt werden, wählen Sie ein Ereignis aus, und klicken Sie dann auf den Aufwärts- oder Abwärtspfeil, um es an die richtige Position zu verschieben.
   - Platzieren Sie die Ereignisse in der gleichen Reihenfolge, in der sie auf dem Ereignismenüband des Instanz-Sicherheitszentrums angezeigt werden sollen.
   - Die Ereignisse, die Sie oben in der Spalte **Verfügbar** platzieren, werden der Reihe nach angezeigt, beginnend auf der linken Seite des Ereignismenübands des Instanz-Sicherheitszentrums. Die Ereignisse, die unten in der Spalte platziert sind, werden rechts im Ereignismenüband angezeigt.
4. So entfernen Sie Sicherheits-Ereignisse aus dem Ereignis-Menüband:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wählen Sie in der Spalte **Ausgewählt** die Sicherheitsereignisse aus, die Sie aus dem Ereignismenüband entfernen möchten.
- Verschieben Sie sie aus der Spalte **Ausgewählt** in die Spalte **Verfügbar**.

5. Klicken Sie auf **Speichern**.

Zugehörige Informationen

Instanz-Sicherheitszentrum

Legen Sie Voreinstellungen für Benachrichtigungen über Sicherheits-Ereignisse fest

Konfigurieren Sie Voreinstellungen für die Arten von Benachrichtigungen, die Sie bei Vorkommen bestimmter Sicherheits-Ereignisse erhalten möchten. Für jeden Typ geben Sie an, ob Sie Benachrichtigungen per E-Mail, per Push-Benachrichtigung in Now Mobileoder in Messaging-Anwendungen von Drittparteien wie Slack oder Microsoft Teamserhalten möchten.

Vorbereitungen

Damit Messaging-Anwendungen von Drittanbietern Benachrichtigungen über Sicherheitsereignisse senden können, müssen Sie das Plugin „Messaging Notification“ (com.glide.notification.messaging) aktivieren. Einzelne Benutzer müssen ihre eigenen Einstellungen konfigurieren. Einzelheiten hierzu finden Sie unter Benachrichtigungen in Messaging-Anwendungen .

Erforderliche Rolle: admin.

Prozedur

1. Klicken Sie auf der Startseite des Instanz-Sicherheitszentrums auf das Profilmenü und dann auf **Notification Preferences**(Benachrichtigungseinstellungen).

Benachrichtigungseinstellungen

Benachrichtigungseinstellung	Beschreibung
Administratoranmeldung	Ausgewählte Benachrichtigungsart senden, wenn sich andere Anwender mit zugewiesenen Administratorrollen von einer anderen IP-Adresse aus bei dieser Instanz anmelden
Administratorentsperrung	Ausgewählte Benachrichtigungsart senden, wenn ein Account für einen Anwender mit hohen Berechtigungen entsperrt wurde.
Fehlgeschlagene Anmeldung	Der ausgewählte Benachrichtigungstyp wird gesendet, wenn andere Anwender nicht in der Lage sind, sich bei dieser Instanz anzumelden, und zwar in weniger als der in der Eigenschaft *glide.user.max_unlock_attempts* definierten Anzahl von Versuchen. Wenn Sie diese Eigenschaft nicht konfigurieren, ist der Standardwert 5. Weitere Informationen zu dieser Eigenschaft finden Sie unter Sperrung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benachrichtigungseinstellung	Beschreibung
	für fehlgeschlagene Anmeldeversuche angeben.
HP-Rolle hinzugefügt	Ausgewählte Benachrichtigungsart senden, wenn einem anderen Anwender eine Sicherheitsrolle mit hohen Berechtigungen gewährt wird (einschließlich Rollen „oauth_admin“, „admin“, „security_admin“ und „identitätswechsel“). Weitere Informationen zum Erhöhen der Benutzersicherheit finden Sie unter Auf eine privilegierte Rolle hochstufen und Rollen mit erhöhten Rechten.
Identitätswechsel	Senden Sie die ausgewählte Benachrichtigungsart, wenn ein anderer Anwender die Identität von Ihnen annimmt. Weitere Informationen dazu, wie Sie die Identität eines Benutzers annehmen, finden Sie unter Identität eines Benutzers annehmen .
Erhöhung der Sicherheit	Senden Sie die ausgewählte Benachrichtigungsart, wenn andere Anwender in dieser Instanz auf eine Sicherheitsadministratorrolle erhöht werden.
Wöchentlicher Digest	Senden Sie eine wöchentliche Zusammenfassung der ausgewählten Benachrichtigungsart. Sie umfasst: ◦ Eine Zusammenfassung aller Sicherheitsaktivitäten, die in dieser Instanz die ganze Woche über stattgefunden haben. ◦ Die aktuelle tägliche Compliance-Punktzahl für die Instanz.

2. Aktivieren Sie für jede Art von Sicherheitsereignis die entsprechenden Kontrollkästchen, um die Art der an Sie gesendeten Benachrichtigungen festzulegen.
Sie können jeweils mehrere Benachrichtigungsmethoden auswählen.

Checkbox	Beschreibung
E-Mail	Senden Sie eine E-Mail für diese Art von Sicherheitsereignis.
Slack	Senden Sie Benachrichtigungen für diese Art von Sicherheitsereignis über Slack. **Hinweis:** Diese Spalte wird nur angezeigt, wenn Sie die Integration Slack für Now Platformeingerichtet haben.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Checkbox	Beschreibung
Teams	Senden Sie Benachrichtigungen für dieses Sicherheitsereignis über Microsoft Teams. **Hinweis:** Diese Spalte wird nur angezeigt, wenn Sie die Integration Microsoft Teams für Now Platformeingerichtet haben.
Veröffentlichen	Senden Sie Push-Benachrichtigungen am Now Mobile für diese Art von Sicherheitsereignis. **Hinweis:** Diese Spalte wird nur angezeigt, wenn Sie sich zum ersten Mal bei Now Mobileanmelden.
Alle auswählen	Wählen Sie einen bestimmten Benachrichtigungstyp für alle Typen von Sicherheitsereignissen aus. Klicken Sie beispielsweise über **E** -Mail auf **Alle** auswählen, wenn Sie E-Mail-Benachrichtigungen für jeden Sicherheitsereignistyp erhalten möchten.

3. Klicken Sie auf **Speichern**.

Überprüfen Sie die tägliche Compliance-Punktzahl, und konfigurieren Sie die Einstellungen für Sicherheitseigenschaften

Überprüfen Sie die Eigenschaften für die Metrik „Tägliche Compliance-Punktzahl“ und die Sicherheitskonfiguration, um festzustellen, ob Ihre Instanz die vorgeschlagenen Sicherheitsanforderungen erfüllt. Sie können die tägliche Compliance-Punktzahl beeinflussen, indem Sie nicht konforme Sicherheitseigenschaften auf der Seite „Compliance-Konfigurationen für Härtung“ aktualisieren.

Wichtig:

Das Instanz-Sicherheitszentrum (ISC) hat seit September 2024 das Ende des Verkaufs erreicht und wird nicht mehr unterstützt und ist nicht mehr für eine erneute Aktivierung verfügbar.

ServiceNow Security Center (SSC) ist die empfohlene Lösung für die Zukunft. Weitere Informationen finden Sie unter Migration des Instanz-Sicherheitszentrums zu ServiceNow Security Center ..

Die Tägliche Compliance-Punktzahl ist eine prozentuale Punktzahl. Sie hängt davon ab, wie konform die aktuellen Einstellungen der Instanzsicherheitseigenschaften mit den im Härtungseinstellungen für die Instanzsicherheitveröffentlichten Compliance-Werten sind.

Überprüfen Sie regelmäßig die tägliche Compliance-Punktzahl Ihrer Instanz. Befolgen Sie diese Richtlinien, wenn Sie Ihre tägliche Compliance-Punktzahl auswerten:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Größer als oder gleich 90 % gibt an, dass die Instanz kritische Sicherheitskontrollen einhält.
- Größer als oder gleich 50 % und kleiner als 90 % zeigen ein moderates Maß an Sicherheits-Compliance an.
- Weniger als 50 % weisen auf ein geringes Maß an Sicherheits-Compliance hin.

Passen Sie die Sicherheitseinstellungen der Instanz an, um die Compliance zu erhöhen

Auf der Seite „Härtungs-Compliance-Konfiguration“ können Sie nicht konforme Sicherheitseigenschaften, die sich auf die tägliche Compliance-Punktzahl Ihrer Instanz auswirken, gehärtet und optimieren. Dadurch wird sichergestellt, dass Ihre Instanz den veröffentlichten Standards für Sicherheitshärtung und gleichzeitig die Sicherheitsanforderungen Ihres Unternehmens entspricht.

Vorbereitungen

Erforderliche Rolle: security_dashboard_user oder admin.

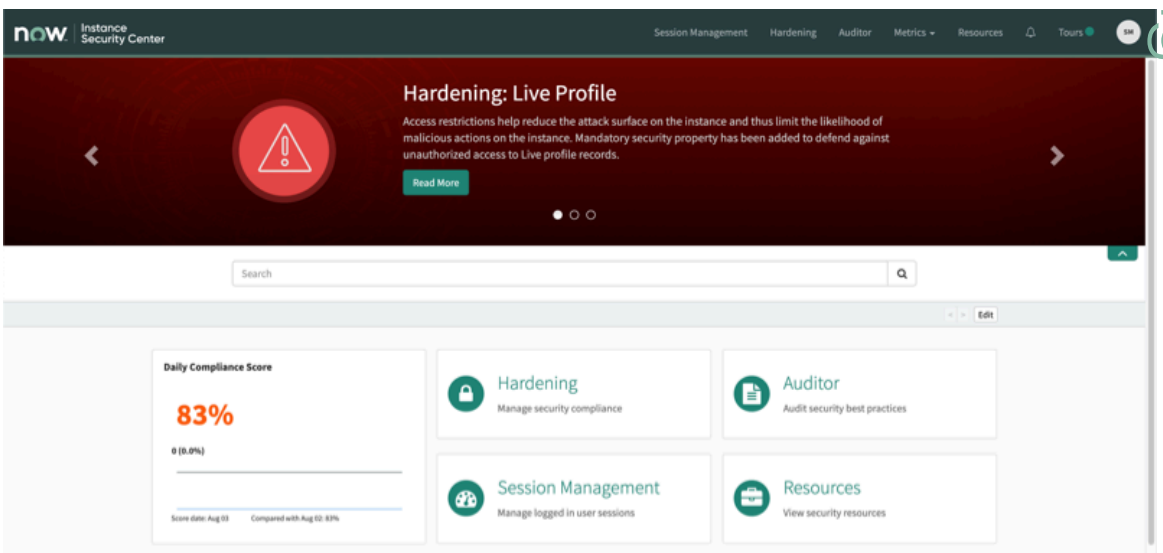
Im Inhalt Härtungseinstellungen für die Instanzsicherheit finden Sie detaillierte Beschreibungen und Compliance-Werte für die sicherheitsbezogenen Systemeigenschaften und Plugins im Now Platform.

- Konsultieren Sie die Härtungseinstellungen für die Instanzsicherheit, wenn Sie sicherheitsbezogene Eigenschaften festlegen oder aktualisieren, auch wenn einige der Compliance-Werte für Ihre Instanz möglicherweise nicht geeignet sind.
- Wenn Sie diese Eigenschaften aktualisieren, vergewissern Sie sich, dass sich die Instanz weiterhin wie erwartet verhält. Wenden Sie sich an die entsprechenden internen Mitarbeiter, die über das nötige Fachwissen verfügen, um die Auswirkungen auf die Sicherheit zu ermitteln.

Hinweis: Mit der Administratorrolle können Sie Sicherheitskontrollen anzeigen und bearbeiten. Mit der Rolle security_dashboard_user können Sie Sicherheitskontrollen anzeigen, aber nicht bearbeiten.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Instanz-Sicherheitszentrum**an.
2. Klicken Sie auf die Kachel **Tägliche Compliance-Punktzahl** oder den Link **Härtung**, um auf die Seite „Konfiguration der Härtungscompliance“ zuzugreifen.

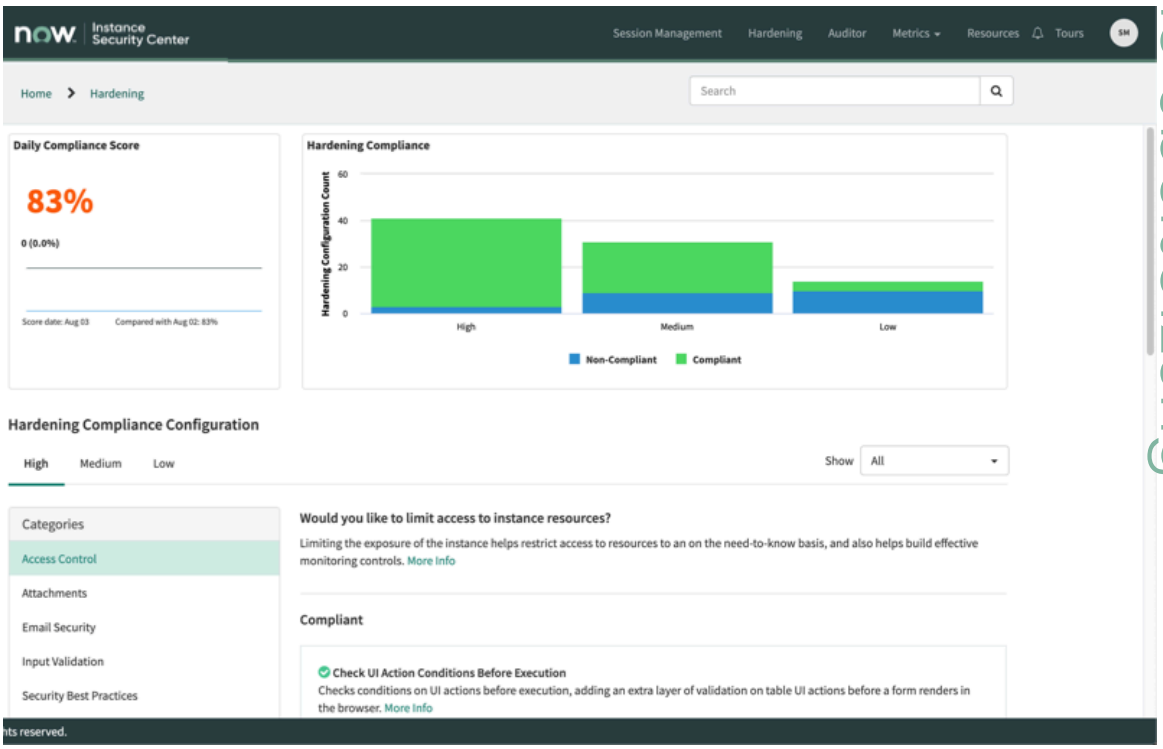


Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Zeigen Sie im Diagramm „Härtungs-Compliance“ die Statistiken für konforme und nicht konforme Sicherheitskonfigurationseigenschaften an.

Option	Bezeichnung
Konform	Anzahl der Sicherheitskonfigurationseigenschaften, die den Compliance-Werten in den Härtungseinstellungen für die Instanzsicherheit entsprechen. **Hinweis:** Sie können die Einstellungen für konforme Sicherheitseigenschaften in der Konfiguration der Härtungscompliance nicht ändern. Wenn Sie dies tun möchten, müssen Sie sie in den Systemeigenschaften aktualisieren. Weitere Informationen finden Sie unter Systemeigenschaft hinzufügen .
Nicht konform	Anzahl der Sicherheitskonfigurationseigenschaften, die nicht den Compliance-Werten in den Härtungseinstellungen für die Instanzsicherheit entsprechen. Sie können die Einstellungen für nicht konforme Eigenschaften aktualisieren.



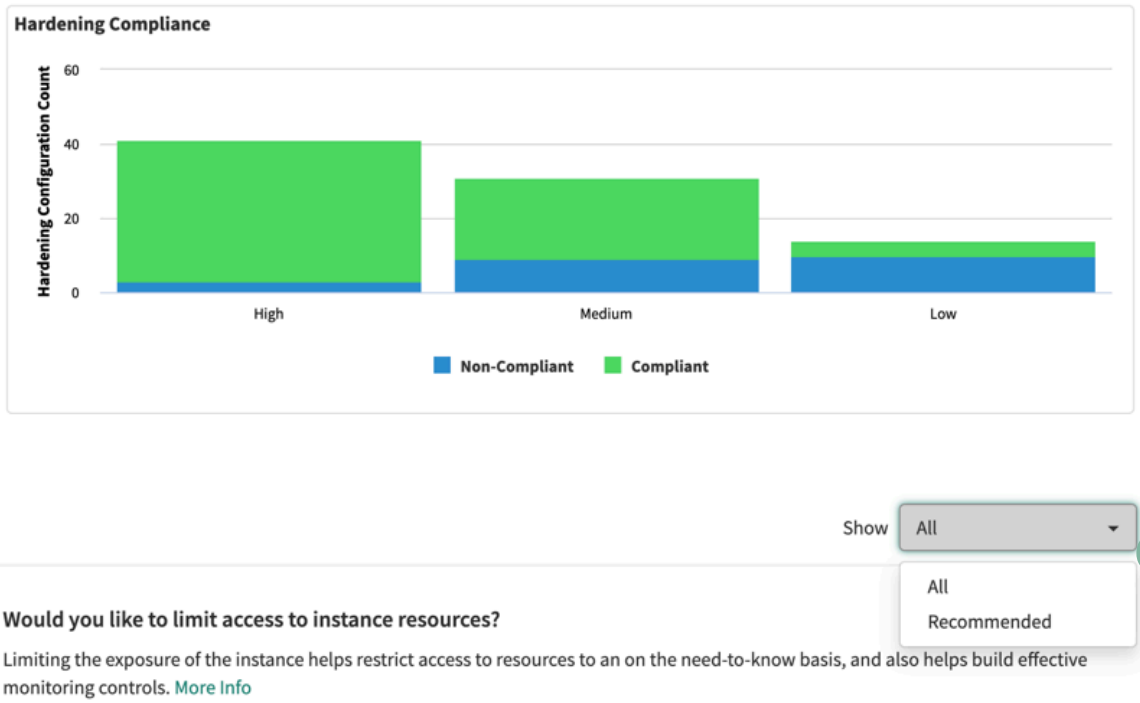
Hinweis: Um die Anzahl der konformen oder nicht konformen Sicherheitspunktzahlen für einen bestimmten Datumsbereich anzuzeigen, verschieben Sie den blauen Punkt auf dem Schieberegler unter Tägliche Compliance-Punktzahl.

4. **Geben** Sie in der Liste Anzeigen unter dem Diagramm an, ob Sie auf alle oder nur empfohlene Sicherheitskonfigurationseigenschaften zugreifen möchten.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

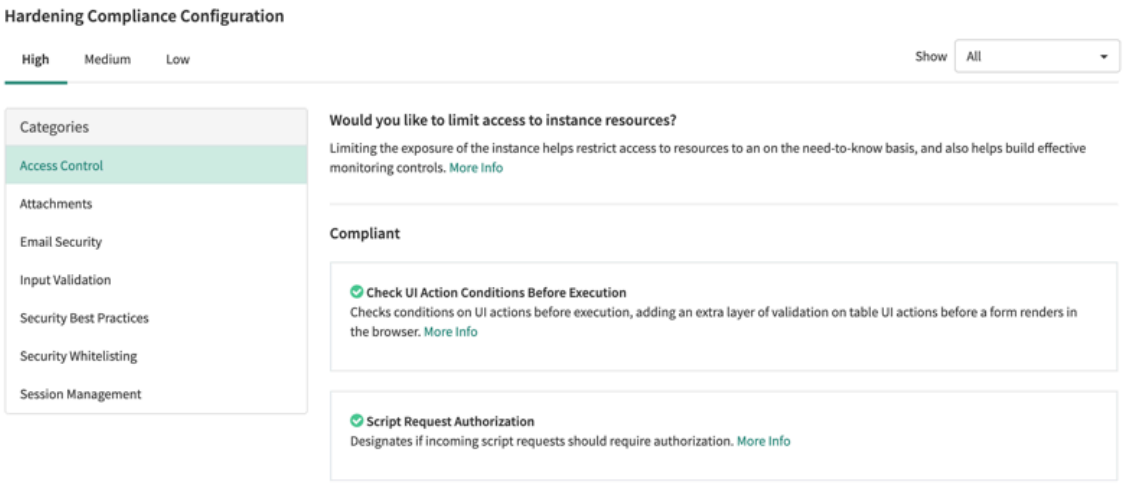
Option	Bezeichnung
Alle	(Standard) Alle konformen und nicht konformen Sicherheitskonfigurationseigenschaften in jeder ausgewählten Kategorie.
Empfohlen	In jeder ausgewählten Kategorie werden nur empfohlene Sicherheitskonfigurationseigenschaften angezeigt. Diese Sicherheitskonfigurationseigenschaften sind eine ausgewählte Teilmenge der kritischsten, die zum Schützen von Now Platformverwendet werden. Betrachten Sie diese Sicherheitskonfigurationseigenschaften als die Mindestanzahl von Einstellungen, die Sie festlegen müssen, um Now Platformzu sichern. **Hinweis:** Um Ihre Instanz vollständig zu sichern, verwenden Sie die Option **Alle**. Sie enthält auch alle empfohlenen Sicherheitskonfigurationseigenschaften.



5. Wählen Sie unter **Kategorien**die Kategorie mit den Sicherheitskonfigurationseigenschaften aus, auf die Sie zugreifen möchten:

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Option	Bezeichnung
Zugriffssteuerung	Zugriffssteuerungen bestimmen, ob der Benutzerzugriff auf eine bestimmte Ressource gewährt oder verweigert wird, je nachdem, wer diese Ressourcen verwenden darf. Weitere Informationen finden Sie unter Zugriffssteuerung in den Härtungseinstellungen für die Instanzsicherheit.
Anhänge	Sicherheitskontrollen für Anhänge ermöglichen die Validierung eingehender Anhänge, um Ihre Instanz vor schädlichen Dateien zu schützen, die von Angreifern gesendet werden. Weitere Informationen finden Sie unter Anhänge in den Härtungseinstellungen für die Instanzsicherheit.
E-Mail-Sicherheit	E-Mail-Sicherheit umfasst Sicherheitskonfigurationseigenschaften, die ein Administrator konfigurieren kann, um sicherzustellen, dass für alle eingehenden E-Mails die richtigen Sicherheitsrichtlinien gelten. Weitere Informationen finden Sie unter E-Mail-Sicherheit (Härtung der Instanzsicherheit) in den Härtungseinstellungen für die Instanzsicherheit.
Eingabevalidierung	Die Eingabevalidierung umfasst sicherheitsbezogene Eigenschaften, die ein Administrator konfigurieren kann, um die Eingabe fehlerhafter Daten unabhängig von der Quelle zu minimieren. Weitere Informationen finden Sie unter Eingabevalidierung in den Härtungseinstellungen für die Instanzsicherheit.
Sichere Kommunikation	Sichere Kommunikationseigenschaften sind diejenigen, die ein Administrator konfigurieren kann, um die Übertragung von HTTP-Datenverkehr zu sichern. Weitere Informationen finden Sie unter Sichere Kommunikation

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	in den Härtungseinstellungen für die Instanzsicherheit.
Best Practices für Sicherheit	Best Practices für Sicherheit umfassen Sicherheitsaufgaben, die ein Administrator regelmäßig innerhalb eines bestimmten Zeitintervalls ausführen sollte, und umfassen zugehörige Konfigurationseigenschaften. Weitere Informationen finden Sie unter Best Practices für Sicherheit in den Härtungseinstellungen für die Instanzsicherheit.
Sicherheitsaufnahmeliste	Die Sicherheitsaufnahmeliste enthält sicherheitsbezogene Eigenschaften, die ein Administrator konfigurieren kann, um das Verhalten auf bekannte Aufnahmelisten einzuschränken. Weitere Informationen finden Sie unter Sicherheitsaufnahmeliste in den Härtungseinstellungen für die Instanzsicherheit
Management von Anwendersitzungen	Die Sitzungsverwaltung umfasst sicherheitsbezogene Eigenschaften, die ein Administrator konfigurieren kann, um eine sichere Sitzungsverwaltung in Now Platformzu gewährleisten. Weitere Informationen finden Sie unter Management von Anwendersitzungen in den Härtungseinstellungen für die Instanzsicherheit

6. Konfigurieren Sie die nicht konformen Sicherheitseigenschaften in der ausgewählten Kategorie.
   - Sofern nicht anders angegeben, wird durch das Schieben des Schalters auf eine Sicherheitseigenschaft auf die empfohlene Einstellung festgelegt. Beispielsweise können Sie die meisten Steuerelemente auf „true“ oder „false“ festlegen, einige erfordern jedoch die Eingabe eines Werts oder von Werten, z. B. eine durch Kommas getrennte Werteliste.
   - Um auf das entsprechende Thema zu den Härtungseinstellungen für die Instanzsicherheit für die Sicherheitskontrolle zuzugreifen und mehr darüber zu erfahren, klicken Sie auf **Weitere Informationen**.

Ergebnisse

Die tägliche Compliance-Punktzahl erhöht oder verringert sich abhängig von den Änderungen, die Sie an den Einstellungen für die nicht konformen Sicherheitskontrollen vornehmen.

Zugehörige Informationen

Instanz-Sicherheitszentrum

Wie tägliche Compliance-Punktzahlen, Trends und Diagrammdaten aktualisiert werden

Trend- und Diagrammdaten im Instanz-Sicherheitszentrum werden aktualisiert, nachdem der Performance Analytics-Auftrag um 02:00 Uhr Ortszeit ausgeführt wurde. Sie wird auf der Kachel „Tägliche Compliance-Punktzahl“, in den Kacheln des Menübands „Ereignis“ und auf der Seite Analytics Hub angezeigt, wenn Sie auf eine der Ereigniskacheln klicken.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Aufgabe „[AppSec] Tägliches Datenmanagement“ ist eine regelmäßig geplante Aufgabe, die jede Nacht ausgeführt wird und folgende Aufgaben ausführt:

1. Überprüft, ob den Aufträgen „[AppSec] Tägliches Datenmanagement“ und „[PA AppSec] Tägliche Datensammlung“ bei der ersten Planung gültige Benutzer zugewiesen wurden.
   - Wenn Sie einen gültigen Benutzer in das Feld **Ausführen als** eingegeben haben, wird die Verarbeitung des Auftrags fortgesetzt. Ein gültiger Benutzer ist ein Benutzer, der nicht für die Instanz gesperrt ist und dem eine Administratorrolle zugewiesen ist.
   - Wenn Sie einen ungültigen Benutzer eingegeben haben, wird im Instanz-Sicherheitszentrum über dem rotierenden Sicherheitsbanner eine Fehlermeldung angezeigt.

   Hinweis: Weitere Informationen zum Aktualisieren des zugewiesenen Anwenders beim Ausführen geplanter Aufgaben finden Sie unter Datensammlungsaufträge erstellen oder planen
2. Führt Geschäftslogik aus, um den Compliance-Status für die Sicherheitseigenschaften festzulegen, die Sie auf der Seite „Konfiguration der Härtungscompliance“ konfigurieren. Weitere Informationen finden Sie unter Überprüfen Sie die tägliche Compliance-Punktzahl, und konfigurieren Sie die Einstellungen für Sicherheitseigenschaften.
3. Führt den Performance Analytics-Auftrag „[PA AppSec] Tägliche Datensammlung“ aus, um Compliance-Daten zu sammeln und die tägliche Compliance-Punktzahl zu aktualisieren.

Tägliche Compliance-Punktzahl wird manuell aktualisiert

Alternativ können Sie, wenn Ihnen eine Administratorrolle zugewiesen ist, die Tägliche Compliance-Punktzahl jederzeit aktualisieren und neu berechnen, indem Sie auf Aktualisieren **klicken**.

Hinweis: Die **Schaltfläche** „Aktualisieren“ wird Benutzern mit der zugewiesenen Rolle „security_dashboard_user“ nicht angezeigt.

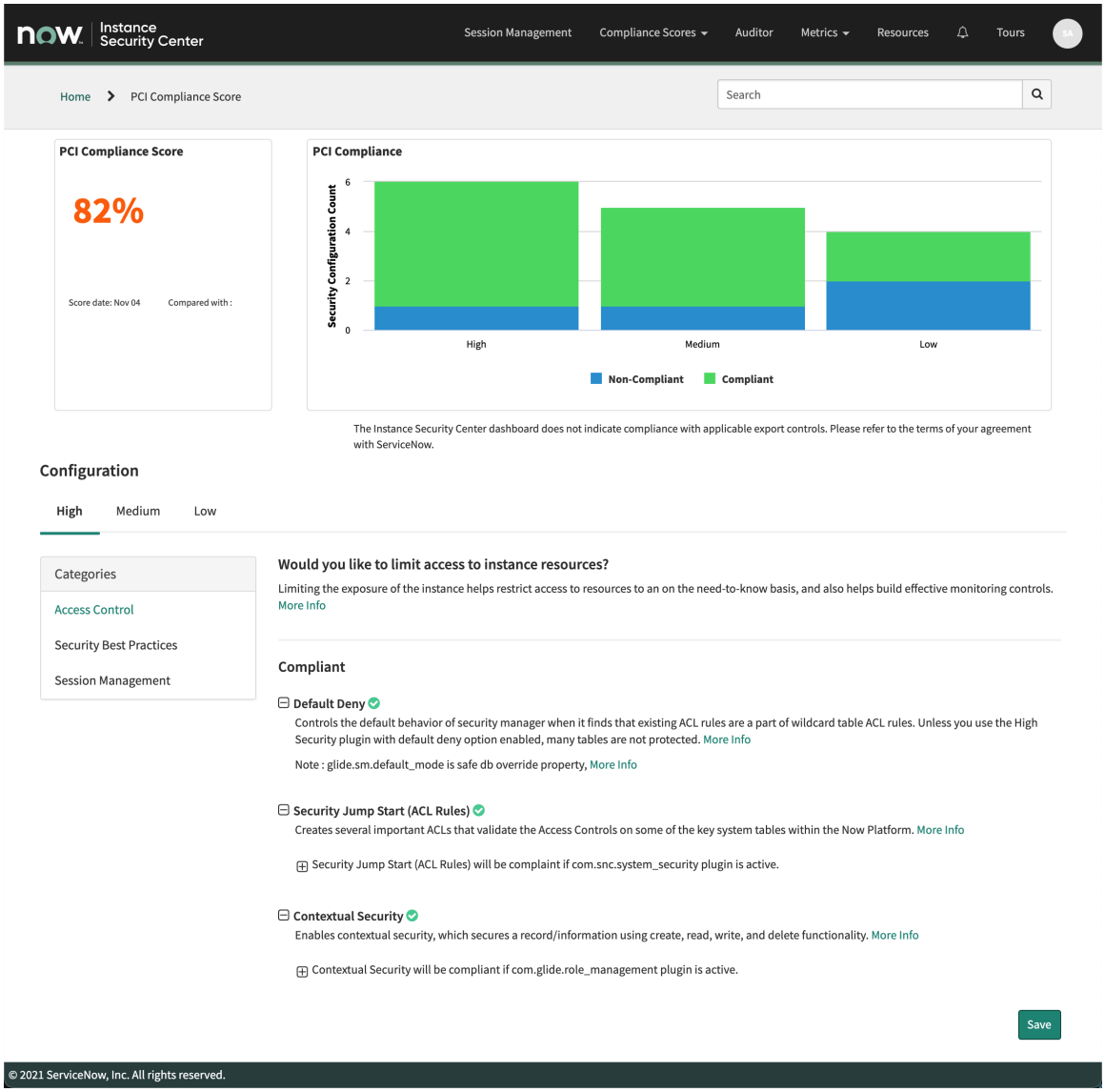
- Die Funktion Aktualisieren führt die gleichen Aufgaben aus wie der Performance Analytics-Auftrag Tägliche Datensammlung, jedoch in Echtzeit und nicht in einem Batch-Prozess.
- Sie verwenden es normalerweise, wenn Sie Aktualisierungen der täglichen Compliance-Punktzahl durchführen möchten, um die Auswirkungen von Instanzsicherheitsaktivitäten sofort anzuzeigen.
- Es kann eine geringfügige Verzögerung geben, bis die aktualisierte Punktzahl angezeigt wird.

Hinweis: Wenn Sie ein Upgrade durchführen (z. B. von London auf Xanadu), wird das Plugin „Instance Security Center (ISC)“ automatisch aktiviert. Ein bereitgestelltes Korrekturskript weist automatisch einen anwenderdefinierten Benutzer ohne zugewiesene Rollen zu.

Dashboard für PCI-Compliance-Punktzahlen

Das Dashboard für die PCI-Compliance-Bewertung zeigt, wie Ihre Instanz den Sicherheitsstandards der Payment Card Industry (PCI) entspricht. Verwenden Sie das -Dashboard, um Ihre Compliance-Bewertung anzuzeigen und Ihre Konfiguration zu ändern, um die Sicherheit zu verbessern.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Erforderliche Now Platform-Rollen

security_dashboard_user oder admin, erforderlich, um das Dashboard für die PCI-Compliance-Bewertung anzuzeigen.

Greifen Sie auf das Dashboard für die PCI-Compliance-Bewertung zu

Um das Dashboard zu öffnen, wechseln Sie zu: **Systemsicherheit** > **Instanz-Sicherheitszentrum**an. Klicken Sie im Header des Instanz-Sicherheitszentrums auf **Compliance** -Bewertungen, und wählen Sie dann **PCI-Compliance**-Bewertung aus.

Anwendungsfälle

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

Anwender	Dashboard-Verwendung
Benutzer des Sicherheitsdashboards (security_dashboard_user)	Kontinuierliche Überwachung und Verwaltung der Compliance der Instanzsicherheit.

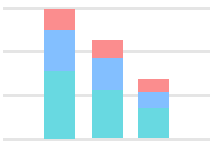
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwender	Dashboard-Verwendung
Administrator (admin)	Überwachen Sie kontinuierlich die Compliance der Instanzsicherheit, um Sicherheitsbedrohungen zu erkennen und darauf zu reagieren.

Indikatoren

Indikator	Beschreibung
PCI-Compliance-Bewertung	Zeigt die Compliance-Punktzahl Ihrer Instanz als Prozentsatz an. Dieser Prozentsatz von stellt den Prozentsatz der Sicherheitskonfigurationen in Ihrer Instanz dar, die Compliance-Standards erfüllen. Der Indikator zeigt auch das Datum an, an dem die Compliance-Punktzahl berechnet wurde, und einen Vergleich mit der zuvor berechneten Punktzahl.

Datenvisualisierung

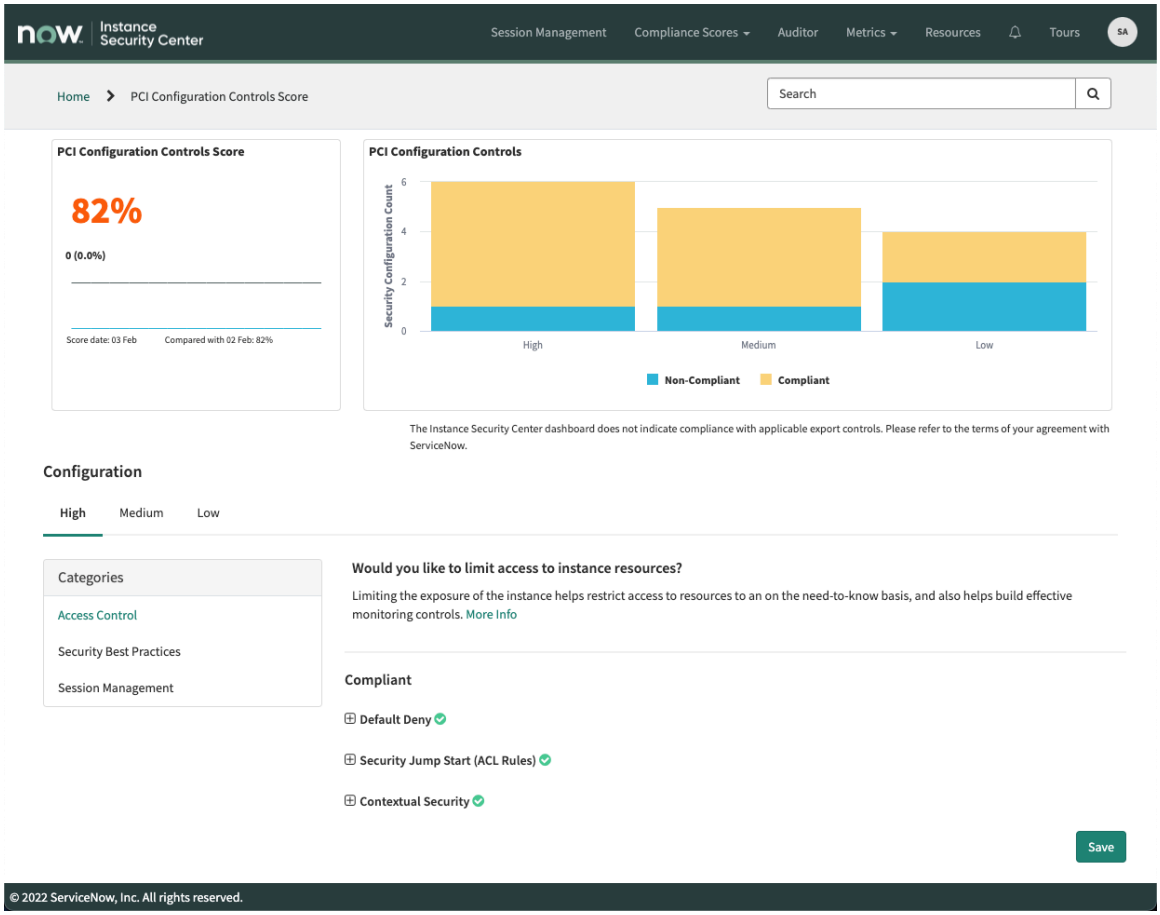
Titel	Typ	Quelltabelle	Beschreibung
PCI-Compliance	 Stapelbalkendiagramm	Sicherheitskonfigurationen [isc_security_configuration]	Zeigt konforme und nicht konforme Sicherheitskonfigurationen in den Kategorien hoch, mittel und niedrig an. Klicken Sie auf einen Bereich des Berichts, um die entsprechenden Sicherheitskonfigurationen anzuzeigen.

Punktzahl-Dashboard für PCI-Konfigurationssteuerungen

Verwenden Sie das Punktzahl-Dashboard für PCI-Konfigurationssteuerungen, um Ihre PCI-Konfiguration zu überprüfen und festzustellen, welche Sicherheitsprüfungen nicht konform sind. Sie können die Konfiguration der nicht konformen Sicherheitsprüfungen im Instanz-Sicherheitszentrum ändern.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Erforderliche Now Platform-Rollen

Die Rolle security_dashboard_user oder admin ist erforderlich, um das Dashboard für die PCI-Compliance-Bewertung anzuzeigen.

Greifen Sie auf das Dashboard für die Punktzahlen der PCI-Konfigurationssteuerungen zu

Um das Dashboard zu öffnen, wechseln Sie zu: **Systemsicherheit** > **Instanz-Sicherheitszentrum**an. Klicken Sie im Header des Instanz-Sicherheitszentrums auf **Compliance** -Bewertungen, und wählen Sie dann **Punktzahl für PCI-Konfigurationskontrollen**aus.

Anwendungsfälle

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

Anwender	Dashboard-Verwendung
Benutzer des Sicherheitsdashboards (security_dashboard_user)	Überwachen und verwalten Sie die Compliance der PCI-Konfigurationssteuerungen in Ihrer Instanz kontinuierlich. Ändern Sie die PCI-Konfiguration, um die Compliance sicherzustellen und die Instanzsicherheit zu verbessern.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

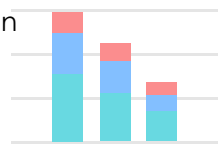
Anwender	Dashboard-Verwendung
Administrator (admin)	Überwachen Sie kontinuierlich die Compliance der PCI-Konfigurationssteuerungen, um potenzielle Sicherheitsbedrohungen zu erkennen und darauf zu reagieren.

Indikatoren

Punktzahl der PCI-Konfigurationssteuerungen

Zeigt die Punktzahl der PCI-Konfigurationssteuerungen Ihrer Instanz als Prozentsatz an. Dieser Prozentsatz von stellt den Prozentsatz der Sicherheits-PCI-Steuerungskonfigurationen in Ihrer Instanz dar, die Compliance-Standards erfüllen. Der Indikator zeigt auch das Datum an, an dem die Compliance-Punktzahl berechnet wurde, und einen Vergleich mit der zuvor berechneten Punktzahl.

Datenvisualisierung

Titel	Typ	Quelltabelle	Beschreibung
PCI-Konfigurationssteuerungen	 Stapelbalkendiagramm	Sicherheitskonfigurationen [isc_security_configuration]	Zeigt konforme und nicht konforme PCI-Steuerungskonfigurationen in den Kategorien hoch, mittel und niedrig an. Klicken Sie auf einen Bereich des Berichts, um die entsprechenden Sicherheitskonfigurationen anzuzeigen.

Suchen Sie nach falschen Sicherheitsdefinitionen

Führen Sie den Auditor aus, um Ihre Instanz zu scannen und falsche Sicherheitsdefinitionen zu finden. Er liefert Ergebnisse, die Sie korrigieren können, um die Sicherheitslage Ihrer Instanz zu verbessern.

Wichtig:

Das Instanz-Sicherheitszentrum (ISC) hat seit September 2024 das Ende des Verkaufs erreicht und wird nicht mehr unterstützt und ist nicht mehr für eine erneute Aktivierung verfügbar.

ServiceNow Security Center (SSC) ist die empfohlene Lösung für die Zukunft. Weitere Informationen finden Sie unter Migration des Instanz-Sicherheitszentrums zu ServiceNow Security Center ..

Der Auditor führt eine Ganzkörperbewertung der Instanzintegrität durch, bei der die Systemkonfiguration analysiert wird. Bei Sicherheitsscans wird Ihre aktuelle Sicherheitskonfiguration mit Definitionen von Best Practices und Compliance-Werten von Sicherheitseigenschaften verglichen.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unter dem Aspekt der Instanzsicherheit erhalten Sie Einblicke und Empfehlungen dazu, was Sie weiterhin tun sollten und wo Sie sich verbessern können. Diese Einblicke und Empfehlungen helfen Ihnen bei der Beantwortung der folgenden Fragen:

- Sind die entsprechenden sicherheitsbezogenen Eigenschaften festgelegt?
- Ist das Plugin „Hochsicherheit“ aktiviert?
- Sind die richtigen Zugriffssteuerungsregeln vorhanden?

Führen Sie den Auditor aus, und analysieren Sie die Scan-Ergebnisse

1. Um den Auditor auszuführen, klicken Sie auf der Startseite des Instanz-Sicherheitszentrums auf **Audit**.
2. Wenn der Vorgang abgeschlossen ist, öffnen Sie Scan-Ergebnisse, um die Sicherheitsfunde zu überprüfen und zu analysieren.
3. Um die Details für ein bestimmtes Scan-Ergebnis zu überprüfen, doppelklicken Sie auf die Ergebnisnummer. Diese Informationen umfassen Status, Scan-Typ, Ausführungszeit und Fehlermeldungen.
4. Jedes der Auditor-Ergebnisse enthält Details zur Lösung und eine URL zum Produktinhalt, wie Sie sie beheben können. Befolgen Sie die dokumentierten Richtlinien, um die Probleme in den einzelnen Ergebnissen zu beheben.

Zugehörige Informationen

Härtungseinstellungen für die Instanzsicherheit

Hochsicherheits-Plugin

Regeln für Zugriffssteuerungsliste

Überwachen Sie Instanzmetriken

Überwachen Sie Benutzer-, Export-, Authentifizierungs-, E-Mail- und Virenschutzmetriken für Ihre Instanz. Beispielsweise können Sie Ihre E-Mail-Sicherheit überwachen, indem Sie Metriken auf Spam, externe E-Mails und eingehende E-Mails von nicht vertrauenswürdigen und vertrauenswürdigen Domänen für Ihre Instanz überprüfen. Analysieren Sie diese Metriken, um nach anomalen Sicherheitsverhaltensweisen zu suchen, die mit Aktivitäten zusammenhängen, die in Ihrer Instanz stattfinden.

Wichtig:

Das Instanz-Sicherheitszentrum (ISC) hat seit September 2024 das Ende des Verkaufs erreicht und wird nicht mehr unterstützt und ist nicht mehr für eine erneute Aktivierung verfügbar.

ServiceNow Security Center (SSC) ist die empfohlene Lösung für die Zukunft. Weitere Informationen finden Sie unter Migration des Instanz-Sicherheitszentrums zu ServiceNow Security Center ..

Anwendermetriken

Analysieren Sie Benutzermetriken, um nach anomalen Verhaltensweisen zu suchen, die mit bestimmten Arten von Benutzeraktivitäten in Ihrer Instanz zusammenhängen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nicht protokolliert im letzten Monat/in den letzten sechs Monaten/im letzten Jahr

Gibt die Anzahl der Benutzer an, die sich im letzten Monat, in den letzten sechs Monaten und im letzten Kalenderjahr nicht bei der Instanz angemeldet haben. So zeigen Sie Benutzerdetails für eine bestimmte Metrik an:

- Klicken Sie auf die Metrik, um eine Liste der Benutzer anzuzeigen, die sich im angegebenen Zeitraum nicht bei der Instanz angemeldet haben.
- Klicken Sie auf einen Anwendernamen, um weitere Details zu diesem Anwender anzuzeigen.

Anwender mit Rollen mit hohen Berechtigungen

Gibt die Anzahl der Benutzer mit den folgenden Rollentypen mit hohen Berechtigungen an:

Anwenderrolle	Beschreibung
Administrator	Primäre Administratorrolle, die unabhängig von Sicherheitsbeschränkungen Zugriff auf alle Features, Funktionen und Daten des Systems hat.
ais_high_security_admin	Rolle mit erhöhten Berechtigungen, die es einem Anwender ermöglicht, auf Einstellungen für hohe Sicherheit für KI-Suchezuzugreifen. Weitere Informationen finden Sie unter Weisen Sie Rollen zu KI-Suche Administratoren und Benutzer an.
password_reset_admin	Administratorrolle, mit der ein Benutzer den Status von Aktivitäten zum Zurücksetzen des Passworts anzeigen, potenzielle Sicherheitsbedrohungen identifizieren und die Compliance mit Richtlinien zur Passwortsicherheit überwachen kann. Weitere Informationen finden Sie unter Passwortzurücksetzung Berichte und Protokolle zu Passwortänderungen erstellen an.
script_include_admin	Administratorrolle, die auch Zugriff auf Skripteinbindungen hat.
security_admin	Rolle mit erhöhten Berechtigungen, die es einem Anwender ermöglicht, Zugriffssteuerungen und Einstellungen für hohe Sicherheit zu erstellen und zu ändern. Weitere Informationen finden Sie unter Rolle Security_admin.
user_admin	Administratorrolle, die auch Benutzer, Rollen, Benutzergruppen, Rollen und Abteilungszuweisungen verwalten kann.

Hinweis: Weitere Informationen zu diesen Administratorrollentypen finden Sie unter Spezielle administrative Rollen .

So zeigen Sie Benutzerdetails für eine bestimmte Benutzerrollenmetrik an:

- Klicken Sie auf die Rollenmetrik für Anwenderanzahl, um eine Liste der Anwender mit diesem Rollentyp mit hohen Berechtigungen anzuzeigen.
- Klicken Sie auf einen Anwendernamen, um weitere Details zu diesem Anwender anzuzeigen. Sie können dann feststellen, ob diese sicherheitskritischen Rollen den richtigen Mitarbeitern zugewiesen sind.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendertrend

Zeigt Informationen zum Trend der Anzahl über einen Zeitraum für die folgenden Benutzertypen an:

Zählungstyp	Beschreibung
Aktive Anwender	Anzahl der Anwender, die in der Instanz als aktiv markiert sind.
Inaktive Anwender	Anzahl der Benutzer, die in der Instanz als inaktiv markiert sind.
Gesperrt	Anzahl der Anwender, die für die Instanz gesperrt sind.

So zeigen Sie Benutzerdetails für eine bestimmte Benutzeranzahl an (z. B. gesperrte Benutzer):

- Klicken Sie **auf die Metrik Gesperrte Benutzer**.
- Klicken Sie auf der Seite Analytics Hub auf **Datensätze**anzeigen .
- Klicken Sie auf einen Anwendernamen, um weitere Details zu diesem Anwender anzuzeigen. Sie können dann feststellen, ob es einen Grund für diese Person gibt, und die Situation beheben.

Ereignistrend

Zeigt Informationen zum Trend der Anzahl für bestimmte Arten von Ereignissen über einen Zeitraum von an:

Ereignistyp	Beschreibung
Administratoranmeldung	Anzahl der Anwender mit Administratorrollen mit hohen Berechtigungen, die sich an einem bestimmten Tag angemeldet haben.
Externer Login	Anzahl der Anwender mit zugewiesener Rolle „snc_external“, die sich während des Kalendertags bei dieser Instanz angemeldet haben. Diese Anmeldungen erfolgen normalerweise zu Wartungs-, Support-, Beratungs- oder Audit-Zwecken. Durch die Überwachung dieser Metrik können Sie überprüfen, ob die externen Anmeldeversuche legitim sind und keine potenziellen Sicherheitsprobleme darstellen.
Fehler bei der Anmeldung	Anzahl der fehlgeschlagenen Anmeldeversuche an einem bestimmten Tag.
Identitätswechsel	Anzahl der an einem bestimmten Tag angemeldeten Anwender, die die Identität anderer Anwender annehmen.
Erhöhung der Sicherheit	Anzahl der Fälle, in denen ein Sicherheitsadministrator die Sicherheit für Standardbenutzer erhöht hat, indem er die zugewiesene Benutzerrolle während des Kalendertags zu einer Sicherheitsrolle mit hohen Berechtigungen geändert hat. Zu diesen Sicherheitsrollen mit hohen Berechtigungen gehören „oauth_admin“, „admin“, „security_admin“ und „impersonator“.
SNC-Anmeldung	Anzahl von Kundenservice und Support, die sich an einem bestimmten Tag mithilfe der Hi-Hopping-Technik bei dieser Instanz angemeldet haben.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

So zeigen Sie Benutzerdetails für eine bestimmte Ereignisanzahl an (z. B. Identitätswechsel):

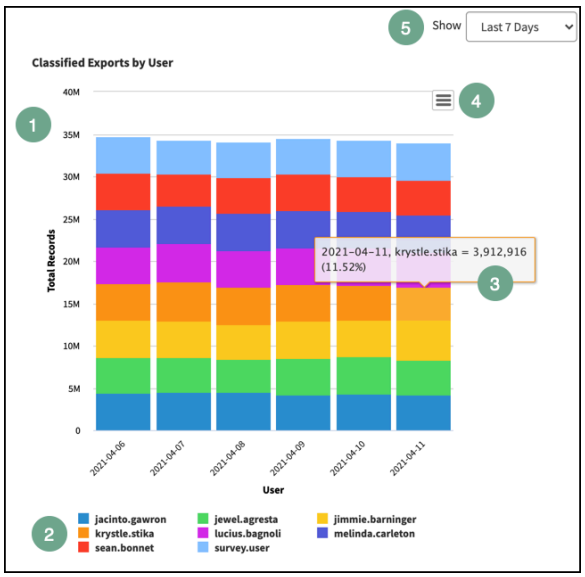
- Klicken Sie auf die Metrik für die Benutzeranzahl. Auf der Seite „Ereignisprotokolle“ des Sicherheits-Dashboards werden Ereignisprotokolle für diese Art von Ereignis aufgelistet.
- Klicken Sie auf einen Anwendernamen, um weitere Details zu diesem Ereignis anzuzeigen.

Zugehörige Informationen

Analytics Hub

Metriken exportieren

Analysieren Sie Exportmetriken, um zu sehen, welche Daten am häufigsten exportiert werden und welche Anwender die meisten Daten exportieren.



1. Exportieren Sie das Diagramm

   In jedem Bericht wird die Anzahl der Exportereignisse nach Datum geordnet angezeigt, wobei mit einem farbcodierten Schlüssel angegeben wird, welche Benutzer den Export durchgeführt haben. Klicken Sie auf den farbigen Abschnitt einer Spalte, um die Liste der Exportereignis-Datensätze [**isc_export_event**] anzuzeigen, die diesem Eintrag entsprechen.

2. Berichtsschlüssel

   Die Legende am unteren Rand des Berichts gibt an, welche Farben welche Benutzer oder Tabellen identifizieren.

3. Vorschau-Popup

   Zeigen Sie auf einen Eintrag im Diagramm, um eine Popup-Vorschau anzuzeigen. Diese Vorschau zeigt den Anwender oder Tabellennamen sowie eine Anzahl der Exporte und einen Prozentsatz der Gesamtzahl in dieser Spalte an.

4. Bildexport

   Klicken Sie auf das Symbol, um den Bericht als Bild zu speichern. Sie können den Bericht im PNG- oder JPEG-Format speichern.

5. Berichtdatumsbereich

   Verwenden Sie die **Liste** Anzeigen, um Exporte innerhalb der letzten 24 Stunden oder der letzten 7 Tage anzuzeigen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metrikberichte exportieren

Auf der Seite „Metriken exportieren“ werden vier Berichte angezeigt.

Exporte nach Anwender

Verwenden Sie den Bericht „ **Exporte nach Anwender** “, um zu sehen, welche Ihrer Anwender die meisten Daten exportieren.

Klassifizierte Exporte nach Anwender

Verwenden Sie den Bericht „ **Klassifizierte Exporte nach Anwender** “, um zu sehen, welche Ihrer Anwender die meisten Daten exportieren, die Klassifizierungen wie vertrauliche, eingeschränkte oder personenbezogene Daten entsprechen. Welche Klassifizierungen dieser Bericht verwendet, können Administratoren auf der Registerkarte „ **Einstellungen** “ definieren.

Exportiert nach Tabelle

Verwenden Sie den Bericht „ **Exporte nach Tabelle** “, um zu sehen, welche Tabellen am häufigsten exportiert werden.

Klassifizierte Exporte nach Tabelle

Verwenden Sie den Bericht „ **Klassifizierte Exporte nach Tabelle** “, um zu sehen, welche Tabellen am häufigsten aus exportiert werden und Klassifizierungen wie vertrauliche, eingeschränkte oder personenbezogene Daten entsprechen. Welche Klassifizierungen dieser Bericht verwendet, können Administratoren auf der Registerkarte „ **Einstellungen** “ definieren.

Hinweis: Exportmetrikberichte verfolgen nur Exportereignisse. Exporte aus anderen Quellen wie REST-APIs oder Workflows werden im Rahmen dieser Funktion nicht nachverfolgt.

Exportieren Sie die Metrikeinstellungen

Verwenden Sie die Konfigurationsoptionen auf der Registerkarte Einstellungen, um die Berichterstellungsergebnisse einzugrenzen.

Greifen Sie auf die Einstellungen für Ihre Exportmetriken zu, indem Sie auf die Registerkarte **Einstellungen** klicken.

Konfigurationsfelder für Einstellungen

Metrikkonfigurationen exportieren

Konfiguration	Beschreibung
Klassifizierungen für Metriken	Fügen Sie diesem Feld Klassifizierungen hinzu, oder entfernen Sie sie, um zu bestimmen, welche Exporte in den Berichten **„Klassifizierte Exporte nach Anwender“** und **„Klassifizierte Exporte nach Tabelle** “ enthalten sind. Diese Berichte unterstützen die folgenden Klassifizierungen: • Persönlich identifizierbare Informationen • Vertraulich • Beschränkt • Intern • Öffentlich

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metrikkonfigurationen exportieren (Fortsetzung)

Konfiguration	Beschreibung
	Weitere Informationen zu Datenklassifizierungen finden Sie unter Datenklassifizierungen
Klassifizierungen für Warnungen	Fügen Sie diesem Feld Klassifizierungen hinzu, oder entfernen Sie sie, um zu bestimmen, welche Exporte Benachrichtigungen zur Instanzsicherheit auslösen. Die im Feld **Klassifizierungen für Metriken** unterstützten Klassifizierungen werden hier unterstützt. Weitere Informationen zu diesen Warnungen finden Sie im Abschnitt zu Sicherheitsbenachrichtigungen auf der Seite Instanz-Sicherheitszentrum. Das Feld **Datensatzschwellenwert** definiert die Anzahl der Datensätze, die exportiert werden, bevor Ihre Instanz eine Warnung auslöst.
Datensatzschwellenwert	Anzahl der Datensätze, die ein Anwender exportieren muss, um eine Warnung auszulösen. Um eine Warnung auszulösen, müssen diese Datensätze auch den Klassifizierungen entsprechen, die im Feld **Klassifizierungen für Warnungen** aufgeführt sind.

Verwenden Sie die Schaltfläche **Speichern (⌘ + s)**, um Ihre Einstellungen zu speichern.

Authentifizierungsmetriken

Analysieren Sie Authentifizierungsmetriken, um Informationen im Zusammenhang mit der Authentifizierung anzuzeigen, z. B. selten verwendete IP-Adressen, fehlgeschlagene Anmeldungen und Arten der von Ihren Anwendern verwendeten Authentifizierungsschemata.

Verwenden Sie die Seite „ **Authentifizierungsmetriken** “, um Berichte zu Ihrer Authentifizierungskonfiguration anzuzeigen. Die folgenden Berichte werden auf dieser Registerkarte angezeigt.

Hinweis: Die Seite mit den Authentifizierungsmetriken erfordert das **Plugin „REST API Access Policy“** (com.glide.rest.policy). Weitere Informationen zu dieser Funktion finden Sie unter REST API-Zugriffsrichtlinien.

APIs ohne Authentifizierungsrichtlinien

Zeigt eine Echtzeitanzahl aller APIs ohne Zugriffsrichtlinie an

Härtung: Flow zur Accountwiederherstellung

Härtung: Rollenbasierte Einstellung im Zusammenhang mit der MFA-Funktion

Accounts mit nur Webservice-Zugriff

Zeigt die Anzahl aller Anwenderdatensätze mit aktivierter Webservice-Zugriffsoption in der Tabelle *User* [sys_user] an.

X509-Zertifikate, die in 30 Tagen ablaufen

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigt die Anzahl aller X.509-Zertifikate aus der Tabelle *X.509 Certificates* [sys_certificate] an, die in 30 Tagen ablaufen sollen.

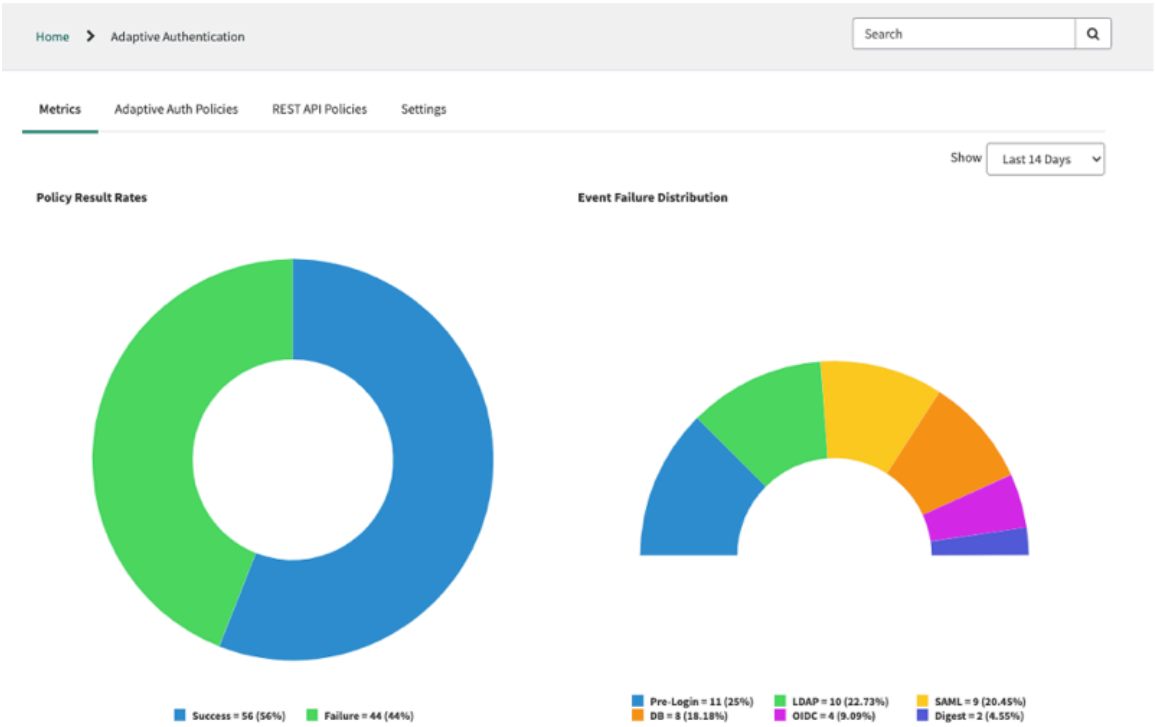
Metriken der adaptiven Authentifizierung

Analysieren Sie Metriken der adaptiven Authentifizierung, um zu überwachen, wie die adaptive Authentifizierung in Ihrer Instanz verwendet wird, und geben Sie dadurch Einblicke.

Zeigen Sie Berichte, Einstellungen und Richtlinien für die adaptive Authentifizierung in vor Ort auf der Seite mit den Metriken für die adaptive Authentifizierung an. Sicherheitsadministratoren können Berichte verwenden, um die Ergebnisse ihrer Richtlinien für adaptive Authentifizierung zu überwachen. Verwenden Sie diese Daten, um Einblicke zu gewinnen und Ihre Richtlinien anzupassen, um ihre Leistung zu verbessern.

Hinweis: Die Seite mit den Metriken für die adaptive Authentifizierung erfordert das Plugin „ **Adaptive Authentifizierung** “ (com.snc.adaptive_authentication). Weitere Informationen zu dieser Funktion finden Sie unter Adaptive Authentifizierung.

Metriken



Verwenden Sie die Registerkarte **Metriken**, um Berichte zu Ihrer Konfiguration der adaptiven Authentifizierung anzuzeigen. Die folgenden Berichte werden auf dieser Registerkarte angezeigt.

- Policenergebnisraten
- Ereignisfehlerverteilung
- Verteilung des Ereigniserfolgs
- Abgelehnete IP-Adressen
- Authentifizierungsanwenderanmeldungen
- API-Anwenderanmeldungen
- Authentifizierungstrend

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie die **Liste** Anzeigen, um eine Zeitspanne für die angezeigten Berichte auszuwählen

Adaptive Authentifizierungsrichtlinien

Verwenden Sie die Registerkarte **Adaptive** Authentifizierungsrichtlinien, um die Richtlinien und Richtlinienkontexte für die adaptive Authentifizierung in Ihrer Instanz anzuzeigen. Klicken Sie auf einen Eintrag in diesen Listen, um den zugehörigen Datensatz anzuzeigen. Weitere Informationen zu diesen Datensätzen finden Sie unter Adaptive Authentifizierung

Einstellungen

Verwenden Sie die Registerkarte „Einstellungen“, um die Systemeigenschaften der adaptiven Authentifizierung anzuzeigen und zu konfigurieren. Weitere Informationen zu diesen Eigenschaften finden Sie unter Adaptive Authentifizierungseigenschaften konfigurieren

E-Mail-Metriken

Analysieren Sie Ihre E-Mail-Metriken, um nach anomalen Verhaltensweisen zu suchen, die mit den eingehenden E-Mails an Ihre Instanz zusammenhängen. Wenn die Metriken beispielsweise eine Spitze bei Spam-E-Mails von bestimmten Domänen anzeigen, können Sie eingehende Aktionen definieren, die die Zustellung an die Instanz verhindern.

Für jede E-Mail-Metrik wird für jeden E-Mail-Typ, der an einem Kalendertag an die Instanz übermittelt oder gesendet wurde, eine Anzahl angezeigt.

Benachrichtigungseinstellung	Beschreibung
Externe eingehende E-Mail	Anzahl der eingehenden E-Mails für den Kalendertag, die von externen E-Mail-Domänen an die Instanz übermittelt wurden. **Hinweis:** Die externen E-Mail-Domänen sind die Domänen, die nicht in der Systemeigenschaft *security.list.internal.domains* aufgeführt sind, da diese Eigenschaft nur Ihre internen E-Mail-Domänen nachverfolgt. Weitere Informationen zu dieser Eigenschaft finden Sie unter Verfügbare Systemeigenschaften .
Spam	Anzahl der eingehenden E-Mails für den Kalendertag, die an die Instanz zugestellt und als Spam markiert wurden. Eine Zahl, die nicht mit historischen Trends übereinstimmt, kann darauf hinweisen, dass versucht wurde, die Sicherheit Ihrer Instanz zu gefährden.
Vertrauenswürdige eingehende E-Mail	Anzahl der eingehenden E-Mails an der Instanz für den Kalendertag von als vertrauenswürdig eingestuften E-Mail-Domänen.
Nicht vertrauenswürdige eingehende E-Mail	Anzahl der eingehenden E-Mails an der Instanz für den Kalendertag von als nicht

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benachrichtigungseinstellung	Beschreibung
	vertrauenswürdig eingestuften E-Mail-Domänen. Sie können nicht vertrauenswürdige oder vertrauenswürdige E-Mail-Domänen im Formular „Nicht vertrauenswürdige und vertrauenswürdige Domäne“ angeben, um die eingehenden E-Mails nachzuverfolgen, die von ihnen gesendet werden. Informationen zum Festlegen nicht vertrauenswürdiger oder vertrauenswürdiger E-Mail-Domänen finden Sie unter Kennzeichnen Sie E-Mail-Domänen als nicht vertrauenswürdig oder vertrauenswürdig.

Nachdem Sie auf eine E-Mail-Metrik geklickt haben, können Sie mehr über die möglichen E-Mail-Sicherheitsprobleme in Ihrer Instanz erfahren, indem Sie auf eine der folgenden Optionen klicken:

Befehl	Beschreibung
Diagramm	Anzahlen der eingehenden E-Mails und Anzahltrends im Zeitverlauf für den ausgewählten E-Mail-Typ (Spam, eingehende externe, nicht vertrauenswürdig oder vertrauenswürdig).
Datensätze	Einzelne E-Mail-Datensätze, die die tägliche Anzahl für den ausgewählten E-Mail-Typ kompromittieren.
Weitere Informationen	Zusätzliche Informationen für den ausgewählten E-Mail-Typ.

Hinweis: Die E-Mail-Metriken gelten nur für eingehende E-Mails an die Instanz. Die Metriken gelten nicht für den normalen Datenverkehr, der über Ihre unternehmensweiten E-Mail-Server verarbeitet wird. Weitere Informationen zum Definieren eingehender Aktionen und ihrer Auswirkungen auf die Verarbeitung eingehender E-Mails finden Sie unter Aktionen für eingehende E-Mails .

Kennzeichnen Sie E-Mail-Domänen als nicht vertrauenswürdig oder vertrauenswürdig

Markieren Sie bestimmte E-Mail-Domänen als nicht vertrauenswürdig oder vertrauenswürdig, damit Sie die Metriken für eingehende E-Mails aus diesen Quellen in Ihrer -Instanz überwachen können.

Vorbereitungen

Erforderliche Rolle: security_dashboard_user oder admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn nicht vertrauenswürdige oder vertrauenswürdige Domänen E-Mails an Ihre Instanz senden, wird deren tägliche Anzahl auf der Seite „E-Mail“ unter den Metriken **„Nichtvertrauenswürdige eingehende E** -Mails“ oder „Vertrauenswürdige eingehende E-Mails“ angezeigt. Sie können dann die E-Mail-Aktivität von diesen Domänen nachverfolgen und E-Mail-Protokolle verwenden, um bestimmte eingehende E-Mails anzuzeigen. Sie können

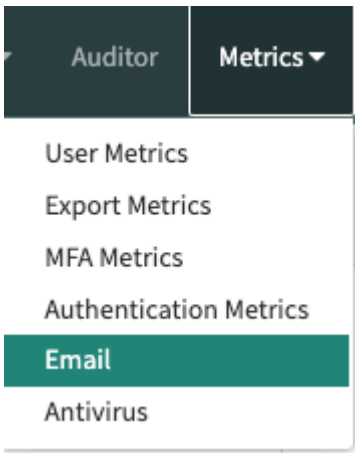
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

auch einen Benutzer (normalerweise einen Manager oder einen Sicherheitsanalysten) angeben, der bei jeder Aktivität in der nicht vertrauenswürdigen Domäne benachrichtigt wird.

Hinweis: Das Kennzeichnen einer E-Mail-Domäne als nicht vertrauenswürdig dient nur der Sicherheitsnachverfolgung. Administratoren können auch einen Systemadressfilter einrichten, um E-Mails von nicht vertrauenswürdigen Domänen zu ignorieren. Weitere Informationen zum Filtern von E-Mails, um ihre Zustellung zu blockieren, finden Sie unter Systemadressfilter .

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Instanz-Sicherheitszentrum**an.
2. Wählen Sie auf der Homepage des Instanz-Sicherheitszentrums die Option E- **Mail** im Menü **Metriken** aus.

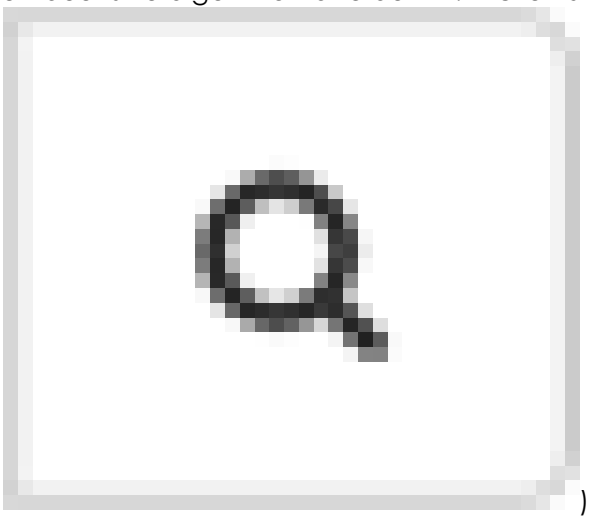


3. Klicken Sie auf der Seite „E-Mail“ im Abschnitt „Nicht vertrauenswürdige und vertrauenswürdige Domänen“ auf **Neu**.
4. Füllen Sie die Felder des Formulars aus.

Formular „Nicht vertrauenswürdige und vertrauenswürdige Domäne“.

Feld	Beschreibung
Domäne	Name der E-Mail-Domäne, die Sie als nicht vertrauenswürdig oder vertrauenswürdig kennzeichnen. Geben Sie beispielsweise `servicenow.com` ein, um festzulegen, dass ServiceNow Mitarbeiter vertrauenswürdige E-Mails an die Instanz senden können.
Kategorie	Kategorie, die angibt, ob die E-Mail-Domäne nicht vertrauenswürdig oder vertrauenswürdig ist: Nicht vertrauenswürdige Gibt an, dass die E-Mail-Domäne als nicht vertrauenswürdig eingestuft wird. Sie verwenden es, um Domänen zu identifizieren, die verdächtige E-Mails senden oder eine potenzielle Sicherheitsbedrohung für die Instanz darstellen. Vertrauenswürdig Markiert die E-Mail-Domäne als vertrauenswürdig. Sie verwenden es, um Domänen zu identifizieren, wenn Ihre Metriken anzeigen, dass die eingehenden E-Mails keine Sicherheitsbedrohungen darstellen. Wenn Sie die Domäne als vertrauenswürdig

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	kennzeichnen, können Sie die Aktivität eingehender E-Mails im Zeitverlauf nachverfolgen.
Aktiv	Checkbox zum Aktivieren oder Deaktivieren des angegebenen Status „nicht vertrauenswürdig“ oder „vertrauenswürdig“ für die angegebene E-Mail-Domäne.
Notify	Name des Anwenders, der per E-Mail benachrichtigt werden soll, wenn eine Aktivität in der nicht vertrauenswürdigen oder vertrauenswürdigen Domäne auftritt. Klicken Sie auf das Spotlight-Suchsymbol (), um nach dem Namen des Anwenders zu suchen. Lassen Sie das Feld **Notify** leer, wenn Sie keine Benachrichtigungen senden möchten.

5. Wählen Sie **Speichern**.

Ergebnisse

Informationen zu nicht vertrauenswürdigen oder nicht vertrauenswürdigen E-Mail-Domänen werden auch der **Liste nicht vertrauenswürdiger und vertrauenswürdiger Domänen** auf der Seite „E-Mail“ hinzugefügt.

Zugehörige Informationen

Instanz-Sicherheitszentrum

E-Mail-Metriken

Antivirus-Metriken

Wenn das Plugin Antivirus-Scanning aktiviert ist, wird in Ihrer Instanz Antivirus-Scanning ausgeführt, um sie vor Virusinfektionen durch Anhänge zu schützen.

Die folgenden Metriken werden für die letzten 60 Tage der Aktivität angezeigt und ermöglichen Ihnen die Bewertung der Effektivität der Funktionen Antivirus-Scanning.

Antivirus-Ereignisse

Antivirus-Ereignisse geben die Anzahl der Antivirus-Ereignisse in Ihrer Instanz nach Datum an. Um auf die Antivirus-Ereignisse zuzugreifen, navigieren Sie zu **Systemsicherheit** > **Instanz-Sicherheitszentrum** und wählen Sie die Registerkarte Metriken. Farbcodierte Diagrammlinien stellen die folgenden Arten von Antivirus-Ereignisse dar:

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Farbe	Beschreibung
Blau	Anzahl der Dateien, die von Antivirus-Scanning in dieser Instanz für das angegebene Datum unter Quarantäne gestellt wurden.
Grün	Anzahl der infizierten Dateien, die in die Instanz heruntergeladen und dann für das angegebene Datum unter Quarantäne gestellt wurden. Diese Dateien sind in erster Linie E-Mail-Anhänge, die einen Virus oder Rouge-Code enthalten.
Gelb	Anzahl der Dateien in Quarantäne in der Instanz, die für das angegebene Datum gelöscht wurden.
Orange	Anzahl der Dateien in Quarantäne in der Instanz, die für das angegebene Datum wiederhergestellt wurden. **Hinweis:** Nachdem Antivirus-Scanning ausgeführt wurde und falsch positive Ergebnisse gefunden wurden, können Sie eine Datei unter Quarantäne stellen und in der Instanz zugänglich machen.

- Um auf die Seite Analytics Hub zuzugreifen und die detaillierte Bewertungsliste und Analyseinformationen für ein bestimmtes Datum anzuzeigen, klicken Sie auf eine farbige Linie im Diagramm Antivirus-Ereignisse. Klicken Sie beispielsweise auf die blaue Grafikzeile, um Analytics-Informationen für Dateien anzuzeigen, die für ein bestimmtes Datum unter Quarantäne gestellt wurden.
- Um die folgenden Aufgliederungen auf der Seite Analytics Hub anzuzeigen, klicken Sie auf das ☰ und dann auf:

Aufgliederung	Beschreibung
AppSec – Antivirus-Ereignisquelle	Quelle des Antivirus-Ereignisses. ◦ **Beim Hochladen:** Tritt aufgrund des Uploads einer infizierten Datei auf, normalerweise eines Anhangs. ◦ **Aus Quarantäne:** Tritt aufgrund der Quarantäne einer infizierten Datei auf, normalerweise eines Anhangs. ◦ **Beim Herunterladen:** Tritt aufgrund des Downloads einer infizierten Datei auf, normalerweise eines Anhangs. ◦ **Aus Datensatz:** Tritt aufgrund eines infizierten Datensatzes in einer Tabelle auf.
AppSec – Antivirus-Ereignistyp	Typ des Antivirus-Ereignisses. ◦ In**Quarantäne:** Tritt aufgrund der Quarantäne einer Datei auf, normalerweise eines Anhangs. ◦ **Heruntergeladen:** Tritt aufgrund des Downloads einer Datei auf, normalerweise eines Anhangs.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgliederung	Beschreibung
	◦ **Wiederhergestellt:** Aufgrund der Wiederherstellung einer Datei unter Quarantäne aufgetreten. ◦ **Gelöscht:** Aufgrund des Löschens einer Datei unter Quarantäne aufgetreten.
AppSec – Antivirus-Uploader	Name des angemeldeten Benutzers, der die Dateien hochgeladen hat, die die Quelle der von der Anwendung Antivirus-Scanning erkannten Virusinfektionen waren.

Dateien in Quarantäne

Listet die infizierten Dateien in der von Antivirus-Scanningunter Quarantäne gestellten Instanz auf:

Feld	Beschreibung
Dateiname	Name der infizierten Datei.
Inhaltstyp	Typ des Inhalts, der in der Datei infiziert wurde. Beispiel: **„application/x-dosexec“** ist eine infizierte Anwendungs- oder DOS-Datei, während „ **text/plain** “ eine infizierte TXT-Datei ist.
Tabelle	Name der Tabelle, die die infizierte Datei enthält. Beispiel: **Der Incident** wird für einen Incident-Datei-Datensatz angezeigt.
Virus	Name der von Antivirus-Scanningunter Quarantäne gestellten Datei.
Erkannt	Datum und Uhrzeit der Erkennung der infizierten Datei.
Erstellt von	Name des Anwenders, der die infizierte Datei unter Quarantäne gestellt hat.
Erstellt	Datum und Uhrzeit der Erstellung des Quarantänedatei-Datensatzes.
Tabellen-Sys-ID	Tabellensystembezeichner, der dem Quarantänedatei-Datensatz zugewiesen ist.

Hinweis: Sie können dem Menüband Ereignis auch Kacheln **Dateien in Quarantäne** und **Virustypen** hinzufügen. Weitere Informationen finden Sie unter Sicherheitsereignisse überwachen und Konfigurieren Sie das Sicherheitsereignis-Menüband.

Zugehörige Informationen

- Antivirus-Scanning
- Antivirus-Scanning konfigurieren
- Dateien in Quarantäne werden überprüft
- Virenschutz-Aktivität wird überprüft
- Analytics Hub
- Performance Analytics – Aufgliederungen
- Analytics, Intelligence and Reporting

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dashboard für MFA-Metriken

Das Dashboard für MFA-Metriken zeigt Informationen zur Konfiguration der Multifaktor-Authentifizierung Ihrer Instanzen an. Verwenden Sie das Dashboard, um sicherzustellen, dass Ihre MFA-Konfiguration Ihren Sicherheitsstandards entspricht.

Erforderliche Now Platform-Rollen

security_dashboard_user oder admin, erforderlich, um das Dashboard für die PCI-Compliance-Bewertung anzuzeigen.

Greifen Sie auf das Dashboard für MFA-Metriken zu

Um das Dashboard zu öffnen, wechseln Sie zu: **Systemsicherheit** > **Instanz-Sicherheitszentrum**an. Klicken Sie im Header des Instanz-Sicherheitszentrums auf **Metriken**, und wählen Sie dann **MFA-Metriken**aus.

Anwendungsfälle

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

Anwender	Dashboard-Verwendung
Benutzer des Sicherheitsdashboards (security_dashboard_user)	Kontinuierliche Überwachung und Verwaltung der Compliance der Instanzsicherheit.
Administrator (admin)	Überwachen Sie kontinuierlich die Compliance der Instanzsicherheit, um Sicherheitsbedrohungen zu erkennen und darauf zu reagieren.

Indikatoren

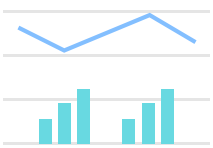
Für MFA registrierte Anwender

Zeigt die Gesamtzahl der Anwender in der für MFA registrierten Instanz an. Klicken Sie, um den Analytics Hub zu öffnen, um weitere Details anzuzeigen.

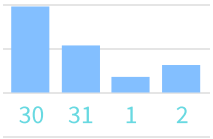
Anwender, die eine MFA-Umgehung verwenden

Zeigt die Gesamtzahl der Anwender an, die die MFA-Umgehung verwenden . Klicken Sie, um den Analytics Hub zu öffnen, um weitere Details anzuzeigen.

Datenvisualisierungen

Titel	Typ	Quelltabelle	Beschreibung
MFA-Anwender mit hohen Berechtigungen			

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Quelltabelle	Beschreibung
MFA-Anwendertrend	 Trend		

Aktivieren Sie die ISC-Schnittstelle Virtual Agent

Wenn Sie über die Administratorrolle verfügen, können Sie das Plugin „ISC Virtual Agent Conversations“ (com.glide.isc_virtualagent) aktivieren. Durch die Aktivierung dieses Plugins werden die Inhaltspakete Virtual Agent und Natural Language Understanding (NLU) installiert und ermöglichen den Zugriff Virtual Agent über das Instanz-Sicherheitszentrum.

Vorbereitungen

Wichtig:

Das Instanz-Sicherheitszentrum (ISC) hat seit September 2024 das Ende des Verkaufs erreicht und wird nicht mehr unterstützt und ist nicht mehr für eine erneute Aktivierung verfügbar.

ServiceNow Security Center (SSC) ist die empfohlene Lösung für die Zukunft. Weitere Informationen finden Sie unter Migration des Instanz-Sicherheitszentrums zu ServiceNow Security Center ..

Die Schnittstelle Virtual Agent im Instanz-Sicherheitszentrum ist nur für Benutzer mit kostenpflichtigen Abonnements Virtual Agent verfügbar, die das Plugin „Glide Virtual Agent“ (com.glide.cs.chatbot) aktiviert haben. Weitere Informationen finden Sie unter Virtual Agent aktivieren .

Erforderliche Rolle: admin.

Warum und wann dieser Vorgang ausgeführt wird

Über die ISC-Schnittstelle Virtual Agent können Sie folgende Aufgaben ausführen:

- Stellen Sie sicherheitsbezogene Fragen, und erhalten Sie dann Antworten in einer Schnellzusammenfassung sowie Referenzlinks, um mehr zu erfahren.
- Erhalten Sie Antworten in Bezug auf das Instanz-Sicherheitszentrum, die Plattformsicherheit, die Sicherheitsrichtlinien von ServiceNow, Vertrauen, Governance, Risiko und andere Prozesse.
- Suchen Sie nach sicherheitsbezogenen Ressourcen, z. B. nach Knowledge Base-Themen im Now Support-Sicherheitsportal.

Plugins für ISC Virtual Agent

Plugin	Beschreibung
ISC Virtual Agent Konversationen [com.glide.isc_virtualagent]	Aktiviert das Inhaltspaket „ISC Virtual Agent Conversations“ für das Instanz-Sicherheitszentrum.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Plugins für ISC Virtual Agent (Fortsetzung)

Plugin	Beschreibung
ISC-Modell Virtual AgentNLU für Konversationen []. [com.glide.isc_nlu]	Aktiviert das Inhaltspaket Natural Language Understanding (NLU) für das Instanz-Sicherheitszentrum.

Hinweis: Durch die Aktivierung des Plugins „com.glide.isc_virtualagent“ wird com.glide.isc_nlu automatisch aktiviert. Wenn Sie jedoch zuerst das Plugin „com.glide.isc_nlu“ aktivieren, müssen Sie auch com.glide.isc_virtualagent manuell aktivieren.

Prozedur

1. Navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie das Plugin über die Filterkriterien und die Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.

3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: `Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.`

   Nach Abschluss der Installation wird eine Meldung angezeigt.

Härtungseinstellungen für die Instanzsicherheit

Der Inhalt „Härtungseinstellungen für die Instanzsicherheit“ enthält detaillierte Beschreibungen und Compliance-Werte für die sicherheitsbezogenen Systemeigenschaften und Plugins im Now Platform. Die meisten dieser Eigenschaften können Sie auf der Seite „Konfiguration der Härtungscompliance“ im Instanz-Sicherheitszentrum festlegen.

Wichtig:

Das Instanz-Sicherheitszentrum (ISC) hat seit September 2024 das Ende des Verkaufs erreicht und wird nicht mehr unterstützt und ist nicht mehr für eine erneute Aktivierung verfügbar.

ServiceNow Security Center (SSC) ist die empfohlene Lösung für die Zukunft. Weitere Informationen finden Sie unter Migration des Instanz-Sicherheitszentrums zu ServiceNow Security Center ..

Übersicht und Zweck

Das Instanz-Sicherheitszentrum berechnet täglich eine Compliance-Punktzahl, ausgedrückt als Prozentsatz. Sie hängt davon ab, wie konform Ihre aktuellen Instanzsicherheitseinstellungen mit den Compliance-Werten in den Härtungseinstellungen für die Instanzsicherheit sind.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auf der Seite „Konfiguration der Härtungscompliance“ können Sie die spezifischen Sicherheitskonfigurationseinstellungen verwalten, die sich auf die Punktzahl für Ihre Instanz auswirken können. Weitere Informationen dazu, wie Sie sicherstellen, dass Ihre Instanzen die Härtungsanforderungen erfüllen, finden Sie unter:

- Instanz-Sicherheitszentrum
- Passen Sie die Sicherheitseinstellungen der Instanz an, um die Compliance zu erhöhen

Konsultieren Sie die Härtungseinstellungen für die Instanzsicherheit, wenn Sie sicherheitsbezogene Eigenschaften festlegen oder aktualisieren, auch wenn einige der Compliance-Werte für Ihre Instanz möglicherweise nicht geeignet sind. Wenn Sie diese Eigenschaften aktualisieren, vergewissern Sie sich, dass sich die Instanz weiterhin wie erwartet verhält. Wenden Sie sich an die entsprechenden internen Mitarbeiter, die über das nötige Fachwissen verfügen, um die Auswirkungen auf die Sicherheit zu ermitteln.

Andere Ressourcen

Zur Benutzerreferenz enthält Now Platform umfangreiche Informationen zu den Konfigurationsfähigkeiten in der Produktdokumentation. Auf die meisten Sicherheitsinhalte können Sie über die Links in Instanz sichernzugreifen. Siehe auch:

- Verfügbare Systemeigenschaften
-
- Strenge Sicherheitseinstellungen

Härtungstabellen für die Instanzsicherheit

Sicherheitskonfigurationstabelle

Datensätze in der Tabelle „Sicherheitskonfigurationen“ [isc_security_configurations] enthalten die Details einer Sicherheitskonfiguration. In einem Datensatz finden Sie die Beschreibung einer Konfiguration, ihren Compliance-Status und andere wichtige Details.

Verwenden Sie den Sicherheitskonfigurationsdatensatz, um alle Eigenschaften und Abhängigkeiten anzuzeigen, die Sie konfigurieren müssen, um Ihre Konfiguration an einem Ort konform zu machen.

Im Sicherheitskonfigurationsdatensatz können Sie die zugehörigen Sicherheitsabhängigkeits- und Abhängigkeitsgruppen-Datensätze sehen, die dieser Konfiguration zugeordnet sind.

Tabelle der Sicherheitsabhängigkeiten

Datensätze in der Tabelle „Sicherheitsabhängigkeiten“ [isc_security_dependencies] definieren die eingehenden und ausgehenden Kriterien sowie einen empfohlenen Typ. Dieser Typ definiert, wie die Abhängigkeit im Instanz-Sicherheitszentrum angezeigt wird.

Tabelle der Abhängigkeitsgruppen

Verwenden Sie Datensätze in der Tabelle „Abhängigkeitsgruppen“ [isc_dependency_groups], um mehrere Abhängigkeiten zu gruppieren. Alle Abhängigkeiten in einer Gruppe müssen konform sein, damit die Gruppe als konform gilt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugriffssteuerung (Härtung der Instanzsicherheit)

Zugriffssteuerungen bestimmen, ob der Zugriff auf eine bestimmte Ressource gewährt oder verweigert werden soll. Sie gewährt nur den Benutzern Zugriff auf Ressourcen, die zu deren Verwendung berechtigt sind.

Autorisierung ist nicht gleichbedeutend mit Authentifizierung, da diese Begriffe und ihre Definitionen häufig verwechselt werden.

- Bei der Authentifizierung wird die Identität bereitgestellt und validiert.
- Die Autorisierung enthält Ausführungsregeln, die bestimmen, auf welche Funktionen und Daten der Benutzer (oder Prinzipal) zugreifen kann, und stellen die ordnungsgemäße Zuteilung von Zugriffsrechten nach erfolgreicher Authentifizierung sicher.

Die Autorisierung ist ein Prozess, der nach einer erfolgreichen Authentifizierung erfolgt. Sie können Sicherheitseigenschaften konfigurieren, die bestimmen, ob die Ressourcenautorisierung erfolgt, nachdem festgestellt wurde, dass ein Benutzer über gültige Anmeldeinformationen verfügt, die einem wohldefinierten Satz von Rollen und Berechtigungen zugeordnet sind.

Im Folgenden finden Sie einige Sicherheitskontrollen, die ein Administrator konfigurieren kann, um den nicht autorisierten Zugriff auf vertrauliche Entitäten innerhalb von Now Platformeinzuschränken.

- Regeln für Zugriffssteuerungsliste
- Konfigurieren einer ACL-Regel
- ServiceNow-Zugriffssteuerung

Zugriff auf skriptfähige GlideSystemUserSession-API

Die vom Client aufrufbare skriptfähige GlideSystemUserSessionSandbox-API macht die Methoden addErrorMessageNoSanitization und addInfoMessageNoSanitization von GlideSystemUserSession für die Javascript-Sandbox verfügbar. Dadurch können alle Anwender diese Methode per Skript aufrufen.

Bei Festlegung auf **true**darf eine Benutzersitzung in einer Sandbox Informations- oder Fehlermeldungen ohne Bereinigung aufrufen. Beim Aufruf der Nachricht wird eine Warnung protokolliert. Bei Festlegung auf **false**ist der Anruf nicht zulässig.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.sandbox.usersession.allow_unsanitized_messages*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurierbar im Instanz-Sicherheitszentrum	Ja
Zweck	Diese Eigenschaft verhindert, dass nicht bereinigte Informations- oder Fehlermeldungen in einer Anwendersitzung mit einer Sandbox aufgerufen werden.
Typ	wahr | falscher boolescher Wert
Empfohlener Wert	falsch

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsabhängigkeiten	Der Wert für diese Eigenschaft ist eine sichere Überschreibung und kann nach der Änderung nicht mehr geändert werden.
Funktionale Auswirkung	(Hoch) Wenn Sie die Eigenschaft auf den Wert „falsch“ festlegen, werden keine Nachrichten erstellt oder protokolliert, wenn diese Funktionen aufgerufen werden.
Sicherheitsrisiko	(Hoch) Ohne entsprechende Bereinigung kann auf potenziell gefährliche Inhalte zugegriffen werden, und die nicht bereinigte Fehlerfunktion ist für das Skript verfügbar.
Referenzen	Zugriffssteuerung Sichere Überschreibung

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Autorisierung für Skriptausführung

Verwenden Sie die Eigenschaft *glide.script_processor.authorized_script_module_role*, um die Verwendung von ausgeführten Skripts aus der Tabelle *„sys_app_module"* auf die in der Eigenschaft definierte Rolle zu beschränken.

Diese Eigenschaft verhindert, dass alle Systemanwender ein Skript aus „sys_app_module“ ausführen, es sei denn, sie verfügen über die in der Eigenschaft angegebene Rolle. Verwenden Sie die Eigenschaft „glide.script_processor.authorized_script_module_role“, um die Rolle anzugeben, die Skripts ausführen kann.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.script_processor.authorized_script_module_role*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um zu erfordern, dass eine bestimmte Rolle ein Skript aus *sys_app_module ausführt*.
Empfohlener Wert	Textfeld mit einer kommagetrennten Liste von Rollen.
Funktionale Auswirkung	(Mittel) Diese Korrektur erzwingt die Authentifizierung in Form von Autorisierung durch die definierte Rolle. • Diese Authentifizierung wird bei der Verarbeitung von Skriptanforderungen in der Instanz durchgeführt. • Sie schränkt alle Gastanwender ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	für Anwender erstellen, die Zugriff auf diesen Inhalt benötigen, mit den erforderlichen Zugriffssteuerungsberechtigungen.
Sicherheitsrisiko	(Hoch) Wenn keine entsprechende Autorisierung für Skriptanforderungen konfiguriert ist, können nicht autorisierte Anwender auf vertrauliche Inhalte/Daten in der Instanz zugreifen.
Referenzen	Zugriffssteuerung

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Standardauthentifizierung: JSONv2-Anforderungen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.basicauth.required.jsonv2*, um festzulegen, ob für eingehende JSONv2-Anforderungen eine Standardautorisierung erforderlich sein soll.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.basicauth.required.jsonv2
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Zum Erzwingen der Autorisierung von JSONv2-Anforderungen.
Empfohlener Wert	wahr
Funktionale Auswirkung	(Mittel) Diese Korrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Standardauthentifizierung und Zugriffssteuerung auf Systemebene. • Diese Authentifizierung wird durchgeführt, während Daten aus Tabellen/Seiten in Form von JSON-Daten in der Instanz abgerufen werden. • Sie schränkt alle Gastanwender ein, die derzeit auf diese Daten zugreifen. • Erstellen Sie einen Account für einen Anwender, der Zugriff auf diesen Inhalt benötigt, mit den erforderlichen Berechtigungen für die Zugriffssteuerung. Weitere Informationen finden Sie unter JSONv2-Webservice JSONv2-Webservice .
Sicherheitsrisiko	(Hoch) Wenn keine entsprechende Autorisierung für die JSON-Anforderungen der Datenquelle konfiguriert ist, kann ein nicht autorisierter Anwender

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	auf vertrauliche Inhalte/Daten in der Zielinstanz zugreifen.
Referenzen	Authentifizierung Basic Authentication für eingehende JSONv2-Anforderungen anfordern

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Standardauthentifizierung: SOAP-Anforderungen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.basicauth.required.soap*, um festzulegen, ob für eingehende SOAP-Anforderungen eine Standardautorisierung erforderlich sein soll.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.basicauth.required.soap
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Zum Erzwingen der Autorisierung von SOAP-Anforderungen.
Empfohlener Wert	wahr
Funktionale Auswirkung	(Mittel) Diese Korrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Standardauthentifizierung und Zugriffssteuerung auf Systemebene. • Es führt diese Authentifizierung durch, während es Daten aus Tabellen/Seiten in Form von SOAP-Daten in der Instanz abruft. • Sie schränkt alle Gastanwender ein, die derzeit auf diese Daten zugreifen. • Erstellen Sie einen Account für einen Anwender, der Zugriff auf diesen Inhalt benötigt, mit den erforderlichen Berechtigungen für die Zugriffssteuerung. Weitere Informationen finden Sie unter SOAP-Webservice- und MID-Server-Authentifizierung, Anmeldeinformationen und SOAP-Anforderungen .
Sicherheitsrisiko	(Mittel) Ohne entsprechende Autorisierung für die Datenquellen-SOAP-Anforderungen kann ein nicht autorisierter Anwender auf vertrauliche Inhalte/Daten in der Zielinstanz zugreifen.
Referenzen	Authentifizierung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Blockieren Sie den Zugriff für delegierte Entwickler

Diese Konfiguration wirkt sich auf den Zugriff für delegierte Entwickler aus, die Anwenderrollen über ein Skript aktualisieren. Wenn die Konfiguration konform ist, kann der Entwickler ohne die Rolle „user_admin“ keine Datensätze in der Tabelle *„sys_user_has_role“* aktualisieren oder einfügen.

Der Wert dieser Eigenschaft wirkt sich darauf aus, ob ein delegierter Entwickler unerwarteten Zugriff auf Funktionen in der Instanz gewähren oder erhalten darf. Wenn die Eigenschaft Rollen enthält, können nur diese Rollen Skriptmodule ausführen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*com.glide.sys.security.delegateddev.block_grant_roles*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Der Wert dieser Eigenschaft wirkt sich darauf aus, ob ein delegierter Entwickler unerwarteten Zugriff auf Funktionen in der Instanz gewähren oder erhalten darf.
Typ	Umschalten
Empfohlener Wert	wahr
Sicherheitsabhängigkeiten	Keine
Funktionale Auswirkung	(Hoch) Wenn ein Benutzer mit der Rolle „delegated_developer“ versucht, einen Datensatz in „sys_user_has_role“zu ändern, aktiviert diese Eigenschaft zusätzliche Sicherheitsprüfungen für den -Vorgang. Die zusätzlichen Sicherheitsprüfungen validieren, dass dem Benutzer die Rolle „user_admin“ zugewiesen wurde, wenn er versucht, „sys_user_has_role“zu erstellen oder zu aktualisieren. Wenn sie nicht über die Rolle „user_admin“ verfügen, wird der Zugriff verweigert. Wenn die Eigenschaft „false“ lautet, werden diese zusätzlichen Prüfungen nicht validiert.
Sicherheitsrisiko	(Hoch) Ohne entsprechende Autorisierung können nicht autorisierte Anwender auf vertrauliche Inhalte/ Daten in der Instanz zugreifen.
Referenzen	Zugriffssteuerung

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

UI-Aktionsbedingungen vor der Ausführung überprüfen (Instanzsicherheitshärtung)

Verwenden Sie die Eigenschaft *glide.security.strict.actions*, um die Überprüfung von Bedingungen für UI-Aktionen in Formularen und Listen zu ermöglichen, bevor sie ausgeführt werden. Wenn Sie diese Eigenschaft auf **true**festlegen, wird den Tabellen-UI-Aktionen eine zusätzliche Validierungsebene hinzugefügt, bevor sie ausgeführt werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.security.strict.actions
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um eine zusätzliche Validierungsebene für die Tabellen-UI-Aktionen sicherzustellen, bevor sie ausgeführt werden.
Empfohlener Wert	wahr
Funktionale Auswirkung	(Niedrig) Diese Korrektur fügt lediglich eine zusätzliche Validierungsebene hinzu, um nach UI-Aktionen in der Zieltabelle/-seite in der Instanz zu suchen. Solange die Zugriffssteuerungen in der Kundeninstanz entsprechend festgelegt sind, sollte dies hier keine Auswirkungen haben.
Sicherheitsrisiko	(Mittel) Zugriffsanforderung wird immer geprüft, wenn Transaktionen zwischen zwei Zonen stattfinden. Dieser Vorgang validiert alle UI-Aktionen, bevor das Formular für den Endanwender gerendert wird.
Referenzen	Hochsicherheits-Plugin

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Contextual Security: Plugin für Rollenverwaltung (Härtung der Instanzsicherheit)

Aktivieren Sie das Plugin „Contextual Security: Role Management“ (*com.glide.role_management*), um die kontextbezogene Sicherheit zu aktivieren, die Datensätze/Informationen mithilfe von Erstellungs-, Lese-, Schreib- und Löschfunktionen sichert.

Nach der Installation und Aktivierung werden die Wörterbuchrollen (vom einfachen Sicherheitsmanager erstellt) nicht mehr getestet. Stattdessen sucht Now Platform in Feldern und Tabellen nach ACL-Regeln. Die Anwendung sichert die Daten mithilfe von ACL-Regeln anstelle von herkömmlichen, rollenbasierten Wörterbuchregeln, die von einem einfachen Sicherheitsmanager implementiert werden. Selbst wenn Sie das Wörterbuchformular konfigurieren und einem Wörterbucheintrag Rollen hinzufügen, werden die Rechte nicht geändert.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Plugin-ID	com.glide.role_management
Konfigurationstyp	Systemdefinition > Plugins
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Im Gegensatz zum einfachen Sicherheitsmanager kennt der Kontextsicherheitsmanager die Systemtabellenhierarchie. Sie können möglicherweise andere Sicherheitsregeln für ein Feld haben, je nachdem, wo es in der Hierarchie angezeigt wird.
Empfohlener Wert	Aktiv (Plugin standardmäßig aktiviert)
Funktionale Auswirkung	(Mittel) Diese Korrektur erzwingt die Funktionsebene von Zugriffssteuerungen, wodurch die Anwendung die Zugriffsbeschränkungen allein auf der ACL-Tabelle bestimmen kann.
Sicherheitsrisiko	(Hoch) Zugriffssteuerungen auf Funktionsebene müssen vor der Ausführung von CRUD-Vorgängen serverseitig erzwungen werden, um Instanzanwendern die entsprechende Zugriffsebene zu gewähren.
Referenzen	Contextual Security Manager

Weitere Informationen zum Aktivieren von Plugins finden Sie unter Plugins aktivieren .

Autorisierung von CSV-Anforderungen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.basicauth.required.csv*, um festzulegen, ob eingehende CSV-Anforderungen (Comma-Separated Values) eine Standardauthentifizierung erfordern sollen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.basicauth.required.csv
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um die Standardauthentifizierung für CSV-Anforderungen zu erzwingen.
Empfohlener Wert	wahr
Funktionale Auswirkung	(Niedrig) Diese Korrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Standardauthentifizierung und Zugriffssteuerung auf Systemebene.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Es führt diese Authentifizierung durch, während Daten aus Tabellen/Seiten in Form von CSV-Daten in der Instanz abgerufen werden. • Sie schränkt alle Gastanwender ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Anwender erstellen, die Zugriff auf diesen Inhalt benötigen, mit den erforderlichen Zugriffssteuerungsberechtigungen. Weitere Informationen finden Sie unter Daten aus einer CSV-formatierten Datei abrufen .
Sicherheitsrisiko	(Mittel) Wenn keine entsprechende Autorisierung für die eingehenden CSV-Anforderungen konfiguriert ist, kann ein nicht autorisierter Anwender Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.
Referenzen	Webservice – Sicherheit

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Standardmäßig verweigern (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.sm.default_mode*, um das Standardverhalten des Sicherheitsmanagers zu steuern, wenn festgestellt wird, dass vorhandene ACL-Regeln Teil von ACL-Regeln der Platzhaltertabelle sind.

Wenn das Plugin „Hohe Sicherheitseinstellungen“ (*com.glide.high_security*) während der Erstinstallation der Instanz aktiviert wird, erstellt es diese Eigenschaft, und es werden Platzhalter-ACL-Regeln erstellt. Um rollenbasierten Zugriff auf Systemtabellen bereitzustellen, steuern diese Regeln eine erhebliche Anzahl von ACLs und die meisten gängigen datensatzbasierten Vorgänge:

- Lesen
- Schreiben
- Erstellen
- Löschen

Wenn Sie das Plugin „Hohe Sicherheit“ mit aktivierter standardmäßiger Ablehnungsoption nicht verwenden, sind viele Tabellen nicht geschützt. Now Platform verwendet ein standardmäßiges Deny-Sicherheitsmodell, das verhindert, dass Benutzer ohne Administratorrechte auf Objekte zugreifen, wenn sie eine übereinstimmende ACL-Regel erfüllen. Mit diesem Modell werden viele Angriffsvektoren entfernt, z. B. unsichere Skripts.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.sm.default_mode
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Die beste Sicherheitsmethode besteht darin, den Zugriff auf die Tabellen durch einen nicht autorisierten Benutzer einzuschränken. • Wenn für Tabellen keine ACL-Regeln vorhanden sind, stellt diese Eigenschaft sicher, dass mindestens Platzhalter-ACLs für jeden CRUD-Vorgang validiert werden, der für die Tabelle/das Feld ausgeführt wird. • Diese Regeln schränken die Lese-, Schreib-, Erstellungs- und Löschvorgänge für alle Tabellen ein, es sei denn, der Benutzer verfügt über die Administratorrolle oder erfüllt die Anforderungen einer anderen Tabellen-ACL-Regel.
Empfohlener Wert	verweigern
Funktionale Auswirkung	(Hoch) Wenn Sie diese Eigenschaft auf **Allow**festlegen, erlauben die ACL-Regeln der Platzhaltertabelle CRUD-Vorgänge für alle Tabellen, es sei denn, es sind bestimmte ACL-Regeln für Tabellen vorhanden, um solche Vorgänge einzuschränken. **Hinweis:** Dieses Plugin ist nicht für vorhandene Instanzen vorgesehen, da es den Sicherheitszugriff auf Tabellen ändern könnte, die bereits in einer Produktionsumgebung verwendet werden.
Sicherheitsrisiko	(Hoch) Benutzer ohne Administratorrechte können auf Objekte zugreifen, die den ACL-Regeln der Platzhaltertabelle entsprechen.
Referenzen	Standardmäßige Verweigerungseigenschaft

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Eingehende Transaktionen doppelt prüfen (Instanzsicherheitshärtung)

Die Eigenschaft *glide.security.strict.updates* ermöglicht die doppelte Überprüfung der Sicherheit bei eingehenden Transaktionen während der Formularübermittlung und fügt eine zusätzliche Ebene der Tabellenvalidierung hinzu, bevor ein Formular im Browser gerendert wird. Diese Eigenschaft ist standardmäßig auf „ **true** “ festgelegt

Weitere Informationen

Hinweis: Diese Eigenschaft ist in Vancouver und späteren Releases standardmäßig auf „ **true** “ festgelegt und kann von Administratoren nicht geändert werden. Wenn Sie einen Anwendungsfall haben, bei dem die Eigenschaft geändert werden muss, wenden Sie sich an den Kundensupport.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Eigenschaftsname	glide.security.strict.updates
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um eine zusätzliche Überprüfungsebene für Benutzerberechtigungen sicherzustellen, bevor das Formular im Browser angezeigt wird.
Empfohlener Wert	wahr
Funktionale Auswirkung	(Niedrig) Diese Korrektur fügt eine zusätzliche Validierungsebene hinzu, um nach Anwenderberechtigungen für die Zieltabelle/-seite in der Instanz zu suchen. Solange die Zugriffssteuerungen in der Kundeninstanz entsprechend festgelegt sind, sollte dies keine Auswirkungen haben.
Sicherheitsrisiko	(Hoch) Sie sollten die Zugriffsanforderung immer überprüfen, wenn Transaktionen zwischen zwei Zonen stattfinden. Dieser Vorgang prüft auf Berechtigungen, wenn das Formular angefordert wird und bevor das Rendern des Formulars erfolgt.
Referenzen	

ACLs zur Steuerung von Live-Profildetails aktivieren (Instanzsicherheitshärtung)

Verwenden Sie die Eigenschaft *`glide.live_profile.details`*, um festzulegen, ob ein Anwender alle Detailfelder in einem Live-Profil anzeigen kann, z. B. Unternehmensname und Telefonnummern.

Je nach Einstellung der Eigenschaft *`glide.live_profile.details`* geschieht Folgendes:

- Wenn der Wert auf **Anzeigen**festgelegt ist, wird der Zugriff auf die Live-Profilinformationen unabhängig von den für das Anwenderprofil erstellten ACLs gewährt.
- Wenn der Wert auf **ACL**festgelegt ist, wird der Zugriff auf die Live-Profilinformationen gemäß den für das Anwenderprofil erstellten ACLs eingeschränkt.
- Wenn der Wert auf **Ausblenden**festgelegt ist, wird der Zugriff auf die Live-Profilinformationen unabhängig von den für das Anwenderprofil erstellten ACLs eingeschränkt.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.live_profile.details
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Der Zweck besteht darin, nur autorisierten Anwendern den Zugriff auf die Details eines Live-Profils (z. B. Unternehmensname, Telefonnummern) zu ermöglichen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Empfohlener Wert	ACL
Funktionale Auswirkung	(Mittel) Wenn die Eigenschaft nicht aktiviert ist, können nicht autorisierte Anwender auf die Live-Profildetails aller anderen Anwender zugreifen.
Sicherheitsrisiko	(Mittel) API-Anforderungen sollten Tabellen-ACLs immer berücksichtigen. Es muss eine Einschränkung angewendet werden, um zu verhindern, dass nicht autorisierte Anwender auf Details eines Live-Profils zugreifen.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

AJAXGlideRecord-ACL-Überprüfung aktivieren (Instanzsicherheitshärtung)

Verwenden Sie die Eigenschaft *glide.script.secure.ajaxgliderecord*, um eine ACL-Validierung (Access Control Rule) durchzuführen, wenn auf serverseitige Datensätze, z. B. Tabellen, mit GlideAjax-APIs in einem Client-Skript zugegriffen wird.

Von Client-Skripts aus können beliebige Daten vom Server abgefragt werden. Verwenden Sie dazu AJAXGlideRecord (GlideAjax -Client)-API, indem eine Syntax verwendet wird, z. B. ein serverseitiger Glide-Datensatz. Es ist ein leistungsstarkes und nützliches Tool für viele Bereitstellungen.

Wenn Sie Zugriffssteuerungslisten (Access Control Lists, ACL) auf GlideAjax-API-Aufrufe anwenden, können Sie nur Daten abfragen, auf die der aktuell verbundene Benutzer Zugriff hat. Wenn beispielsweise ein ESS-Benutzer angemeldet ist, der keine Rechte zum Lesen der Tabelle „cmn_location“ hat, schlagen alle Aufrufe der GlideAjax-API für diese Tabelle fehl.

Wenn Now Platform ohne GlideAjax-ACL-Aufrufprüfung ausgeführt wird, kann eine API Informationen zurückgeben, auf die der aktuell angemeldete Benutzer sonst nicht zugreifen könnte.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.script.secure.ajaxgliderecord
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Stellen Sie sicher, dass Sicherheits-ACLs überprüft und validiert werden, auch wenn der Zugriff auf die Datensätze über clientseitige APIs erfolgt.
Empfohlener Wert	wahr
Funktionale Auswirkung	(Hoch) Diese Korrektur erzwingt die ACL-Beziehung zu serverseitigen Datensätzen, wenn die Anforderungen mithilfe der AJAXGlideRecord-API-Aufrufe gestellt werden. Wenn die ACL-Konfiguration nicht ordnungsgemäß konfiguriert ist, hat dies potenzielle Auswirkungen. Weitere Informationen zu seinen Auswirkungen und zur Identifizierung finden Sie im

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Artikel Client-seitige GlideRecord-Transaktionen (AJAXGlideRecord) prüfen und überprüfen [KB0550828] in der HI Knowledge Base .
Sicherheitsrisiko	(Hoch) Mithilfe von Client-Skripts können beliebige Daten vom Server über die GlideAjax-API abgefragt werden. Der Zugriff auf serverseitige Ressourcen ist ohne ordnungsgemäße Autorisierung möglich. Die Verwendung der ACL-Validierung hilft der Anwendung, die Anforderung basierend auf der konfigurierten Autorisierung zu validieren.
Workaround	Stellen Sie sicher, dass die richtigen ACLs für Skripteinbindungen, Prozessoren und andere Entitäten erstellt werden, die von einer GlideAjax-API (AJAXGlideRecord) verwendet werden, damit sie mit der richtigen Autorisierung ausgeführt werden kann. Implementieren Sie Methoden wie `canRead ()`, `canWrite()`, `canCreate ()` und `canDelete ()`, um vor dem Zugriff auf Tabellendatensätze mit GlideRecord eine Anwenderautorisierung durchzuführen. Eine andere Methode ist die Verwendung von GlideRecordSecure. Die Klasse wird vom GlideRecord-Server geerbt, der die gleichen Funktionen wie GlideRecord ausführt und außerdem ACLs erzwingt.
Referenzen	ACLs auf AJAXGlideRecord (clientseitiger Glide-Datensatz) anwenden Diese Eigenschaft gehört zu derselben Familie von Eigenschaften, die die Ausführung von Skripts sichern und einschränken, die vom Client stammen: • *glide.script.use.sandbox*: Siehe Sandbox für vom Client generierte Skripts. • *glide.script.allow.ajaxevaluate*: Siehe „AJAXEvaluate aktivieren“

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Autorisierung von Excel-Anforderungen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.basicauth.required.excel*, um festzulegen, ob für eingehende Excel-Anforderungen eine Standardauthentifizierung erforderlich sein soll.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.basisauth.erforderlich.excel
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um die Standardauthentifizierung für Excel-Anforderungen zu erzwingen.
Empfohlener Wert	wahr
Funktionale Auswirkung	(Niedrig) Diese Korrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Standardauthentifizierung und Zugriffssteuerung auf Systemebene. • Es führt diese Authentifizierung durch, während Daten aus Tabellen/Seiten in Form von Excel-Daten in der Instanz abgerufen werden. • Sie schränkt alle Gastanwender ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Anwender erstellen, die Zugriff auf diesen Inhalt benötigen, mit den erforderlichen Zugriffssteuerungsberechtigungen.
Sicherheitsrisiko	(Mittel) Wenn keine entsprechende Autorisierung für eingehende Excel-Anforderungen konfiguriert ist, kann ein nicht autorisierter Anwender Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Plugin „Explicit Role“ (Härtung der Instanzsicherheit)

Aktivieren Sie das Plugin Explicit Role (*com.glide.explicit_roles*), um der Instanz die neuen Rollen „snc_internal“ und „snc_external“ für B2B- und B2C-Anwendungen bereitzustellen, wodurch verhindert wird, dass externe Benutzer auf interne Daten zugreifen. Enterprise-Anwender (Mitarbeiter) müssen über die interne Rolle verfügen, während Enterprise-Anwender (Nicht-Mitarbeiter) über die externe Rolle verfügen müssen.

Wenn Sie das Plugin für die explizite Rolle installieren:

- Sie weist allen vorhandenen Benutzern die neue Rolle snc_internal zu. Außerdem werden alle Tabellen ohne Rolle mit der Rolle „snc_internal“ zugewiesen.
- Wenn Sie einen Anwender oder eine Tabelle erstellen, nachdem Sie das Plugin „Explicit Role“ aktiviert haben, weist Now Platform dem Anwender oder der Tabelle die Rolle snc_internal zu.
- Das Now Platform verhindert, dass Benutzer mit der Rolle „snc_external“ auf eine Tabelle zugreifen, die nicht explizit mit der Rolle „snc_external“ zugewiesen ist.
- Auf Tabellen mit der öffentlichen Rolle können sowohl interne als auch externe Benutzer zugreifen.
- Einige Serviceportal-Widgets erfordern eine Anmeldung, aber keine bestimmten Anwenderrollen. Nach der Installation des Plugins für explizite Rollen sind diese Portale für externe Anwender nicht mehr zugänglich.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- ◦ Um den Zugriff für externe Benutzer zu ermöglichen, bearbeiten Sie Ihr Widget, um die erforderlichen Rollen von „ **leer** “ in **„snc_internal“ und „snc_external“**zu ändern.
  - ◦ Ein Beispiel für dieses Problem sind Kunden, die die Fallverwaltungsanwendung verwenden und möchten, dass externe Benutzer Dateien an ihre Falldatensätze anhängen können. Wenn Sie die Konfiguration für das Widget „ **cryption-context-auswahl** “ wie beschrieben ändern, können externe Benutzer wie erwartet anhängen.
  - ◦ Weitere Informationen zum Konfigurieren von Widgets finden Sie unter Widget-Instanzoptionen konfigurieren

Hinweis: Verschieben Sie keine System-Update Sets zwischen Instanzen, unabhängig davon, ob das Plugin „Explicit Roles“ aktiviert oder deaktiviert ist. Weitere Informationen finden Sie unter System-Update Sets .

Rollenzusammenfassung

snc_internal

Diese Rolle wird allen internen Anwendern (Mitarbeiter oder intern für eine Organisation) zugewiesen. Jeder neue Anwender, der hinzugefügt wird, erhält diese Rolle auch bei der ersten Anmeldung/dem ersten Identitätswechsel, sofern dem Anwender nicht bereits die Rolle „snc_external“ zugewiesen ist. Alle vorhandenen Zugriffssteuerungsregeln (ACLs) ohne Rolle werden mit der Rolle „snc_internal“ gepatcht. Bei neuen ACLs fügt Now Platform diese Rolle automatisch hinzu, wenn die ACL ohne Rolle gespeichert wird.

snc_external

Diese Rolle gibt an, dass sich der Anwender außerhalb Ihrer Organisation befindet und keinen Zugriff auf Ressourcen haben sollte, es sei denn:

- Sie gestatten den Zugriff explizit über ACLs für die Rolle snc_external oder
- Sie gewähren ihnen explizit zusätzliche Rollen.

Standardmäßig können Benutzer mit der Rolle „snc_external“ nicht auf Ressourcen ohne Datensätze zugreifen, z. B. auf Prozessoren und UI-Seiten.

Öffentlich

Alle Entitäten mit zugewiesener öffentlicher Rolle sind für snc_internal- und snc_external-Benutzer zugänglich.

Bei Verwendung des Plugins „Explicit Role“:

1. Überprüfen und validieren Sie, dass eine Tabelle mit der öffentlichen Rolle keine vertraulichen Datensätze für externe Anwender (einschließlich nicht authentifizierter öffentlicher Anwender) enthält.
2. Wenn die Tabelle mit der Rolle „public“ vertrauliche Daten enthält und Sie die Verwendung vertraulicher Datensätze für externe Benutzer einschränken möchten, führen Sie eine der folgenden Optionen aus:
   - ◦ Entfernen Sie die öffentliche Rolle aus der Tabelle oder
   - ◦ Fügen Sie der Tabelle eine zusätzliche geskriptete ACL hinzu.
3. Überprüfen und validieren Sie, ob alle Endpunkte, z. B. die geskripteten REST APIs, die Rollen *`GlideRecordSecure`* verwenden oder explizit Rollen mit `canRead()`, `canWrite()`, `canUpdate()` und `canDelete() überprüfen`.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Plugin-Name	com.glide.explicit_roles
Konfigurationstyp	Systemdefinition > Plugin
Konfigurieren Sie im Instanz-Sicherheitszentrum	Nein
Zweck	Um zu verhindern, dass externe Benutzer auf interne Daten zugreifen.
Empfohlener Wert	Aktiv
Funktionale Auswirkung	(Niedrig) Keine signifikanten Auswirkungen, da das Plugin der Tabelle automatisch die Rolle „snc_internal“ zuweist, sodass die vorhandenen internen Benutzer weiterhin über den erforderlichen Zugriff verfügen.
Sicherheitsrisiko	(Hoch) Externe Anwender (Nicht-Mitarbeiter) können auf viele vertrauliche Tabellen in Now Platform zugreifen, denen keine Rollen zugewiesen sind. Sie sollen nur internen Benutzern (Mitarbeitern) zugänglich sein.
Referenzen	Explizite Rollen

Schritte zum Konfigurieren von

Beim Erstellen einer Funktion oder Anwendung mit den expliziten Rollen:

1. Erstellen Sie eine Rolle, die die Rolle snc_external für Ihre neue Funktion oder Anwendung erbt.
2. Wenn Sie einen externen Benutzer erstellen, entfernen Sie die Rolle „snc_internal“ und fügen Sie die neu erstellte Rolle hinzu, die die Rolle „snc_external“ erbt.
3. Wenn Sie der vorhandenen Tabelle die neue Rolle hinzufügen, die die Rolle „snc_external“ erbt, überprüfen und validieren Sie, dass die Tabelle keine vertraulichen Datensätze enthält.
4. Validieren Sie beim Erstellen einer Tabelle, dass auf die Tabelle nur autorisierte interne und externe Anwenderrollen zugreifen können.
5. Wenn Sie Endpunkte wie die Scripted REST API erstellen, verwenden Sie GlideRecordSecure, oder überprüfen Sie Rollen explizit mit `canRead()`, `canWrite()`, canUpdate() und `canDelete()`.

Stellen Sie beim Erstellen einer Tabelle mit der Rolle „public“ sicher, dass die Tabelle keine vertraulichen Datensätze für die externen Anwender enthält, einschließlich nicht authentifizierter öffentlicher Anwender.

Autorisierung der Importanforderung (Instanzsicherheitshärtung)

Verwenden Sie die Eigenschaft *`glide.basicauth.required.importprocessor`*, um festzulegen, ob für eingehende Importanforderungen eine Standardauthentifizierung erforderlich sein soll.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.basisauth.erforderlich.importprozessor
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Erzwingen der Standardauthentifizierung bei Importanforderungen.
Empfohlener Wert	wahr
Funktionale Auswirkung	(Niedrig) Diese Korrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Standardauthentifizierung und Zugriffssteuerung auf Systemebene. • Diese Authentifizierung wird beim Importieren von Datenquellen in die Instanztabellen/-seiten durchgeführt. • Sie schränkt alle Gastanwender ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Anwender erstellen, die Zugriff auf diesen Inhalt benötigen, mit den erforderlichen Zugriffssteuerungsberechtigungen. Weitere Informationen finden Sie unter Daten aus einer CSV-formatierten Datei abrufen .
Sicherheitsrisiko	(Mittel) Wenn keine entsprechende Autorisierung für die Importanforderungen der Datenquelle konfiguriert ist, kann ein nicht autorisierter Anwender Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.
Referenzen	Sicherheit von SOAP-Webservices SOAP-Webservice

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Autorisierung von PDF-Anforderungen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.basicauth.required.pdf*, um festzulegen, ob für eingehende PDF-Anforderungen eine Standardauthentifizierung erforderlich sein soll.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.basicauth.required.pdf
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um die Standardauthentifizierung für PDF-Anforderungen zu erzwingen.
Empfohlener Wert	wahr
Funktionale Auswirkung	(Niedrig) Diese Korrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Standardauthentifizierung und Zugriffssteuerung auf Systemebene. • Es führt diese Authentifizierung durch, während Daten aus Tabellen/Seiten in Form von PDF-Daten in der Instanz abgerufen werden. • Sie schränkt alle Gastanwender ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Anwender erstellen, die Zugriff auf diesen Inhalt benötigen, mit den erforderlichen Zugriffssteuerungsberechtigungen. Weitere Informationen finden Sie unter Webservice-Importsätze .
Sicherheitsrisiko	(Mittel) Wenn keine entsprechende Autorisierung für die eingehenden PDF-Anforderungen konfiguriert ist, kann ein nicht autorisierter Anwender Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Leistungsüberwachung (ACL) (Instanzsicherheitshärtung)

Verwenden Sie die Eigenschaft *glide.security.diag_txns_acl*, um den Zugriff auf „stats.do“, „threads.do“, „thread_pool_stats“ und „replication.do“ über eine nicht authentifizierte Verbindung zu steuern.

Wenn Sie diese Eigenschaft auf „ **true**“ festlegen, ermöglicht die Eigenschaft *glide.security.diag_txns_acl* nur den Zugriff auf Folgendes durch das Administratorkonto:

- https://<instancename>.servicenow.com/stats.do
- https://<instancename>.servicenow.com/threads.do
- https://<instancename>.servicenow.com/replication.do
- https://<instancename>.servicenow.com/thread_pool_stats.do

Ohne diese Einstellung zu aktivieren, ist es weiterhin möglich, über eine nicht authentifizierte Verbindung auf diese Ressourcen zuzugreifen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.security.diag_txns_acl
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Beschränken Sie den Zugriff auf Konfigurationsseiten auf das Administratorkonto
Empfohlener Wert	wahr
Funktionale Auswirkung	(Niedrig) Diese Korrektur erzwingt, dass nur der Administratoraccount zu Protokollierungs- und Problembehandlungszwecken Zugriff auf die vertraulichen Anwendungsdaten erhält.
Sicherheitsrisiko	(Niedrig) Sensible Daten wie Serverdetails, Threads und Prozesse, die auf dem Server ausgeführt werden, sollten für Endanwender ohne entsprechende Berechtigungen niemals sichtbar oder zugänglich sein.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

IP-Beschränkung für Leistungsüberwachung (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.custom.ip.authenticate.allow*, um nur einer angegebenen kommagetrennten Liste oder einem bestimmten IP-Adressenbereich den Zugriff auf die Seiten stats.do, threads.do und replication.do zu ermöglichen. Wenn diese Eigenschaft nicht aktiviert ist, ist ein Zugriff auf diese Seitentypen von jeder IP-Adresse möglich.

Hinweis: Basierend auf einigen kürzlichen Änderungen muss die IP-Adresszugriffssteuerung für alle IP-Einschränkungen verwendet werden. Weitere Informationen finden Sie im Abschnitt „Konfigurationsschritte“ in Zugriff auf bestimmte IP-Bereiche beschränken.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.custom.ip.authenticate.allow
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Nein
Zweck	Beschränken Sie den Zugriff nur auf Konfigurationsseiten auf die IP-Adressen in der Aufnahmeliste.
Empfohlener Wert	Kommagetrennte Liste der IP-Adressen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Funktionale Auswirkung	Auf (niedrig) Seiten mit vertraulichen Informationen kann auch von einer nicht vertrauenswürdigen IP-Adresse aus zugegriffen werden.
Sicherheitsrisiko	(Niedrig) Die unnötige Offenlegung der Zielinstanz im Internet sollte mithilfe der IP-Zugriffssteuerungsfunktion eingeschränkt werden.
Referenz	Verfügbare Systemeigenschaften

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Datenschutz für vom Client aufrufbare Skripteinbindungen (Härtung der Instanzsicherheit)

Standardmäßig sind vom Client aufrufbare Skripteinbindungen, die die Sichtbarkeit nicht explizit festlegen, öffentlich. Fügen Sie bei Bedarf die Eigenschaft *glide.script.ccsi.ispublic* hinzu, um die Datenschutzsteuerung für alle vom Client aufrufbaren Skripteinbindungen zu aktivieren, auf die von öffentlichen Seiten zugegriffen wird.

Wenn Sie diese Eigenschaft hinzufügen, müssen Sie den Wert auf **false**festlegen. Dadurch werden alle vom Client aufrufbaren Skripteinbindungen als privat festgelegt und ihre Sichtbarkeit auf öffentlichen Seiten geändert.

Hinweis: Sie können die Eigenschaft nicht mit dem Wert **true**hinzufügen oder ihren Wert von **false** in **true**ändern. Wenn Sie dies versuchen, wird eine Fehlermeldung angezeigt.

Bei Bedarf können Sie die Datenschutzeinstellung für eine einzelne vom Client aufrufbare Skripteinbindung ändern, indem Sie die Funktion `isPublic()` hinzufügen.

- Die Einstellung „`isPublic()`“ hat Vorrang vor der Eigenschaft *glide.script.ccsi.ispublic*.
- Wenn Sie beispielsweise `isPublic()` in einem einzelnen Skript auf „ **true** “ festlegen, wird es öffentlich gemacht. Dadurch wird die Eigenschaft *glide.script.ccsi.ispublic* überschrieben, die alle anderen vom Client aufrufbaren Skripteinbindungen privat macht.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.script.ccsi.ispublic
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Das Festlegen von vom Client aufrufbaren Skripteinbindungen als privat bedeutet, dass Gäste, die auf öffentliche Seiten zugreifen, nicht auf die vom Client aufrufbare Skripteinbindung zugreifen können. Ein nicht angemeldeter Anwender kann kein privates Skript ausführen.
Empfohlener Wert	falsch

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Funktionale Auswirkung	(Hoch) Wenn die vom Client aufrufbaren Skripteinbindungen als öffentlich gekennzeichnet sind (d. h. diese Eigenschaft fehlt), können nicht authentifizierte Benutzer Client-Skripts ausführen. Fügen Sie die Eigenschaft hinzu, die die Ausführung von Skripts durch einen nicht angemeldeten Benutzer einschränkt.
Sicherheitsrisiko	(Hoch) Wenn Sie diese Eigenschaft nicht hinzufügen, werden clientseitige Skripteinbindungen umgangen, was zu unbeabsichtigten öffentlichen Funktionen führen kann. Wenn das Client-Skript vertrauliche Informationen bereitstellt, kann dies ein nachteiliges potenzielles Sicherheitsrisiko darstellen.
Workaround	Wenn Sie die Eigenschaft *glide.script.ccsi.ispublic* auf „ **false** “ setzen, werden alle vom Client aufrufbaren Skripteinbindungen privat. Sie können die Datenschutzeinstellung für eine einzelne vom Client aufrufbare Skripteinbindung ändern, indem Sie die Funktion `isPublic()` hinzufügen. Die Funktion `isPublic` hat Vorrang vor der Eigenschaft *glide.script.ccsi.ispublic*. Fügen Sie der Skripteinbindung die folgende Syntax hinzu: `isPublic:function(){return[wahr/falsch];},`

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Öffentlichen Zugriff auf Favoriten deaktivieren

Geben Sie mit *glide.ui.magellan.favorites.allow_public* an, ob nicht authentifizierte Benutzer **Favoriten** im Navigator anzeigen dürfen.

Öffentlicher Zugriff auf Favoriten ist konform, wenn *glide.ui.magellan.favorites.allow_public* auf „ **false**“ festgelegt ist.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.ui.magellan.favorites.allow_public*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Steuern Sie, ob nicht authentifizierte Anwender **Favoriten** im Navigator anzeigen dürfen.
Typ	wahr/falsch

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Empfohlener Wert	*false*
Sicherheitsabhängigkeiten	Legen Sie *glide.ui.magellan.favorites.allow_public* auf „ **falsch**“ fest.
Funktionale Auswirkung	(Mittel) Das Aktivieren dieser Eigenschaft dient als Schutzschicht vor nicht autorisierten Anwendern.
Sicherheitsrisiko	(Mittel) Wenn diese Eigenschaft nicht aktiviert ist, besteht das Risiko eines nicht autorisierten Zugriffs auf vertrauliche Daten.
Referenzen	Favoriten erstellen oder anzeigen

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Zugriff auf bestimmte IP-Bereiche beschränken (Instanzsicherheitshärtung)

Verwenden Sie die Eigenschaft *com.snc.ipauthenticator*, um den Zugriff auf bestimmte IP-Bereiche zu beschränken. Sofern kein öffentlicher Zugriff für die Instanz vorgesehen ist, sollten Administratoren den Zugriff auf die ihnen zugewiesenen IP-Netzblöcke beschränken.

Voraussetzungen

Bevor Sie diese Eigenschaft festlegen, müssen Sie das Plugin „Auf dem IP-Adressbereich basierende Authentifizierung *com.snc.ipauthenticator*“ aktivieren. Weitere Informationen finden Sie unter Authentifizierung mit IP-Adressbereich und im Abschnitt „Schritte zum Konfigurieren“ (unten).

Weitere Informationen

Attribut	Beschreibung
Plugin-Name	com.snc.ipauthenticator
Konfigurationstyp	System Security > IP-Adressen-Zugriffssteuerung
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um den Bereich der IP-Adressen, die auf die Instanz zugreifen können oder nicht, zur Liste der vertrauenswürdigen und nicht vertrauenswürdigen Domänen hinzuzufügen.
Empfohlener Wert	Aktiv
Funktionale Auswirkung	(Niedrig) Für dieses Korrekturelement werden vom Kunden verweigerte IP-Bereiche verwendet. Keine Auswirkung, da der Kunde die Zielliste definiert.
Sicherheitsrisiko	(Niedrig) Die unnötige Offenlegung der Zielinstanz im Internet sollte mithilfe der IP-Zugriffssteuerungsfunktion eingeschränkt werden.
Referenzen	Authentifizierung mit IP-Adressbereich

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schritte zum Konfigurieren von

1. Stellen Sie sicher, dass das Plugin „com.snc.ipauthenticator“ aktiv ist.
2. Navigieren zu **Systemsicherheit** > **IP-Adressen-Zugriffssteuerung**an.
3. Klicken Sie auf **Neu**, um eine Ausschlussliste (Deny) oder eine Aufnahmeliste (Allow) von IP-Adressen zu erstellen.
4. Klicken Sie auf **Absenden**.

Autorisierung von RSS-Anforderungen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.basicauth.required.rss*, um festzulegen, ob für eingehende RSS-Anforderungen eine Standardauthentifizierung erforderlich sein soll.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.basicauth.required.rss
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um die Standardauthentifizierung für RSS-Anforderungen zu erzwingen.
Empfohlener Wert	wahr
Funktionale Auswirkung	(Niedrig) Diese Korrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Standardauthentifizierung und Zugriffssteuerung auf Systemebene. • Diese Authentifizierung wird bei der Verarbeitung von RSS-Anforderungen in der Instanz durchgeführt. • Sie schränkt alle Gastanwender ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Anwender erstellen, die Zugriff auf diesen Inhalt benötigen, mit den erforderlichen Zugriffssteuerungsberechtigungen. Weitere Informationen finden Sie unter RSS-Feed-Generator .
Sicherheitsrisiko	(Mittel) Wenn keine entsprechende Autorisierung für die eingehenden RSS-Anforderungen konfiguriert ist, kann ein nicht autorisierter Anwender Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.
Referenzen	RSS-Basic Authentication

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SSO-Profil für SAML 2.0-Webbrowser (Instanzsicherheitshärtung)

Das Plugin *com.snc.integration.sso.saml20.update1* stellt sicher, dass der Status des SAML 2.0 Single Sign-on-Plugins aktiv ist.

Security Assertion Markup Language (SAML) ist ein XML-basierter Standard für den Austausch von Authentifizierungs- und Autorisierungsdaten zwischen Sicherheitsdomänen. SAML tauscht Sicherheitsinformationen zwischen einem Identitätsanbieter (einem Ersteller von Assertionen) und einem Service Provider (einem Verbraucher von Assertionen) aus.

Das Plugin *com.snc.integration.sso.saml20.update1* ist ein erforderliches Plugin, Sie müssen es jedoch nicht manuell aktivieren. *sso.multi.installer* installiert alle erforderlichen SAML-bezogenen Plugins und enthält auch SAML2-Implementierungsskripts, die Optionen für die Antwortvalidierung bieten. Weitere Informationen finden Sie in den Themen unter Referenzen in Weitere Informationen.

Weitere Informationen

Attribut	Beschreibung
Plugin-Name	com.snc.integration.sso.saml20.update1 (neu)
Konfigurationstyp	Systemdefinition > Plugins
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Zur Verhinderung von Cross Site Scripting-Angriffen.
Empfohlener Wert	Aktiv
Erforderliche Rolle	Ihr Administrator kann das Plugin nicht aktivieren. Fordern Sie die Person mit erhöhten Sicherheitsberechtigungen an, diese in der Instanz zu aktivieren.
Referenzen	Authentifizierung mit SAML- SAML Integration Aktualisieren Sie Ihre vorhandene SAML 2.0-Integration

Weitere Informationen zum Aktivieren von Plugins finden Sie unter Plugins aktivieren .

Autorisierung von Skript-Anforderungen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.basicauth.required.scriptedprocessor*, um festzulegen, ob für eingehende Skriptanforderungen eine Standardauthentifizierung erforderlich sein soll.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.basicauth.required.scriptedprocessor
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Erzwingen der Standardauthentifizierung für Skriptanforderungen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Empfohlener Wert	wahr
Funktionale Auswirkung	(Mittel) Diese Korrektur erzwingt die Authentifizierung in Form von Standardautorisierung. • Diese Authentifizierung wird bei der Verarbeitung von Skriptanforderungen in der Instanz durchgeführt. • Sie schränkt alle Gastanwender ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Anwender erstellen, die Zugriff auf diesen Inhalt benötigen, mit den erforderlichen Zugriffssteuerungsberechtigungen.
Sicherheitsrisiko	(Hoch) Ohne entsprechende Konfiguration der Autorisierung für eingehende Skriptanforderungen greift ein nicht autorisierter Anwender auf vertrauliche Inhalte/Daten in der Zielinstanz zu.
Referenzen	Authentifizierung

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Sicherheits-Jump-Start (ACL-Regeln) (Instanzsicherheitshärtung)

Aktivieren Sie das Plugin „Security Jump Start (ACL Rules)“ (*com.snc.system_security*), um mehrere wichtige ACLs zu erstellen, die die Zugriffssteuerungen für einige der wichtigsten Systemtabellen in Now Platformvalidieren.

Diese Regeln bieten eine Starthilfe für die Sicherung vieler Systemtabellen und erleichtern es einer Organisation, eine Instanz in die Produktion zu bringen. Das Plugin „Security Jump Start (ACL Rules)“ wird automatisch auf allen neuen Instanzen installiert.

Weitere Informationen

Attribut	Beschreibung
Plugin-ID	com.snc.system_security
Konfigurationstyp	Systemdefinition > Plugins
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Aktivieren Sie das Plugin „Security Jump Start (ACL Rules)“, um eine ordnungsgemäße Sicherheits-Compliance zu erreichen. Sie stellt einige grundlegende ACLs bereit, die Systemtabellen von Anfang an sichern, anstatt sie manuell für jede Systemtabelle zu erstellen, die mit der Standardbereitstellung einer Instanz einhergeht. Diese ACLs sind hilfreich, wenn die neu erstellte Instanz schnell in die Produktion wechseln muss.
Empfohlener Wert	Aktiv

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Funktionale Auswirkung	(Mittel) Es gibt erhebliche funktionale Auswirkungen, wenn dieses Plugin ohne Audit der vorhandenen ACLs in der Instanz installiert wird. Bevor die Korrektur durchgeführt werden kann, sind eine Kontaktaufnahme mit dem Kunden und Definitionen erforderlich.
Sicherheitsrisiko	(Hoch) Die Zugriffssteuerung sollte erzwungen werden, um den unbeabsichtigten Zugriff auf die Instanz zu sperren. ACL-Jumpstart-Regeln wurden erstellt, um einen Ausgangspunkt für das Sichern vieler Systemtabellen zu bieten, damit eine Organisation schnell in die Produktion gehen kann.
Referenzen	Sicherheitshilfe – ACL-Regeln

Schritte zum Konfigurieren von

Wenn dieses Plugin in Ihrer -Instanz nicht aktiviert ist, wenden Sie sich an den ServiceNow Support. Durch die Aktivierung des Plugins an dieser Stelle kann sich der Sicherheitszugriff auf Tabellen ändern, die bereits in einer Produktionsumgebung verwendet werden. Wenn ein Administrator an den neuen ACL-Regeln interessiert ist, die das Plugin bereitstellt, können Sie eine oder mehrere davon bei Bedarf manuell in einer vorhandenen Instanz erstellen. Diese Liste von ACLs kann in diesem Fall als Leitfaden verwendet werden.

Weitere Informationen zum Aktivieren von Plugins finden Sie unter Plugins aktivieren .

Plugin „SNC Access Control“ (Härtung der Instanzsicherheit)

Aktivieren Sie das Plugin „SNC Access Control“ (*com.snc.snc_access_control*), um den Zugriff auf Ihre Instanzen durch Mitarbeiter von Kundenservice und Support zu steuern.

Die Standardkonfiguration für Now Platform ermöglicht dem Kundenservice und dem Support den Zugriff auf -Instanzen über einen internen Prozess, der Anmeldeinformationen für den kurzfristigen Support erstellt. Obwohl jeder Zugriff geprüft wird, ziehen es einige Kunden vor, diesen Zugriff zu kontrollieren.

Mit diesem Plugin kann der Kundenadministrator den Kundenservice und Support -Mitarbeitern den Zugriff auf die Instanz untersagen. Diese Entscheidung wirkt sich auf Support-SLAs aus, da Sie den Zugriff Now Platform aktivieren müssen, bevor Support-Aktivitäten beginnen können. Weitere Informationen finden Sie unter ServiceNow-Zugriffssteuerung.

Weitere Informationen

Attribut	Beschreibung
Plugin-Name	com.snc.snc_access_control
Konfigurationstyp	Systemdefinition > Plugins
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Verbietet Mitarbeitern Kundenservice und Support den Zugriff auf die Instanz
Empfohlener Wert	Aktiv

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Erforderliche Rolle	Der Kundenadministrator kann dieses Plugin nicht aktivieren. Es muss explizit angefordert werden, da es erweiterte Berechtigungen zum Aktivieren des Plugins erfordert.
Funktionale Auswirkung	(Niedrig) Wenn dieses Plugin inaktiv ist, können alle Kundenservice und Support -Mitarbeiter auf die Instanz des Kunden zugreifen. Durch Aktivieren des Plugins kann der Kunde den Zugriff auf autorisierte Mitarbeiter von Kundenservice und Support beschränken.
Sicherheitsrisiko	(Niedrig) Unnötige Offenlegung des Instanzzugriffs für eine größere Gruppe von Personen.
Referenzen	ServiceNow-Zugriffssteuerung

Schritte zum Konfigurieren von

1. Um das Plugin anzufordern, führen Sie die Schritte in Die Zugriffssteuerung ServiceNow wird aktiviertaus. Kunden müssen das Plugin „SNC Access Control“ (com.snc.snc_access_control) von HI anfordern.
2. Führen Sie zum Aktivieren der SNC-Zugriffssteuerung die Schritte in Die Zugriffssteuerung für ServiceNow wird konfiguriertaus. Konfigurieren Sie einen Zugriffssteuerungsdatensatz, um einen oder mehrere Kundenservice und Support Mitarbeiter anzugeben, die berechtigt sind, sich bei Ihrer -Instanz anzumelden.

Überprüfung des SOAP-Inhaltstyps (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.soap.require_content_type_xml*, um die Validierung eines Inhaltstyps als Text/XML zu aktivieren und vor ungültigen SOAP-Anforderungen zu schützen.

- Bei Festlegung auf **true**validiert Now Platform den Inhaltstyp als Text/XML und schützt vor ungültigen SOAP-Anforderungen.
- Bei Festlegung auf „ **false**“ ist jeder Inhaltstypwert zulässig.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.soap.require_content_type_xml
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Vor ungültigen SOAP-Anforderungen schützen
Empfohlener Wert	wahr
Funktionale Auswirkung	(Niedrig) Diese Korrektur ermöglicht die Validierung des SOAP-Inhaltstyps für alle eingehenden SOAP-Anforderungen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Wenn Sie für eingehende Anforderungen einen anderen Inhaltstyp als Text/XML verwenden, kann dies zu einem potenziellen Fehler bei SOAP-Transaktionen führen. • Wenn Sie nicht den richtigen MIME-Typ verwenden, kann dies zu Störungen bei Integrationen von Drittanbietern führen.
Sicherheitsrisiko	(Hoch) Bei der Annahme eingehender SOAP-Anforderungen wird die entsprechende Validierung durchgeführt, um sicherzustellen, dass der relevante Inhaltstyp als Teil der Anforderung definiert wird. Sie schränkt die ungültigen SOAP-Antworten ein, die als Sicherheitsrisiko angesehen werden können.
Referenz	Inhaltstypen

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Strikte IP-Beschränkung (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *`glide.ip.authenticate.strict`*, um einem strikten Satz von IP-Adressen, z. B. DC und sicherem VPN, den Zugriff auf diese Instanz zu ermöglichen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ip.authentifizieren.strikt
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Ermöglicht ServiceNow-Mitarbeitern, nur über einen gesicherten Satz von IP-Bereichen auf die Instanz zuzugreifen
Empfohlener Wert	wahr
Funktionale Auswirkung	(Niedrig) Wenn diese Eigenschaft nicht aktiviert ist, können ServiceNow-Mitarbeiter über alle IP-Bereiche auf die Instanz des Kunden zugreifen. Durch Aktivieren der Eigenschaft wird der Zugriff auf einen sicheren Satz von IP-Bereichen (sicheres VPN, DC) eingeschränkt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Hinweis: Wenn Sie diese Eigenschaft auf „true“ festlegen, verwendet Now Platform] anstelle der IP-Beschränkung für die Leistungsüberwachung eine restriktivere *glide.ip.authenticate.allow.secured* -Eigenschaft. Diese Eigenschaft kann nicht überschrieben werden.*glide.ip.authenticate.allow.secured*)-Eigenschaft für eine Reihe von IP-Bereichen, die auf die Instanz zugreifen können.
Sicherheitsrisiko	(Niedrig) Unnötige Offenlegung des Instanzzugriffs für eine größere Gruppe von Personen.
Referenz	Authentifizierung mit IP-Adressbereich

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Hinweis: Die Regel „Alle verweigern“ muss der IP-Zugriffssteuerung hinzugefügt werden, um den Zugriff von IPs einzuschränken, die nicht der IP-Zugriffssteuerung hinzugefügt wurden. Alle erforderlichen zulässigen IPs müssen dann der IP-Zugriffssteuerung hinzugefügt werden.

Autorisierung von Entlade-Anforderungen (Instanzsicherheitshärtung)

Verwenden Sie die Eigenschaft *glide.basicauth.required.unl* (useUnloadFormat), um festzulegen, ob für eingehende Entladeanforderungen eine Standardauthentifizierung erforderlich sein soll.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.basicauth.required.unl
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Zum Erzwingen der Standardauthentifizierung bei Entladeanforderungen.
Empfohlener Wert	wahr
Funktionale Auswirkung	(Mittel) Diese Korrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Standardauthentifizierung und Zugriffssteuerung auf Systemebene. Diese Authentifizierung wird beim Abrufen von Daten aus Tabellen/Seiten in Form von Entladedaten in der Instanz durchgeführt.
Sicherheitsrisiko	(Hoch) Wenn keine entsprechende Autorisierung für die Entladeanforderungen für Datenquellen konfiguriert ist, kann ein nicht autorisierter Anwender

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.
Referenzen	Authentifizierung

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Autorisierung von WSDL-Anforderungen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.basicauth.required.wsdl*, um festzulegen, ob für eingehende WSDL-Anforderungen (Web Services Description Language) eine Standardauthentifizierung erforderlich sein soll.

Hinweis: Wenn Sie keine Standardauthentifizierung für eingehende WSDL-Anforderungen vorschreiben möchten, müssen Sie die Regeln für die Zugriffssteuerung (ACL) ändern, um Gastbenutzern den Zugriff auf WSDL-Inhalt zu ermöglichen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.basicauth.required.wsdl
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um die Standardauthentifizierung für WSDL-Anforderungen zu erzwingen.
Empfohlener Wert	wahr
Funktionale Auswirkung	(Niedrig) Diese Korrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Standardauthentifizierung und Zugriffssteuerung auf Systemebene. • Diese Authentifizierung wird durchgeführt, während Daten aus Tabellen/Seiten in Form von WSDL-Daten in der Instanz abgerufen werden. • Sie schränkt alle Gastanwender ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Anwender erstellen, die Zugriff auf diesen Inhalt benötigen, mit den erforderlichen Zugriffssteuerungsberechtigungen.
Sicherheitsrisiko	(Mittel) Wenn keine entsprechende Autorisierung in den WSDL-Webservices konfiguriert ist, kann ein nicht autorisierter Anwender Zugriff auf vertrauliche WSDL-Inhalte/-Daten in der Zielinstanz erhalten.
Referenzen	Webservice – Sicherheit

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Autorisierung von XML-Anforderungen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.basicauth.required.xml*, um anzugeben, ob für eingehende XML-Anforderungen eine Standardauthentifizierung erforderlich sein soll.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.basicauth.required.xml
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Erzwingen der Standardauthentifizierung für XML-Anforderungen.
Empfohlener Wert	wahr
Funktionale Auswirkung	(Niedrig) Diese Korrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Standardauthentifizierung und Zugriffssteuerung auf Systemebene. • Es führt diese Authentifizierung durch, während es Daten aus Tabellen/Seiten in Form von XML-Daten in der Instanz abruft. • Sie schränkt alle Gastanwender ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Anwender erstellen, die Zugriff auf diesen Inhalt benötigen, mit den erforderlichen Zugriffssteuerungsberechtigungen. Weitere Informationen finden Sie unter XML-Parser-Schritt .
Sicherheitsrisiko	(Mittel) Wenn keine entsprechende Autorisierung für die eingehenden XML-Anforderungen konfiguriert ist, kann ein nicht autorisierter Anwender Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.
Referenzen	Authentifizierung

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Autorisierung von XSD-Anforderungen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.basicauth.required.xsd*, um festzulegen, ob für eingehende XSD-Anforderungen (XML-Schemadefinition) eine Standardauthentifizierung erforderlich sein soll.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.basisauth.erforderlich.xsd
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um die Standardauthentifizierung für XSD-Anforderungen zu erzwingen.
Empfohlener Wert	wahr
Funktionale Auswirkung	(Niedrig) Diese Korrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Standardauthentifizierung und Zugriffssteuerung auf Systemebene. • Es führt diese Authentifizierung durch, während Daten aus Tabellen/Seiten im Formular von XSD-Daten in der Instanz abgerufen werden. • Sie schränkt alle Gastanwender ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Anwender erstellen, die Zugriff auf diesen Inhalt benötigen, mit den erforderlichen Zugriffssteuerungsberechtigungen. Weitere Informationen finden Sie unter Nicht interaktive Sitzungen .
Sicherheitsrisiko	(Mittel) Wenn keine entsprechende Autorisierung für die eingehenden XSD-Anforderungen konfiguriert ist, kann ein nicht autorisierter Anwender Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.
Referenzen	Authentifizierung

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Anhänge (Härtung der Instanzsicherheit)

Viele Now Platform Geschäftsprozesse ermöglichen das Hochladen von Daten/Informationen. Es überprüft regelmäßig die Gültigkeit und Sicherheit von Text, aber die Annahme dieser Dateien kann noch höhere Risiken bergen.

Um das Risiko zu verringern, sollten Sie auf schädliche Dateien validieren, damit Now Platform ordnungsgemäß vor Angreifern schützen kann, die diese Dateien senden. Sie verarbeiten diese Dateien, indem Sie eine Geschäftslogik einbinden, die Dateien während des Upload-Vorgangs scannt und die als schädlich erkannten Dateien ablehnt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Interne Referenzen

- Anhänge werden verwaltet
- Konfigurieren Sie die Systemeigenschaften von Anhängen

Herunterladbare MIME-Typen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.ui.attachment.download_mime_types*, um eine Liste von kommagetrennten MIME-Anhangtypen anzugeben, die heruntergeladen, aber nicht inline im Browser gerendert werden sollen.

Um eine Liste vorhandener MIME-Typen anzuzeigen, `geben Sie / sys_attachment_icon_rule_list.do ein`. Sie können jeden dieser MIME-Typen aktivieren, um die Sicherheits-Compliance-Anforderungen in Now Platformzu erfüllen.

Hinweis: Wenn Sie die Eigenschaft „ **Download MIME-Typen** erzwingen“ auf **true**festlegen, wird die Eigenschaft Herunterladbare **MIME** -Typen überschrieben, bei der es sich um eine durch Kommas getrennte Liste herunterladbarer MIME-Typen handelt. Weitere Informationen finden Sie unter Download von MIME-Typen erzwingen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.attachment.download_mime_types
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um die Darstellung der Dateitypen im Browser einzuschränken, um die Ausführung versteckter schädlicher Skripts zu vermeiden.
Empfohlener Wert	Einige definierte Dateitypen, z. B. text/html,text/csv.
Funktionale Auswirkung	(Niedrig) Diese Korrektur erzwingt die Leistung von Validierungsprüfungen, bevor eine Aktion ausgeführt wird, wenn Sie in einer Anwendung Now Platform auf einen Anhang klicken. Es gibt keine potenziellen Auswirkungen, aber die Anwender-Experience wird geändert.
Sicherheitsrisiko	(Mittel) Client-seitige Skripting-Angriffsvektoren gibt es in verschiedenen Varianten, und der Missbrauch von MIME-Typanhängen ist keine Ausnahme. Angreifer können MIME-Typen missbrauchen und unbeabsichtigte Skriptinhalte im Anhang auf der Seite des Opfers platzieren, um vertrauliche Informationen zu erfassen. Füllen Sie die Eigenschaft im aktuellen Kontext mit einer Liste kommagetrennter MIME-Typen für Anhänge aus, die nicht inline im Browser gerendert werden sollen. Beispiel: text/html

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Deny-Liste für Anhänge aktivieren (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.security.attachment_type.use_blacklist*], um anzugeben, ob Now Platform den Anhang anhand einer angegebenen Ausschlussliste validieren soll.

Hinweis: Legen Sie die Eigenschaft *glide.security.attachment_type.use_blacklist* erst dann auf „ `true` “ fest, wenn Sie die Eigenschaften *glide.attachment.blacklisted.extensions* und *glide.attachment.blacklisted.types* konfiguriert haben. Weitere Informationen finden Sie unter Geben Sie abgelehnte Erweiterungen an und Geben Sie die abgelehnten Dateitypen an.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.security.attachment_type.use_blacklist
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Hochladen (Einfügen/Schreiben/Aktualisieren) von Anhängen mit fragwürdigen Dateierweiterungen und Dateitypen wie exe, dll, JAR, Text/HTML einschränken.
Empfohlener Wert	wahr
Funktionale Auswirkung	(Niedrig) Keine Beeinträchtigung der Funktionalität, es sei denn, es wird versucht, Dateierweiterungen oder Dateitypen hochzuladen, die unter den Eigenschaften auf der Ausschlussliste (*glide.attachment.blacklisted.extensions* und *glide.attachment.blacklisted.types*) angegeben sind.
Sicherheitsrisiko	(Mittel) Ein böswilliger Anwender kann mit Malware infizierte Anhänge mit gängigen ausführbaren Dateierweiterungen und/oder -typen hochladen.
Workaround	Im Basissystem sind Eigenschaften verfügbar, die das gleiche Problem mit Einschlusslisten anstelle von Ausschlusslisten beheben. Weitere Informationen finden Sie unter: • Dateierweiterungen einschränken • MIME-Typeinschränkung für Uploads

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einschränkungen beim Dateidownload aktivieren (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.ui.strict_customer_uploaded_static_content*, um Einschränkungen für die Dateitypen zu aktivieren, die heruntergeladen werden können, wenn sie mit der Funktion „Datei hochladen“ hochgeladen wurden.

Sie verwenden diese Eigenschaft mit der Eigenschaft *glide.ui.strict_customer_uploaded_content_types*, die eine durch Kommas getrennte Liste mit eingeschränkten herunterladbaren Dateitypen erstellt. Weitere Informationen finden Sie unter Herunterladbare Dateitypen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.strict_customer_uploaded_static_content
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Nein
Zweck	Um sicherzustellen, dass sichere Dateitypen aus der Anwendung heruntergeladen werden dürfen.
Empfohlener Wert	wahr
Funktionale Auswirkung	(Niedrig) Diese Korrektur erzwingt die Einschränkung von Dateidownloads basierend auf den Werten, die in der Eigenschaft *glide.ui.strict_customer_uploaded_content_types* angegeben sind. Weitere Informationen finden Sie unter Herunterladbare Dateitypen.
Sicherheitsrisiko	(Mittel) Dateidownload-Einschränkungen sollten auf alle nicht vertrauenswürdigen Benutzereingabequellen angewendet werden.

Strikten Upload von Anwenderbildern erzwingen (Instanzsicherheitshärtung)

Verwenden Sie die Eigenschaft *glide.security.strict.user_image_upload*, um die Zugriffssteuerung für das Hochladen/Aktualisieren eines Profilbilds zu aktivieren, wenn sie für einen Anwenderdatensatz ausgeführt wird.

Diese Einstellung ermöglicht es einem nicht autorisierten Anwender, ein Bild in das Profil eines anderen Anwenders hochzuladen.

- Wenn Sie diese Eigenschaft auf „ **true**“ festlegen, werden die Tabellen-ACLs beim Hochladen von Fotos erzwungen, sodass nur autorisierte Benutzer ein Bild hochladen können.
- Wenn Sie die Option auf **false**setzen, werden ACLs für Bild-Uploads in das Feld Foto nicht erzwungen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.security.strict.user_image_upload

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um das Hochladen von Anwenderbildern auf autorisierte Anwender zu beschränken
Empfohlener Wert	wahr
Funktionale Auswirkung	(Niedrig) Keine Auswirkungen auf die Funktionalität, da autorisierte Anwender weiterhin Bilder in ihr Anwenderprofil hochladen können.
Sicherheitsrisiko	(Mittel) Wenn Sie diese Eigenschaft auf „ **false**“ festlegen, kann ein authentifizierter Anwender ein Bild ohne Autorisierung in den Account eines anderen Anwenders hochladen.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Download von MIME-Typen erzwingen (Instanzsicherheitshärtung)

Verwenden Sie die Eigenschaft *glide.ui.attachment.force_download_all_mime_types*, um den Download aller Anhänge vom Typ MIME zu erzwingen.

Hinweis: Wenn Sie die Eigenschaft „ **Download MIME-Typen** erzwingen“ auf **true**festlegen, wird die Eigenschaft Herunterladbare **MIME** -Typen überschrieben, bei der es sich um eine durch Kommas getrennte Liste herunterladbarer MIME-Typen handelt. Weitere Informationen finden Sie unter Herunterladbare MIME-Typen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.attachment.force_download_all_mime_types
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Nein
Zweck	Erzwingen des Downloads aller Anhänge, anstatt sie im Browser auszuführen.
Empfohlener Wert	wahr
Funktionale Auswirkung	(Mittel) Diese Korrektur erzwingt den Download aller Anhänge. Es hat keine Auswirkungen auf die Funktionalität, führt jedoch zu einer veränderten Anwender-Experience.
Sicherheitsrisiko	(Hoch) Um clientseitige Skripting-Angriffe zu reduzieren, sollte das Herunterladen von Dateianhängen erzwungen werden, anstatt im Browserkontext gerendert zu werden.
Referenzen	Verfügbare Systemeigenschaften

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Dateierweiterungen einschränken (Härtung der Instanzsicherheit)

Definieren Sie mit der Systemeigenschaft *glide.attachment.extensions*, welche Dateitypen in Ihre Instanz hochgeladen werden können. Diese Eigenschaft verwendet eine durch Kommas getrennte Liste zulässiger Dateierweiterungstypen. Nur die angegebenen Dateierweiterungstypen werden als Anhänge hochgeladen.

Verwenden Sie die Eigenschaft *glide.attachment.extensions* in Ihrer -Instanz, um die folgenden Vorteile bereitzustellen:

Mehr Sicherheit

Verwenden Sie diese Eigenschaft, um die Sicherheit zu verbessern, indem Sie verhindern, dass Anwender schädliche Dateien (z. B. Viren) als Anhänge hochladen. Sichern Sie Ihre Instanz durch das Blockieren von Typen, die normalerweise von ausführbaren Programmen oder Skripts verwendet werden.

Vermeiden Sie inkompatible Dateitypen

Verwenden Sie diese Eigenschaft, um zu verhindern, dass Anwender inkompatible Dateien hochladen. Einige Browser unterstützen beispielsweise keine Symbole im PNG-Format. Indem Sie die PNG-Dateierweiterung nicht `einbeziehen`, können Sie verhindern, dass Anwender PNG-Dateien hochladen.

Wichtig: Diese Eigenschaft schränkt Dateien nicht basierend auf dem tatsächlichen Dateityp (MIME-Typ) ein, sondern nur basierend auf der Erweiterung. Um Uploads basierend auf dem MIME-Typ einzuschränken, konfigurieren Sie die Eigenschaft *glide.security.file.mime_type.validation*, nachdem Sie die Konfiguration der Eigenschaft *glide.attachment.extensions* abgeschlossen haben. Einzelheiten zur Konfiguration von *glide.security.file.mime_type.validation*finden Sie unter MIME-Typeinschränkungfür Uploads.

Schritte zum Konfigurieren von

1. Geben Sie im Filternavigator Ihrer Instanz `sys_properties.list`ein, und drücken Sie die Eingabetaste.
2. Suchen und öffnen Sie die Eigenschaft *glide.attachment.extensions*.
3. Geben Sie im Feld **Wert** die Dateierweiterungen ein, die als Anhänge hochgeladen werden dürfen. Trennen Sie mehrere Einträge im Feld durch Kommas. Ein Beispielwert für mehrere Einträge wäre *doc,docx,xls,xlxs,pdf,jpeg,jpg,png,ico*.

   Hinweis: Wenn im Feld **„Wert“** keine Dateitypen angegeben sind, kann jeder Dateityp als Anhang hochgeladen werden.

4. Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.attachment.extensions
Konfigurationstyp	Systemeigenschaft (/sys_properties_list.do)
Konfigurierbar im Instanz-Sicherheitszentrum	Nein

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Zweck	Um nur das Hochladen zulässiger Dateierweiterungen während des Dateianhangs zu aktivieren. Es blockiert den Versuch, potenziell schädliche Erweiterungen hochzuladen.
Empfohlener Wert	Einige definierte Dateierweiterungen, z. B. doc, docx, pdf, xls, xlsx
Funktionale Auswirkung	(Mittel) Diese Korrektur schränkt alle Dateierweiterungen mit Ausnahme der in der Aufnahmeliste enthaltenen Dateiendungen ein. Keine Auswirkungen auf die Funktionalität, es sei denn, es wird versucht, eine andere Datei als von der Organisation akzeptierte Erweiterungen hochzuladen.
Sicherheitsrisiko	(Mittel) Da die Verifizierung des MIME-Typs von dieser Eigenschaft abhängt, wird empfohlen, die Schwachstellen im Zusammenhang mit dem Hochladen schädlicher Dateien zu minimieren.

Nicht authentifizierten Zugriff auf Anhänge beschränken (Instanzsicherheitshärtung)

Verwenden Sie die Eigenschaft *glide.image_provider.security_enabled*, um die Sicherheitseinstellungen für Bilder zu steuern. Bei Festlegung auf **wahr**sind Bilder nur für authentifizierte und autorisierte Benutzer sichtbar. Bei Festlegung auf **false**sind die Bilder für alle sichtbar, die eine URL zum Anhang haben.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.image_provider.security_enabled
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um den nicht authentifizierten Zugriff auf den Anhang zu verhindern, wenn er im iix-Format gerendert wird.
Empfohlener Wert	wahr
Funktionale Auswirkung	(Niedrig) Keine signifikanten Auswirkungen auf die Funktionalität. Die Anwender-Experience kann etwas beeinträchtigt werden, da der Anwender, der zuvor direkt auf die .iix-Datei zugegriffen hat, sich authentifizieren muss.
Sicherheitsrisiko	(Hoch) Für nicht authentifizierte Anwender muss Einschränkung angewendet werden, da Anhänge möglicherweise vertrauliche Informationen enthalten.
Referenzen	Anhänge werden verwaltet Verfügbare Systemeigenschaften

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausgeschlossene Anhangserweiterungen angeben (Instanzsicherheitshärtung)

Wenn Sie die Validierung der Ausschlussliste in Now Platformaktivieren, verwenden Sie die Eigenschaft *glide.attachment.blacklisted.extensions*, um eine durch Kommas getrennte Liste mit eingeschränkten hochladbaren Dateierweiterungstypen zu erstellen. Das Hochladen der angegebenen Dateierweiterungstypen ist eingeschränkt.

Voraussetzungen

Legen Sie diese Eigenschaft fest, bevor Sie die Eigenschaft *glide.security.attachment_type.use_blacklist* auf „wahr“ setzen. Weitere Informationen finden Sie unter Schwarze Liste für Anhänge aktivieren.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.attachment.blacklisted.extensions
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Hochladen (Einfügen/Schreiben/Aktualisieren) von Anhängen mit fragwürdigen Dateierweiterungen beschränken.
Typ	Zeichenfolge
Empfohlener Wert	Vom Anwender angegebene Dateierweiterungen. Gängige Beispiele sind ex, dll, xslx.
Funktionale Auswirkung	(Niedrig) Keine Beeinträchtigung der Funktionalität, es sei denn, es wird versucht, eine unter dieser Eigenschaft angegebene Dateierweiterung hochzuladen.
Sicherheitsrisiko	(Mittel) Ein böswilliger Anwender kann mit Malware infizierte Anhänge mit gängigen ausführbaren Dateierweiterungen hochladen.
Workaround	In der Basissystemfunktionalität sind Eigenschaften verfügbar, die dasselbe Problem beheben, mit Einschlussliste statt Ausschlussliste. Weitere Informationen finden Sie unter: • Dateierweiterungen einschränken • MIME-Typeinschränkung für Uploads

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Ausgeschlossene Anhangsdateitypen angeben (Instanzsicherheitshärtung)

Wenn die Validierung der Ausschlussliste in Now Platformaktiviert ist, verwenden Sie die Eigenschaft *glide.attachment.blacklisted.types*, um eine durch Kommas getrennte Liste mit eingeschränkten hochladbaren Dateitypen zu erstellen. Das Hochladen der angegebenen Dateitypen ist eingeschränkt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Voraussetzungen

Legen Sie diese Eigenschaft fest, bevor Sie die Eigenschaft *glide.security.attachment_type.use_blacklist* auf „wahr“ setzen. Weitere Informationen finden Sie unter Schwarze Liste für Anhänge aktivieren.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.attachment.blacklisted.types
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Hochladen (Einfügen/Schreiben/Aktualisieren) von Anhängen mit fragwürdigen Dateitypen einschränken. Beispiel: text/html.
Empfohlener Wert	Einige definierte Dateitypen (z. B. text/html, text/csv).
Funktionale Auswirkung	(Niedrig) Keine Auswirkung auf die Funktionalität, es sei denn, es wird versucht, einen unter dieser Eigenschaft angegebenen Dateityp hochzuladen.
Sicherheitsrisiko	(Mittel) Ein böswilliger Anwender kann mit Malware infizierte Anhänge mit gängigen ausführbaren Dateitypen hochladen.
Workaround	In der Basissystemfunktionalität sind Eigenschaften verfügbar, die dasselbe Problem mit der Aufnahmeliste und nicht mit der Ausschlussliste beheben. Weitere Informationen finden Sie unter: • Dateierweiterungen einschränken • MIME-Typeinschränkung für Uploads

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Herunterladbare Dateitypen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.ui.strict_customer_uploaded_content_types*, um eine durch Kommas getrennte Liste mit eingeschränkten herunterladbaren Dateitypen zu erstellen. Die angegebenen Dateitypen sind die einzigen, die als statischer Inhalt aus einer Instanz heruntergeladen werden können.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.strict_customer_uploaded_content_types
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Zweck	Um sicherzustellen, dass nur Dateitypen in Aufnahmelisten heruntergeladen werden dürfen.
Empfohlener Wert	Anwenderdefiniert (Allgemein: doc, docx, xls, xlsx, pdf usw.)
Funktionale Auswirkung	(Mittel) Nur Dateien, die sich in Aufnahmelisten befinden, können heruntergeladen werden, was sich auf die Organisationsrichtlinie auswirken kann. Die kommagetrennte Aufnahmeliste muss geändert werden, um den Unternehmensrichtlinien für zulässige herunterladbare Dateitypen zu entsprechen.
Sicherheitsrisiko	(Niedrig) Dateidownload-Einschränkungen sollten auf alle nicht vertrauenswürdigen Benutzereingabequellen angewendet werden.
Referenzen	Inhaltstypen

Schritte zum Konfigurieren von

1. Navigieren zu **/sys_properties_list.do**an.
2. Suchen Sie nach der Eigenschaft *glide.ui.strict_customer_uploaded_content_types*.
3. Geben Sie die zulässigen herunterladbaren Dateitypen in einer durch Kommas getrennten Liste an (siehe Abbildung), und klicken Sie dann auf **Aktualisieren**. Ein Beispiel für einen korrekt formatierten Wert für die Liste wäre *ico,gif,png,jpg,jpeg,bmp,ogg,mp3,doc,docx,xls,pdf*.

MIME-Typeinschränkung für Uploads (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.security.file.mime_type.validation*, um die Überprüfung des MIME-Typs für Uploads zu aktivieren. Sie können die MIME-Typvalidierung für Dateianhänge aktivieren (setzen Sie die Eigenschaft auf **wahr**) oder deaktivieren (setzen Sie sie auf **falsch**).

Voraussetzungen

Legen Sie vor dem Festlegen dieser Eigenschaft die Eigenschaft *glide.attachment.extensions* fest. Nur die in *glide.attachment.extensions* angegebenen Erweiterungen werden während des Uploads auf den MIME-Typ überprüft. Weitere Informationen finden Sie unter Dateierweiterungen einschränken.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.security.file.mime_type.validation
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Erzwingen der Überprüfung von MIME-Typ/magischen Bytes während Datei-Uploads.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Empfohlener Wert	wahr
Funktionale Auswirkung	(Mittel) Diese Korrektur aktiviert die Verifizierung des MIME-Typs für die Anhänge zur Anwendung. Keine Auswirkungen auf die Funktionalität, es sei denn, beim Hochladen der Dateien liegt eine böswillige Absicht vor, da diese Validierung lediglich überprüft, ob die Synchronisierung zwischen dem MIME-Typ und den Daten fehlerhaft ist.
Sicherheitsrisiko	(Mittel) Um Schwachstellen wie Dateieinschluss und das Hochladen schädlicher Dateien zu reduzieren, sollte die Verifizierung des MIME-Typs aktiviert sein.
Referenzen	Anhänge werden verwaltet

Weitere Informationen zum Konfigurieren von Eigenschaften für die Härtung finden Sie unter Härtungseinstellungen für die Instanzsicherheit.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

E-Mail-Sicherheit (Härtung der Instanzsicherheit)

Dieser Abschnitt enthält Sicherheitskontrollen, die ein Administrator konfigurieren kann, um sicherzustellen, dass für alle eingehenden E-Mails die richtigen Sicherheitsrichtlinien gelten.

Eingehende HTML-E-Mails konvertieren (Instanzsicherheitshärtung)

Verwenden Sie die Eigenschaft *glide.email.inbound.convert_html_inline_attachment_references*, um anzugeben, ob eingehende HTML-E-Mails so konvertiert werden sollen, dass E-Mail-Bilder in der HTML-Textvorschau der E-Mail angezeigt werden.

Folgendes geschieht, wenn die Systemeigenschaft *glide.email.inbound.convert_html_inline_attachment_reference* auf „false“ festgelegt ist:

- In Now Platformwerden anstelle der empfangenen Bilder defekte CID-Links (Inhalts-ID) angezeigt. Das Format, in dem das E-Mail-Bild angezeigt wird, hängt von der Eigenschaftseinstellung zum Zeitpunkt des Empfangs der E-Mail ab, nicht von der aktuellen Eigenschaftseinstellung.
- Der im Anhang empfangene „böswillige“ Inhalt wird im HTML-Code der E-Mail nicht referenziert. Der Anhang selbst wird in der Tabelle „sys_attachment“ gespeichert.
- Bei der Verarbeitung eingehender E-Mails werden die HTML-Daten der E-Mail nicht aktualisiert, um den gespeicherten Speicherort des Anhangs in der Tabelle „sys_attachment“ widerzuspiegeln. Dies hat folgende Auswirkungen:
  - Inline-Bilder werden in der E-Mail-Anzeige im Aktivitätsformatierer nicht angezeigt.

    Hinweis: Um dieses Problem mit dem Aktivitätsformatierer zu beheben, überprüfen Sie zunächst, ob keine Sicherheitsbedenken bestehen. Legen Sie dann die Systemeigenschaft *glide.email.inbound.convert_html_inline_attachment_reference* auf „**true** “ fest, damit zukünftige empfangene E-Mails die erforderliche HTML-URL enthalten, um auf das Bild zu verweisen. Durch das Ändern der Eigenschaft werden bereits empfangene E-Mails nicht aktualisiert. Der neue Wert wirkt sich nur auf eingehende E-Mails aus, die nach dem Ändern der Eigenschaft empfangen wurden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Inline-Bilder werden nicht angezeigt, wenn die E-Mail in der HTML-Vorschau der E-Mail angezeigt wird.
- Beim Anfügen von „email.body_htm“ in eingehenden Aktionen zwischen Code-Tags fehlen die Bilder.

Voraussetzungen

Legen Sie vor dem Festlegen dieser Eigenschaft die Eigenschaft *glide.email.read.active* auf „wahr“ fest. Weitere Informationen finden Sie unter Verwendung eigenen POP3-Servers aktivieren .

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.email.inbound.convert_html_inline_attachment_references
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um das Rendern von Bildern in der HTML-Textvorschau einzuschränken.
Empfohlener Wert	falsch
Funktionale Auswirkung	(Mittel) Sobald diese Eigenschaft konfiguriert ist, kann der Anwender die Bildvorschau nicht im E-Mail-Text anzeigen.
Sicherheitsrisiko	(Mittel) Wenn die Eigenschaft nicht aktiviert ist, kann ein Angreifer ein schädliches Bild mit Malware senden.
Referenzen	E-Mail-Eigenschaften Konfiguration für eingehende E-Mails

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Bewertung und Filterung von E-Mail-Spam (Instanzsicherheitshärtung)

Installieren Sie das Plugin „E-Mail-Filter“ (*com.glide.email_filter*), um die E-Mail-Filterung innerhalb der Instanz zu installieren. Diese Filterung identifiziert vorhandene Header, sodass Sie basierend auf dem zugeordneten Header entscheiden können, was mit der E-Mail geschehen soll.

Jede über E-Mail-Server Now Platform gesendete Nachricht wird auf die Wahrscheinlichkeit geprüft, Spam zu sein.

Hinweis: Wenn eine Instanz einen privaten E-Mail-Server verwendet, ist dieses Thema nicht anwendbar. Weitere Informationen finden Sie unter Bewertung und Filterung von E-Mail-Spam.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Voraussetzungen

Vor dem Festlegen dieser Eigenschaft:

- Legen Sie die Eigenschaft *glide.email.read.active* auf „Wahr“ fest. Weitere Informationen finden Sie unter Verwendung eigenen POP3-Servers aktivieren .
- Dieser Filter überschreibt die Eigenschaft *glide.pop3.ignore_headers*. Weitere Informationen finden Sie unter Verfügbare Systemeigenschaften .

Weitere Informationen

Attribut	Beschreibung
Plugin-Name	com.glide.email_filter
Konfigurationstyp	Systemdefinition > Plugins
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um Filterung zu erzwingen, um Spam von E-Mails zu vermeiden.
Empfohlener Wert	Aktiv
Funktionale Auswirkung	E-Mails (niedrig) werden im Rahmen der Spam-Bewertung niemals in der Instanz gefiltert, blockiert oder unter Quarantäne gestellt. Er wird nur bewertet und dann an die Instanz gesendet. Alle Filter werden innerhalb der Instanz mit dem Plugin „E-Mail-Filter“ durchgeführt.
Sicherheitsrisiko	(Mittel) E-Mail-Filter ermöglichen Administratoren die Verwendung eines Bedingungsgenerators oder eines bedingten Skripts, um anzugeben, wann böswillige eingehende E-Mails von bekannten/unbekannten Absendern ignoriert werden sollen.
Referenzen	E-Mail-Filter https://support.servicenow.com/kb_view.do?sysparm_article=KB0549426

Weitere Informationen zum Aktivieren von Plugins finden Sie unter Plugins aktivieren .

Zugriff auf E-Mails mit leerer Zieltabelle beschränken (Instanzsicherheitshärtung)

Aktivieren Sie die Eigenschaft *glide.email.email_with_no_target_visible_to_all*, um den Zugriff von Anwendern auf E-Mails einzuschränken, mit Ausnahme des jeweiligen Absenders oder Administratoren.

Nicht autorisierte Benutzer können auf E-Mails in der Tabelle „E-Mails“ [sys_email] zugreifen, für die ein Zieldatensatz fehlt. Anstatt ACLs für E-Mail-Einträge zu erzwingen, beschränkt diese Eigenschaft den Zugriff nur auf den E-Mail-Absender und Benutzer mit der Administratorrolle.

Hinweis: E-Mails, die an die Instanz gesendet und von ihr empfangen werden, werden in der Tabelle E-Mails [sys_email] angezeigt. Allerdings sollten nur empfangene E-Mails, die mit dem Status „Fehler“ und „Ignoriert“ markiert wurden, eine leere Zieltabelle haben.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.email.email_with_no_target_visible_to_all
Konfigurationstyp	Systemeigenschaften [sys_properties]
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um zu blockieren, dass der E-Mail-Client E-Mails anzeigt, wenn der Anwender den Zugriff nicht autorisiert.
Empfohlener Wert	falsch
Funktionale Auswirkung	(Niedrig) Anwender können keine E-Mails mehr anzeigen, bei denen die Zieltabelle leer ist, es sei denn, sie sind Administratoren oder waren der Absender der E-Mail.
Sicherheitsrisiko	(Mittel) Wenn die Eigenschaft nicht aktiviert ist, können nicht autorisierte Anwender auf alle E-Mails zugreifen, bei denen das Feld „target_table“ leer ist.
Referenzen	Erweiterte E-Mail-Eigenschaften https://support.servicenow.com/kb_view.do?sysparm_article=KB0690043

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

E-Mails nach Domäne für Anwendererstellung einschränken (Instanzsicherheitshärtung)

Verwenden Sie die Eigenschaft *glide.user.trusted_domain*, um die kommagetrennte Liste der vertrauenswürdigen Domänen anzugeben, die bei der Erstellung von Anwendern aus eingehenden E-Mails verwendet wird.

Standardmäßig wird ein Sternchen (*) verwendet, um allen Domänen zu vertrauen. Bestimmte Domänen sollten angegeben werden, wenn nicht E-Mails von jeder Domäne zugelassen werden müssen. Die Instanz ignoriert eingehende E-Mails von anderen Domänen, es sei denn, sie stammen von der -Adresse eines vorhandenen Benutzers. Die Instanz erstellt keine Gastanwender aus E-Mails von nicht vertrauenswürdigen Domänen.

Voraussetzungen

Vor dem Festlegen dieser Eigenschaft:

- Legen Sie die Eigenschaft *glide.email.read.active* auf „Wahr“ fest. Weitere Informationen finden Sie unter Verwendung eigenen POP3-Servers aktivieren .
- Legen Sie die Eigenschaft *glide.pop3readerjob.create_caller* auf „Wahr“ fest. Weitere Informationen finden Sie unter Automatische Anwendererstellung aktivieren .

> **Hinweis:** Überspringen Sie die Eigenschaft *glide.user.default_password*, wenn die Eigenschaft *glide.pop3readerjob.create_caller* auf **false**festgelegt ist.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.user.trusted_domain
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Empfohlener Wert	Kommagetrennte Liste vertrauenswürdiger Domänen [z. B. servicenow.com (ein bestimmter Domänenname)].
Funktionale Auswirkung	(Mittel) Sobald diese Eigenschaft konfiguriert ist, akzeptiert die Instanz nur E-Mails von vertrauenswürdigen Domänen. Wenn Sie die Domäne nicht in die Liste der vertrauenswürdigen Domänen aufnehmen, hat dies Auswirkungen auf Gastbenutzer, da Konten automatisch erstellt werden.
Sicherheitsrisiko	(Mittel) Wenn die Eigenschaft nicht aktiviert ist, kann ein Angreifer eine E-Mail-Spoofing-/Spam-Kampagne verwenden, um mehrere E-Mails zu senden, was zur Erstellung weiterer unnötiger Gastanwender führt.
Referenzen	E-Mail-Eigenschaften Konfiguration für eingehende E-Mails

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Eingabevalidierung (Härtung der Instanzsicherheit)

Now Platform führt eine Eingabevalidierung durch, um Probleme zu vermeiden, die aus der Eingabe fehlerhafter Daten resultieren.

In diesem Abschnitt werden Sicherheitskontrollen in Now Platform beschrieben, die ein Administrator konfigurieren kann, um die Eingabe fehlerhafter Daten unabhängig von der Quelle zu minimieren. Diese Quellen umfassen manuelle Anwendereingaben oder Eingaben aus einer Infrastruktur, externen Entitäten oder Datenbanksystemen.

Eingebetteten HTML-Code zulassen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.ui.security.allow_codetag*, um die Unterstützung für das Einbetten von HTML-Code zu deaktivieren, der mit dem Tag [code] erstellt wurde.

Now Platform entschärft viele Einschleusungs- und websiteübergreifende Angriffe durch die Implementierung von Escaping- und Codierungstechniken. Daher können Anwender keine HTML-formatierten Eingaben für Journalfelder schreiben/senden. Journalfelder können jedoch Text, der in Code-Tags eingeschlossen ist, als HTML rendern.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Es ist jedoch ein Sicherheitsrisiko verbunden. Bei Festlegung auf `wahr`können böswillige Anwender schädlichen HTML JS-Code schreiben, der nach dem Rendern von Journalfeldern in einem anderen Client-Browser ausgeführt werden kann.
- Legen Sie diese Eigenschaft auf „ `falsch` “ fest, damit Administratoren verhindern können, dass Journalfelder HTML-Code rendern, indem sie die Unterstützung für das `[code]` -Tag deaktivieren.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.security.allow_codetag
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Schützen Sie sich vor websiteübergreifendem Skripting und der Ausführung schädlicher Skripts
Empfohlener Wert	falsch
Funktionale Auswirkung	(Mittel) Diese Korrektur erzwingt die HTML-Codierung auf der Anwenderoberfläche und rendert die codierten Ergebnisse für den Anwender. Diese Eigenschaft ist standardmäßig auf „ `true` “ festgelegt. In diesem Status zeigt Ihre Instanz gerenderten HTML-Code in Journalfeldern und Formularen an. Wenn diese Eigenschaft auf „ `false`“ festgelegt ist, wird HTML nicht ordnungsgemäß gerendert, und HTML-Tags werden möglicherweise in Journalfeldern in Formularen angezeigt. Dies kann sich nachteilig auf die Funktionalität und die Benutzerinteraktionen mit den resultierenden Daten auswirken.
Sicherheitsrisiko	(Mittel) Die Eingabevalidierung muss in der Anwendung erfolgen, um sich gegen websiteübergreifende Skripting-Angriffe zu schützen. Diese Angriffe ermöglichen die Ausführung fremder Skripts in einer Benutzersitzung im Kontext des angemeldeten Browsers. Angreifer können damit Sitzungsinformationen und vertrauliche Daten stehlen.
Referenzen	Beschränken Sie das CODE-Tag in Journalfeldern Journalfeldeinträge als HTML rendern Strenge Sicherheitseinstellungen

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

JavaScript-Tags in eingebettetem HTML zulassen (Härtung der Instanzsicherheit)

Die Eigenschaft *glide.ui.security.codetag.allow_script* deaktiviert die Unterstützung für die Einbettung von HTML-JavaScript-Code, der mit dem Tag [code] erstellt wurde.

Hinweis: Diese Eigenschaft ist in Vancouver und späteren Releases standardmäßig auf „ **false** “ festgelegt und kann von Administratoren nicht geändert werden. Wenn Sie einen Anwendungsfall haben, bei dem die Eigenschaft geändert werden muss, wenden Sie sich an den Kundensupport.

Now Platform entschärft viele Einschleusungs- und websiteübergreifende Angriffe durch die Implementierung von Escaping- und Codierungstechniken. Daher können Anwender keine HTML-formatierten Eingaben für Journalfelder schreiben und übermitteln. Journalfelder können jedoch Text, der in Code-Tags eingeschlossen ist, als HTML rendern.

- Es ist jedoch ein Sicherheitsrisiko verbunden. Bei Festlegung auf **wahr**können böswillige Anwender schädlichen HTML-JavaScript-Code schreiben, der nach dem Rendern von Journalfeldern in einem anderen Client-Browser ausgeführt werden kann.
- Legen Sie diese Eigenschaft auf „ **falsch** “ fest, damit Administratoren verhindern können, dass Journalfelder HTML-JavaScript-Code rendern, indem sie die Unterstützung für das `[code]` -Tag deaktivieren.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.security.codetag.allow_script
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Schützt vor websiteübergreifendem Skripting und der Ausführung böswilliger Skripts
Empfohlener Wert	falsch
Standardwert	falsch
Funktionale Auswirkung	(Mittel) Diese Korrektur erzwingt JavaScript-Escaping auf der Anwenderoberfläche und rendert die codierten Ergebnisse für den Anwender. Sie kann basierend auf der Interaktion des Instanzanwenders mit den resultierenden Daten Auswirkungen auf die Funktionalität haben.
Sicherheitsrisiko	(Hoch) Die Eingabevalidierung muss in der Anwendung erfolgen, um sich gegen websiteübergreifende Skripting-Angriffe zu schützen. Diese Angriffe ermöglichen die Ausführung fremder Skripts in der Anwendersitzung im Kontext des angemeldeten Browsers. Angreifer können damit Sitzungsinformationen und vertrauliche Daten stehlen.
Referenzen	Beschränken Sie das CODE-Tag in Journalfeldern Journalfeldeinträge als HTML rendern

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Strenge Sicherheitseinstellungen

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Nicht bereinigte HTML überprüfen (Instanzsicherheitshärtung)

Verwenden Sie die Eigenschaft *com.glide.security.check_unsanitized_html*, um das Bereinigungsverhalten von translated_html-Feldern auf globaler Ebene für Feldzuweisungen zu erzwingen.

HTML ist einer der Typen, die den Wörterbuchfeldern zugewiesen werden können. Durch das Zuweisen von HTML-Feldern an einen beliebigen Feldtyp erhalten Sie die Funktionalität zum Formatieren von Inhalten mithilfe von HTML-Tags (z. B. `<p>`, `<a href>`, `<b>`, `<font>`, `<img>`). Um böswillige Aktivitäten zu verhindern, können bestimmte HTML-Tags mithilfe einer Sperrliste deaktiviert werden. Diese Eigenschaft verhindert, dass unzulässige Tags in „translated_html"-Feldern in Ihrer Instanz verwendet werden.

- Legen Sie diese Eigenschaft auf „ **erzwingen** " fest, um das Bereinigungsverhalten von translated_html-Feldern zu erzwingen.
- Legen Sie die Eigenschaft auf „ **deaktiviert** " fest, um die HTML-Bereinigung zu deaktivieren und blockierte HTML-Tags in „translated_html"-Feldern zuzulassen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	com.glide.security.check_unsanitized_html
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Verhindert die Verwendung unsicherer HTML-Tags zum Schutz vor Angriffen wie websiteübergreifendem Skripting.
Typ	Zeichenfolge
Empfohlener Wert	*erzwingen*
Funktionale Auswirkung	(Mittel) Diese Korrektur erzwingt die HTML-Bereinigung auf der Anwenderoberfläche und rendert übersetzte HTML-Felder für den Anwender. Dies kann Auswirkungen auf die Lesbarkeit und Formatierung haben.
Sicherheitsrisiko	(Hoch) Die Eingabevalidierung muss in der Anwendung erfolgen, um sich gegen websiteübergreifende Skripting-Angriffe zu schützen. Diese Angriffe ermöglichen die Ausführung fremder Skripts in Anwendersitzungen im Kontext des angemeldeten Browsers. Angreifer können damit Sitzungsinformationen und vertrauliche Daten stehlen.
Referenzen	HTML-Bereinigung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Vom Client generierte Skripts-Sandbox (Instanzsicherheitshärtung)

Verwenden Sie die Eigenschaft *glide.script.use.sandbox*, um das Skript-Sandboxing zu aktivieren.

Es gibt zwei Fälle in Now Platform, die es dem Client ermöglichen, Skripts zur Bewertung an den Server zu senden:

Filter oder Abfragen

Es ist zulässig, einen Filter an den Server zu senden, z. B. `assigned_to=JavaScript:getMyGroups()`.

System-API

Ein API-Aufruf ermöglicht es dem Client, beliebige Skripts auf dem Server auszuführen und eine Antwort zu erhalten.

Wenn Sie Skript-Sandboxing aktivieren, wird das an einem dieser beiden Einstiegspunkte ausgewertete Skript in einer Sandbox mit reduzierten Rechten und mit den folgenden Eigenschaften ausgeführt:

- Nur die als vom Client aufrufbar markierten Business-Regeln sind in der Sandbox verfügbar.
- In der Sandbox sind nur Skripteinbindungen verfügbar, die als vom Client aufrufbar markiert sind.
- Bestimmte API-Aufrufe (weitgehend, aber nicht vollständig, beschränkt auf Aufrufe, die den direkten DB-Zugriff betreffen) sind nicht zulässig.
- Sie können in der Sandbox keine Daten einfügen, aktualisieren oder löschen. Beispielsweise werden alle Aufrufe von `current.update()` ignoriert. Wenn Sie Now Platform ausführen, ohne Skript-Sandboxing zu aktivieren, gelten keine dieser Einschränkungen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.script.use.sandbox
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Erzwingt die Validierung für die clientseitigen JavaScript-Abfragen, die für die Plattform gestartet werden
Empfohlener Wert	wahr
Funktionale Auswirkung	(Hoch) Diese Korrektur erzwingt die Validierung für die clientseitigen JavaScript-Abfragen, die für Now Platformgestartet werden. Es kann potenziell Auswirkungen haben, wenn der Kunde Anpassungen verwendet hat, die hartcodierte JavaScript-Abfragen zur Durchführung von CRUD-Vorgängen enthalten.
Sicherheitsrisiko	(Hoch) Now Platform bietet eine Vielzahl von Funktionen und Funktionalitäten durch JavaScript-Abfragen. Ohne entsprechende Autorisierung und Validierung besteht jedoch die Möglichkeit, dass ein

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Angreifer nicht autorisierte Vorgänge auf der Plattform durchführt.
Referenzen	Sandbox-Eigenschaft für Skript konfigurieren *glide.script.use.sandbox* gehört zu derselben Familie von Eigenschaften, die die Ausführung von Skripts sichern und einschränken, die vom Client stammen: • *glide.script.allow.ajaxevaluate*: Siehe „AJAXEvaluate aktivieren“ • *glide.script.secure.ajaxgliderecord*: Siehe Aktivieren der AJAXGlideRecord-ACL-Überprüfung:

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

AJAXEvaluate aktivieren (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.script.allow.ajaxevaluate*, um die Ausführung beliebiger Clientskripts mithilfe der System-API auf der Serverseite einzuschränken.

Es gibt zwei Fälle in Now Platform, die es dem Client ermöglichen, Skripts zur Bewertung an den Server zu senden:

Filter und/oder Abfragen

Es ist zulässig, einen Filter an den Server zu senden, z . B.: `assigned_to=javascript:getMyGroups()`

System-API

Mit dem API-Aufruf AJAXEvaluate kann der Client beliebige Skripts auf dem Server ausführen und eine Antwort erhalten.

Wenn Sie diese Eigenschaft auf „ **false**“ festlegen, aktiviert Now Platform nicht die Verwendung des AJAXEvaluate-API-Aufrufs aus dem Client-Skript.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.script.allow.ajaxevaluieren
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Beschränken Sie die Ausführung eines beliebigen Client-Skripts mithilfe der System-API auf der Serverseite
Empfohlener Wert	falsch
Funktionale Auswirkung	(Mittel) Diese Korrektur erzwingt das Ausschalten des AJAEvaluate-Prozessors. Es kann sich auf die Funktionalität auswirken, wenn Sie den AJAX-Auswertungsprozessor explizit als Teil von anwenderdefinierten Skripts verwenden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Weitere Informationen finden Sie unter GlideAjax .
Sicherheitsrisiko	(Hoch) AJAXEvaluate kann die Ausführung von beliebigem JavaScript-Code im Client-Browser zulassen, indem die serverseitigen Objekte angewendet werden.
Referenzen	Sandbox-Eigenschaft für Skript konfigurieren GlideAjax *glide.script.allow.ajaxevaluate* gehört zu derselben Familie von Eigenschaften, die die Ausführung von Skripts sichern und einschränken, die vom Client stammen: • *glide.script.use.sandbox*: Siehe Sandbox für vom Client generierte Skripts. • *glide.script.secure.ajaxgliderecord*: Siehe AJAXGlideRecord-ACL-Überprüfung aktivieren.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Excel-Formel codieren (Instanzsicherheitshärtung)

Verwenden Sie die Eigenschaft *glide.export.escape_formulas*, um die Excel-Injektion, auch bekannt als Formelinjektion, zu verhindern.

Eine Excel-Einschleusung tritt auf, wenn Websites nicht vertrauenswürdige Einträge in Excel-Dateien einbetten. Wenn Sie eine Tabellenkalkulationsanwendung wie Microsoft Excel oder LibreOffice Call verwenden, um eine Datei zu öffnen, werden alle Zellen, die mit +, -, = oder @ beginnen, als Formel interpretiert. Wenn Sie die Eigenschaft *glide.export.escape_formulas* auf **true**festlegen, wird Zeichenfolgenwerten, die mit +, -, = oder @ beginnen, beim Exportieren in CSV-, XLS- oder XLSX-Dateien ein einzelner Apostroph vorangestellt.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.export.escape_formulas
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um die Anwendung gegen die Excel- oder Formelinjektion zu verhindern.
Empfohlener Wert	wahr
Funktionale Auswirkung	(Niedrig) Böswillig erstellte Formeln können für einen Hijacking-Angriff auf den Computer des Benutzers

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	verwendet werden, indem Schwachstellen in der Tabellenkalkulationssoftware ausgenutzt werden.
Sicherheitsrisiko	(Mittel) Böswillige Formeln stellen ein Risiko dar, auch wenn die Einbettungstabelle keine vertraulichen Informationen enthält, da sie verwendet werden können, um den Computer des Betrachters zu gefährden.
Workaround	Erwägen Sie als Alternative, nach Möglichkeit alle nachfolgenden Leerzeichen zu entfernen und alle vom Client bereitgestellten Daten auf alphanumerische Zeichen zu beschränken.
Referenzen	Verfügbare Systemeigenschaften

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

HTML codieren (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.ui.escape_html_list_field*, um HTML-Escape-Zeichen für HTML-Felder in einer Listenansicht zu erzwingen.

HTML ist einer der Typen, die den Wörterbuchfeldern zugewiesen werden können. Durch das Zuweisen von HTML-Feldern an einen beliebigen Feldtyp erhalten Sie die Funktionalität zum Formatieren von Inhalten mithilfe von HTML-Codes (z. B. `<p>`, `<a href>`, `<b>`, `<font>`, `<img>`). Ein böswilliger Anwender kann HTML-Code in das Formularfeld einschleusen, um unerwünschte Skripts in verschiedenen Client-/Benutzersitzungen auszuführen.

- Legen Sie diese Eigenschaft auf „ **wahr** “ fest, um ein HTML-Escaping auszuführen, bevor die Datensätze/Felder im Browser gerendert werden, wenn die Tabelle als Listenansicht angezeigt wird.
- Wenn dies auf **false**eingestellt ist und Sie diese Spalte in einer Listenansicht auswählen, wenn Sie eine Tabellen- oder Datensatzliste anzeigen, werden diese HTML-formatierten Felder möglicherweise angezeigt.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.escape_html_list_field
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um die Anwendung gegen websiteübergreifende Skripting-Angriffe zu schützen
Empfohlener Wert	wahr
Funktionale Auswirkung	(Mittel) Diese Korrektur erzwingt die HTML-Codierung in der Anwenderoberfläche auf HTML-Parser-Ebene und gibt dem Anwender daher codierte Ergebnisse zurück. Sie kann basierend auf der Interaktion des Instanzanwenders mit den resultierenden Daten Auswirkungen auf die Funktionalität haben.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	(Hoch) Die Eingabevalidierung muss in der Anwendung erfolgen, um sich gegen websiteübergreifende Skripting-Angriffe zu schützen. Diese Angriffe ermöglichen die Ausführung fremder Skripts in Anwendersitzungen im Kontext des angemeldeten Browsers. Angreifer können damit Sitzungsinformationen und vertrauliche Daten stehlen.
Referenzen	Strenge Sicherheitseinstellungen

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Escape-Zeichen für JavaScript (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.html.escape_script*, um in HTML-Feldern während Listenansichten Escape-Zeichen für JavaScript-Tags (`<script></script>`) zu erzwingen.

HTML ist einer der Typen, die den Wörterbuchfeldern zugewiesen werden können. Durch das Zuweisen von HTML-Feldern an einen beliebigen Feldtyp wird dem Anwender die Möglichkeit gegeben, den Inhalt mithilfe von HTML-Codes zu formatieren (z. B. `<p>`, `<a href>`, `<b>`, `<font>`, `<img>`). Wenn Sie *glide.html.escape_script* auf **false**setzen, werden die Tags (`<script></script>`) möglicherweise angezeigt, wenn Sie diese Spalte in einer Listenansicht auswählen, während Sie eine Tabellen- oder Datensatzliste anzeigen.

Ein böswilliger Angreifer kann JavaScript-Code einfügen, indem er ihn in die Tags (`<script></script>`) einbettet. Der Angreifer kann einen Vorteil ausnutzen, indem er einen ausgefeilten JS-Vektor einschleust, der ausgeführt werden kann, wenn ein Benutzer den Tabellendatensatz öffnet.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.html.escape_script
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Verhinderung von Cross Site Scripting-Angriffen auf eine Anwendung
Empfohlener Wert	wahr
Funktionale Auswirkung	(Mittel) Diese Korrektur erzwingt JavaScript-Escaping in der Anwenderoberfläche und rendert codierte Ergebnisse für den Anwender. Dies kann sich je nach Interaktion des Instanzbenutzers mit den resultierenden Daten auf die Funktionalität auswirken
Sicherheitsrisiko	(Hoch) Die Eingabevalidierung muss in der Anwendung erfolgen, um sich gegen websiteübergreifende Skripting-Angriffe zu schützen. Diese Angriffe ermöglichen die Ausführung fremder Skripts in einer Anwendersitzung im Kontext des

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	angemeldeten Browsers. Angreifer können damit Sitzungsinformationen und vertrauliche Daten stehlen.
Referenzen	Verfügbare Systemeigenschaften Strenge Sicherheitseinstellungen

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Escape-Zeichen für Jelly (Instanzsicherheitshärtung)

Verwenden Sie die Eigenschaft *glide.ui.escape_all_script*, um das Escape-Zeichen für alle in Jelly eingefügten Skripts zu erzwingen.

Versieht alle in enthaltenen JS- und HTML-Zeichenfolgen mit Escape-Zeichen<j:jelly> ... </j:jelly> bevor sie in den Ausgabestream geschrieben werden, wodurch mehrere XSS-Probleme verhindert werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.escape_all_script
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja

Zweck	Wenn die Eigenschaft nicht auf **true**festgelegt ist, müssen Entwickler für jedes anwenderdefinierte Jelly-Skript mehrere Schritte ausführen, um XSS-Probleme zu vermeiden. Diese Schritte umfassen das Auffinden der Jelly-Variablen, die an den Ausgabestream gesendet werden, um sie auf Webseiten zu rendern, und das Ausführen von Escape-Zeichen für jedes der folgenden Tags:
	
	`$ - {JS: Ausdruck}`
	
	`$ - {HTML: Ausdruck}`
	
	ODER
	
	`$ - {JS, HTML: Ausdruck}`

Empfohlener Wert	wahr
Funktionale Auswirkung	(Mittel) Diese Korrektur erzwingt Jelly-Escaping auf Parser-Ebene. Sie kann sich auf die Funktionalität der Benutzerinteraktion mit den resultierenden Daten auswirken.
Sicherheitsrisiko	(Hoch) Die Eingabevalidierung muss für alle Anwendereingaben erfolgen, die in der Anwendung eingegeben werden. Auf diese Weise können

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Einschleusungsangriffe auf die Plattform verteidigt und geschützt werden.
Workaround	Die Anwenderoberfläche kann betroffen sein, da einige der Skripts und HTML-Tags, die für das Rendern auf einer Webseite entwickelt wurden, fehlerhaft erscheinen können. Diese Korrektur sendet die codierte Ausgabeseite zum Rendern an den Browser. Anstelle von „`meine Zeichenfolge hier`"könnte beispielsweise „`<u>meine</u>` Zeichenfolge hier" angezeigt werden, da das Tag `<u>` ordnungsgemäß mit Escape-Zeichen versehen wurde. In diesem Fall fügen Sie dem Jelly-Ausdruck das Präfix „NOESC" hinzu, um ein Escape-Zeichen für JS zu verhindern. Beispiel: • Vor: ($[jvar_context_menus]); • Nach: `($[NOESC:jvar_context_menus]);` • Vor: $[jvar_ui_policy_scripts] • Nach: `$[NOESC:jvar_ui_policy_scripts]`
Referenzen	Strenge Sicherheitseinstellungen Jelly Tags

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

XML codieren (Härtung der Instanzsicherheit)

Die Eigenschaft *`glide.ui.escape_text`* erzwingt das Escape-Zeichen für XML-Werte auf Parser-Ebene, bevor sie an den Browser des Clients übertragen werden.

Hinweis: Diese Eigenschaft ist in Vancouver und späteren Releases standardmäßig auf „ **true** " festgelegt und kann von Administratoren nicht geändert werden. Wenn Sie einen Anwendungsfall haben, bei dem die Eigenschaft geändert werden muss, wenden Sie sich an den Kundensupport.

Site-übergreifendes Skripting tritt auf, wenn ein Angreifer schädliches JavaScript in einen Einstiegspunkt einschleust. Die Plattform/Anwendung kann das schädliche JavaScript nicht mit Escape-Zeichen versehen, bevor sie zur Ausführung an den Browser des Opfers übertragen wird. Escape-Zeichen bedeutet in diesem Kontext Folgendes:

- **&** --> `&`
- **<** --> `<`
- **>** --> `>`
- **"** --> `"`
- **'** --> `'`
- **/** --> `/`

Beispiel: <![CDATA[<script> `alert('XSS-Angriff');`</script>]]>

Escape-Zeichen: <script>alert('XSS Attack');</script>

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.escape_text
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Das Codieren von XML stellt sicher, dass Browser das schädliche JavaScript, das in nicht vertrauenswürdigen Daten eingebettet ist, nicht analysieren und als JavaScript ausführen. • Ein böswilliger Anwender kann einen XSS-Angriff versuchen, um entweder die Sitzung anderer Anwender zu kapern oder den Anwender auf eine schädliche Website umzuleiten. • Now Platform enthält Code zum Sichern von Cookies. Um ihn jedoch mit Escape-Zeichen zu versehen, muss diese Eigenschaft auf **true**festgelegt sein.
Empfohlener Wert	wahr
Funktionale Auswirkung	(Mittel) Diese Korrektur erzwingt die XML-Codierung auf XML-Parser-Ebene in der Anwenderoberfläche. Sie rendert die codierten Ergebnisse für den Benutzer, was je nach Interaktion des Instanzbenutzers mit den resultierenden Daten Auswirkungen auf die Funktionalität haben kann.
Sicherheitsrisiko	(Hoch) Die Eingabevalidierung muss in der Anwendung erfolgen, um sich gegen websiteübergreifende Skripting-Angriffe zu schützen. Diese Angriffe ermöglichen die Ausführung fremder Skripts in einer Anwendersitzung im Kontext des angemeldeten Browsers. Angreifer können damit Sitzungsinformationen und vertrauliche Daten stehlen.

Workaround	Nachdem Sie diese Eigenschaft auf **true**festgelegt haben, wird das Rendern für die HTML-Tags in der Katalogelementbeschreibung oder im Hilfetext der Katalogelementvariablen angehalten. Sie können möglicherweise für einige Felder keine HTML-Formatierung verwenden.
	
	Wenn jedoch die Eigenschaft *glide.ui.escape_text* deaktiviert ist, wird allen JEXL-Ausdrücken ein Ausgabecodierer vorangestellt:
	
	`${JS:Ausdruck}`
	
	`${HTML:Ausdruck}`
	
	oder

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	`${JS,HTML:Ausdruck}`
Referenzen	Strenge Sicherheitseinstellungen

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

HTML-Bereinigung (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.html.sanitize_all_fields*, um die HTMLSanitizer-Skripteinbindung zu aktivieren, die HTML-Eingaben basierend auf den in einem Skript konfigurierten Attributen auf der Ausschluss- und Aufnahmeliste bereinigt.

Die für Dictionary/Fields verfügbaren Feldtypen sind HTML und Übersetztes HTML. Mit diesen HTML-Eingabefeldern können Anwender Eingaben im HTML-Format schreiben, z. B.:

`<h1>Test</h1>`) unter Verwendung der einfachsten HTML-Tags wie `<img>`, `<a href …>`und `<iframe>`.

Sie kann einem böswilligen Angreifer die Möglichkeit geben, bösartige Vektoren mit HTML-Tags einzuschleusen, z. B.:

```
[<IMG SRC=" &#14; JavaScript:alert('XSS');">][<IMG
onmouseover="alert('xss')">],[a href="" onclick=alert(/xss/)].
```

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.html.sanitize_all_fields
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Verhindert Cross Site Scripting- und HTML-Einschleusungsangriffe auf die Anwendung
Empfohlener Wert	wahr
Funktionale Auswirkung	(Hoch) Diese Korrektur erzwingt den HTML-Ausgabecodierungsmechanismus, bevor die Anwenderdaten an den Anwender zurückgegeben werden. Wenn der Kunde Anpassungen vorgenommen hat, die das Rendern des HTML-Attributs oder der Inhaltsdaten umfassen, wirkt sich dies auf die Funktionalität aus.
Sicherheitsrisiko	(Hoch) Anwendereingaben sollten sicher behandelt werden, wenn die Daten in der Anwendung gespeichert und verarbeitet werden. Dies reduziert clientseitige Cross Site Scripting-Angriffe durch Ausgabecodierung der Daten.
Workaround	Diese Eigenschaft bereinigt alle HTML-Felder im System. Wenn Sie die HTML-Bereinigung für

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	einzelne Felder aktivieren müssen, finden Sie weitere Informationen unter Bereinigung einzelner Felder aktivieren. Sie können auch die Aufnahme- oder Ausschlussliste konfigurieren, um HTML-Tags und Attribute gemäß den Richtlinien Ihrer Organisation zu bereinigen.
Referenzen	HTML-Bereinigung aktivieren HTML-Bereinigung

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Jelly/JS-Interpolation (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.ui.jelly.js_interpolation.protect*, um sicherzustellen, dass JavaScript-Code, der auf einer Jelly-Seite ausgeführt werden soll, mithilfe der Jelly-Interpolation vor der Einschleusung geschützt ist.

Wenn Sie die Eigenschaft auf „ **true**“ festlegen, durchläuft eine Anwendung eine Jelly-Skriptstruktur (verschachtelt). Es umschließt potenziell gefährliche Jelly-Ausdrücke mit einem Filter, der:

- Codiert aus Sicherheitsgründen ein Escape-Zeichen für die Ergebnisse, oder
- Wenn ihre Sicherheit nicht garantiert werden kann, generiert eine SecurityException, da der Ausdruck, der ausgewertet wurde, ein mögliches Sicherheitsproblem darstellt.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.jelly.js_interpolation.protect
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Zur Abwehr von Angriffen mit böswilliger Codeausführung, die mit Jelly Injection auftreten können.
Empfohlener Wert	True
Funktionale Auswirkung	(Hoch) Diese Eigenschaft ermöglicht eine bestmögliche Schätzung, ob ein Ausdruck in Anführungszeichen gesetzt ist. Möglicherweise wird ein berechtigter Ausdruck falsch angegeben. In diesem Fall muss ein Ausdruck möglicherweise manuell als sicher markiert werden.
Sicherheitsrisiko	Die (mittel) JEXL-Injektion ist eine für Now Platform eindeutige Form der Eingabeinjektion, die sowohl zu websiteübergreifender Anforderungsfälschung als auch zu Codeausführung führen kann. Durch

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	das vollständige Deaktivieren des Schutzes können möglicherweise viele P1-Sicherheitsschwachstellen geöffnet werden.
Workaround	Um einen Ausdruck manuell als sicher zu markieren, fügen Sie dem Jelly-Ausdruck das SAFE-Präfix hinzu: `${SAFE:sysparm_input};` Das blinde Hinzufügen von SAFE zu jedem Ausdruck ist die falsche Herangehensweise, da dies zu einer Sicherheitsschwachstelle führen kann. • Fügen Sie einem Ausdruck nur dann SAFE hinzu, wenn Sie garantieren können, dass der Ausdruck keine Eingaben vom Client enthält. • Wenn dies der Fall ist, kann ein böswilliger Client die Auswertung von privilegiertem JavaScript verursachen.
Referenzen	Jelly Tags Strenge Sicherheitseinstellungen

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Strikte Sicherheit für SOAP-Anforderungen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.soap.strict_security*, um die Sicherheit von Webdiensten zu erzwingen.

Diese Eigenschaft verwendet eine Kombination aus:

- Abfrage/Rückmeldung der Standardauthentifizierung über das HTTP-Protokoll und
- Zugriffssteuerungen auf Systemebene im Plugin „Kontextsicherheit: Rollenverwaltung“.

Wenn Sie diese Eigenschaft auf **true**festlegen, werden die folgenden Aktionen ausgeführt:

- Wenn der Benutzer über die entsprechende Rolle zum Ausführen des Vorgangs verfügt, prüft er die eingehende SOAP-Anforderung auf Rollenberechtigung, um sie zu validieren. Es tritt während SOAP-Webservice-Aufrufen/-Anforderungen auf, die an Now Platform -Tabellen gestellt werden, wenn CREATE-, READ-, UPDATE- oder DELETE-Vorgänge ausgeführt werden.
- Überprüft die ACLs auf Systemebene, während Daten in Form von SOAP-Daten in der Tabelle abgerufen werden.
- Überprüft die ACLs auf Feldebene für CRUD-Vorgänge, die für ein Feld der Tabelle ausgeführt werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.soap.strict_security

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Stellen Sie sicher, dass Sicherheits-ACLs überprüft und validiert werden, auch wenn der Zugriff auf die Datensätze über SOAP-Aufrufe erfolgt
Empfohlener Wert	wahr
Funktionale Auswirkung	(Hoch) Diese Korrektur erzwingt die Zugriffssteuerung auf Systemebene beim Abrufen von Daten aus Tabellen/Seiten in Form von SOAP-Daten in der Instanz. Wenn derzeit Anwender auf diese Daten zugreifen, ist der Zugriff auf die Daten gemäß den ACL-Regeln eingeschränkt/erlaubt. Informationen zu den Standardrollen mit Zugriff auf die SOAP-Daten finden Sie unter SOAP-Rollen .
Sicherheitsrisiko	(Hoch) Wenn keine entsprechende Autorisierung für die eingehenden SOAP-Anforderungen konfiguriert ist, kann ein nicht autorisierter Anwender Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.
Referenzen	Strikte Sicherheit für eingehende SOAP durchsetzen SOAP Web Service

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Sichere Kommunikation (Härtung der Instanzsicherheit)

Die sicheren Kommunikationseigenschaften beziehen sich auf die Sicherheit der Übertragung von HTTP-Datenverkehr.

Zertifikatvertrauen (Härtung der Instanzsicherheit)

Standardmäßig ist die Eigenschaft *com.glide.communications.trustmanager_trust_all* auf **false**festgelegt. Now Platform vertraut nur Zertifikaten, die anhand des JVM-Zertifikatspeichers verifiziert werden können. Selbst- und unternehmenssignierte Zertifikate sind nicht vertrauenswürdig.

Hinweis: Die Werte für diese Eigenschaften sind und können nach der Änderung nicht mehr geändert werden (sie können nicht rückgängig gemacht werden). Ändern Sie aus Sicherheitsgründen diesen Eigenschaftswert nicht. Wenn Sie weitere Fragen haben, wenden Sie sich an Kundenservice und Support.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	com.glide.communications.trustmanager_trust_all
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Erzwingen der Zertifikatvalidierung für ausgehende Anforderungen.
Empfohlener Wert	falsch
Funktionale Auswirkung	(Mittel) Diese Korrektur erzwingt eine strikte Validierung für das Feld „Zertifizierungsstelle“ (Zertifizierungsstelle). Wenn das Zertifikat von einer vertrauenswürdigen Entität (CA) ausgestellt wurde, akzeptiert die Instanz das Zertifikat zur weiteren Verwendung.
Sicherheitsrisiko	(Mittel) Aus Vertraulichkeits- und Integritätsgründen sollte die Anwendung die Zertifizierungsstelle des Zertifikats validieren, bevor das Zertifikat für Transaktionsvorgänge verwendet wird.
Referenzen	Zertifikate Verifizierung des Hostnamens des HTTP-Clients

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

SSLv2/SSLv3 deaktivieren (Instanzsicherheitshärtung)

Verwenden Sie die Eigenschaft *glide.outbound.sslv3.disabled*, um den MID-Server zur Verwendung von TLS bei ausgehenden Verbindungen wie REST- und SOAP-Anforderungen zu zwingen. Normalerweise wird für ausgehende Verbindungen einer Instanz die Verwendung von TLS anstelle von SSL erzwungen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ausgehend.sslv3.deaktiviert
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Erzwingen der Verwendung von TLS für alle ausgehenden Verbindungen von der ServiceNow-Instanz.
Empfohlener Wert	wahr
Funktionale Auswirkung	(Mittel) Diese Korrektur erzwingt die Verwendung der TLS-Protokollversion bei der Kommunikation über HTTPS. Wenn von Kunden/Benutzern der Instanz Geräte verwendet werden, die keine TLS-Kommunikation unterstützen, kann ein Ausfall auftreten.
Sicherheitsrisiko	(Mittel) Veraltete Versionen von SSL haben sich bei der Verwendung für die Implementierung der sicheren HTTP-Shell aufgrund clientseitiger Angriffe,

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	einschließlich BEAST und SSL-Heart-Bleed, als unsicher erwiesen.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Verifizierung des Hostnamens des HTTP-Clients

Verwenden Sie *com.glide.communications.httpclient.verify_hostname*, um den Hostnamen und die Zertifikatkette zu überprüfen, die von Remote-SSL-Hosts dargestellt werden.

Legen Sie *com.glide.communications.httpclient.verify_hostname* auf „ **true** “ fest, um sich vor MitM-Angriffen (Man-in-the-Middle) zu schützen, bei denen die Kommunikation zwischen zwei Parteien abgefangen wird. Durch das Festlegen dieser Eigenschaft wird die Eigenschaft *com.glide.communications.trustmanager_trust_all* überschrieben.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*com.glide.communications.httpclient.verify_hostname*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Deaktivieren Sie den Zertifizierungsverifizierungsprozess, der alle Zertifizierungen in der Zertifizierungskette durch Überprüfen des Sperrstatus bewertet.
Typ	wahr | falsch
Empfohlener Wert	wahr
Funktionale Auswirkung	(Mittel) Ermöglicht einem Zertifikat, das nicht validiert ist, eine Verbindung zu einem unsicheren Host herzustellen.
Sicherheitsrisiko	(Mittel) Ermöglicht oder verhindert, dass der HTTP-Client ohne Ausnahme eine Verbindung zu einem potenziell schädlichen Hostnamen herstellt.
Referenzen	Zertifikate Zertifikatvertrauen

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Widerrufene Zertifikatverifizierung

Verwenden Sie diese Eigenschaft, um den Zertifizierungsverifizierungsprozess zu deaktivieren, der alle Zertifizierungen in der Zertifizierungskette durch Überprüfen des Widerrufstatus bewertet.

API-Aufrufe, die das Hochsicherheits-Plugin verwenden, möchten diese Eigenschaft möglicherweise konfigurieren. Wenn die vollständige Zertifizierungskette im Instanz-Trust Store

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

nicht definiert ist oder die verwendeten Zertifikate möglicherweise nicht mit einer OCSP-Widerrufprüfung (Online Certificate Status Protocol) kompatibel sind, können Fehler an die API-Aufrufe zurückgegeben werden.

Die Prüfung der Zertifikatwiderrufung kann deaktiviert werden, indem die Eigenschaft *com.glide.communications.httpclient.verify_revoked_certificate* auf „ **false**“ festgelegt wird.

Fehler, die mit einer Unmöglichkeit der Prüfung verbunden sind, sind „NPE“, „SSLPeerUnverifiedException“ und „CertPathValidatorException“. Diese Fehler können in eine HttpException eingeschlossen werden. Mehrere Faktoren können sich darauf auswirken, ob eine Prüfung erfolgreich durchgeführt werden kann:

- Der URI muss für die Instanz zugänglich sein. Beachten Sie, dass die ursprüngliche OCSP-Implementierung möglicherweise keinen Zugriff auf eine Proxy-Verbindung hat.
- Der Referrer-OCSP-Service muss online sein, wenn die Überprüfung durchgeführt wird.

Hinweis: Die Werte für diese Eigenschaften sind und können nach der Änderung nicht mehr geändert werden (sie können nicht rückgängig gemacht werden). Wenn Sie weitere Fragen haben, wenden Sie sich an Kundenservice und Support.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*com.glide.communications.httpclient.verify_revoked_certi*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Deaktivieren Sie den Zertifikatverifizierungsprozess, der alle Zertifikate in der Zertifikatkette durch Überprüfen des Sperrstatus auswertet. Nur ein selbstsigniertes Serverzertifikat muss in den Instanz-Truststore geladen werden.
Typ	true | false
Standardwert	wahr
Empfohlener Wert	wahr
Funktionale Auswirkung	(Mittel)
Sicherheitsrisiko	(Mittel) API-Aufrufe, die das Plugin „Hohe Sicherheit“ verwenden, werden nicht mit einer OCSP-Widerrufsprüfung im Instanz-Trust Store verifiziert.
Referenzen	Zertifikate

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Best Practices für Sicherheit (Härtung der Instanzsicherheit)

Zusätzlich zu den Sicherheitskonfigurationen ist ein zusätzlicher manueller Aufwand erforderlich, um die Anwendung Now Platform täglich zu sichern. Dieser Abschnitt enthält

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitsaufgaben, die ein Administrator regelmäßig innerhalb eines bestimmten Zeitintervalls ausführen sollte.

Inhaltstypoptionen automatisch festlegen [In Security Center 1.3.3 entfernt]

Der HTTP-Header der X-Inhaltstypoption-Antwort wird vom Server verwendet, um anzugeben, dass die in den Inhaltstyp-Headern angegebenen MIME-Typen (Multifunktions-Internet-Mail-Erweiterungen) befolgt werden sollen.

Durch das Festlegen dieses Headers wird verhindert, dass der Browser Dateien als etwas anderes interpretiert, als vom Inhaltstyp in den HTTP-Headern deklariert wird. Dieser Header kann dazu beitragen, MIME-Verwirrungsangriffe abzuschwächen.

Die Option zum automatischen Festlegen von Inhaltstypen ist konform, wenn *glide.security.header.auto_set_x_content_type_options* auf „ **true**“ festgelegt ist.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.security.header.auto_set_x_content_type_options*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Verhindert, dass der Browser Dateien als etwas anderes interpretiert als durch den Inhaltstyp in den HTTP-Headern deklariert.
Typ	boolean
Empfohlener Wert	wahr
Funktionale Auswirkung	(Hoch) Dieser Header kann dazu beitragen, MIME-Verwirrungsangriffe abzuschwächen.
Sicherheitsrisiko	(Hoch) Wenn diese Eigenschaft nicht aktiviert ist, kann der Browser den Inhaltstyp in den HTTP-Headern falsch interpretieren.
Referenzen	Herunterladbare MIME-Typen

Cache-Steuerung – HTTP-Headerwert (Instanzsicherheitshärtung)

Verwenden Sie die Eigenschaft *glide.http.cache_control*, um den Standardwert für die Cachesteuerung in den HTTP-Antwortheadern festzulegen, die von Now Platform gesendet werden, wenn statische Inhaltsdaten für eine Seite angefordert werden. Beispiele für statische Inhalte sind Bilder, CSS und JavaScript, die von innerhalb einer Seite gerendert werden.

Die Eigenschaft *glide.http.cache_control* legt den Standardwert für Cache-Steuerung in HTTP-Antwortheadern auf **private** oder **öffentlich**fest. Der Standardwert ist **public**.

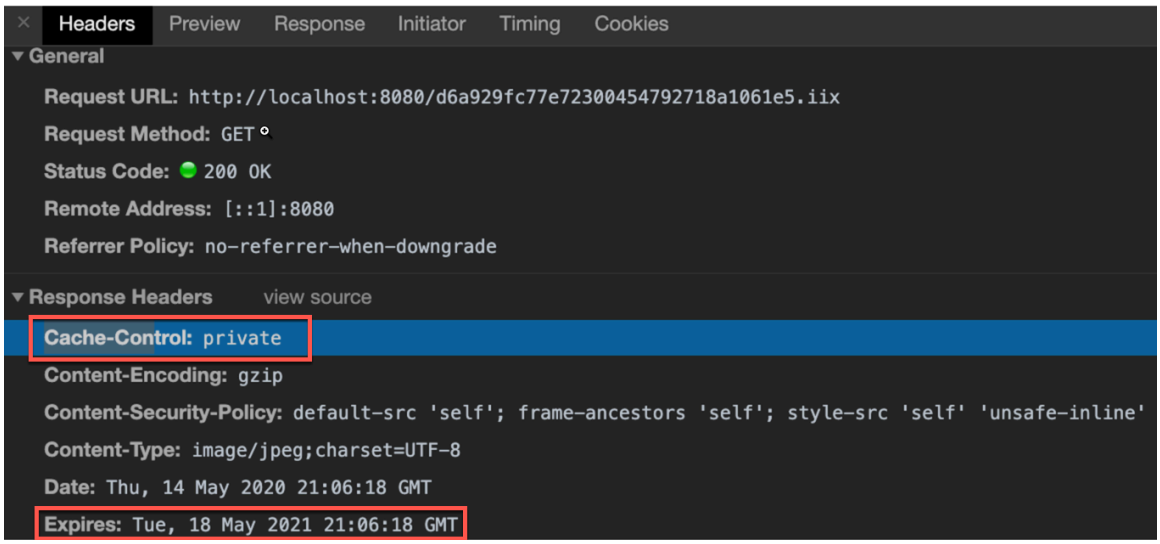
Wert	Beschreibung
Privat	Statische Inhalte können auf Browserebene (Client-Ebene) zwischengespeichert werden, nicht jedoch auf Proxyserverebene.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wert	Beschreibung
Öffentlich	Statische Inhalte können auf Browserebene (Client) und auch auf Proxyserverebene zwischengespeichert werden.

Der Wert Expires in den HTTP-Antwortheadern steuert, wann der statische Inhalt abläuft. Er hat einen Standardwert von 369 Tagen. Um den Standardwert manuell zu überschreiben, verwenden Sie die Eigenschaft *glide.http.expire.days*.



Hinweis: Mit der Eigenschaft *glide.http.cache* können Sie festlegen, ob das Festlegen der Werte für Cache-Steuerung und Ablauf in HTTP-Antwortheadern aktiviert oder deaktiviert werden soll. Der Standardwert ist **true**, wodurch Sie Folgendes festlegen können:

- Cache-Steuerungswert standardmäßig unter Verwendung der Eigenschaft *glide.http.cache_control*.
- Läuft standardmäßig mit der Eigenschaft *glide.http.expire.days* ab.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.http.cache_control
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Zum Konfigurieren des HTTP-Antwort-Header-Werts „Cache-Steuerung“ für statischen Inhalt.
Standardwert	Öffentlich
Empfohlener Wert	Privat
Funktionale Auswirkung	(Mittel) Legt den Standardwert für „Cache-Control“ in einem HTTP-Antwortheader fest.
Sicherheitsrisiko	(Hoch) Wenn Sie diese Eigenschaft auf „ **public**“ festlegen, können Instanzen mit CDN/Proxys statischen

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Inhalt zwischenspeichern und ohne Authentifizierung rendern. • **„privat“** ist eine geeignetere Einstellung für Instanzen mit CDN-/Proxy-Setup. • Wenn für die Instanz kein CDN/Proxy eingerichtet ist, sollten beide Werte geeignet sein.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Sicherheit für Berichte durchsetzen

Deaktivieren Sie diese Eigenschaft, um zu verhindern, dass der Anwender Berichte veröffentlicht oder auf sie zugreift. Diese Eigenschaft deaktiviert die Funktion für veröffentlichte Berichte in der Berichterstellung.

Aktivieren Sie das Veröffentlichen von Berichten, indem Sie *glide.report.published_reports.enabled* auf **true** setzen.

Sicherheit für Berichte erzwingen ist konform, wenn *glide.report.published_reports.enabled* auf „ **falsch**“ festgelegt ist.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.report.published_reports.enabled*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Deaktiviert die Funktion „Veröffentlichte Berichte“ in der Berichterstellung.
Typ	wahr | falsch
Empfohlener Wert	**false**
Funktionale Auswirkung	(Mittel) Der Anwender kann keine Berichte veröffentlichen.
Sicherheitsrisiko	(Mittel) Wenn diese Eigenschaft nicht aktiviert ist, können Anwender möglicherweise auf Berichte zugreifen oder diese veröffentlichen, die vertrauliche Daten verfügbar machen. Durch das Veröffentlichen eines Berichts wird eine URL erstellt, über die alle Benutzer auf den Bericht zugreifen können, auch Personen, die keine Benutzer von sind. Wenn jemand zur URL navigiert, wird der Bericht mit aktuellen Daten aus der Instanz generiert.
Referenzen	Berichte veröffentlichen

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Plugin für hohe Sicherheit (Härtung der Instanzsicherheit)

Wenn Sie das Plugin „Hohe Sicherheit“ aktivieren, erstellt oder aktualisiert es Hunderte verschiedener Konfigurationen, um das Sicherheitsniveau in Ihrer Instanz zu steuern. Diese Konfigurationen entschärfen viele der häufigsten OWASP-Angriffe, indem sie eine strenge Zugriffssteuerung, Eingabevalidierung und Ausgabecodierung ermöglichen.

Diese Konfigurationen umfassen:

- Zugriffssteuerung
- Business-Regeln
- Systemeigenschaften
- UI-Richtlinienaktion
- Skriptaktionen
- Skripteinbindungen

Beispiel

In den Beispielen finden Sie die folgenden Eigenschaften:

Eigenschaft	Thema
glide.ui.escape_all_script	Escape Jelly
glide.security.strict.actions	UI-Aktion vor der Ausführung überprüfen
glide.security.csrf_ previous.allow	Anti-CSRF-Token
glide.security.csrf.strict.validation.mode	Strikte CSRF-Validierung

Weitere Informationen

Attribut	Beschreibung
Plugin-Name	com.glide.high_security
Konfigurationstyp	Systemdefinition > Plugins – Entwicklung
Zweck	Dieses Plugin muss aktiviert werden. Sie erhöht die Sicherheitsstufe einer Instanz, wodurch die Angriffsfläche reduziert wird, indem die 10 häufigsten OWASP-Angriffe abgeschwächt werden, einschließlich CSRF, XSS, sichernder Sitzungscookies und Datei-Uploads.
Empfohlener Wert	Aktiv
Funktionale Auswirkung	(Hoch) Dieses Plugin ermöglicht verschiedene Systemsicherheitskonfigurationen, die sich auch auf die Anwenderoberfläche und die Funktionalität auswirken können.
Sicherheitsrisiko	(Hoch) Viele Sicherheitskonfigurationen sind unbeabsichtigt offen gelassen, was einige der kritischen Schwachstellen öffnen kann.
Referenzen	Einstellungen für hohe Sicherheit werden aktiviert

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Strenge Sicherheitseinstellungen

Weitere Informationen zum Aktivieren von Plugins finden Sie unter Plugins aktivieren .

Individuelle Anmelde-IDs (Härtung der Instanzsicherheit)

Stellen Sie sicher, dass alle Benutzer über individuelle Benutzer-IDs verfügen, wodurch alle Benutzeraktivitäten überwacht werden können.

Hinweis: Für lokale Anwenderaccounts, die nicht verwendet werden, muss die Kennzeichnung „ **Aktiv** “ auf „falsch“ gesetzt sein.

- Wenn Sie die Kennzeichnung **Aktiv** auf „ **falsch** “ setzen, wird die Kennzeichnung **Gesperrt** automatisch auf **wahr gesetzt**. Wenn die Kennzeichnung **Gesperrt** auf **true**festgelegt ist, kann dieser Anwenderaccount sich nicht bei der Instanz authentifizieren.
- Wenn Sie die Kennzeichnung „ **Aktiv** “ auf „ **false** “ setzen, wird kein Anwender aus dem Now Platformentfernt, aber die Sichtbarkeit für Nicht-Admin-Accounts wird entfernt.
- Wenn die Kennzeichnung „ **Aktiv** “ auf „ **falsch**“ und die Kennzeichnung **„Gesperrt“** ebenfalls auf **„falsch**“ festgelegt ist, kann sich ein Anwender weiterhin bei diesem Account anmelden.

Weitere Informationen zu Anwenderaccounts finden Sie unter Anwenderverwaltung .

Verschleierung der mobilen Anwenderoberfläche (Instanzsicherheitshärtung)

Verwenden Sie die Eigenschaft *glide.ui.m.blur_ui_when_backgrounded*, um alle Felder aus dem Snapshot zu verschleiern, da das Bild während des Hintergrundprozesses gespeichert wird. zu verschleiern.

Auf Android-Geräten erstellt das Android-Betriebssystem einen Screenshot zur Verwendung im Menü für aktuelle Aufgaben, wenn die Anwendung im Hintergrund ausgeführt wird. Benutzer können auch manuelle Screenshots der Anwendung erstellen, die öffentlich auf dem Gerät gespeichert werden.

Auf iOS-Geräten können Anwendungen mit dem iOS-Betriebssystem auch Bilddateien speichern. Diese Datei stellt den letzten Bildschirm dar, den der Anwender sieht, wenn die Anwendung in den Hintergrund verschoben wird. Der Zweck besteht zwar darin, eine bessere Anwender-Experience zu bieten, stellt jedoch auch ein Sicherheitsrisiko dar, da die Bilder als PNG-Bilddateien gespeichert werden.

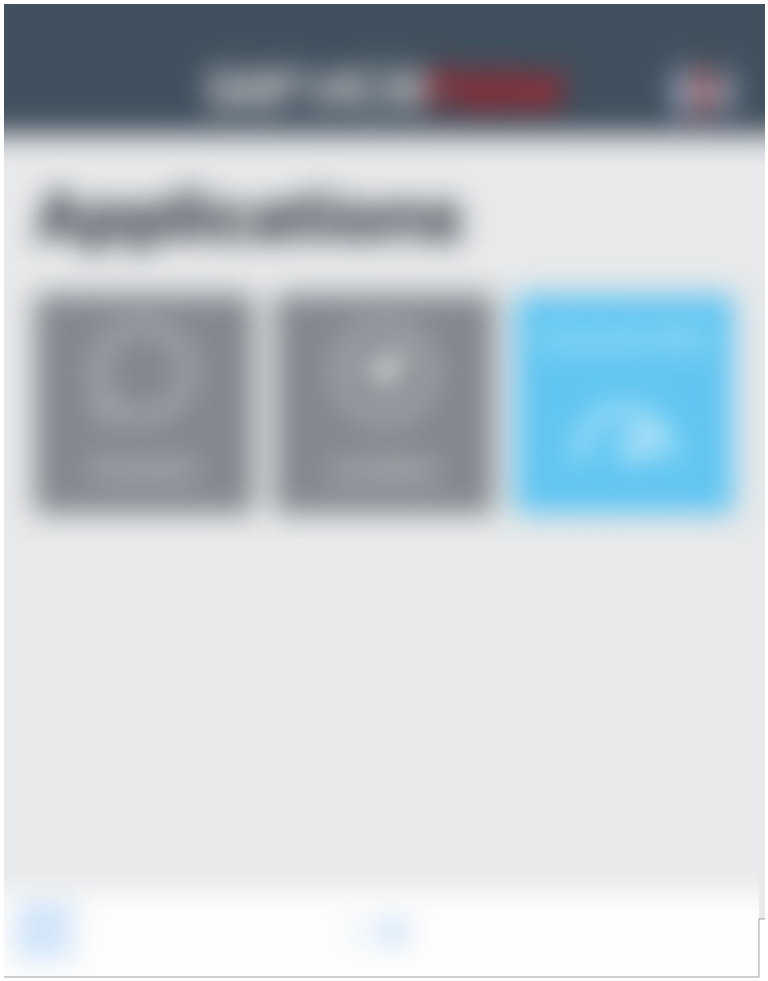
Hinweis: Diese Einstellung oder Konfiguration gilt pro Instanz, daher muss der Anwender eine Verbindung zur Instanz mit der konfigurierten Eigenschaft herstellen.

Informationen zum Verschleiern aller Felder aus dem Snapshot in der ServiceNow Classic-App finden Sie unter Option zum Unscharfmachen von Apps konfigurieren, um die Sicherheit zu verbessern .

Beispiel

Wenn Sie diese Eigenschaft auf **true**festlegen, . Die Hintergrundanwendung wird für iOS-Geräte verschleiert und für Android-iOS-Geräte geschwärzt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Weitere Informationen

Attribut	Beschreibung
Eigenschafts-/Plugin-Name	glide.ui.m.blur_ui_when_backgrounded
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurierbar im Instanz-Sicherheitszentrum	Nein
Zweck	Dient zum Verschleiern aller Felder des Snapshots, da das Bild während des Hintergrundprozesses gespeichert wird.
Empfohlener Wert	wahr
Funktionale Auswirkung	(Niedrig) Wenn die Eigenschaft *glide.ui.m.blur_ui_when_backgrounded* auf **true** festgelegt ist, verwenden die nativen Apps den auf dem Server definierten Parameter, um den Bildschirm unscharf zu machen, wenn die App in den Hintergrund verschoben wird.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Die von iOS- und Android-Geräten aufgenommenen Screenshots werden unscharf, wenn die App in den Hintergrund verschoben wird. • Die Anwender-Experience kann beeinträchtigt werden, da der Inhalt nicht angezeigt wird, wenn die App im Hintergrund ausgeführt wird.
Sicherheitsrisiko	(Mittel) Ein gefährdetes Gerät (mit Jailbreak) würde einem Angreifer vollständigen Zugriff auf das Dateisystem ermöglichen, d. h. auf Dateien/Snapshots mit eingebetteten vertraulichen Informationen.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Patches und Updates (Härtung der Instanzsicherheit)

Stellen Sie sicher, dass auf der Instanz die aktuelle Patch-Ebene ausgeführt wird. Sicherheitsfixes werden regelmäßig für Now Platform im Rahmen vieler Patches und Hotfixes veröffentlicht, die mit Produktfeature-Updates geliefert werden. Ein Upgrade, wenn neue Patches und Hotfixes verfügbar sind, reduziert das Risiko potenzieller Schwachstellen.

Now Platform wird durchschnittlich zwei Penetrationstests pro Woche unterzogen.

- Die meisten dieser Tests führen zwar nicht zu nennenswerten Schwachstellen, es werden jedoch regelmäßig Schwachstellen gefunden und behoben.
- Informationen zu den Releases, Patches und Hotfixes für Now Platform finden Sie im Abschnitt „Release-Hinweise“ in der Produktdokumentation. Weitere Informationen finden Sie in den Versionshinweisen zu Upgrades .

Demodaten entfernen (Härtung der Instanzsicherheit)

Demodaten, insbesondere Demo-Accounts, werden normalerweise beim Erstellen einer Instanz berücksichtigt. In diesem Fall sollten alle Demodaten entfernt werden, bevor die Instanz außerhalb der Produktion oder in der Produktion verwendet wird.

Öffnen Sie eine Anforderung in HI. Stellen Sie sicher, dass Sie ein Administratorkonto erstellen, bevor Sie die Anforderung senden.

Es wird dringend empfohlen, dass das Entfernen von Demodaten in der Produktion in einer Test- und Entwicklungsumgebungsinstanz erfolgreich verifiziert wird, die ein aktueller Klon der Produktionsinstanz ist.

Interne Ressourcen

https://support.servicenow.com/kb_view.do?sysparm_article=KB0550107

https://community.servicenow.com/community?id=community_blog&sys_id=786eaeaddbd0dbc01dcaf3231f961959

Demodaten werden mithilfe des Servicekatalogs entfernt

Anstatt die Anforderung als Incident zu übermitteln, können bestimmte Benutzer die Entfernung von Demodaten für eine Instanz mithilfe des Servicekatalogs anfordern. Zu diesen Anwendern gehören interne Anwender und Anwender mit der Rolle „customer_admin“ oder „partner_admin“.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Navigieren Sie zu https://support.servicenow.com/now .
2. Geben Sie die Instanz an, aus der die Demodaten entfernt werden sollen.

   Wenn Sie Probleme haben, Ihre Instanz zu finden, stellen Sie dem Instanznamen ein * voran, um eine „Enthält"-Abfrage durchzuführen.
3. Klicken **Self-Service** > **Demodaten entfernen** > **an.**
4. Geben Sie Datum und Uhrzeit zum Entfernen der Demodaten aus der ausgewählten Instanz an.

   Datum und Uhrzeit müssen mindestens vier Stunden nach der aktuellen Uhrzeit liegen.
5. Klicken Sie auf **Absenden**.

Eine neue Change-Anforderung wird erstellt und automatisch angezeigt. Das **geplante Enddatum** wird automatisch basierend auf dem **geplanten Startdatum** plus fünf Stunden (je nachdem, wie lange der Prozess dauert) berechnet. In der Change-Anforderung Verwenden Sie die Beobachtungsliste, um weitere Mitglieder Ihres Teams hinzuzufügen, die über den Status der Change-Anforderung Bescheid wissen müssen.

Sicherheitsaufnahmeliste (Härtung der Instanzsicherheit)

Ein „positives" Sicherheitsmodell (auch als „Einschlussliste" bezeichnet) definiert, was zulässig ist, und lehnt alles andere ab. Dieser Abschnitt enthält Sicherheitskontrollen, die ein Administrator konfigurieren kann, um das Verhalten auf bekannte Aufnahmelisten einzuschränken.

Hinweis: Die Eigenschaften der Sicherheitsaufnahmeliste müssen manuell für jede Instanz eingerichtet werden, da Update Sets die Konfiguration nicht heraufstufen und einen Fehler zurückgeben.

Aufrufe von Allow-Listenmitgliedern überprüfen (Instanzsicherheitshärtung)

Überprüfen und entfernen Sie Anrufeinträge für Aufnahmelistenmitglieder nach Bedarf aus der Tabelle „sys_whitelist_member".

Aufrufeinträge von Mitgliedern können auf die Java-Ressourcen auf der Serverseite zugreifen, um anwendungsbasierte Vorgänge ohne entsprechende Validierung durchzuführen. Da dies zu unbefugten Offenlegungen oder Änderungen von Kundendaten führen kann, stellt dies ein erhebliches Sicherheitsproblem dar.

Weitere Informationen

Attribut	Beschreibung
Tabellenname	sys_whitelist_member **Hinweis:** In den letzten Releases können nur ServiceNow-Mitarbeiter auf diese Tabelle zugreifen. dazu sind nicht einmal Administratoren in der Lage.
Konfigurationstyp	Tabelle
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Zweck	Zum Überprüfen und Entfernen von Einträgen aus dieser Tabelle.
Empfohlener Wert	In der Tabelle darf kein Datensatz vorhanden sein (Liste muss leer sein).
Funktionale Auswirkung	(Niedrig) Es sollte keine Auswirkungen geben, solange Sie die Ergebnisse überprüfen und genehmigen, die beim Ausführen des Tools zum Entfernen von Paketaufrufen generiert werden. Um sicherzustellen, dass die Instanz ordnungsgemäß funktioniert, testen Sie die Changes in einer Umgebung außerhalb der Produktion, bevor Sie sie in der Produktionsumgebung bereitstellen. Weitere Informationen finden Sie unter Tool zum Entfernen von Paketaufrufen.
Sicherheitsrisiko	(Hoch) Clientseitige API-Aufrufe, die zum Abruf von Daten oder zum Objektzugriff auf dem Server führen, gelten unter Sicherheitsaspekten als gefährlich. Validieren Sie diese Elemente für die Autorisierung und Einschränkung des Zugriffs auf vertrauliche Objekte.

Schritte zum Konfigurieren von

Hinweis: Die folgenden Schritte ähneln den in den Abschnitten „Schritte zum Konfigurieren“ in beschriebenen Schritten:

- Tool zum Entfernen von Paketenaufrufen
- Überprüft die Allow-Liste der Paketaufrufe

Wenn Sie sie bereits abgeschlossen haben, können Sie diese Schritte überspringen.

1. Aktivieren Sie das Plugin „Tool zum Entfernen von Paketenaufrufen“. Weitere Informationen finden Sie unter Tool zum Entfernen von Paketaufrufen.
2. Navigieren Sie mit dem **Filternavigator zu Pakete Anrufentfernung Dienstprogramm**.
3. Klicken Sie auf die einzelnen Skripts von (1) bis (4). Warten Sie auf die Ausgabe, und fahren Sie dann mit der nächsten fort.
4. Sobald Sie das Skript (4) ausgeführt haben, wird auf der Seite „Paketeaufruf-Elemente“ eine Liste der betroffenen Felder angezeigt.
5. Lösen Sie alle Elemente in den Abschnitten Vorgeschlagen und Fehler.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Dieses Tool kann einige Paketaufrufe melden, die in `„sa_mapping_ext_commands“` und `„sa_custom_operation“`verwendet werden. Diese Paketaufrufe gehören zum MID-Server. Da es keine Klassen gibt, wird der Code im MID-Server ausgeführt. Wenn Sie die folgenden Mitgliederaufrufe im Abschnitt „Fehler“ finden, markieren Sie sie als **Abgelehnt** (Ignoriert). Das Tool meldet diesen Mitgliedsanruf nicht erneut.

- `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_content);`
- `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(Dateiname);`
- `Packages.com.snc.sw.commands.HttpCallHandler`
- `Packages.com.snc.sw.dto.ProviderType.SSH`

6. Wenden Sie sich für eine weitere Korrektur an den Support von ServiceNow.

Paketaufrufe für Allow-Liste prüfen (Instanzsicherheitshärtung)

Überprüfen und entfernen Sie Paketaufrufeinträge in der Aufnahmeliste nach Bedarf aus der Tabelle „sys_whitelist_package“.

Paketaufrufeinträge können auf serverseitige Java-Ressourcen zugreifen, um anwendungsbasierte Vorgänge ohne entsprechende Validierung durchzuführen. Da dies zu unbefugten Offenlegungen oder Änderungen von Kundendaten führen kann, stellt dies ein erhebliches Sicherheitsproblem dar.

Weitere Informationen

Attribut	Beschreibung
Tabellenname	sys_whitelist_package **Hinweis:** In neueren Releases kann nur Kundenservice und Support auf diese Tabelle zugreifen. dazu sind nicht einmal Administratoren in der Lage.
Konfigurationstyp	Tabelle
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Zum Überprüfen und Entfernen von Einträgen aus dieser Tabelle.
Empfohlener Wert	In der Tabelle darf kein Datensatz vorhanden sein (Liste muss leer sein).
Funktionale Auswirkung	(Niedrig) Es sollte keine Auswirkungen geben, solange die Ergebnisse der Ausführung des Tools zum Entfernen von Paketaufrufen überprüft und genehmigt werden. Um sicherzustellen, dass die Instanz ordnungsgemäß funktioniert, testen Sie die Changes in einer Umgebung außerhalb der Produktion, bevor Sie sie in der Produktionsumgebung bereitstellen. Weitere Informationen finden Sie unter Tool zum Entfernen von Paketenaufrufen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	(Hoch) Clientseitige API-Aufrufe, die zum Abruf von Daten oder zum Objektzugriff auf dem Server führen, gelten unter Sicherheitsaspekten als gefährlich. Validieren Sie diese Elemente für die Autorisierung und Einschränkung des Zugriffs auf vertrauliche Objekte.
Workaround	Wenden Sie sich an den Support von ServiceNow, um Unterstützung zu erhalten.

Schritte zum Konfigurieren von

1. Aktivieren Sie das Plugin „Tool zum Entfernen von Paketenaufrufen“. Weitere Informationen finden Sie unter Tool zum Entfernen von Paketaufrufen.
2. Navigieren Sie mit dem **Filternavigator zu Pakete Anrufentfernung Dienstprogramm**.
3. Klicken Sie auf die einzelnen Skripts von (1) bis (4). Warten Sie auf die Ausgabe, und fahren Sie dann mit der nächsten fort.
4. Sobald Sie das Skript (4) ausgeführt haben, wird auf der Seite „Paketeaufruf-Elemente“ eine Liste der betroffenen Felder angezeigt.
5. Lösen Sie alle Elemente in den Abschnitten Vorgeschlagen und Fehler.

   Hinweis: Dieses Tool kann einige Paketaufrufe melden, die in `„sa_mapping_ext_commands“` und `„sa_custom_operation“`verwendet werden. Diese Paketaufrufe gehören zum MID-Server. Da es keine Klassen gibt, wird der Code im MID-Server ausgeführt. Wenn Sie im Abschnitt „Fehler“ die folgenden Paketaufrufe finden, markieren Sie sie als **Abgelehnt** (Ignoriert). Das Tool meldet diesen Paketaufruf nicht erneut.

   - `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_content);`
   - `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(Dateiname);`
   - `Packages.com.snc.sw.commands.HttpCallHandler`
   - `Packages.com.snc.sw.dto.ProviderType.SSH`

6. Wenden Sie sich für eine weitere Korrektur an den Support von ServiceNow.

URL-Allow-Liste für ursprungsübergreifende IFrame-Kommunikation aktivieren (Instanzsicherheitshärtung)

Verwenden Sie die Eigenschaft *`glide.ui.concourse.onmessage_enforce_same_origin`*, um die ursprungsübergreifende Kommunikation zwischen `iframes`zu aktivieren.

`Openframe` kann nur Nachrichten aus vertrauenswürdigen Domänen verarbeiten, die in der Eigenschaft *`glide.ui.concourse.onmessage_enforce_same_origin_whitelist`* angegeben sind. Weitere Informationen finden Sie unter UTL-Allow-Liste für ursprungsübergreifende IFrame-Kommunikation festlegen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.concourse.onmessage_enforce_same_origin
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um die Aufnahme vertrauenswürdiger Domänen zu aktivieren, damit diese zwischen IFrames für OpenFrame kommunizieren können.
Empfohlener Wert	wahr
Funktionale Auswirkung	(Mittel) Wenn Sie beabsichtigte Domänen nicht in die Aufnahmeliste aufnehmen, ist die Möglichkeit zum Einbetten anderer Seiten in Now Platform -Instanzen möglicherweise eingeschränkt.
Sicherheitsrisiko	(Hoch) Wenn eine Webseite Ereignishandler enthält, die keine ordnungsgemäße Validierung des Ursprungs durchführen, kann eine Webseite oder ein Skript von einem beliebigen Ursprung mit der Seite kommunizieren. Sie können auch beliebige Funktionen initiieren, die vom Ereignis-Handler ausgeführt werden.
Referenzen	OpenFrame-Übersicht

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Relative Links erzwingen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.cms.catalog_uri_relative*, um relative Links vom URI-Parameter für `/ess/catalog.do`zu erzwingen.

- Bei Festlegung auf **true**werden nur relative URLs über die Seite „ `/ess/catalog.do` “ unter Verwendung des Parameters *uri* zugelassen.
- Bei Festlegung auf **„falsch**“ sind alle URLs zulässig, was auch Verknüpfungen zu externen, nicht autorisierten Inhalten zulassen kann.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.cms.catalog_uri_relative
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um Versuche einzuschränken, externe, nicht autorisierte Inhalte zu verknüpfen.
Empfohlener Wert	wahr
Funktionale Auswirkung	(Niedrig) Diese Korrektur erzwingt die Validierung auf der Katalogseite, sodass nur relative URLs zulässig sind. Vorhandene Links zu externen Webanwendungen werden beschädigt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	(Hohe) absolute URLs können ein Sicherheitsrisiko darstellen, wenn sie als Teil von Parametern oder Feldwerten verwendet werden und so die Quellseite auf eine von Angreifern kontrollierte Website umleiten.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Tool zum Entfernen von Paketaufrufen (Härtung der Instanzsicherheit)

Aktivieren und starten Sie das Plugin Packages Call Entfernung Tool (*com.glide.script.packages_call_removal*), und überlegen Sie dann, ob jede der vorgeschlagenen Änderungen abgeschlossen oder abgelehnt werden soll.

Das Tool zum Entfernen von Paketenaufrufen ist ein Plugin, das:

- Durchsucht Skripts nach Paketaufrufen für Now Platform Java-Klassen.
- Schlägt Änderungen vor, um sie durch bevorzugte GlideScriptable-Namen zu ersetzen.
- Erleichtert die Skriptänderungen.

Hinweis: Wenn es sich bei diesem Datensatz um einen Basissystemdatensatz handelt, wird das Element durch Verwendung der Empfehlung des Tools als „customer_update“ markiert. Dieses Skript kann in Zukunft keine weiteren Updates annehmen. In späteren Releases wird erwartet, dass die Tabellen „sys_whtelist_xxx“ leer sind. Es kann jedoch dennoch nützlich sein, dieses Tool zu verwenden, da es Pakete,xxx-Aufrufe kennzeichnet.

Das Tool zum Entfernen von Paketaufrufen meldet möglicherweise einige Paketaufrufe, die in `„sa_mapping_ext_commands“` und `„sa_custom_operation“`verwendet werden. Diese Paketaufrufe gehören zum MID-Server. Da es keine Klassen gibt, wird der Code im MID-Server ausgeführt. Wenn Sie im Abschnitt „Fehler“ einen der folgenden aufgelisteten Paketaufrufe finden, markieren Sie ihn als Abgelehnt (Ignoriert). Das Tool meldet diesen Paketaufruf nicht erneut.

- `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_content);`
- `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(Dateiname);`
- `Packages.com.snc.sw.commands.HttpCallHandler`
- `Packages.com.snc.sw.dto.ProviderType.SSH`

Weitere Informationen

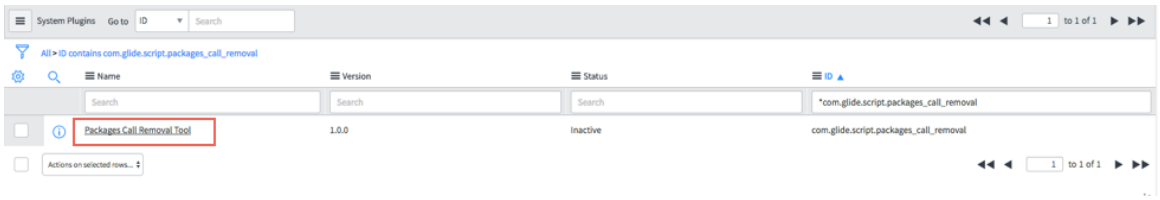
Attribut	Beschreibung
Plugin-Name	com.glide.script.packages_call_removal
Konfigurationstyp	Systemdefinition > Plugins
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Entfernen/Ersetzen nicht autorisierter Paket-/Mitgliedsaufrufe durch zulässige Glide-Namen (GlideScriptable), die nur autorisierten Zugriff auf Daten ermöglichen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

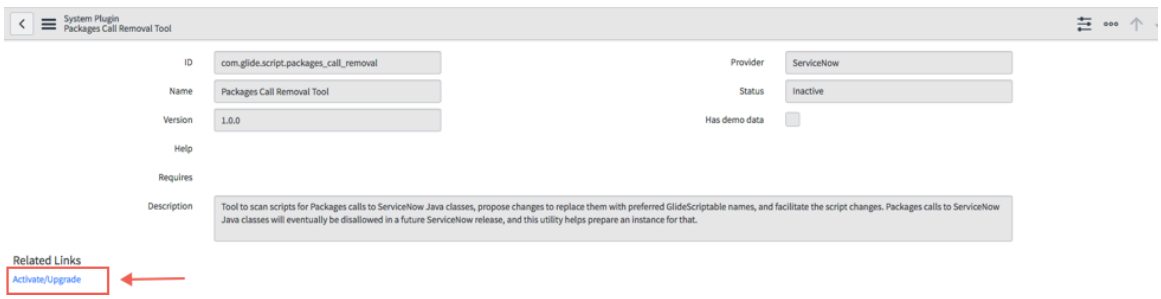
Attribut	Beschreibung
Empfohlener Wert	Aktiv
Funktionale Auswirkung	(Niedrig) Diese Korrektur würde die Paketaufrufe durch *GlideScriptable* APIs ersetzen und kann sich auf die Anpassungen auswirken, die Paketaufrufe enthalten. Das Tool ersetzt Paketaufrufe nicht automatisch. Stattdessen werden Vorschläge bereitgestellt, die in der Tabelle „packages_call_item“ gespeichert sind. Ihr Administrator kann dann entscheiden, ob er den vorgeschlagenen Change akzeptiert oder ablehnt.
Sicherheitsrisiko	(Mittel) Clientseitige API-Aufrufe, die zum Abruf von Daten oder zum Objektzugriff auf dem Server führen, gelten unter Sicherheitsaspekten als gefährlich. Sie sollten für die Autorisierung und Einschränkung des Zugriffs auf vertrauliche Objekte validiert werden.

Schritte zum Konfigurieren von

1. Navigieren zu **Systemdefinition** > **Plugins**

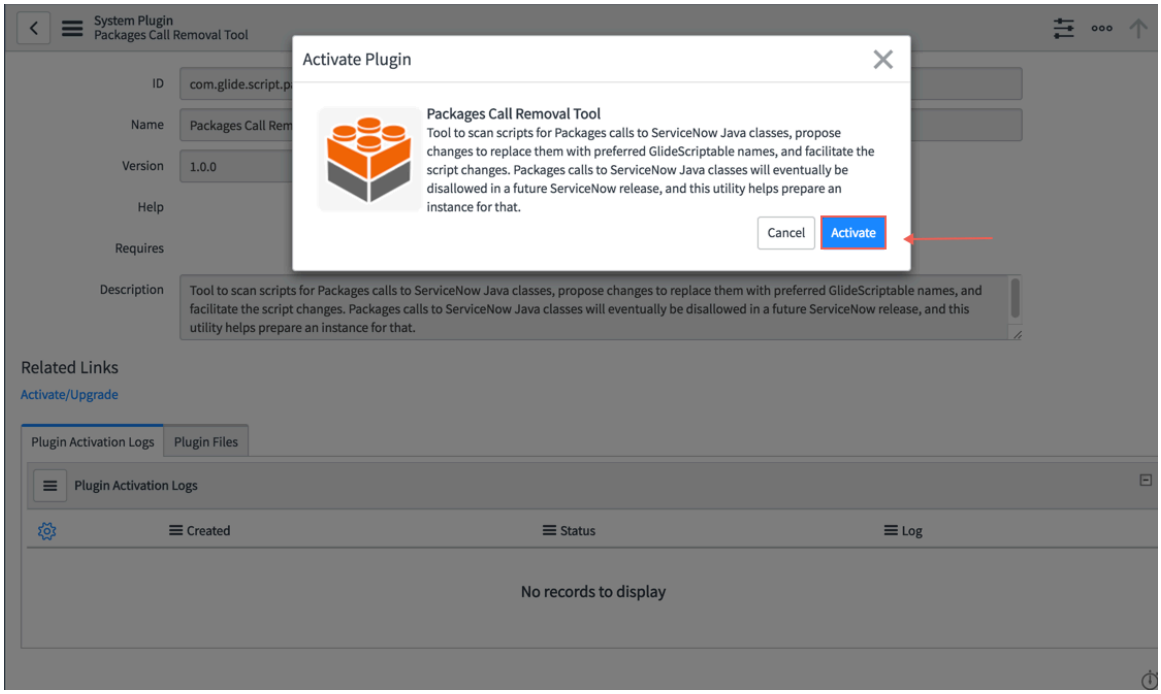


2. Suchen Sie nach der Plugin-ID = *com.glide.script.packages_call_removal*.



3. Klicken Sie auf **Aktivieren/Upgrade**, um das Plugin zu aktivieren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Um Aufrufe von Aufnahmelistenpaketen und Aufnahmelistenmitglieder zu überprüfen, führen Sie die in den Abschnitten „Schritte zum Konfigurieren“ in den folgenden Themen beschriebenen Aktionen aus:
   - Überprüft die Anrufe von Allow-Listenmitgliedern
   - Überprüft die Allow-Liste der Paketaufrufe

URL-Allow-Liste für ursprungsübergreifende iFrame-Kommunikation angeben (Instanzsicherheitshärtung)

Verwenden Sie die Eigenschaft *glide.ui.concourse.onmessage_enforce_same_origin_whitelist*, um die ursprungsübergreifende Kommunikation zwischen `iframes` aus vertrauenswürdigen Domänen zu ermöglichen, die Sie in einer Aufnahmeliste angeben.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.concourse.onmessage_enforce_same_origin_whitelist
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Nein
Zweck	Zum Aktivieren der Aufnahmeliste von vertrauenswürdigen Domänen, damit diese zwischen IFrames für OpenFrame kommunizieren können.
Anforderung	Obligatorisch
Funktionale Auswirkung	(Mittel) Wenn Sie die gewünschten Domänen nicht in die Aufnahmeliste aufnehmen, ist die Möglichkeit zum Einbetten anderer Seiten in den Now Platform -Instanzen möglicherweise eingeschränkt.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	(Hoch) Wenn eine Webseite Ereignishandler enthält, die keine ordnungsgemäße Validierung des Ursprungs durchführen, kann eine Webseite oder ein Skript von einem beliebigen Ursprung mit der Seite kommunizieren. Sie können auch beliebige Funktionen initiieren, die vom Ereignis-Handler ausgeführt werden. Die Kommunikation mit IFrames aus anderen Domänen stellt ein Sicherheitsrisiko dar.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

URL-Allow-Liste für Abmeldeumleitungen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.security.url.whitelist*, um eine zusätzliche Validierungsebene hinzuzufügen, um sicherzustellen, dass eine eingeführte externe URL Teil der URLs auf der Aufnahmeliste sein muss.

Eine offene Umleitung tritt auf, wenn eine angreifbare Webseite zu einer nicht vertrauenswürdigen und böswilligen Seite umgeleitet wird, die den Benutzer gefährden kann. Offene Umleitungsangriffe gehen mit einem Phishing-Angriff einher, da der geänderte angreifbare Link mit der ursprünglichen Website identisch ist, was die Erfolgswahrscheinlichkeit des Phishing-Angriffs erhöht.

Diese Eigenschaft gilt in den folgenden Fällen:

- `/logout.do?sysparm_goto_url={Externe URL}`
- `/cms_login_redirect.do?sysparm_goto_url={Externe URL}`

Benutzer werden zu einer externen vertrauenswürdigen Site weitergeleitet, nachdem sie sich von der Instanz abgemeldet haben:

- `/logout_redirect.do?sysparm_url={Externe URL}`
- `/saml_redirector.do?sysparm_uri={Externe URL}`

Wenn SAML aktiviert ist, wird eine Abmelde-URL eines Identitätsanbieters (IDP) aufgerufen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.security.url.whitelist
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Dient zur Implementierung einer sicheren URL-Umleitung während der Anmeldung, Abmeldung oder anderen Umleitungen. Diese Eigenschaft mindert einen der OWASP-Top-10-Angriffe namens „Ungültige Umleitungen und Weiterleitungen“.
Typ	Durch Kommas und Leerzeichen getrennte Zeichenfolge. Beispiel: `https://beispiel.com, https://wiki.beispiel.com`.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Wert	Die genehmigten URLs Ihrer Organisation [Ein definierter FQDN (vollständig qualifizierter Domänenname)] z. B. http://www.servicenow.de]
Funktionale Auswirkung	(Mittel) Diese Korrektur erzwingt die Validierung auf der Abmeldeseite. Dies kann sich auf einen Benutzer einer Instanz mit einer SSO/SAML-Konfiguration auswirken.
Sicherheitsrisiko	(Hoch) Die clientseitige offene Umleitung kann es Angreifern ermöglichen, Opfer/Anwender auf die vom Angreifer kontrollierte Website umzuleiten, und wird als Sicherheitsrisiko angesehen.
Referenzen	Fehler und Korrekturen für Multi-SSO (SAML 2.0).

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Sicherheitsrichtlinie für eingebetteten Virtual Agent-Client-Inhalt (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *com.glide.cs.embed.csp_frame_ancestors*, um die Konfiguration der Richtlinie „frame-ancestors“ nur für `https://` zu aktivieren.<your-instance> Seite .service-now.com/sn_va_web_client_app_embed.do

Das Virtual Agent-Plugin ermöglicht die Einbettung eines Clients in eine externe Webseite. Damit die Clientseite in eine Webseite eingebettet werden kann, muss die Inhaltssicherheitsrichtlinie die externe Seite als übergeordneten Frame zulassen.

Hinweis: Vermeiden Sie es, nur „`*`“ als Inhaltssicherheitsrichtlinie zu verwenden, da dadurch alle Domänen aktiviert würden und die Anwendung potenziell angreifbar für Clickjacking wäre.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	com.glide.cs.embed.csp_frame_ancestors
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Nein
Zweck	Um die Erstellung einer anwenderdefinierten Inhaltssicherheitsrichtlinie für die einbettbare Virtual Agent-Seite zu ermöglichen.
Empfohlener Wert	Auf vertrauenswürdige Domänen festlegen
Funktionale Auswirkung	(Hoch) Einbettbarer Virtual Agent-Client lässt nicht zu, dass er in externe Websites eingebettet wird, wenn die Inhaltssicherheitsrichtlinie nicht ordnungsgemäß konfiguriert ist.
Sicherheitsrisiko	(Mittel) Bei falscher Konfiguration (alle übergeordneten Frames zulassen) kann die

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	einbettbare Client-Seite möglicherweise angreifbar für Clickjacking werden.
Referenzen	Betten Sie den Virtual Agent-Webclient in eine externe Webseite ein Weitere Informationen zum Erstellen einer Inhaltssicherheitsrichtlinie für Frame-Vorgänger finden Sie hier.

Schritte zum Konfigurieren von

1. Navigieren zu **/sys_properties_list.do**an.
2. Suchen Sie nach der Eigenschaft *com.glide.cs.embed.csp_frame_ancestors*.
3. Weisen Sie eine akzeptable Sicherheitsrichtlinie für Inhalte zu (nur Unternehmens- oder andere akzeptierte Domänen zulassen), und klicken Sie dann auf **Aktualisieren**.

X-Frame-Options für eingebetteten Virtual Agent-Client (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *com.glide.cs.embed.xframe_options*, um die Konfiguration des X-Frame-Headers nur für `https://` zu aktivieren.<your-instance> Seite .service-now.com/sn_va_web_client_app_embed.do

Das Virtual Agent-Plugin ermöglicht die Einbettung eines Clients in eine externe Webseite. Damit die Clientseite in eine Webseite eingebettet werden kann, muss der X-Frame-Options-Header die Einbindung des `IFrame` in den übergeordneten Frame ermöglichen.

Hinweis: Vermeiden Sie die Verwendung von „ `allow-from *` “ als Headerwert für X-Frame-Options, da dadurch alle Domänen aktiviert würden und die Anwendung potenziell angreifbar für Clickjacking wäre.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	com.glide.cs.embed.xframe_options
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Nein
Zweck	Zum Aktivieren der Angabe der Direktive für den X-Frame-Options-Header für die einbettbare Virtual Agent-Seite.
Empfohlener Wert	gleicher Herkunft
Funktionale Auswirkung	(Hoch) Der einbettbare Virtual Agent-Client ermöglicht sich nicht die Einbettung in externe Websites, wenn der X-Frame-Options-Header nicht ordnungsgemäß konfiguriert ist.
Sicherheitsrisiko	(Mittel) Bei falscher Konfiguration (alle übergeordneten Frames zulassen) kann die

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	einbettbare Client-Seite möglicherweise angreifbar für Clickjacking werden.
Referenzen	Betten Sie den Virtual Agent-Webclient in eine externe Webseite ein

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

X-Frame-Options: SAMEORIGIN (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.set_x_frame_options*, um den X-Frame-Options-Antwortheader für alle UI-Seiten auf SAMEORIGIN festzulegen.

Verwenden Sie den HTTP-Antwortheader „X-Frame-Options“, um anzugeben, ob der Browser eine Seite in `<frame>` oder `<iframe>`rendern darf. Websites können diese Funktion verwenden, um Clickjacking-Angriffe zu vermeiden, indem sichergestellt wird, dass ihr Inhalt nicht in andere Websites eingebettet wird. Ein Angreifer könnte Ihre Seite in seine eigene Seite einbetten und Ihre Seitenelemente in böswillige Absichten überführen. Der Endanwender hält die Seite möglicherweise für legitim, da sie Ihrer Seite ähnelt. Der Endanwender kann wie üblich auf Elemente klicken, um schädliche Skripts oder Elemente auszuführen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.set_x_frame_options
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Zur Abwehr von ClickJacking-Angriffen.
Empfohlener Wert	wahr
Funktionale Auswirkung	(Niedrig) Diese Korrektur erzwingt die Einschränkung für das Rendern einer Now Platform -Anwendung in einer Drittparteianwendung in Form eines iFrame. Wenn Sie über eine solche Integration verfügen, wird die Anwendung in der angepassten Drittanbieter-App nicht gerendert.
Sicherheitsrisiko	(Mittel) Mit der Richtlinie „Same Origin“ können Sie verhindern, dass eine Domäne ein Skript oder eine Ressource aus einer anderen Domäne abruft. Alle modernen Browser unterstützen diese Funktionalität. Die Richtlinie validiert die Verbindung basierend auf Protokoll, Port und Host. CORS (Cross Origin Request) ist eine Änderung der Richtlinie für gleiche Herkunft, die den Zugriff auf Ressourcen/Skripts aus einer anderen Domäne ermöglicht, wenn sie explizit als Teil des Headerwerts angegeben wird.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• In diesem Fall steuert der **X-Frame-Options-** Header, ob die Anwendung Now Platform auf der Website des Drittanbieters gerendert werden kann. • Reduziert das sensible Risiko, da der Eigenschaftswert, wenn er auf **SAMEORIGIN** festgelegt ist, das Rendern nicht ermöglicht.
Referenzen	Verfügbare Systemeigenschaften iFrames konfigurieren

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Validierung der Verarbeitung externer XML-Entitäten

Diese Eigenschaften ermöglichen die Erweiterung von Entitäten und schränken jede externe Entität (z. B. URL) ein, wenn sie als Teil der XML-DOCTYPE-Referenz enthalten ist. DTD ist im Grunde ein XML-Schema. Wenn Sie nach einer Lösung für Entitätsdeklarationen suchen, die Potenzial für XXE (externe Entität) haben könnten, aktivieren Sie mithilfe der Systemeigenschaften einen auf der Einschlussliste aufgeführten Schutz gegen XXE.

Für XMLDocument- und XMLUtil-Analysen

Wenn Ihre Anpassungen `XMLDocument` oder `XMLUtil verwenden`, legen Sie die folgenden Systemeigenschaften fest. Sie steuern die Entitätserweiterung und ermöglichen die Validierung externer Entitäten, die nur die Verarbeitung von Entitäten in Aufnahmelisten zulassen.

Schwellenwert für die Entitätserweiterung festlegen (Instanzsicherheitshärtung)

Verwenden Sie die Eigenschaft *`glide.xmlutil.max_entity_expansion`*, um die maximale Entitätserweiterungsgrenze in eine kleinere Zahl zu ändern.

Now Platform verarbeitet keine weiteren Entitätserweiterungen, die größer als der in dieser Eigenschaft angegebene zulässige Grenzwert sind.

Hinweis: 3000 ist das von Now Platformfestgelegte Standardminimum, was als sicherer Schwellenwert gilt. Daher berücksichtigt die Plattform diesen Standardwert, wenn der von Ihnen eingegebene ganzzahlige Wert unter 3000 liegt.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.xmlutil.max_entity_expansion
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Diese Korrektursteuerung muss aktiviert sein, um sich gegen XML-Entitätserweiterungs-/Billion-Lach-Angriffe zu schützen.
Empfohlener Wert	3000

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Funktionale Auswirkung	(Niedrig) Wenn die Anpassung eine große Entitätserweiterung verwendet, blockiert Now Platform möglicherweise die weitere Verarbeitung.
Sicherheitsrisiko	(Hoch) Ein Angreifer kann diese Schwachstelle nutzen, um Daten exponentiell zu erweitern, wodurch schnell alle Systemressourcen verbraucht werden.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

XMLdoc/XMLUtil-Entitätsvalidierung mit Allow-Liste (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.xml.entity.whitelist.enabled*, um die Validierung einer externen Entität zu aktivieren. Sie lässt nur die Verarbeitung von Entitäten zu, die auf der Aufnahmeliste stehen.

- Wenn Sie diese Eigenschaft auf „ **true**“ festlegen, können nur Entitäten auf der Einschlussliste verarbeitet werden (empfohlene Einstellung).
- Wenn Sie diese Eigenschaft auf **false**festlegen, können alle externen Entitäten verarbeitet werden.

Voraussetzungen

Definieren Sie vor dem Festlegen dieser Eigenschaft eine Liste von kommagetrennten FQDNs in der Eigenschaft *glide.xml.entity.whitelist*, die die einzigen URLs sind, die über die Verarbeitung von XML-Entitäten erreicht werden können. Eigenschaft. Weitere Informationen finden Sie unter Verarbeitung externer XML-Entitäten – Allow-Liste.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.xml.entity.whitelist.enabled*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Diese Korrektursteuerung muss aktiviert sein, um sich gegen XXE-Angriffe zu schützen.
Empfohlener Wert	wahr
Funktionale Auswirkung	(Niedrig) Wenn die Anpassung eine externe Entität verwendet, die nicht in der Eigenschaft *glide.xml.entity.whitelist* aufgeführt ist, kann Now Platform die weitere Verarbeitung blockieren. Weitere Informationen finden Sie unter Verarbeitung externer XML-Entitäten – Allow-Liste.
Sicherheitsrisiko	(Hoch) Ein Angreifer kann die DTD verwenden, um beliebige HTTP-Anforderungen einzubinden, die vom Server ausgeführt werden könnten. Dies könnte zu weiteren Angriffen führen, die die Vertrauensstellung des Servers zu anderen Entitäten nutzen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Workaround	Wenn Sie die Erweiterung externer Entitäten nicht verwenden, deaktivieren Sie sie. Weitere Informationen finden Sie unter Entitätserweiterung deaktivieren.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Für XMLDocument2-Parser

Wenn Ihre Anpassungen einen XMLDocument2-Parser verwenden, verwenden Sie die folgenden Systemeigenschaften, um die Validierung externer Entitäten zu aktivieren.

Entitätserweiterung deaktivieren (Instanzsicherheitshärtung)

Wenn Anpassungen keine Entitätserweiterung erfordern, verwenden Sie die Eigenschaft *glide.stax.allow_entity_resolution*, um die externe Entitätserweiterung vollständig zu deaktivieren. Die XML-Datei schließt die Analyse ab, enthält jedoch keine internen oder externen Entitäten.

- Wenn Sie diese Eigenschaft auf **true**festlegen, versuchen alle externen Entitäten, abhängig von der Einstellung in der Eigenschaft *glide.stax.whitelist_enabled*, die betreffenden Entitäten aufzulösen oder zu erweitern.
- Wenn Sie diese Eigenschaft auf **false**festlegen, werden alle Auflösungen und Erweiterungen von Entitäten blockiert. Weitere Informationen finden Sie unter XMLdoc2-Entitätsvalidierung mit Allow-Liste.

Voraussetzungen

Vor dem Festlegen dieser Eigenschaft:

- Legen Sie die Eigenschaften *glide.xml.entity.whitelist.enabled*und *glide.stax.whitelist_enabled*auf „wahr“ fest. Weitere Informationen finden Sie unter XMLdoc/XMLUtil-Entitätsvalidierung mit Allow-Liste und XMLdoc2-Entitätsvalidierung mit Allow-Liste.
- Definieren Sie eine Liste von kommagetrennten FQDNs in der Eigenschaft *glide.xml.entity.whitelist*, den einzigen URLs, die über die Verarbeitung von XML-Entitäten erreicht werden können. Eigenschaft. Weitere Informationen finden Sie unter Verarbeitung externer XML-Entitäten – Allow-Liste.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.stax.allow_entity_resolution
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Diese Korrektursteuerung muss aktiviert sein, um sich gegen einen Angriff der XML-Entitätserweiterung/ Billion Leign zu schützen.
Empfohlener Wert	falsch

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Funktionale Auswirkung	(Niedrig) Wenn die Anpassung die Entitätserweiterung verwendet, blockiert Now Platform möglicherweise die weitere Verarbeitung.
Sicherheitsrisiko	(Hoch) Ein Angreifer kann diese Schwachstelle nutzen, um Daten exponentiell zu erweitern, wodurch schnell alle Systemressourcen verbraucht werden.
Workaround	Wenn die Anpassung eine Erweiterung der Entität erfordert, legen Sie diese Eigenschaft auf „true“ fest, und befolgen Sie die in XMLdoc2-Entitätsvalidierung mit Allow-Listedokumentierten Schritte.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Weitere Informationen zu OWASp-Ressourcen finden Sie unter OWASp .

XMLdoc2-Entitätsvalidierung mit Allow-Liste (Instanzsicherheitshärtung)

Verwenden Sie eine Eigenschaft, um die Verarbeitung von externen Entitäten, die in die Aufnahmeliste aufgenommen wurden, mit XMLDocument2 zu ermöglichen.

Voraussetzungen

Vor dem Festlegen dieser Eigenschaft:

- Legen Sie die Eigenschaft *glide.xml.entity.whitelist.enabled* auf „Wahr“ fest. Weitere Informationen finden Sie unter XMLdoc/XMLUtil-Entitätsvalidierung mit Allow-Liste.
- Definieren Sie eine Liste von kommagetrennten FQDNs in der Eigenschaft *glide.xml.entity.whitelist*, die die einzigen URLs sind, die über die Verarbeitung von XML-Entitäten erreicht werden können. Eigenschaft. Weitere Informationen finden Sie unter Verarbeitung externer XML-Entitäten – Allow-Liste.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.stax.whitelist_enabled
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Diese Korrektursteuerung muss aktiviert sein, um sich gegen Angriffe von externen XML-Entitäten zu schützen.
Empfohlener Wert	wahr
Funktionale Auswirkung	(Niedrig) Wenn die Anpassung eine externe Entität verwendet, die nicht in der Aufnahmeliste aufgeführt ist, blockiert Now Platform möglicherweise die weitere Verarbeitung. Weitere Informationen finden Sie unter Verarbeitung externer XML-Entitäten – Allow-Liste.
Sicherheitsrisiko	(Hoch) Ein Angreifer kann mithilfe der DTD beliebige HTTP-Anforderungen einschließen, die der Server

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	ausführen kann. Wenn die Vertrauensstellung des Servers zu anderen Entitäten verwendet wird, kann dies zu weiteren Angriffen führen.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Verarbeitung externer XML-Entitäten – Allow-Liste (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.xml.entity.whitelist*, um bei Bedarf den Zugriff auf eine Liste von durch Kommas getrennten FQDNs zu ermöglichen. Diese URLs sind die einzigen, die über die Verarbeitung von XML-Entitäten erreicht werden können.

Voraussetzungen

Bevor Sie diese Eigenschaft festlegen, legen Sie die Eigenschaft *glide.xml.entity.whitelist.enabled* fest, die die Validierung einer externen Entität und nur die Verarbeitung der Aufnahmeliste ermöglicht, die Sie in der Eigenschaft *glide.xml.entity.whitelist* angeben. Weitere Informationen finden Sie unter XMLdoc/XMLUtil-Entitätsvalidierung mit Allow-Liste.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.xml.entity.whitelist
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Zum Erstellen einer Aufnahmeliste von URLs, auf die die XML-Entitätsverarbeitung zugreifen kann.
Empfohlener Wert	Vom Anwender angegeben (z. B. https://google.com)
Funktionale Auswirkung	(Niedrig) Die Verarbeitung externer Entitäten kann blockiert werden, wenn sie nicht in der Aufnahmeliste aufgeführt ist. Wenn die Aufnahmeliste aktiviert ist, erfordert sie die PUBLIC-Form einer externen Entitätsdefinition.
Sicherheitsrisiko	(Hoch) Ein Angreifer kann mithilfe der DTD beliebige HTTP-Anforderungen einschließen, die der Server ausführen kann. Dies könnte zu weiteren Angriffen führen, die die Vertrauensstellung des Servers zu anderen Entitäten nutzen

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Management von Anwendersitzungen (Härtung der Instanzsicherheit)

Die Verwaltung von Anwendersitzungen hilft dabei, den Datenverkehr, der einem bestimmten Anwender gehört, richtig zu identifizieren. Treffen Sie Vorkehrungen, um sicherzustellen, dass die Vertrauensstellung nicht missbraucht wird.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Webanwendungen können Sitzungen erstellen, um anonyme Benutzer nach der ersten Benutzeranfrage nachzuverfolgen. Ein Beispiel wäre die Beibehaltung der Anwenderspracheinstellung, um Folgendes sicherzustellen:

- Identifizierung des Benutzers bei allen nachfolgenden Anforderungen.
- Anwendung von Sicherheitszugriffssteuerungen.
- Autorisierung des Zugriffs auf die privaten Daten des Anwenders.
- Erhöhung der Nutzbarkeit der Anwendung.

Daher können aktuelle Webanwendungen Sitzungsfunktionen sowohl vor als auch nach der Authentifizierung bereitstellen.

Authentifizierung und Sitzungsverwaltung

Bei der Authentifizierung wird überprüft, ob eine Person, Entität oder Website die Person ist, für die sie sich ausgibt.

Bei der Authentifizierung wird versucht, die digitale Identität des Absenders einer Kommunikation zu überprüfen. Das Testen des Authentifizierungsschemas bedeutet, dass Sie verstehen, wie der Authentifizierungsprozess funktioniert, und diese Informationen verwenden, um den Authentifizierungsmechanismus zu umgehen. Ein gängiges Beispiel ist der Anmeldevorgang. Die Authentifizierung erfolgt nach der Übermittlung eines Anwendernamens, einer Anwender-ID und mindestens eines privaten Informationselements, das nur der Anwender kennt.

Die Sitzungsverwaltung umfasst sicherheitsbezogene Eigenschaften, die ein Administrator konfigurieren kann, um sicherzustellen, dass in Now Platformsichere Mechanismen für die Sitzungsverwaltung eingerichtet werden.

Absolute Zeitüberschreitung für Sitzung (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.ui.user_cookie.max_life_span_in_days*, um eine maximale Lebensdauer für Anwendercookies festzulegen, die erstellt werden, wenn sich Anwender mit **aktiviertem** Kontrollkästchen „Anwendernamen speichern“ anmelden. Wenn das **Cookie** abläuft, werden Benutzer, die das Kontrollkästchen „Anwendernamen speichern“ aktiviert, müssen sich erneut bei der Instanz authentifizieren.

Dadurch kann das Benutzercookie für die Dauer angegebener Tage gültig sein, beginnend mit der ersten Ausgabe des Cookies. Der Standardwert beträgt 30 Tage, und die maximale Obergrenze liegt bei 365 Tagen.

Hinweis: Informationen zum Erzwingen einer maximalen Sitzungsdauer für aktive Benutzersitzungen finden Sie unter Konfigurieren Sie eine maximale aktive Zeit für Benutzersitzungen .

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.ui.user_cookie.max_life_span_in_days*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um zu erzwingen, dass Benutzer, die das Kontrollkästchen **Anwendernamen** speichern

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	aktiviert haben, sich nach bestimmten Tagen erneut authentifizieren.
Funktionale Auswirkung	(Mittel) Diese Eigenschaft erzwingt die obligatorische erneute Anmeldung, indem jede Art von Cookie-Rotation nach einem bestimmten Zeitrahmen vermieden wird.
Sicherheitsrisiko	(Mittel) Dass Anwendercookies für unbestimmte Zeit aktiv sind, stellt ein Sicherheitsrisiko dar und sollte bei einer zeitbasierten Konfiguration ablaufen.
Referenzen	Verfügbare Systemeigenschaften Anwendernamen speichern

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Anti-CSRF-Token (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.security.use_csrf_token*, um sicherzustellen, dass ein sicheres Token zum Identifizieren und Validieren eingehender Anforderungen verwendet wird, die wiederum zum Verhindern dieser Angriffe verwendet werden.

Cross-Site Request Forgery (CSRF) ist ein Angriff, der einen Endanwender dazu zwingt, unerwünschte Aktionen in einer Webanwendung auszuführen, in der er sich derzeit authentifiziert hat. CSRF-Angriffe zielen speziell auf Anforderungen zur Statusänderung ab, nicht auf den Diebstahl von Daten, da der Angreifer keine Möglichkeit hat, die Antwort auf die gefälschte Anforderung zu sehen.

Die folgenden Eigenschaften können für hinzugefügte Steuerungen für das CSRF-Token aktiviert werden:

- *glide.security.csrf_previous.time_limit*
- *glide.security.csrf_previous.allow*
- *glide.security.csrf.strict.validation.mode*

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.security.use_csrf_token
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Zum Schutz der Anwendung vor potenziellen CSRF-Angriffen.
Empfohlener Wert	wahr
Funktionale Auswirkung	(Niedrig) Diese Korrektur ermöglicht einen zusätzlichen Validierungsschritt, bevor der Instanzanwender eine Schreibanforderung an die Instanz sendet. Jede Schreibanforderung enthält ein CSRF-Token (also

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	eine Validierungs-/CSRF-ID, die an die Benutzersitzung gebunden ist). Wenn die Benutzersitzung abläuft, läuft auch das sichere Token ab.
Sicherheitsrisiko	(Hoch) Cross Site Request Forgery stellt ein erhebliches Sicherheitsrisiko dar, das die Integrität der Instanzdaten verletzt. Ein Angreifer kann den CSRF-Angriff starten, indem er das Vertrauen eines Instanzbenutzers missbraucht. Mithilfe von Social Engineering-Angriffen kann ein Benutzer im Namen des Angreifers in der Instanz eine fehlerhafte Anforderung senden.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Standardanmeldeinformationen ändern (Härtung der Instanzsicherheit)

Verwenden Sie das Kontrollkästchen **Passwort muss zurückgesetzt** werden in Anwendern und Gruppen, um sicherzustellen, dass ein unberechtigter Anwender die Standarddaten nicht ausnutzen kann.

Now Platform enthält einige Standarddaten, wenn die Instanz zbootet wird oder wenn Sie eine neue Instanz bereitstellen. Sie kann die Demo-Anwenderaccounts wie „Standardadministrator", „ITIL" und „Mitarbeiter" enthalten. Wenn Sie die Eigenschaft festlegen, müssen bei der Anmeldung bei der Anwendung die standardmäßigen Administrator-, ITIL- und Mitarbeiter-Anmeldeinformationen geändert werden.

Schritte zum Konfigurieren von

1. Melden Sie sich mit dem Anwendernamen **admin** und dem Passwort **admin**an.
2. Navigieren zu **Systemsicherheit** > **Anwender** > **Benutzer und Gruppen**
3. Suchen Sie unter Anwender-ID **admin** und Name **Administrator**nach dem Benutzer. Klicken Sie auf die ID des **Administratoranwenders**, um die Einstellungen des Anwenders zu ändern.
4. Ändern Sie das Feld E- **Mail** so, dass eine gültige E-Mail-Adresse für diesen Anwender angegeben wird.
5. Aktivieren Sie das Kontrollkästchen **Passwort muss zurückgesetzt** werden.
6. Klicken Sie auf **Aktualisieren**.
7. Melden Sie sich ab.
8. Melden Sie sich erneut an, um aufgefordert zu werden, ein neues Passwort festzulegen.
9. Wiederholen Sie die Schritte 3 bis 7 für ITIL- und Mitarbeiterkonten.

Cookies nur HTTP (Instanzsicherheit Härtung)

Verwenden Sie die Eigenschaft *glide.cookies.http_only*, um das HTTPOnly-Attribut für vertrauliche Cookies zu aktivieren.

Verwenden Sie das Attribut HTTPOnly, um Angriffe wie websiteübergreifendes Skripting zu verhindern, da es keinen Zugriff auf das Cookie mit einem clientseitigen Skript wie JavaScript zulässt. Dadurch werden die Risiken von websiteübergreifendem Skripting nicht eliminiert, es werden jedoch einige Angriffsvektoren eliminiert.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.cookies.http_only
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um das Risiko eines clientseitigen Skriptzugriffs auf das geschützte Cookie zu minimieren.
Empfohlener Wert	wahr
Funktionale Auswirkung	(Niedrig) Diese Korrektur fügt Sitzungscookies eine zusätzliche HTTPOnly-Kennzeichnung hinzu und schützt sie so vor Diebstahl. • Wenn Sie über eine anwenderdefinierte Funktionalität verfügen, für die JavaScript erforderlich ist, um auf das Cookie des Anwenders zuzugreifen, wird diese Funktionalität beeinträchtigt. Unter normalen Umständen sollte dies nicht der Fall sein. • Now Platform übernimmt die Sitzungsverwaltung, und es darf keinen Grund dafür geben, dass ein benutzerdefiniertes Skript auf die Cookies des Benutzers zugreift.
Sicherheitsrisiko	(Mittel) Sitzungscookies in der Anwendung authentifizieren Endanwender und gewähren implizite Zugriffsberechtigungen für die Anwendung. Das heißt, sie müssen vor Diebstahl oder Export geschützt werden. Nur-HTTP-Kennzeichnungen schützen die Sitzungscookies vor JavaScript-Einschleusungen oder websiteübergreifenden Skripting-Schwachstellen, die sie stehlen.
Referenzen	Verfügbare Systemeigenschaften

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Strikte CSRF-Validierung (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.security.csrf.strict.validation.mode*, um die strikte Validierung des CSRF-Tokens zu aktivieren. Wenn das CSRF-Token nicht übereinstimmt, wird die erneute Übermittlung der Anforderung verhindert.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.security.csrf.strict.validation.mode
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Erzwingt die strikte Validierung des CSRF-Tokens und verhindert dessen Wiederverwendung.
Empfohlener Wert	wahr
Funktionale Auswirkung	(Mittel) Diese Korrektur ermöglicht einen zusätzlichen Validierungsschritt, bevor der Instanzanwender eine Schreibanforderung an die Instanz sendet. Prüft, ob das aktuelle CSRF-Token zuvor verwendet wurde. Falls „Ja“, wird die Übermittlung weiterer Schreibanforderungen verhindert.
Sicherheitsrisiko	(Mittel) Websiteübergreifende Anforderungsfälschung stellt ein erhebliches Sicherheitsrisiko dar, das die Integrität der Instanzdaten verletzt. Ein Angreifer kann den CSRF-Angriff auf jeden Instanzbenutzer starten, indem er das Vertrauen des Instanzbenutzers missbraucht. Mithilfe von Social Engineering-Angriffen kann ein Benutzer im Namen des Angreifers eine fehlerhafte Anforderung an die Instanz senden.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Passwortlose Authentifizierung deaktivieren (Instanzsicherheitshärtung)

Verwenden Sie die Eigenschaft *glide.login.no_blank_password*, um zu verhindern, dass sich Benutzer mit leeren Passwörtern bei Now Platform anmelden, oder indem Sie das Feld **Passwort** leer lassen.

Selbst wenn der Administrator absichtlich einen leeren Wert oder ein leeres Passwort in Benutzerdatensätzen zuweist, kann sich ein Anwender nicht anmelden, ohne einen Wert im Feld **Passwort** anzugeben.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.login.no_blank_password
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um eine starke Authentifizierung sicherzustellen, da der Anwendername innerhalb einer Organisation manchmal leicht zu erraten ist.
Empfohlener Wert	wahr
Funktionale Auswirkung	(Niedrig) Vorgänge sollten keine leeren Passwörter verwenden, da dies als kritisches Sicherheitsrisiko angesehen wird. Wenn jedoch ein gültiger Fall für eine solche Verwendung vorliegt, besteht die Möglichkeit

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	eines Ausfalls. Anwender mit leeren Passwörtern können sich nicht bei der Instanz anmelden.
Sicherheitsrisiko	(Hoch) Ein Angreifer kann sich bei der Instanz mit den Standardanwendernamen oder einer bestimmten Person/Gruppe (normalerweise Vorname.Nachname) ohne Passwort anmelden. Dies wird als kritisches Sicherheitsrisiko angesehen, da ein öffentlicher Benutzer dadurch die Vertraulichkeit und Integrität der Instanzdaten verletzen könnte.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Multifaktor-Authentifizierung (MFA) aktivieren (Instanzsicherheitshärtung)

Verwenden Sie die Eigenschaft *glide.authenticate.multifactor*, um die Multifaktor-Authentifizierung (MFA) für die Instanz zu aktivieren. MFA ist eine Sicherheitsanforderung, die von einem Benutzer die Eingabe von mehr als einem Satz von Anmeldeinformationen erfordert, um sich bei einer Instanz zu authentifizieren.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.authenticate.multifactor
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Verstärken Sie die Instanzsicherheit, indem Sie die Multifaktor-Authentifizierung für interaktive Benutzeranmeldungen einführen.
Empfohlener Wert	wahr
Funktionale Auswirkung	(Mittel) Durch Aktivieren dieser Eigenschaft verbessert sich die Experience des Anwenders. Sie dient als zusätzliche Schutz- und Sicherheitsebene gegen kompromittierte Anmeldeinformationen.
Sicherheitsrisiko	(Mittel) Wenn diese Eigenschaft nicht aktiviert ist, besteht das Risiko eines nicht autorisierten Zugriffs auf vertrauliche Daten.
Referenzen	Systemeigenschaften der Multifaktor-Authentifizierung

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Legen Sie Kriterien für rollenbasierte Multifaktor-Authentifizierung fest

Verwenden Sie die Eigenschaft *glide.authenticate.multifactor*, um die rollenbasierte Multifaktor-Authentifizierung (MFA) für alle Benutzer zu erzwingen, die bestimmten Rollen zugewiesen sind.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erzwingen Sie die Multifaktor-Authentifizierung basierend auf den Rollen, die dem Anwender zugewiesen sind. Wenn einem Anwender in der Liste der Multifaktor-Rollen die Rollen „admin“, „security_admin“ oder „user_admin“ zugewiesen wurden, wird MFA erzwungen.

- Legen Sie diese Eigenschaft auf **„wahr** “ fest, um die rollenbasierte Multifaktor-Authentifizierung für alle Anwender zu erzwingen, die bestimmten Rollen zugewiesen sind.
- Legen Sie diese Eigenschaft auf „ **falsch** “ fest, um die rollenbasierte Multifaktor-Authentifizierung für alle Anwender zu deaktivieren, die bestimmten Rollen zugewiesen sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.authenticate.multifactor`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Erzwingen Sie die rollenbasierte Multifaktor-Authentifizierung für alle Anwender, die bestimmten Rollen zugewiesen sind.
Typ	wahr/falsch
Empfohlener Wert	`true`
Sicherheitsabhängigkeiten	Aktivieren **Sie die rollenbasierte Multifaktor-Authentifizierung** in der **Tabelle Multifaktor-Kriterien**.
Funktionale Auswirkung	(Mittel) Durch Aktivieren dieser Eigenschaft verbessert sich die Experience des Anwenders. Sie dient als zusätzliche Schutz- und Sicherheitsebene gegen kompromittierte Anmeldeinformationen.
Sicherheitsrisiko	(Mittel) Wenn diese Eigenschaft nicht aktiviert ist, besteht das Risiko eines nicht autorisierten Zugriffs auf vertrauliche Daten.
Referenzen	Konfigurieren Sie rollenbasierte Multifaktor-Kriterien

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Richtlinienprüfungen für die Passwortzurücksetzung aktivieren (Instanzsicherheitshärtung)

Verwenden Sie die Eigenschaft **„glide.enable.password_policy“**, um Prüfungen der Passwortrichtlinie zu aktivieren, wenn ein Benutzer sein Passwort über die Anwenderoberfläche ändert.

Um zu definieren, welche Passwortrichtlinie verwendet werden soll, sobald diese Eigenschaft aktiviert ist, siehe Passwortrichtlinien für Ihre Instanz aktivieren.

Hinweis: **glide.enable.password_policy** gilt nicht, wenn ein Administrator ein Passwort ändert oder einen Anwender über ein Skript hinzufügt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.enable.password_policy
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Zweck	Zum Anwenden der Passwortrichtlinie zum Zeitpunkt der Passwortänderung.
Empfohlener Wert	true (für Passwörter mit höherer Sicherheit)
Funktionale Auswirkung	(Mittel) Wenn Sie die Eigenschaft auf „true“ setzen, werden Passwortrichtlinienprüfungen aktiviert, wenn ein Benutzer sein Passwort zurücksetzt.
Sicherheitsrisiko	(Mittel) Ohne eine Passwortrichtlinie kann ein Anwender ein schwaches Passwort erstellen, was die Wahrscheinlichkeit erhöht, dass ein Angreifer Zugriff auf die Instanz erhält.

Schritte zum Konfigurieren von

Wenn Sie diese Einstellung auf der Seite „Konfiguration der Härtungscompliance“ im Instanz-Sicherheitszentrum konfigurieren:

1. Wählen Sie unter **Mittel**die Option **Management**von Sitzungen aus.
2. **Wählen Sie in der Einstellung Richtlinienprüfung für Passwortzurücksetzung aktivieren** die Option **Mittel** für Passwörter mit mittlerer Stärke oder **Stark** für robustere Passwörter mit höherer Stärke aus. Wenn Sie eine dieser Optionen auswählen, wird die Eigenschaft **„glide.enable.password_policy“** auf „true“ festgelegt und ein Workflow gestartet, der Ihre Passwortrichtlinie automatisch aktualisiert.

Darüber hinaus können Sie die Systemeigenschaft *glide.apply.password_policy.on_login* festlegen, um Prüfungen der Passwortrichtlinie zum Zeitpunkt der Anmeldung zu ermöglichen.

Fehlgeschlagene Anmeldungsversuche verwalten (Instanzsicherheitshärtung)

Es sind zwei Skriptaktionen verfügbar, mit denen ein Site-Administrator verwalten kann, wie oft ein Benutzer ein falsches Passwort eingeben kann, bevor er von Now Platformgesperrt wird. Sie können eine dieser Skriptaktionen aktivieren, um fehlgeschlagene Anmeldungsversuche zu verwalten.

Weitere Informationen

Attribut	Beschreibung
Eigenschafts-/Plugin-Name	N/V
Konfigurationstyp	Systemrichtlinie > Skriptaktionen
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Zweck	Um eine strikte Richtlinie für fehlgeschlagene Anmeldungsversuche zu erzwingen, um das Brute-Forcing von Anmeldeinformationen zu vermeiden.
Empfohlener Wert	Aktiv
Funktionale Auswirkung	(Niedrig) Diese Korrektur würde es dem Administrator der Instanz ermöglichen, böswilligen Anwenderzugriff zu überwachen und zu melden. Keine Auswirkung auf die Funktionalität, nur Änderung der Anwender-Experience.
Sicherheitsrisiko	(Mittel) Wenden Sie eine definierte Protokollierungs- und Auditstrategie an, damit Sie verdächtige Aktivitäten rechtzeitig erkennen und entsprechende Maßnahmen ergreifen können.
Referenzen	

Schritte zum Konfigurieren von

1. Navigieren zu **Systemrichtlinie** > **Skriptaktionen.**
2. Suchen Sie nach dem Namen *`*SNC User`*.
3. Um die Verwaltung fehlgeschlagener Anmeldungsversuche zu ermöglichen, ändern Sie den Status Aktiv der Skriptaktionen *`SNC User Lockout Check with Auto Unlock`* oder *`SNC User Lockout Check`* von **false** in **true**.
4. Um den Zähler für fehlgeschlagene Anmeldungen nach einer erfolgreichen Anmeldung zurückzusetzen, können Sie die Skriptaktion *`SNC User Clear`* aktivieren.

Automatische Vervollständigung für Passwortfeld (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *`glide.login.autocomplete`*, um Browsern die automatische Vervollständigung für Passwortfelder in Anmeldeformularen zu ermöglichen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.login.autocomplete
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um den Browser für die automatische Vervollständigung für ein Passwortfeld zu deaktivieren.
Empfohlener Wert	falsch
Funktionale Auswirkung	(Niedrig) Diese Korrektur führt dazu, dass die Kennzeichnung zur automatischen Vervollständigung des **Passwortfelds deaktiviert** wird, sodass der Passwortverlauf-Cache des Browsers nicht im Feld angezeigt wird. Die Funktionalität sollte nicht beeinträchtigt werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	(Niedrig) Anwenderauthentifizierungsfelder müssen validiert werden und dürfen niemals eine clientseitige Zwischenspeicherung zulassen.
Referenzen	https://support.servicenow.com/kb_view.do?sysparm_article=KB0563953

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Anmeldeinformationen von Willkommensseite entfernen (Härtung der Instanzsicherheit)

Ändern Sie den Standardinhalt auf der Willkommensseite, um die Standardanmeldeinformationen zu entfernen.

Hinweis: Zwei Datensätze zum Anmelden sind Teil der Demodaten für das CMS-Plugin. Wenn Sie die Demodaten für eine Instanz nicht installieren, sind diese Datensätze nicht vorhanden. In diesem Fall gilt die Konfiguration als sicherheitskonform gemäß den empfohlenen Sicherheitspraktiken. Weitere Informationen finden Sie unter Best Practices für Sicherheit.

Schritte zum Konfigurieren von

1. Navigieren zu **System-UI** > **Inhalt der Willkommensseite** > **an.**
2. Suchen Sie die beiden Abschnitte mit einer Kurzbeschreibung der **Anmeldung**.
3. Ändern Sie den Status Aktiv von **wahr** in **falsch**.

„Anwendernamen speichern“ entfernen (Instanzsicherheitshärtung)

Verwenden Sie die Eigenschaft *glide.ui.forgetme*, um das Kontrollkästchen Anwendernamen speichern von der **Anmeldeseite** zu entfernen, um zu verhindern, dass Anmeldeinformationen zwischengespeichert werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.vergissmich
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um sicherzustellen, dass keine Authentifizierungsinformationen zwischengespeichert werden.
Empfohlener Wert	wahr
Funktionale Auswirkung	(Niedrig) Diese Korrektur würde die Anwender-Experience ändern, indem sie automatisch aus der Instanz abgemeldet werden, wenn ihre Sitzung abläuft. Der Ablauf der Sitzung hängt ausschließlich von dem Wert ab, der in der Systemeigenschaft festgelegt ist (siehe Benutzersitzungen verwalten).

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	(Mittel) Wenn Sie bei der **Anmeldung** das Kontrollkästchen „Anwendernamen speichern“ aktivieren, wird ein zusätzliches Cookie auf dem Computer des Benutzers gespeichert. • Sein Zweck besteht darin, die Sitzung für die nachfolgenden Besuche des angemeldeten Anwenders automatisch wiederherzustellen. • Dies stellt ein Sicherheitsrisiko dar, da die Benutzersitzung aktiv bleiben kann, bis sie sich absichtlich abmeldet. Die Wahrscheinlichkeit eines Angriffs in diesem Szenario erhöht sich, wenn der Endanwender den Browser unbeaufsichtigt gelassen hat oder wenn er durch einen anderen Angriff gefährdet ist.
Referenzen	Kontrollkästchen „Anwendernamen speichern“ entfernen

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

HTTP-Sitzungs-IDs rotieren (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.ui.rotate_sessions*, um die Rotation der HTTP-Sitzungsbezeichner zu aktivieren und so Sicherheitsschwachstellen zu reduzieren.

Wenn sich die Sitzungs-ID eines nicht authentifizierten Benutzers nach der Authentifizierung nicht ändert, ist eine Webanwendung angreifbar für einen Angriff zur Sitzungskorrektur . Ein böswilliger Benutzer könnte eine nicht authentifizierte Sitzung starten und dem Opfer die zugehörige Sitzungs-ID geben. Sobald sich das Opfer authentifiziert hat, gibt der böswillige Anwender diese authentifizierte Sitzung jetzt frei.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.rotate_sessions
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um eine sicherere Sitzungsauthentifizierung zu erreichen.
Empfohlener Wert	wahr
Funktionale Auswirkung	(Mittel) Diese Korrektur hat die SessionID geändert, wenn der Anwender von einer nicht authentifizierten Seite zu authentifizierten Seiten navigiert. • Wenn Sie einen Proxy verwenden oder die SessionID bei der ersten Anmeldung eines Anwenders oder aus anderen Gründen codieren, kann dies eine potenzielle Auswirkung auf die Funktionalität haben.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Wenn Sie das SAML 2.0-Plugin für die Single Sign-on-Authentifizierung verwenden, kann dies die gemeinsame Nutzung von Sitzungsinformationen zwischen der Instanz und dem Identitätsanbieter beeinträchtigen. In diesem Fall können Sie diese Eigenschaft auf „falsch“ festlegen.
Sicherheitsrisiko	Die (verspätete) SessionID wird zum Verarbeiten und Authentifizieren des Instanzanwenders verwendet, indem der Sitzungsstatus im Browser verwaltet wird. Daher gilt die SessionID als vertrauliche Daten und sollte standardmäßig sicher sein. Die Sitzungsrotation ist eine Sicherheitskontrolle, die die Änderung der Sitzungs-ID erzwingt, wenn der Anwender von nicht authentifizierten Seiten zu authentifizierten Seiten navigiert.
Referenzen	Authentifizierung mit SAML

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Sitzungscookies (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.ui.secure_cookies*, um ordnungsgemäß formatierte Cookies anzufordern

Wenn Sie die Eigenschaft auf „true“ festlegen, lehnt Ihre Instanz eine Sitzung ab, wenn das zugehörige Cookie nicht das erwartete Format aufweist.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.secure_cookies
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um eine sicherere Sitzungsauthentifizierung zu erreichen.
Empfohlener Wert	wahr
Funktionale Auswirkung	(Niedrig) Wenn die Eigenschaft auf „true“ festgelegt ist, werden falsch formatierte Cookies abgelehnt. Wenn ein solches Cookie abgelehnt wird, muss sich der Benutzer erneut anmelden.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitsverweisrichtlinie (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *com.glide.security.referrerpolicy*, um zu steuern, welche Referrer-Daten in HTTP-Antwortheadern gesendet werden sollen, wenn Seiten vom Typ Now Platform Datenanforderungen senden. Der Wert für die Referrer-Richtlinie in einem HTTP-Header steuert, welche Referrer-Informationen in Datenanforderungen enthalten sein sollen.

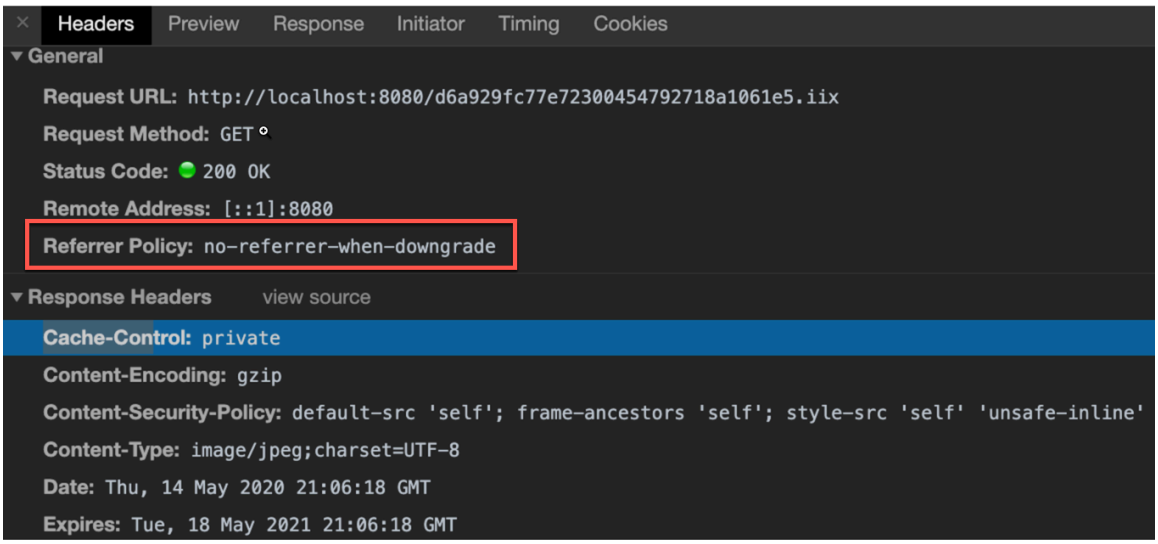
Werte der Sicherheitsreferenzrichtlinie

Legen Sie die Eigenschaft *com.glide.security.referrerpolicy* auf einen der folgenden Werte fest.

Wert	Beschreibung
Standard	Die InstanzNow Platform verwaltet die Ebene der in Referrer-Headern gesendeten Informationen, die für die spezifische Seitenanforderung von Now Platform geeignet sind.
gleichen Ursprungs	Now Platform -Seiten senden eine vollständige Referrer-URL innerhalb der Instanz und derselben Domäne und keinen Referrer-Header an den externen Ursprung. Diese Einstellung gewährleistet ein gutes Maß an Instanzsicherheit.
origin	Now Platform -Seiten senden die Basis-URL im Referrer-Header innerhalb der Instanz und derselben Domäne sowie extern. Diese Einstellung gewährleistet ein gutes Maß an Instanzsicherheit.
Ursprung-wenn-übergreifend	Now Platform -Seiten senden die gesamte URL im Referrer-Header innerhalb der Instanz und derselben Domäne, extern senden sie nur die Basis-URL. Diese Einstellung gewährleistet ein gutes Maß an Instanzsicherheit.
„no-referrer-when-downgrade“	Now Platform -Seiten senden den Ursprung, den Pfad und die Abfragezeichenfolge in der URL, sofern in einem Sicherheitsprotokoll kein Downgrade vorhanden ist. **Hinweis:** Diese Einstellung gewährleistet kein gutes Maß an Instanzsicherheit in Now Platform und sollte nicht verwendet werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für Empfehlungsrichtlinie und Zusammenfassung der Werte



Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	com.glide.sicherheit.empfehlungsrichtlinie
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Nein
Zweck	Steuert, wie viele eingehende Daten über den Header „Referrer“ gesendet werden, wenn eine Seite Now Platform eine Datenanforderung sendet.
Empfohlener Wert	Standard
Funktionale Auswirkung	(Niedrig) Bei Festlegung auf „Standard“ verwaltet die Instanz Now Platform die Ebene der Informationen, die in Referrer-Headern gesendet werden.
Sicherheitsrisiko	(Hoch) Das Festlegen dieses Eigenschaftswerts auf „no-referrer-when-downgrade“ stellt kein gutes Sicherheitsniveau für Ihre Instanz sicher.
Referenz	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy https://developer.mozilla.org/en-US/docs/Glossary/origin

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeitüberschreitung bei Sitzungsaktivität (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.ui.session_timeout*, um den Zeitüberschreitungswert der Aktivität in Minuten anzugeben.

Das Festlegen dieser Eigenschaft hat mehrere funktionale Auswirkungen:

- Je länger die angegebene Sitzungsüberschreitung ist, desto mehr Arbeitsspeicher wird während einer Verarbeitungssitzung verwendet. Das Basissystem verwendet eine standardmäßige Apache Tomcat-Zeitüberschreitungsdauer von 30 Minuten.
- Der Now Platform meldet Benutzer weiterhin mit „Anwendernamen speichern“ ab. Nach 30 Minuten Inaktivität in der Anwendung meldet die Plattform den Benutzer automatisch ab, es sei denn, das Kontrollkästchen „Anwendernamen speichern“ auf der **Anmeldeseite** ist aktiviert. Der Unterschied von besteht darin, dass sie sich nicht erneut anmelden müssen, um fortzufahren.
- Wenn auf den Homepages von Anwendern Anzeigen oder Inhalte vorhanden sind, die automatisch aktualisiert werden, kann diese Zeitüberschreitung möglicherweise nie erreicht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.session_timeout
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Zum Erzwingen der Zeitüberschreitung bei Sitzung.
Empfohlener Wert	Vom Anwender angegebene Zeitüberschreitung in Minuten. Der empfohlene Wert beträgt 30 Minuten, dieser Wert kann jedoch je nach Funktionalität und Sicherheitsanforderung variieren. Legen Sie diesen Wert nicht auf mehr als einen Tag fest.
Funktionale Auswirkung	(Mittel) Diese Korrektur erzwingt das rechtzeitige Ablaufen des Anwenderaccounts. Keine Auswirkungen auf die Funktionalität, jedoch die Anwender-Experience wird geändert.
Sicherheitsrisiko	(Mittel) Wenn Anwendersitzungen für unbestimmte Zeit aktiv sind, stellen sie ein Sicherheitsrisiko dar und sollten bei einer zeitbasierten Konfiguration ablaufen.
Referenzen	Verwalten Sie Benutzersitzungen

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Zeitüberschreitung des Sitzungsfensters (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.ui.user_cookie.life_span_in_days*, um den Ablaufzeitraum für das „Anwendernamen speichern“-Cookie festzulegen. Der Standardwert beträgt 15 Tage, und die maximale Obergrenze beträgt 30 Tage.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.user_cookie.life_span_in_days
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um den standardmäßigen Ablauf des Cookies „Anwendernamen speichern“ zu aktivieren.
Empfohlener Wert	Benutzerdefinierter ganzzahliger Wert (Anzahl der Tage) [Beispiel: 15]
Funktionale Auswirkung	(Mittel) Diese Eigenschaft wird vom Endanwender aktiviert, wenn der Endanwender auf der **Anmeldeseite** das Kontrollkästchen Anwendernamen speichern aktiviert und sich bei Now Platformanmeldet.
Sicherheitsrisiko	(Mittel) Dass Anwendercookies für unbestimmte Zeit aktiv sind, stellt ein Sicherheitsrisiko dar und sollte bei einer zeitbasierten Konfiguration ablaufen.
Referenzen	Verfügbare Systemeigenschaften Anwendernamen speichern

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Konfigurieren Sie Passwörter für automatisch erstellte Benutzeraccounts

Verwenden Sie die Systemeigenschaften *glide.email.inbound.use_default_password* und *glide.user.default_password*, um zu definieren, wie Passwörter für neue Benutzer erstellt werden, die aus eingehenden E-Mails erstellt wurden.

Die in diesem Dokument beschriebenen Systemeigenschaften definieren, wie die Instanz Passwörter für Anwenderkonten behandelt, die aus eingehenden E-Mails generiert wurden. Ihre Instanz muss so konfiguriert sein, dass sie E-Mails empfängt und die automatische Benutzererstellung ermöglicht. Weitere Informationen zu diesen Konfigurationen finden Sie im Abschnitt weiter unten.

Nachdem Ihre Instanz für die automatische Erstellung von Accounts konfiguriert ist, können Sie mithilfe der Eigenschaften ermitteln, ob ein Standardpasswort verwendet werden soll, und dieses Passwort bei Bedarf definieren.

Voraussetzungen

Um diese Eigenschaften zu verwenden, muss Ihre -Instanz so konfiguriert sein, dass automatisch neue Benutzeraccounts erstellt werden.

- Sie müssen Ihren eigenen POP3-Server zum Speichern und Empfangen von E-Mails für Ihre Instanz konfigurieren. Dann müssen Sie die Systemeigenschaft *glide.email.read.active* auf „True“ setzen. Weitere Informationen zum Konfigurieren eines POP3-Servers in Ihrer Instanz finden Sie unter Verwendung eines eigenen POP3-Servers aktivieren .

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Legen Sie die Eigenschaft *glide.pop3readerjob.create_caller* auf „Wahr“ fest. Mit dieser Eigenschaftsänderung kann Ihre -Instanz automatisch Benutzer aus eingehenden E-Mails erstellen. Weitere Informationen finden Sie unter Automatische Anwendererstellung aktivieren .

  Hinweis: Überspringen Sie die Eigenschaft *glide.user.default_password*, wenn die Eigenschaft *glide.pop3readerjob.create_caller* auf **false**festgelegt ist.

Wie Ihre Instanz Passwörter definiert

In Quebec und früheren Versionen von ServiceNowerstellt Ihre -Instanz aus eingehenden E-Mails neue Benutzerkonten mit einem komplexen Passwort, das in der Systemeigenschaft *glide.user.default_password* definiert ist. Benutzer verwenden dieses Passwort bei der ersten Anmeldung. Anschließend werden sie von der Instanz zur Eingabe eines neuen Passworts aufgefordert. Wenn Sie Ihre Instanz von auf Rome oder höher aktualisiert haben, bleibt dieser Prozess unverändert. Als Administrator können Sie Ihre -Instanz so aktualisieren, dass die unten beschriebene neue Methode verwendet wird.

In neuen Instanzen, die mit dem Release Rome beginnen, haben Anwenderaccounts, die aus eingehenden E-Mails erstellt werden, kein Passwort. Wenn ein Benutzer mit seinem neuen Account zum ersten Mal auf die Instanz zugreift, muss er seinen Benutzernamen eingeben und auf die **Schaltfläche Passwort vergessen?** klicken. um ein anfängliches Passwort zu erstellen.

In Rome und späteren Releases können Sie auswählen, welchem Prozess Ihre Instanz folgt, indem Sie einen Wert in der Systemeigenschaft *glide.email.inbound.use_default_password* festlegen. Um das oben beschriebene Standardverhalten zu ändern, erstellen Sie diese Systemeigenschaft mithilfe der folgenden Informationen:

Feld „Systemeigenschaft	Wert
Name	glide.email.inbound.use_default_password
Typ	Wahr | Falsch
Wert	Wählen Sie einen Wert basierend auf Ihrem gewünschten Verhalten aus: wahr Neue Accounts verwenden ein Standardpasswort, das in der Systemeigenschaft *glide.user.default_password* definiert ist. falsch Neue Accounts haben kein Standardpasswort. Benutzer müssen ein Passwort definieren, wie weiter oben in diesem Abschnitt beschrieben.

Weitere Informationen zum Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Definieren Sie ein Standardpasswort

Wenn Ihre Instanz für die Verwendung eines Standardpassworts konfiguriert ist, müssen Sie dieses Passwort mit der Systemeigenschaft *glide.user.default_password* definieren. Erstellen Sie diese Eigenschaft mit den folgenden Informationen:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld „Systemeigenschaft	Wert
Name	glide.user.default_password
Typ	Kennwort 2
Wert	Geben Sie ein eindeutiges Passwort ein, das als Standard verwendet werden soll. Verwenden Sie eine starke Passwortkomplexität, um die Sicherheit Ihrer Instanz zu gewährleisten.

Härtungseinstellungen

Der Inhalt ServiceNow, Inc. Security Center-Härtungseinstellungen enthält detaillierte Beschreibungen und Compliance-Werte für die sicherheitsbezogenen Systemeigenschaften und Plugins im Now Platform. Sie können diese Eigenschaften mit der App für die Härtungseinstellungen im Security Center festlegen.

Übersicht und Zweck

Security Center berechnet eine tägliche Compliance-Punktzahl, ausgedrückt als Prozentsatz, der darauf basiert, wie konform Ihre aktuellen Sicherheitseinstellungen für Instanzen mit den Compliance-Werten in den Härtungseinstellungen von Security Center sind.

Sie können die spezifischen Sicherheitskonfigurationseinstellungen, die sich auf die Punktzahl für Ihre Instanz auswirken können, direkt über das Security Center verwalten.

Die Konfigurationen der Härtungseinstellungen werden anhand mehrerer Attribute in der Tabelle erläutert.

Konfigurationsdetails für Härtungseinstellungen

Konfigurationsattribut	Beschreibung
Übersicht	Bietet eine allgemeine Übersicht über die Empfehlung.
Konfigurationsname	Die Eigenschaft oder der Plugin-Name.
Konfigurationstyp	Beschreibt, wo die Eigenschaft außerhalb des Sicherheitscenters konfiguriert werden kann, z. B. in den Systemeigenschaften (*sys_properties_list.do*).
Datentyp	Beschreibt den Werttyp, der für die Konfiguration erforderlich ist. Beispiele sind wahr/falsch boolescher Wert, Installation, Plugin, Zeichenfolge usw.
Empfohlener Wert	Der Wert, der vom Sicherheitscenter empfohlen wird, um die Sicherheits-Compliance in Ihrer Instanz zu verbessern.
Standardwert	Der Wert, auf den die Konfiguration im Basissystem festgelegt ist.
Kategorie	Name und Link zur Kategorie für die Härtungseinstellung.
Sicherheitsrisiko	**Schweregrad-Punktzahl**: Die Punktzahl gibt das potenzielle Sicherheitsrisiko für Ihre Instanz anhand der Wahrscheinlichkeit an, dass die Schwachstelle ausgenutzt wird. Die Sicherheitsschwachstelle wird einzeln betrachtet und bewertet anhand der CVSS-Punktzahl (Common Vulnerability Bewertungssystem) auf einer Skala von **0,0** bis

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationsdetails für Härtungseinstellungen (Fortsetzung)

Konfigurationsattribut	Beschreibung
	10,0. Weitere Informationen finden Sie unter https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator .
	Schweregradbewertung pro CVSS-Punktzahl: • Kritisch: 9,0–10,0 • Hoch: 7,0–8,9 • Mittel: 4,0–6,9 • Niedrig: .01–3.9 • Keine: 0,0
	Sicherheitsrisikodetails: Beschreibt die Bedeutung der Einstellungskonfiguration und das Risiko, die empfohlene Konfiguration nicht zu verwenden.
Abhängigkeiten und Voraussetzungen	Zugehörige Einstellungen oder Konfigurationen, die vor oder in Verbindung mit der Härtungskonfiguration erforderlich sind.
Funktionale Auswirkung	Die Auswirkungen, die diese Härtungseinstellung auf den Betrieb Ihrer Instanz hat.
Referenzen	Links zu Konfigurationsdokumentation oder anderen hilfreichen Informationen.

Hinweis: Einige der Konfigurationen können nur von Kundenservice und Support abgeschlossen werden und werden als solche angezeigt.

Weitere Informationen dazu, wie Sie dafür sorgen, dass Ihre Instanzen die Härtungsanforderungen erfüllen, finden Sie unter Sicherheitshärtung.

Andere Ressourcen

Zur Benutzerreferenz enthält Now Platform umfangreiche Informationen zu den Konfigurationsfähigkeiten in der Produktdokumentation. Auf die meisten Sicherheitsinhalte können Sie über die Links in Instanz sichernzugreifen. Siehe auch:

- Verfügbare Systemeigenschaften
- Allgemeine Sicherheitseinstellungseigenschaften
- Strenge Sicherheitseinstellungen

Baseline der Härtungseinstellungen

Erfahren Sie, wie unterschiedliche Baselineversionen für die Härtungseinstellungen mit verschiedenen Familien- und Store-Releases übereinstimmen.

Security Center erfasst eine Teilmenge der Systemeigenschaften aus einer Instanz und zeigt die zugehörigen Konfigurationsdetails sowie die Sicherheitsauswirkungen von Nicht-Compliance in der App an. Die Baseline dient als Referenzpunkt für die Systemeigenschaften, die mit jedem Release der App Security Center erfasst werden.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übersicht über Baseline der Härtungseinstellungen

Security Center-Version	Baseline-Version der Härtungseinstellung	Unterstützte Familien	Store-Release-Datum	Wird standardmäßig mit installiert
SSC v1.1	Baseline v1.0	Utah, Vancouver	Mai 2023	Vancouver-Familie
SSC v1.2	Baseline v1.0	Utah, Vancouver	August 2023	Nur Store
SSC v1.3	Baseline v2.0	Vancouver, Washington	November 2023	Washington-Familie
SSC v1.5	Baseline v4.0	Washington, Xanadu	Mai 2024	Xanadu
SSC v1.6	Baseline v4.0	Washington DC, Xanadu	August 2024	

Neue Härtungseinstellungen für Baselineversion 4.0

Nachstehend finden Sie eine Liste aller neuen Härtungseinstellungen, die mit der Baseline von Security Center Version 4.0 veröffentlicht wurden.

- Zugriffssteuerungsbedingungen für explizite externe Rollen überprüfen [In Security Center 1.5 entfernt]
- Abfrageregeln für das Arbeitsauftragsmanagement für Serviceorganisationen aktivieren [Neu in Security Center 1.5]
- Root of Trust für ServiceNow deaktivieren
- Lesezugriff auf Flow-Kontext einschränken [Neu in Security Center 1.5]
- Intervall für mobiles Aktualisierungstoken für richtlinienbasierten Sitzungszugriff beschränken [Neu in Security Center 1.5]
- Richtlinienbasierten Sitzungszugriff für Mobilgeräte aktivieren [Neu in Security Center 1.5]
- Verhindern, dass sich inaktive Benutzer anmelden [Neu in Security Center 1.5]
- Administratorrollen für Ereignismanagement-Zuweisungsgruppen konfigurieren [Neu in Security Center 1.5]
- Sicherheitsbereich für Mitarbeiterbereich für HR-Fallverwaltung erzwingen [Neu in Security Center 1.5]
- Sicherheitsbereich für Playbook für Lizenzen und Berechtigungen erzwingen [Neu in Security Center 1.5]

Neue Härtungseinstellungen für Baselineversion 2.0

Nachstehend finden Sie eine Liste aller neuen Härtungseinstellungen, die mit der Baseline Security Center Version 2.0 veröffentlicht wurden.

- Nutzung des Alias für Anmeldeinformationen erzwingen [Neu in Security Center 1.3 und aktualisiert in 1.5]
- OCSP-Prüfung bei Netzwerkfehler erzwingen [Neu in Security Center 1.3]
- Zertifikatkette und Hostname verifizieren [Neu in Security Center 1.3]
- Zertifikatwiderrufung verifizieren [Neu in Security Center 1.3]

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Legen Sie eine Sicherheitsrichtlinie für sichere Inhalte für SVG-Dateien fest [Neu in Security Center 1.3]
- Verwendung des Vorgangs zum mehrfachen sicheren Einfügen in der Importsatz-API [Neu in Security Center 1.3]
- Plugin „Protected Tables“ aktivieren [Neu in Security Center 1.3]
- Sichere Referrer-Richtlinie erzwingen [Neu in Security Center 1.3]
- Ausnahmerollen für Zeitüberschreitung bei aktiver Sitzung definieren [Neu in Security Center 1.3]
- Inaktive Sitzungen proaktiv für ungültig erklären [Neu in Security Center 1.3]
- Validiert den Datei-MIME-Typ im SOAP-Webservice „AttachmentCreator“ [Neu in Security Center 1.3]
- Zertifikatbasierte Authentifizierung nicht erzwungen [Neu in Security Center 1.3]
- Sitzungsaudit-Ereignisse protokollieren [Neu in Security Center 1.3]
- Authentifizierung für Ereignismanagement-HTTP-Prozessor erforderlich [Neu in Security Center 1.3]
- Sicherheitsregeln für die Freigabe von Dashboards erzwingen [Neu in Security Center 1.3]
- Klonen von Zielen nicht zulassen [Neu in Security Center 1.3]
- Bereichssicherheit für Digitale Dienste für den öffentlichen Bereich erzwingen [Neu in Security Center 1.3]
- Bereichsbezogenen ACL-Zugriff für Playbooks zur Informationsanforderung erzwingen [Neu in Security Center 1.3]
- Lebensdauer aktiver Sitzungen von Gästen begrenzen [Neu in Security Center 1.3]
- Lebensdauer aktiver Sitzungen von Integrationen begrenzen [Neu in Security Center 1.3]
- Zugriff auf Knowledge Bases beschränken [Neu in Security Center 1.3]
- Benutzerkommentare zu Artikeln ausblenden [Neu in Security Center 1.3]
- OAuth-Parameter auf Post-Text beschränken [Neu in Security Center 1.3]
- Anhangsgröße in Trainings- und Vorhersage-Flows begrenzen [Neu in Security Center 1.3 und aktualisiert in 1.5]
- Sicherstellen, dass das Erstellen/Löschen von Dashboards eine Zugriffsprüfung erfordert [Neu in Security Center 1.3]
- Verhalten der Vorgängerversion für die Umgrenzung des GlideRecord-Bereichs deaktivieren [Neu in Security Center 1.3]
- Einschränkungen des Anwendungsbereichs erzwingen [Neu in Security Center 1.3]
- Schreibzugriff erfordern, um auf die Seite „Element hinzufügen“ des Servicekatalogs zuzugreifen [Neu in Security Center 1.3]
- Validierungszeit des Anti-CSRF-Tokens [Neu in Security Center 1.3]
- Sicherstellen, dass Archivtabellen-ACLs aktiviert sind [Neu in Security Center 1.3]
- Sicherheitsmanager für gehärtetes Java aktivieren [Neu in Security Center 1.3]
- Strikte Erhöhungsberechtigung erzwingen [Neu in Security Center 1.3]
- Löschen der Zwischenablage anfordern, wenn die mobile Anwendung im Hintergrund ausgeführt wird [Neu in Security Center 1.3]
- Anforderungen für Geräteverschlüsselung und Passcode erzwingen [Neu in Security Center 1.3]

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Lebensdauer aktiver Sitzungen von UI begrenzen [Neu in Security Center 1.3]
- MID-Audit-Protokoll aktivieren [Neu in Security Center 1.3 und aktualisiert in 1.5]
- Erforderliche JMS-Verbindungsfactorys [Neu in Security Center 1.3 und aktualisiert in 1.5]
- Captcha für Walk-Up Experience der Kundenservice-Anwendung für Gäste anfordern [Neu in Security Center 1.3 und aktualisiert in 1.5]
- Identitätswechsel bei ACL-Bewertung in HR-App überprüfen [Neu in Security Center 1.3 und aktualisiert in 1.5]
- Aktualisierungen von HR-Fällen auf persönliche E-Mails beschränken [Neu in Security Center 1.3 und aktualisiert in 1.5]

Die Härtungseinstellungen wurden für die Baselineversion 4.0 aktualisiert

Die Liste der Härtungseinstellungen, die in Security Center Baselineversion 4.0 aktualisiert wurden.

Baselineversion 4.0 enthält mehrere Updates für Kurzbeschreibungen für Stil und Konsistenz zwischen Datensätzen. Darüber hinaus wurden viele eigenschaftsbezogene Skripts aktualisiert, um die Genauigkeit des Standardwerts für Fälle zu verbessern, in denen die Eigenschaft aus der Tabelle „sys_property“ entfernt wurde.

Dokumentation	Updates
Autorisierung für SOAP-Anforderungen erfordern [Aktualisiert in Security Center 1.3 und 1.5]	• Neuer Name der technischen Konfiguration: *glide.basicauth.required.soap, glide.soap.require_ws_security* • Alter technischer Konfigurationsname: *glide.basicauth.required.soap*
HTML-Bereinigung in Virtual Agent aktivieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: HTML-Bereinigung in Virtual Agent aktivieren • Alte Kurzbeschreibung: HTML-Bereinigung aktivieren
Internen Zugriff auf explizite externe Rollen verweigern [Aktualisiert in Security Center 1.5]	• Neuer Name der technischen Konfiguration: *glide.security.explicit_roles.enable_internal_u* • Alter technischer Konfigurationsname: *glide.security.explicit_roles.enable_internal_u*
Eingeschränkt herunterladbare MIME-Typen definieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Eingeschränkt herunterladbare MIME-Typen definieren • Alte Kurzbeschreibung: Herunterladbare MIME-Typen einschränken

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	Updates
E-Mail-Domänen für die Registrierung externer Anwender einschränken [Aktualisiert in Security Center 1.5]	• Neue Kurzbeschreibung: Eingeschränkt herunterladbare MIME-Typen definieren • Alte Kurzbeschreibung: Herunterladbare MIME-Typen einschränken
Ablaufdauer des Links zur Registrierung externer Anwender minimieren [Aktualisiert in Security Center 1.3 und 1.5]	• Neue Kurzbeschreibung: Ablaufdauer des Links für die Registrierung externer Anwender minimieren • Alte Kurzbeschreibung: Ablaufdauer des Links für die Registrierung externer Anwender minimieren (Plugin-Anwendbarkeit: Registrierung externer Anwender)
Download infizierter Dateien nicht zulassen	• Neue Kurzbeschreibung: Download infizierter Dateien nicht zulassen • Alte Kurzbeschreibung: Download infizierter Dateien nicht zulassen
Multisso-Debugging deaktivieren	• Neue Kurzbeschreibung: MultiSSO-Debugging deaktivieren • Alte Kurzbeschreibung: MultiSSO-Debugging deaktivieren (Plugin-Anwendbarkeit: Single Sign-on für mehrere Anbieter)
Zulässige ServiceNow interne IP-Adressen definieren [Aktualisiert in Security Center 1.3 und 1.5]	• Neuer Name der technischen Konfiguration: *glide.ip.authenticate.strict* • Alter technischer Konfigurationsname: *glide.ip.authenticate.strict,glide.ip.authentic*
Domain Separation auf Dot-Walking-Felder anwenden [Aktualisiert in Security Center 1.3 und 1.5]	• Neue Kurzbeschreibung: Domain Separation auf Dot-Walking-Felder anwenden • Alte Kurzbeschreibung: Domain Separation auf Dot-Walking-Felder anwenden (Plugin-Anwendbarkeit: Domain Separation)

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	Updates
Accountwiederherstellung aktivieren [In Security Center 1.3 und 1.5aktualisiert]	• Neue Kurzbeschreibung: Accountwiederherstellung aktivieren • Alte Kurzbeschreibung: Accountwiederherstellung aktivieren (Plugin-Anwendbarkeit: Single Sign-on für mehrere Anbieter)
Schwellenwert für Entitätserweiterung minimieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Schwellenwert für Entitätserweiterung für skriptfähiges GlideXMLUtil minimieren • Alte Kurzbeschreibung: Schwellenwert für Entitätserweiterung minimieren
Aktualisierte Version des MultiSSO-Plugins aktivieren [In Security Center 1.3 und 1.5aktualisiert]	• Neue Kurzbeschreibung: Aktualisierte Version des Multi-SSO-Plugins aktivieren • Alte Kurzbeschreibung: Aktualisierte Version des Multi-SSO-Plugins aktivieren (Plugin-Anwendbarkeit: Single Sign-on für mehrere Anbieter)
Keine Demozertifikate für aktive SAML-Konfigurationen verwenden [Aktualisiert in Security Center 1.5]	• Neue Kurzbeschreibung: Keine Demozertifikate für aktive SAML-Konfigurationen verwenden • Alte Kurzbeschreibung: Keine Demozertifikate für aktive SAML-Konfigurationen verwenden (Plugin-Anwendbarkeit: Single Sign-on für mehrere Anbieter)
SAML-Dauer von „notBefore“ und „notOnOrAfter“ minimieren [Aktualisiert in Security Center 1.3 und 1.5]	• Neue Kurzbeschreibung: SAML-Einschränkungsdauer für „notBefore“ oder „notOnOrAfter“ minimieren • Alte Kurzbeschreibung: SAML-Einschränkungsdauer für „notBefore“ oder „notOnOrAfter“ minimieren (Plugin-Anwendbarkeit: Single Sign-on für mehrere Anbieter)
Abgelaufene Anti-CSRF-Token blockieren [in Security Center 1.5 aktualisiert]	• Neue Kurzbeschreibung: Abgelaufene Anti-CSRF-Token blockieren • Alte Kurzbeschreibung: Abgelaufene CSRF-Token des Blocks

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	Updates
Captcha für Walk-Up Experience der Kundenservice-Anwendung für Gäste anfordern [Neu in Security Center 1.3 und aktualisiert in 1.5]	• Neue Kurzbeschreibung: Captcha für Walk-Up Experience für Gäste in der Kundenservice-Anwendung erforderlich • Alte Kurzbeschreibung: Captcha für Walk-Up Experience für den Kundenservice in der Anwendung erforderlich (Plugin-Anwendbarkeit: Walk-Up Experience für den Kundenservice)
Identitätswechsel bei ACL-Bewertung in HR-App überprüfen [Neu in Security Center 1.3 und aktualisiert in 1.5]	• Neue Kurzbeschreibung: Identitätswechsel bei ACL-Auswertung in HR-App überprüfen • Alte Kurzbeschreibung: Identitätswechsel bei ACL-Bewertung in HR-App überprüfen (Plugin-Anwendbarkeit: Bereichsbezogene Human Resources-App)
Aktualisierungen von HR-Fällen auf persönliche E-Mails beschränken [Neu in Security Center 1.3 und aktualisiert in 1.5]	• Neue Kurzbeschreibung: HR-Fallaktualisierungen aus persönlichen E-Mails beschränken • Alte Kurzbeschreibung: HR-Fallaktualisierungen aus persönlichen E-Mails beschränken (Plugin-Anwendbarkeit: Bereichsbezogene App für Human Resources)
MID-Audit-Protokoll aktivieren [Neu in Security Center 1.3 und aktualisiert in 1.5]	• Neue Kurzbeschreibung: MID-Audit-Protokoll aktivieren • Alte Kurzbeschreibung: MID-Audit-Protokoll aktivieren (Plugin-Anwendbarkeit: MID Server)
Nutzung des Alias für Anmeldeinformationen erzwingen [Neu in Security Center 1.3 und aktualisiert in 1.5]	• Neue Kurzbeschreibung: Nutzung des Alias für Anmeldeinformationen erzwingen • Alte Kurzbeschreibung: Nutzung des Alias für Anmeldeinformationen erzwingen (Plugin-Anwendbarkeit: MID Server)
Erzwingen Sie die strikte Validierung des CSRF-Tokens	• Neue Kurzbeschreibung: Strikte CSRF-Token-Validierung erzwingen • Alte Kurzbeschreibung: Strikte CSRF-Validierung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	Updates
Erforderliche JMS-Verbindungsfactorys [Neu in Security Center 1.3 und aktualisiert in 1.5]	• Neue Kurzbeschreibung: Erforderliche JMS Connection Factory • Alte Kurzbeschreibung: Erforderliche JMS Connection Factory (Plugin-Anwendbarkeit: MID Server)
Anhangsgröße in Trainings- und Vorhersage-Flows begrenzen [Neu in Security Center 1.3 und aktualisiert in 1.5]	• Neue Kurzbeschreibung: Anhangsgröße in Trainings- und Vorhersage-Flows begrenzen • Alte Kurzbeschreibung: Anhangsgröße in Trainings- und Vorhersage-Flows begrenzen (Plugin-Anwendbarkeit: Platform Document Intelligence)
Größe des HTTP-Antworttexts begrenzen [Neu in Security Center 1.3 und aktualisiert in 1.5]	• Neue Kurzbeschreibung: Größe des HTTP-Antworttexts begrenzen • Alte Kurzbeschreibung: Stellt sicher, dass HTTP-Antworten aufgrund der Größe des Antworttexts keine „OutofMemory"-Ausnahme auslösen

Die Härtungseinstellungen wurden für die Baselineversion 2.0 aktualisiert

Diese Liste enthält die Härtungseinstellungen, die in der Baselineversion Security Center 2.0 aktualisiert wurden.

Dokumentation	Updates
JSONP-Anforderungen auf vertrauenswürdige URLs beschränken [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: JSONP-Anforderungen auf vertrauenswürdige URLs beschränken • Alte Kurzbeschreibung: Aufnahmeliste für JSONP-Anforderung
Zulässige Anhangsgröße minimieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Zulässige Anhangsgröße minimieren • Alte Kurzbeschreibung: Maximal zulässige Anhangsgröße
Zertifikatvertrauen erzwingen [In Security Center 1.3 aktualisiert und in 1.5 entfernt]	• Neue Kurzbeschreibung: Certificate Trust erzwingen • Alte Kurzbeschreibung: Certificate Trust

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	Updates
Xframe-Optionen festlegen, um das Einbetten von Websites von Drittanbietern zu verhindern [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Legen Sie die Xframe-Optionen fest, um das Einbetten von Websites von Drittparteien zu verhindern • Alte Kurzbeschreibung: Xframe-Optionen
HTML-Bereinigung in Virtual Agent aktivieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: HTML-Bereinigung in Virtual Agent aktivieren • Alte Kurzbeschreibung: HTML-Bereinigung aktivieren
Lesezugriff delegierter Entwickler einschränken [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Lesezugriff delegierter Entwickler einschränken • Alte Kurzbeschreibung: Zulassungsliste für Lesezugriff von delegierten Entwicklern
Bewertung und Filterung von E-Mail-Spam aktivieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Bewertung und Filterung von E-Mail-Spam aktivieren • Alte Kurzbeschreibung: Bewertung und Filterung von E-Mail-Spam
Plugin für hohe Sicherheit [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Plugin für hohe Sicherheit aktivieren • Alte Kurzbeschreibung: Hochsicherheits-Plugin
Plugin für kontextbezogene Sicherheit aktivieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Plugin für kontextbezogene Sicherheit aktivieren • Alte Kurzbeschreibung: Plugin für kontextbezogene Sicherheit
HTML-Bereinigung erzwingen [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: HTML-Bereinigung erzwingen • Alte Kurzbeschreibung: Nicht bereinigten HTML-Code prüfen
Gastanwender für SOAP-Anforderungen festlegen [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Gastanwender für SOAP-Anforderungen festlegen • Alte Kurzbeschreibung: Gastanwender für SOAP-Anforderungen

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	Updates
SNC-Zugriffssteuerungs-Plugin aktivieren [In Security Center 1.3 aktualisiert]	• Neue Kurzbeschreibung: SNC-Zugriffssteuerungs-Plugin aktivieren • Alte Kurzbeschreibung: SNC Access Control Plugin
Sicherheits-Jump-Start-Plugin aktivieren (ACL-Regeln) [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Sicherheits-Jump-Start-Plugin aktivieren • Alte Kurzbeschreibung: Sicherheits-Jump-Start-Plugin (ACL-Regeln)
Legacy-AngularJS-Verhalten deaktivieren [in Security Center 1.3 aktualisiert]	• Neue Kurzbeschreibung: Legacy-AngularJS-Verhalten deaktivieren • Alte Kurzbeschreibung: Legacy AngularJS Behavior
Gleichzeitige interaktive Sitzungen begrenzen [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Gleichzeitige interaktive Sitzungen begrenzen • Alte Kurzbeschreibung: Beschränkung gleichzeitiger interaktiver Sitzungen auf Glide-Authentifizierung
Gleichzeitige Sitzungen über alle Knoten hinweg begrenzen [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Gleichzeitige Sitzungen über alle Knoten hinweg begrenzen • Alte Kurzbeschreibung: Glide-Authentifizierung für Begrenzung gleichzeitiger Sitzungen über alle Knoten hinweg
Anzahl der gleichzeitigen interaktiven Sitzungen minimieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Minimieren Sie die Anzahl der gleichzeitigen interaktiven Sitzungen • Alte Kurzbeschreibung: Max. gleichzeitige interaktive Sitzungen für Glide-Authentifizierung
Rollenbasierte Multifaktor-Authentifizierung aktivieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Rollenbasierte Multifaktor-Authentifizierung aktivieren • Alte Kurzbeschreibung: Rollenbasierte Multifaktor-Authentifizierung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	Updates
Aktualisierte Version des MultiSSO-Plugins aktivieren [In Security Center 1.3 und 1.5aktualisiert]	• Neue Kurzbeschreibung: Aktualisierte Version des Multi-SSO-Plugins aktivieren • Alte Kurzbeschreibung: Aktualisierte Version des Multi-SSO-Plugins ist aktiviert
SAML-Dauer von „notBefore“ und „notOnOrAfter“ minimieren [Aktualisiert in Security Center 1.3 und 1.5]	• Neue Kurzbeschreibung: SAML-Einschränkungsdauer für „notBefore“ oder „notOnOrAfter“ minimieren • Alte Kurzbeschreibung: SAML-Einschränkung „notBefore“ oder „notOnOrAfter“.
Autorisierung für API-Anforderungen erfordern [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Autorisierung für API-Anforderungen erfordern • Alte Kurzbeschreibung: Autorisierung von API-Anforderungen
Autorisierung für CSV-Anforderungen erfordern [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Autorisierung für CSV-Anforderungen erfordern • Alte Kurzbeschreibung: Autorisierung von CSV-Anforderungen
Autorisierung für Daten-Broker-REST-API erfordern [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Autorisierung für Daten-Broker-REST-API erforderlich • Alte Kurzbeschreibung: REST-API-Autorisierung für Daten-Broker
Autorisierung für Excel-Anforderungen erfordern [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Autorisierung für Excel-Anforderungen erfordern • Alte Kurzbeschreibung: Autorisierung von Excel-Anforderungen
Autorisierung für Importanforderungen erfordern [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Autorisierung für Importanforderungen erfordern • Alte Kurzbeschreibung: Autorisierung der Importanforderung
Autorisierung für JSONv2-Anforderung erfordern [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Autorisierung für JSONv2-Anforderung erforderlich • Alte Kurzbeschreibung: Autorisierung von JSONv2-Anforderungen

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	Updates
Autorisierung für PDF-Anforderungen erfordern [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Autorisierung für PDF-Anforderungen erforderlich • Alte Kurzbeschreibung: Autorisierung von PDF-Anforderungen
Autorisierung für RSS-Anforderungen erfordern [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Autorisierung für RSS-Anforderungen erfordern • Alte Kurzbeschreibung: Autorisierung von RSS-Anforderungen
Autorisierung für SCHEMA-Anforderungen erfordern [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Autorisierung für SCHEMA-Anforderungen erforderlich • Alte Kurzbeschreibung: Autorisierung von SCHEMA-Anforderungen
Autorisierung für SOAP-Anforderungen erfordern [Aktualisiert in Security Center 1.3 und 1.5]	• Neue Kurzbeschreibung: Autorisierung für SOAP-Anforderungen erfordern • Alte Kurzbeschreibung: Autorisierung von SOAP-Anforderungen
Autorisierung von Entlade-Anforderungen	• Neue Kurzbeschreibung: Autorisierung für Entlade-Anforderungen erforderlich • Alte Kurzbeschreibung: Autorisierung von Entlade-Anforderungen
Autorisierung für WSDL-Anforderung erfordern [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Autorisierung für WSDL-Anforderung erforderlich • Alte Kurzbeschreibung: Autorisierung von WSDL-Anforderungen
Autorisierung für XML-Anforderungen erfordern [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Autorisierung für XML-Anforderungen erfordern • Alte Kurzbeschreibung: Autorisierung von XML-Anforderungen
Berechtigung für XML-Ausgabeanforderungen anfordern	• Neue Kurzbeschreibung: Autorisierung für XML-Ausgabeanforderungen erfordern • Alte Kurzbeschreibung: Autorisierung der XML-Ausgabe

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	Updates
Kennzeichnung für „Nur-HTTP-Cookie“ aktivieren [In Security Center 1.3 aktualisiert]	• Neue Kurzbeschreibung: Kennzeichnung für „Nur-HTTP-Cookie“ aktivieren • Alte Kurzbeschreibung: Kennzeichnung für „Nur-HTTP-Cookie“
Ausführung von Rohdatenbankabfragen deaktivieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Ausführung von Rohdatenbankabfragen deaktivieren • Alte Kurzbeschreibung: Anforderungen für die Zugriffssteuerung auf Vorgangsebene
SQL-Fehlermeldungen deaktivieren [In Security Center 1.3 aktualisiert]	• Neue Kurzbeschreibung: SQL-Fehlermeldungen deaktivieren • Alte Kurzbeschreibung: SQL-Fehlermeldungen werden deaktiviert
Eingehende E-Mail-Bilder in Anhänge konvertieren [In Security Center 1.3 aktualisiert und in 1.5 entfernt]	• Neue Kurzbeschreibung: Eingehende E-Mail-Bilder in Anhänge konvertieren • Alte Kurzbeschreibung: Eingehende HTML-E-Mails konvertieren
SMTP-Empfängermenge minimieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: SMTP-Empfängermenge minimieren • Alte Kurzbeschreibung: Max. SMTP-Empfänger
Excel-Formeln codieren [In Security Center 1.3 aktualisiert]	• Neue Kurzbeschreibung: Excel-Formeln mit Escape-Zeichen • Alte Kurzbeschreibung: Excel-Formel mit Escape-Zeichen
HTML-Bereinigung aktivieren [In Security Center 1.3 aktualisiert]	• Neue Kurzbeschreibung: HTML-Bereinigung aktivieren • Alte Kurzbeschreibung: HTML-Bereinigung
Cache-Steuerung – HTTP-Headerwert [In Security Center 1.3 aktualisiert]	• Neue Kurzbeschreibung: Cache-Steuerung – HTTP-Headerwert • Alte Kurzbeschreibung: HTTP-Headerwert „Cache-Steuerung“.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	Updates
Verhalten von Produktionsinstanz erzwingen [Aktualisiert in Security Center 1.3 und 1.5]	• Neue Kurzbeschreibung: Verhalten von Produktionsinstanz erzwingen • Alte Kurzbeschreibung: Verhalten von Produktionsinstanz
Zulässige ServiceNow interne IP-Adressen definieren [Aktualisiert in Security Center 1.3 und 1.5]	• Neue Kurzbeschreibung: Zulässige interne ServiceNow-IP-Adressen definieren • Alte Kurzbeschreibung: Zulassungsliste für IP-Adressenzugriff
Legacy-JQuery-Verhalten deaktivieren [in Security Center 1.3 aktualisiert]	• Neue Kurzbeschreibung: Legacy-JQuery-Verhalten deaktivieren • Alte Kurzbeschreibung: Legacy JQuery-Verhalten
Anfänglicher eindeutiger LDAP-Namen löschen [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Einstellung des anfänglichen differenzierten LDAP-Namens löschen • Alte Kurzbeschreibung: Initial Distinguished Name (LDAP)
Zugriff auf anwenderdefinierte Journaleinträge beschränken [In Security Center 1.3 aktualisiert]	• Neue Kurzbeschreibung: Zugriff auf anwenderdefinierte Journaleinträge beschränken • Alte Kurzbeschreibung: Sichere anwenderdefinierte Journaleinträge
Einmalige Lebensdauer der Verifizierung außerhalb des Bereichs minimieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Einmalige Lebensdauer der Verifizierung außerhalb des Bereichs minimieren • Alte Kurzbeschreibung: Kurze einmalige Lebensdauer der Verifizierung außerhalb des Bereichs
Ausgehende SSLv2-/SSLv3-Verbindungen deaktivieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Ausgehende SSLv2-/SSLv3-Verbindungen deaktivieren • Alte Kurzbeschreibung: SSLv2/SSLv3 wird deaktiviert

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	Updates
Erstellen von Anwendern aus eingehenden E-Mails deaktivieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Erstellen von Anwendern aus eingehenden E-Mails deaktivieren • Alte Kurzbeschreibung: E-Mails nach Domäne beschränken
Zugriff auf skriptfähige GlideSystemUserSession-API beschränken [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Standardmäßige Authentifizierung für vom Client aufrufbare Skripteinbindungen erfordern • Alte Kurzbeschreibung: Datenschutz für vom Client aufrufbare Skripteinbindungen
Standardmäßige Authentifizierung für vom Client aufrufbare Skripteinbindungen anfordern [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Standardmäßige Authentifizierung für vom Client aufrufbare Skripteinbindungen erfordern • Alte Kurzbeschreibung: Datenschutz für vom Client aufrufbare Skripteinbindungen
AJAXGlideRecord-ACL-Überprüfung erfordern [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: AJAXGlideRecord-ACL-Überprüfung erforderlich • Alte Kurzbeschreibung: AJAXGlideRecord-ACL-Überprüfung wird aktiviert
Vom Client generierte Skripts-Sandbox erzwingen [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Vom Client generierte Skripts in der Sandbox erzwingen • Alte Kurzbeschreibung: Vom Client generierte Skripts-Sandbox
Hochgeladene MIME-Typen einschränken [in Security Center 1.3 aktualisiert]	• Neue Kurzbeschreibung: Kurzbeschreibung für „Hochgeladene MIME-Typen beschränken“* • Alte Kurzbeschreibung: MIME-Typeinschränkung für Uploads, STANDARDWERT VON WAHR IN FALSCH GEÄNDERT

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	Updates
ACLs für bereichsbezogenen Administratoranwendungen aktivieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: ACLs für bereichsbezogenen Administratoranwendungen aktivieren • Alte Kurzbeschreibung: ACLs für bereichsbezogenen Administratoranwendungen verwalten
Anti-CSRF-Token aktivieren [Neu in Security Center 1.3 und entfernt in 1.5]	• Neue Kurzbeschreibung: Anti-CSRF-Token aktivieren • Alte Kurzbeschreibung: Anti-CSRF-Token
Implementieren Sie den Sicherheitsheader „x-frame-options: SAMEORIGIN“ [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Implementieren Sie den Sicherheitsheader „X-Frame-Options: SAMEORIGIN“. • Alte Kurzbeschreibung: X-Frame-Optionen: SAMEORIGIN
Verschleierung der Mobile-App-UI erfordern [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Verschleierung der Mobile-App-UI erforderlich • Alte Kurzbeschreibung: UI-Verschleierung in mobilen Apps
Standardmäßig mit leeren ACLs verweigern [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Standardmäßig mit leeren ACLs verweigern • Alte Kurzbeschreibung: Sicherheitsmanager-Standard Deny
SOAP-Inhaltstyp validieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: SOAP-Inhaltstyp validieren • Alte Kurzbeschreibung: Überprüfung des SOAP-Inhaltstyps
Strikte Sicherheit für SOAP-Anforderungen erzwingen [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Strikte Sicherheit für SOAP-Anforderungen erzwingen • Alte Kurzbeschreibung: Strikte Sicherheit für SOAP-Anforderungen
Accountwiederherstellung aktivieren [In Security Center 1.3 und 1.5aktualisiert]	• Neue Kurzbeschreibung: Accountwiederherstellung aktivieren • Alte Kurzbeschreibung: Accountwiederherstellung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	Updates
XMLdoc2-Entitätsvalidierung mit allowlistDisable-Entitätserweiterung erfordern [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Erfordert die Validierung der XMLdoc2-Entität mit der Entitätserweiterung „allowlistDisable“. • Alte Kurzbeschreibung: Validierung der XMLdoc2-Entität mit AllowlistDisable-Entitätserweiterung
Domain Separation auf Dot-Walking-Felder anwenden [Aktualisiert in Security Center 1.3 und 1.5]	• Neue Kurzbeschreibung: Domain Separation auf Dot-Walking-Felder anwenden • Alte Kurzbeschreibung: Domain Separation anwenden
Eingeschränkt herunterladbare MIME-Typen definieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Herunterladbare MIME-Typen einschränken • Alte Kurzbeschreibung: Deny-Liste für herunterladbare MIME-Typen
Herunterladbare MIME-Typen	• Neue Kurzbeschreibung: Eingeschränkt herunterladbare MIME-Typen definieren • Alte Kurzbeschreibung: Herunterladbare MIME-Typen
Escape-Zeichen für Jelly-Skript [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Jelly-Skript mit Escape-Zeichen • Alte Kurzbeschreibung: Escape-Zeichen für Jelly
HTML in Listenansichten codieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: HTML in Listenansichten codieren • Alte Kurzbeschreibung: Escape-Zeichen für HTML
Skripts in Scratchpad codieren [In Security Center 1.3 aktualisiert]	• Neue Kurzbeschreibung: Escape-Skripts in Scratchpad • Alte Kurzbeschreibung: Scratchpad mit Escape-Zeichen
XML-Markup codieren [In Security Center 1.3 aktualisiert]	• Neue Kurzbeschreibung: Escape-XML-Markup • Alte Kurzbeschreibung: Escape-XML

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	Updates
Verschleierung der klassischen mobilen App-UI vorschreiben [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Verschleierung der Classic Mobile-App-UI erforderlich • Alte Kurzbeschreibung: Obfuskation für Classic Mobile-App-UI
Öffentlichen Zugriff auf Favoriten deaktivieren	• Neue Kurzbeschreibung: Öffentlichen Zugriff auf Favoriten deaktivieren • Alte Kurzbeschreibung: Öffentlicher Zugriff auf Favoriten
Strikte Sicherheit von Sitzungscookies erzwingen [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Strikte Sicherheit von Sitzungscookies erzwingen • Alte Kurzbeschreibung: Sitzungscookies
Eingebetteten HTML-Code deaktivieren [In Security Center 1.3 aktualisiert]	• Neue Kurzbeschreibung: Eingebetteten HTML-Code deaktivieren • Alte Kurzbeschreibung: Eingebetteter HTML-Code
JavaScript-Tags in eingebettetem HTML deaktivieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Deaktivieren Sie JavaScript-Tags in eingebettetem HTML • Alte Kurzbeschreibung: Javascript-Tags in eingebettetem HTML zulassen
Zeitüberschreitungsdauer der Sitzungsaktivität minimieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Zeitüberschreitungsdauer der Sitzungsaktivität minimieren • Alte Kurzbeschreibung: Zeitüberschreitung bei Sitzungsaktivität
Herunterladbare Dateitypen in statischen Inhalten beschränken [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Herunterladbare Dateitypen in statischen Inhalten beschränken • Alte Kurzbeschreibung: Einschränkungen beim Herunterladen von Dateitypen aus statischem Inhalt
Zeitüberschreitungsdauer des Sitzungsfensters minimieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Zeitüberschreitungsdauer des Sitzungsfensters minimieren • Alte Kurzbeschreibung: Zeitüberschreitung beim Sitzungsfenster

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	Updates
Absolute Zeitüberschreitungsdauer für Sitzung minimieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Absolute Zeitüberschreitungsdauer der Sitzung minimieren • Alte Kurzbeschreibung: Absolute Zeitüberschreitung für Sitzung
Zeitüberschreitungsdauer beim Entsperren bei fehlgeschlagener Anmeldung maximieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Zeitüberschreitungsdauer beim Entsperren bei fehlgeschlagener Anmeldung maximieren • Alte Kurzbeschreibung: Zeitüberschreitung beim Entsperren nach fehlgeschlagenen Anmeldungen verwalten
Externe XML-Entitäten einschränken [in Security Center 1.3 aktualisiert]	• Neue Kurzbeschreibung: Externe XML-Entitäten einschränken • Alte Kurzbeschreibung: Allow-Liste für URLs zur Validierung von XML-Entitäten
Schwellenwert für Entitätserweiterung minimieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Schwellenwert für Entitätserweiterung minimieren • Alte Kurzbeschreibung: Schwellenwert für Entitätserweiterung wird festgelegt
Ablaufdauer für die Anforderung einer Passwortzurücksetzung minimieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Ablaufdauer für Anforderung einer Passwortzurücksetzung minimieren • Alte Kurzbeschreibung: Ablaufdatum für Anforderung zum Zurücksetzen des Passworts
Maximale Versuchsanzahl für die Anforderung einer Passwortzurücksetzung minimieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Minimieren Sie die zulässigen Höchstversuche für die Anforderung einer Passwortzurücksetzung • Alte Kurzbeschreibung: Max. Versuche für die Anforderung zum Zurücksetzen des Passworts

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	Updates
Fensterdauer bei maximalen Versuchen für die Anforderung einer Passwortzurücksetzung minimieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Fensterdauer bei maximalen Versuchen für die Anforderung einer Passwortzurücksetzung minimieren • Alte Kurzbeschreibung: Fenster für max. Versuche für Anforderung zum Zurücksetzen des Passworts
Wiederholungsfensterdauer für die Anforderung einer Passwortzurücksetzung maximieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Fensterdauer beim Wiederholen für Anforderung zum Zurücksetzen des Passworts maximieren • Alte Kurzbeschreibung: Wiederholungsfenster für Anforderung zum Zurücksetzen des Passworts
Fensterdauer bei erfolgreicher Anforderung einer Passwortzurücksetzung minimieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Fensterdauer bei erfolgreicher Anforderung einer Passwortzurücksetzung minimieren • Alte Kurzbeschreibung: Erfolgsfenster für Anforderung zum Zurücksetzen des Passworts
Fensterdauer beim Entsperren für Anforderung zum Zurücksetzen des Passworts maximieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Fensterdauer beim Entsperren für Anforderung zum Zurücksetzen des Passworts maximieren • Alte Kurzbeschreibung: Fenster zum Entsperren für Anforderung zum Zurücksetzen des Passworts
SMS- Komplexität bei der Passwortzurücksetzung maximieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: SMS-komplexität für „Passwort zurücksetzen“ maximieren • Alte Kurzbeschreibung: SMS-komplexität für „Passwort zurücksetzen“.
SMS-Ablaufzeit bei Passwortzurücksetzung minimieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Ablaufdauer für SMS bei Passwortzurücksetzung minimieren • Alte Kurzbeschreibung: SMS-Ablaufdatum für Passwort zurücksetzen
Max. SMS pro Tag für die Passwortzurücksetzung minimieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Max. SMS pro Tag für Passwortzurücksetzung minimieren • Alte Kurzbeschreibung: Max. SMS pro Tag für Passwort zurücksetzen

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	Updates
Fensterdauer bei SMS-Pause für Passwortzurücksetzung maximieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Fensterdauer beim Anhalten der SMS-Pause für Passwortzurücksetzung maximieren • Alte Kurzbeschreibung: SMS-Pause-Fenster für „Passwort zurücksetzen“.
SMS-Codebenachrichtigung für die Registrierung und Verifizierung aktivieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: SMS-Codebenachrichtigung für die Registrierung und Verifizierung aktivieren • Alte Kurzbeschreibung: SMS-Codebenachrichtigung für die Registrierung und Verifizierung
Verzögerungsdauer für die Verifizierung der Verifizierung der Passwortzurücksetzung maximieren [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Verzögerungsdauer der Verifizierung der Verifizierung der Passwortzurücksetzung maximieren • Alte Kurzbeschreibung: Verzögerung bei der Verifizierung des Passwortzurücksetzens
Benachrichtigen Sie Anwender während des Prozesses zum Zurücksetzen/Ändern des Passworts	• Neue Kurzbeschreibung: Anwender während des Passwortzurücksetzungs-/Change-Prozesses benachrichtigen • Alte Kurzbeschreibung: Prozess für Passwortzurücksetzung/Change-Benachrichtigung
E-Mail-Domänen für die Registrierung externer Anwender einschränken [Aktualisiert in Security Center 1.5]	• Neue Kurzbeschreibung: E-Mail-Domänen für Registrierung externer Anwender einschränken • Alte Kurzbeschreibung: Allow-Liste für E-Mail-Domänen zur Registrierung externer Anwender
Ablaufdauer des Links zur Registrierung externer Anwender minimieren [Aktualisiert in Security Center 1.3 und 1.5]	• Neue Kurzbeschreibung: Ablaufdauer des Links für die Registrierung externer Anwender minimieren • Alte Kurzbeschreibung: Ablaufdatum des Registrierungslinks für externe Anwender

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	Updates
Zulässige Java-Pakete einschränken [Aktualisiert in Security Center 1.3]	• Neue Kurzbeschreibung: Zulässige Java-Pakete einschränken • Alte Kurzbeschreibung: Allow-Liste für Java-Pakete

Härtungseinstellungen für Baselineversion 4.0 gelöscht

Diese Liste enthält die Härtungseinstellungen, die in Security Center Baselineversion 4.0 entfernt wurden.

- Einschränkungen des Anwendungsbereichs erzwingen
- Anwender während des Passwortzurücksetzungs-/Change-Prozesses benachrichtigen
- Cache-Steuerung – HTTP-Headerwert
- Eingehende E-Mail-Bilder in Anhänge konvertieren
- Anti-CSRF-Token aktivieren
- Zertifikatvertrauen erzwingen
- Inhaltstypoptionen automatisch festlegen

Härtungseinstellungen für Baselineversion 2.0 gelöscht

Diese Liste enthält die Härtungseinstellungen, die in der Baselineversion Security Center 2.0 entfernt wurden.

- Codesignatur für Anwendungskonfigurationsdaten und Skripte aktivieren
- Glide KMF-Verschlüsseler aktivieren
- Verwendung des Verschlüsselers auf Instanzebene deaktivieren
- Alle ausgehenden HTTP-Anforderungsfelder protokollieren

Zugriffssteuerung

Die Kategorie „Zugriffssteuerung“ prüft den Prozess, Ressourcen vor nicht autorisiertem Zugriff zu schützen, indem Anforderungen basierend auf einem Berechtigungsmodell gewährt und verweigert werden. Dies umfasst sicherzustellen, dass eine Entität, die auf eine Ressource zugreift, über gültige Anmeldeinformationen verfügt, um einen wohldefinierten Satz von Rollen oder Berechtigungen zu erstellen und zu schützen und sicherzustellen, dass Rollen- oder Berechtigungssteuerungen vor Wiedergabe und Manipulation geschützt sind.

Zugriffssteuerungen bestimmen, ob der Zugriff auf eine bestimmte Ressource gewährt oder verweigert werden soll. Sie gewährt nur den Benutzern Zugriff auf Ressourcen, die zu deren Verwendung berechtigt sind.

Validierungszeit des Anti-CSRF-Tokens [Neu in Security Center 1.3]

Die Eigenschaft *glide.security.csrf_previous.time_limit* gibt die Zeit in Sekunden an, bis ein sicheres Token abläuft.

Wenn eine Benutzersitzung abläuft, läuft auch das sichere Token ab, es sei denn, die Eigenschaft, die **die Wiederverwendung abgelaufener Token zulässt, ist aktiviert, und der** Vorgang liegt innerhalb des durch diese Eigenschaft beschriebenen Zeitrahmens. Dieses

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Token wird verwendet, um Site-übergreifende Angriffe durch gefälschte Anforderungen zu verhindern.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.security.csrf_previous.time_limit*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer
Empfohlener Wert	86400 Sekunden oder 1 Tag
Standardwert	86400 Sekunden oder 1 Tag
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 5.3 • CVSS-Punktzahl: Mittel • Details zu Sicherheitsrisiken: Wenn Sie diese Eigenschaft nicht auf den empfohlenen Wert festlegen, wird die Tokenvalidierung deaktiviert, die verwendet wird, um Site-übergreifende Angriffe durch gefälschte Anforderungen zu verhindern.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Diese Eigenschaft bestimmt die Dauer in Sekunden, für die ein sicheres Token gültig bleibt. Das sichere Token läuft ab, wenn die Benutzersitzung abläuft, es sei denn, die Eigenschaft, die **die Wiederverwendung abgelaufener Token** ermöglicht, ist aktiviert, und das Token liegt innerhalb des in dieser Eigenschaft angegebenen Zeitrahmens. Dieses Token verhindert Site-übergreifende Angriffe durch gefälschte Anforderungen. Sie hat einen Standardwert von 86.400 Sekunden oder 1 Tag.

Domain Separation auf Dot-Walking-Felder anwenden [Aktualisiert in Security Center 1.3 und 1.5]

Die Eigenschaft *glide.sys.domain.include_domain_condition_on_join* steuert, ob Teilnahmeabfragen domänengetrennte Bedingungen erhalten oder nicht, um sicherzustellen, dass sie die Domain Separation-Funktion für Dot-Walking-Felder anwenden.

Diese Eigenschaft *glide.sys.domain.include_domain_condition_on_join* steuert, ob Teilnahmeabfragen domänengetrennte Bedingungen erhalten oder nicht, um sicherzustellen, dass sie die Domain Separation-Funktion für Dot-Walking-Felder anwenden. Wenn *glide.sys.domain.include_domain_condition_on_join* auf einer Instanz mit Domänentrennung nicht auf den empfohlenen Wert „true“ festgelegt ist, können vertrauliche Informationen offengelegt werden, die nicht mit einer bestimmten Domäne geteilt werden sollen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn das Domain Separation-Plugin installiert ist, wird ein sys_properties-Datensatz für diese Eigenschaft installiert, dessen Wert auf **true**festgelegt ist, was der nicht standardmäßige Wert ist. Andernfalls ist in dem Basissystem ohne installierte Domänentrennung der Eigenschaftsdatensatz nicht vorhanden, und er hat seinen nicht standardmäßigen -Wert [].

Warnung: Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.sys.domain.include_domain_condition_on_join*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	„True“, wenn Domain Separation installiert ist, andernfalls ist die Eigenschaft nicht vorhanden.
Standardwert	falsch
Kategorie	Zugriffssteuerung
Zweck	Steuert, ob Teilnahmeabfragen domänengetrennte Bedingungen erhalten oder nicht, um sicherzustellen, dass sie die Domain Separation-Funktion für Dot-Walking-Felder anwenden.
Sicherheitsrisiko	• Schweregrad-Punktzahl: 6,5 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn *glide.sys.domain.include_domain_condition_on_join* nicht auf den empfohlenen Wert **true**festgelegt ist, können vertrauliche Informationen offengelegt werden, die nicht mit einer bestimmten Domäne geteilt werden sollen.
Referenzen	Domänentrennung für Service Provider

ACLs für bereichsbezogenen Administratoranwendungen aktivieren [Aktualisiert in Security Center 1.3]

glide.security.scoped_administration.honor_global_acl bestimmt, ob eine Anwendungsverwaltungs-App globale Regeln für Zugriffssteuerungslisten (ACL) erben kann.

Diese Eigenschaft ist besonders nützlich, wenn für den Datensatzbereich keine ACLs für bereichsbezogene Administratoranwendungen definiert sind.

Legen Sie *glide.security.scoped_administration.honor_global_acl* auf „wahr“ fest, um zu verhindern, dass ein Benutzer mit geringen Berechtigungen, der über Berechtigungen für die Anwendung verfügt, potenziell auf vertrauliche Datensätze zugreifen kann.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.security.scoped_administration.honor_global_acl*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Steuert die ACL-Zugriffsregel in der bereichsbezogenen Administratoranwendung.
Empfohlener Wert	True
Standardwert	True
Konfigurationstyp	Boolean
Sicherheitsrisiko	(Niedrig) Wenn der Eigenschaftswert „wahr“ ist und keine bereichsbezogenen Administratoranwendungs-ACLs für den Datensatzbereich definiert sind, werden die globalen ACLs berücksichtigt. Bei Festlegung auf „falsch“ werden ACL-Prüfungen ignoriert, wenn keine bereichsbezogenen Administratoranwendungs-ACLs für den Datensatzbereich definiert sind.
Sicherheitsrisikobewertung	3.8
Referenzen	Zugriffskontrollregeln in Anwendungsverwaltungs-Apps

Weitere Informationen zum Aktivieren eines Plugins finden Sie unter Plugins aktivieren

Abfrageregeln für das Arbeitsauftragsmanagement für Serviceorganisationen aktivieren [Neu in Security Center 1.5]

Verwenden Sie die Eigenschaft *sn_fsm.use_query_rules*, um Regeln und Filter auf die Außendienst-Management-Tabellen anzuwenden.

Wenn die Eigenschaft *sn_fsm.use_query_rules* auf „wahr“ festgelegt ist, werden die Regeln und Filter aus der Tabelle „sn_query_rule“ verwendet, um den Lesezugriff auf Außendienst-Management-Tabellen authentifizierter Benutzer zu bestimmen. Dies geschieht durch Abfragen von Business-Regeln und Lese-ACLs. Wenn diese Eigenschaft auf „false“ festgelegt ist, werden die Datensätze nicht basierend auf Abfrageregeln gefiltert. Abfrage-Business-Regeln fügen zusätzliche Sicherheitsvalidierungen hinzu, wenn sie für diese Eigenschaft aktiviert sind, und filtern Datensätze für Service Desk-Mitarbeiter, Qualifizierer und Zuteiler basierend auf dem zugewiesenen Gebiet oder der Gebietsmitgliedschaft. Dies implementiert das Prinzip der geringsten Berechtigung beim Lesen von Datensätzen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*sn_fsm.use_query_rules*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	falsch

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Standardwert	falsch
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 4.3 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft auf „wahr“ festgelegt ist, werden Regeln und Filter aus „sn_query_rule“ verwendet, um den Lesezugriff auf Außendienst-Management-Tabellen zu bestimmen und das Prinzip der geringsten Rechte zu implementieren. Bei Festlegung auf „falsch“ werden die Datensätze nicht basierend auf Abfrage-Business-Regeln gefiltert, und das Risiko der Offenlegung von Daten durch Außendienst-Management-Tabellen ist möglicherweise erhöht.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Bei Festlegung auf „wahr“ werden Regeln/Filter aus der Tabelle „sn_query_rule“ verwendet, um den Lesezugriff auf Tabellen im Zusammenhang mit dem Außendienst-Management zu bestimmen. Beispiel: Arbeitsauftrag (WO) und Arbeitsauftragstabelle (WOT) für den angemeldeten Benutzer durch Abfragen von Business-Regeln und Lese-ACLs. Bei „false“ werden die Datensätze nicht basierend auf Abfrageregeln gefiltert. Durch Aktivieren dieser Eigenschaft werden die Daten gesichert, und alle Daten (wm_task und wm_order) sind für die Anwender nicht sichtbar.
Referenzen	Referenz für Außendienst-Management

Blockieren Sie den Zugriff für delegierte Entwickler

Diese Konfiguration wirkt sich auf den Zugriff für delegierte Entwickler aus, die Anwenderrollen über ein Skript aktualisieren. Wenn die Konfiguration konform ist, kann der Entwickler keine Datensätze in der Tabelle sys_user_has_role [] aktualisieren oder einfügen, ohne dass auch über die Rolle user_admin für verfügt.

Der Wert dieser Eigenschaft wirkt sich darauf aus, ob ein delegierter Entwickler unerwarteten Zugriff auf Funktionen in der Instanz gewähren oder erhalten darf. Wenn die Eigenschaft Rollen enthält, können nur diese Rollen Skriptmodule ausführen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`com.glide.sys.security.delegateddev.block_grant_roles`

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Der Wert dieser Eigenschaft wirkt sich darauf aus, ob ein delegierter Entwickler unerwarteten Zugriff auf Funktionen in der Instanz gewähren oder erhalten darf.
Typ	Umschalten
Standardwert	wahr
Empfohlener Wert	wahr
Sicherheitsabhängigkeiten	Keine
Sicherheitsrisikobewertung	6.7
Funktionale Auswirkung	(Hoch) Wenn ein Benutzer mit der Rolle „delegated_developer“ versucht, einen Datensatz in der Tabelle „sys_user_has_role“ zu ändern, aktiviert diese Eigenschaft zusätzliche Sicherheitsprüfungen für den Vorgang. Die zusätzlichen Sicherheitsprüfungen validieren, dass dem Benutzer die Rolle user_admin gewährt wurde, wenn er versucht, die [Tabelle „sys_user_has_role“] zu erstellen oder zu aktualisieren. Wenn sie nicht über die Rolle user_admin verfügen, wird der Zugriff verweigert. Wenn die Eigenschaft „false“ lautet, werden diese zusätzlichen Prüfungen nicht validiert.
Sicherheitsrisiko	(Mittel) Ohne entsprechende Autorisierung können nicht autorisierte Anwender auf vertrauliche Inhalte/ Daten in der Instanz zugreifen.
Referenzen	Zugriffssteuerung

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Abgelaufene Anti-CSRF-Token blockieren [in Security Center 1.5 aktualisiert]

Blockieren Sie abgelaufene CSRF-Token, um Site-übergreifende Angriffe durch gefälschte Anforderungen zu verhindern.

Übersicht

Site-übergreifende Anforderungsfälschungen sind eine Art von böswilligem Exploit, bei der nicht autorisierte Befehle im Namen eines authentifizierten Anwenders ausgeführt werden.

Konfigurationsdetails

Attribut	Beschreibung
Übersicht	Steuert die Verwendung eines abgelaufenen sicheren Tokens zum Identifizieren und Validieren eingehender Anforderungen. Legen Sie den Wert auf „ **falsch** “ fest, um zu verhindern, dass ein zuvor

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	abgelaufenes Token zum Validieren einer eingehenden Anforderung verwendet wird.
Konfigurationsname	*glide.security.csrf_previous.allow*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	**false**
Standardwert	**true**
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	**Schweregrad-Punktzahl**: 6,5
	Schweregradbewertung pro CVSS-Punktzahl: Mittel
	Details zum Sicherheitsrisiko: Erzwingt einen sicheren Anti-CSRF-Mechanismus zum Schutz authentifizierter Funktionen, und eine effektive Anti-Automatisierungs- oder Anti-CSRF-Mechanismen schützt nicht authentifizierte Funktionen.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Anti-CSRF-Token aktivieren [Neu in Security Center 1.3 und entfernt in 1.5], websiteübergreifende Anforderungsfälschung .

Überprüfen Sie die Bedingungen für UI-Aktionen vor der Ausführung

Verwenden Sie die Eigenschaft *glide.security.strict.actions*, um die Überprüfung von Bedingungen für UI-Aktionen in Formularen und Listen zu ermöglichen, bevor sie ausgeführt werden. Wenn Sie diese Eigenschaft auf truefestlegen, wird den Tabellen-UI-Aktionen eine zusätzliche Validierungsebene hinzugefügt, bevor sie ausgeführt werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.security.strict.actions*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Um eine zusätzliche Validierungsebene für die Tabellen-UI-Aktionen sicherzustellen, bevor sie ausgeführt werden.
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	3.3
Funktionale Auswirkung	(Niedrig) Diese Korrektur fügt lediglich eine zusätzliche Validierungsebene hinzu, um nach UI-Aktionen in der Zieltabelle/-seite in der Instanz zu suchen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Solange die Zugriffssteuerungen in der Kundeninstanz entsprechend festgelegt sind, sollte dies hier keine Auswirkungen haben.
Sicherheitsrisiko	(Niedrig) Zugriffsanforderung wird immer geprüft, wenn Transaktionen zwischen zwei Zonen stattfinden. Dieser Vorgang validiert alle UI-Aktionen, bevor das Formular für den Endanwender gerendert wird.
Referenzen	Hochsicherheits-Plugin

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Administratorrollen für Ereignismanagement-Zuweisungsgruppen konfigurieren [Neu in Security Center 1.5]

Verwenden Sie die Eigenschaft *evt_mgmt.connector_assignment_group_admin_roles*, um festzulegen, welche Rollen für den Administratorzugriff über das Zuweisungsgruppenfeld in Connector-Instanzen berechtigt sind.

Die Eigenschaft *evt_mgmt.connector_assignment_group_admin_roles* enthält eine kommagetrennte Zeichenfolge, die die Rollennamen angibt, die in Connector-Instanzen über das Feld „Zuweisungsgruppe“ Administratorzugriff haben. Durch das Ändern der Standardrollen in dieser Liste können nicht autorisierte Anwender Event-Integrationen in der Instanz ändern. Um den nicht autorisierten Zugriff auf Rollen zu verhindern, legen Sie *evt_mgmt.connector_assignment_group_admin_roles* auf den Wert admin,evt_mgmt_admin,sn_sow_srm.srm_admin fest. Überprüfen Sie alle zusätzlichen Rollen in der Zeichenfolge des empfohlenen Werts, um sicherzustellen, dass die Rolle enthalten ist.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*evt_mgmt.connector_assignment_group_admin_roles*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	admin, evt_mgmt_admin, sn_sow_srm.srm_admin
Standardwert	admin, evt_mgmt_admin, sn_sow_srm.srm_admin
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 3,1 • CVSS-Punktzahl: Niedrig • Details zu Sicherheitsrisiken: Durch das Ändern der Standardrollen können nicht autorisierte Benutzer Event-Integrationen in der Instanz ändern.
Abhängigkeiten und Voraussetzungen	Keine

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Referenzen	Erstellen von Gruppen

Internen Zugriff auf explizite externe Rollen verweigern [Aktualisiert in Security Center 1.5]

Mehrere Eigenschaften bilden zusammen die Konfiguration für die Härtungseinstellung für die **Aktivierung expliziter Rollen für die interne Deny-Liste**. Die Eigenschaft *glide.security.explicit_roles.enable_internal_user_blacklist* verhindert, dass externen Benutzern die Rolle „snc_internal“ zugewiesen wird, und ermöglicht die Eigenschaft *glide.security.explicit_roles.internal_user_blacklist*, um die Rolle „snc_external“ zuzuweisen.

Glide.security.explicit_roles.enable_internal_user_blacklist

Sie können internen Benutzern und externen Benutzern Zugriff auf Ihre Instanz gewähren. Um die Sicherheit zu erhöhen, muss jeder Benutzer mindestens eine Rolle besitzen, damit die Instanz zwischen internen und externen Benutzern unterscheiden kann.

Legen Sie die Eigenschaft *glide.security.explicit_roles.enable_internal_user_blacklist* auf den empfohlenen Wert **true** fest, um die Zuweisung der Rolle snc_external zu ermöglichen.

Legen Sie den Wert auf „ **false** “ fest, um die Möglichkeit zum Zuweisen der Rolle „snc_external“ zu deaktivieren. Allen Anwendern wird standardmäßig die Rolle snc_internal zugewiesen

Hinweis: Instanzen ohne installierte explizite Rollen sind nicht betroffen. Ab dem Paris-Release erhalten neue Installationen von expliziten Rollen die Eigenschaft mit dem Standardwert true.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.security.explicit_roles.enable_internal_user_black*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Ermöglicht die Zuweisung angegebener Anwenderklassen zur Rolle „snc_external“ anstelle der Rolle „snc_internal“.
Empfohlener Wert	True
Standardwert	True
Konfigurationstyp	Boolean
Sicherheitsrisiko	(Moderat) Das Deaktivieren der Eigenschaft kann zu einer unangemessenen Standardrollenzuweisung führen.
Sicherheitsrisikobewertung	5.4
Referenzen	Explizite Rollen in CSM ,

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Glide.security.explicit_roles.internal_user_blacklist

Der Wert *glide.security.explicit_roles.internal_user_blacklist* bestimmt, welchen Anwenderklassen (Tabellen, die „sys_user“ erweitern) die Rolle „snc_external“ anstelle der Rolle „snc_internal“ zugewiesen werden soll. Der Standardwert csm_consumer_user,customer_contact ist zur Ausrichtung an den Anwendungsfällen in den Plugins für das Kundenservice-Management definiert.

Der Eigenschaftswert muss nur geändert werden, wenn zusätzliche oder andere Anwenderklassen vorhanden sind, denen standardmäßig die Rolle „snc_external“ anstelle der Rolle „snc_internal“ zugewiesen werden muss. Wenden Sie sich an den Support, um diese Werte zu ändern.

Attribut	Beschreibung
Eigenschaftsname	*glide.security.explicit_roles.internal_user_blacklist*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Ermöglicht standardmäßig die Zuweisung der Rolle „snc_external“ anstelle der Rolle „snc_internal“.
Empfohlener Wert	*csm_consumer_user*, *Customer_contact*
Konfigurationstyp	Zeichenfolge
Sicherheitsrisiko	(Moderat) Das Deaktivieren der Eigenschaft kann zu einer unangemessenen Standardrollenzuweisung führen.
Sicherheitsrisikobewertung	5.4
Referenzen	Explizite Rollen, Zuweisungen externer Anwenderrollen korrigieren

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Verweigern Sie den nicht autorisierten Zugriff auf Anforderungselemente

Die Eigenschaft *glide.sc.req_for.roles.default* definiert ein Standardverhalten für die *RetrieveAddress*-API.

Diese Eigenschaft funktioniert nur, wenn *glide.sc.req_for.roles* keine Werte hat. Wenn *glide.sc.req_for.roles* Werte aufweist, hat diese Eigenschaft keine Bedeutung, und Benutzer mit nur definierten Rollen erhalten Zugriff auf die API.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.sc.req_for.roles.default*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Wenn in der Eigenschaft keine Rollen angegeben sind, kann die vom Client aufrufbare *Skripteinbindung*

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

	ScriptServiceCatalogGetLocation von jedem nicht privilegierten angemeldeten Benutzer aufgerufen werden und die Adressen anderer Benutzer im System abrufen. Diese Eigenschaft verhindert, dass diese API für nicht privilegierte Anwender verfügbar gemacht wird.
Empfohlener Wert	verweigern
Standardwert	verweigern
Konfigurationstyp	Auswahlliste (zulassen | verweigern)
Sicherheitsrisiko	(Moderat) Wenn *glide.sc.req_for.roles.default* nicht auf den empfohlenen Wert „ **verweigern** “ (zulassen) festgelegt ist und der Wert von *glide.sc.req_for.roles* leer ist, kann jeder Anwender Elemente für andere Anwender anfordern, die nicht autorisierten Ressourcenzugriff gewähren.
Referenzen	Vom Client aufrufbare Skripteinbindungen

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Anti-CSRF-Token aktivieren [Neu in Security Center 1.3 und entfernt in 1.5]

Verwenden Sie die Eigenschaft *glide.security.use_csrf_token*, um sicherzustellen, dass ein sicheres Token zum Identifizieren und Validieren eingehender Anforderungen verwendet wird, die wiederum zum Verhindern dieser Angriffe verwendet werden.

Cross-Site Request Forgery (CSRF) ist ein Angriff, der einen Endanwender dazu zwingt, unerwünschte Aktionen in einer Webanwendung auszuführen, in der er sich derzeit authentifiziert hat. CSRF-Angriffe zielen speziell auf Anforderungen zur Statusänderung ab, nicht auf den Diebstahl von Daten, da der Angreifer keine Möglichkeit hat, die Antwort auf die gefälschte Anforderung zu sehen.

Die folgenden Eigenschaften können für hinzugefügte Steuerungen für das CSRF-Token aktiviert werden:

- *glide.security.csrf_previous.time_limit*
- *glide.security.csrf_previous.allow*
- *glide.security.csrf.strict.validation.mode*

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.security.use_csrf_token*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Zum Schutz der Anwendung vor potenziellen CSRF-Angriffen.
Sicherheitsrisikobewertung	8.1
Empfohlener Wert	wahr
Standardwert	wahr
Funktionale Auswirkung	(Niedrig) Diese Korrektur ermöglicht einen zusätzlichen Validierungsschritt, bevor der Instanzanwender eine Schreibanforderung an die Instanz sendet. Jede

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

	Schreibanforderung enthält ein CSRF-Token (also eine Validierungs-/CSRF-ID, die an die Benutzersitzung gebunden ist). Wenn die Benutzersitzung abläuft, läuft auch das sichere Token ab.
Sicherheitsrisiko	(Hoch) Cross Site Request Forgery stellt ein erhebliches Sicherheitsrisiko dar, das die Integrität der Instanzdaten verletzt. Ein Angreifer kann den CSRF-Angriff starten, indem er das Vertrauen eines Instanzbenutzers missbraucht. Mithilfe von Social Engineering-Angriffen kann ein Benutzer im Namen des Angreifers in der Instanz eine fehlerhafte Anforderung senden.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Sicherstellen, dass Archivtabellen-ACLs aktiviert sind [Neu in Security Center 1.3]

Die Eigenschaft *glide.security.enable_archive_table_acls* steuert, ob Zugriffssteuerungslisten (ACLs) der ursprünglichen Tabelle, der Tabelle, aus der die Archivtabelle erstellt wurde, als „falsch“ ausgewertet werden.

Die Eigenschaft *glide.security.enable_archive_table_acls* darf nicht auf „false“ festgelegt werden, da die ACLs der ursprünglichen Tabelle unabhängig von ihrem Wert ausgewertet werden. Sie können zusätzliche ACLs für eine Archivtabelle vermeiden, indem Sie sie nicht hinzufügen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.security.enable_archive_table_acls*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 3 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn die Eigenschaft auf „false“ festgelegt ist, werden archivierten Tabellen hinzugefügte ACLs ignoriert. Diese Aktion ist kontraintuitiv und kann daher zu einer Umgehung der Autorisierung führen.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Wenn diese Eigenschaft auf „wahr“ festgelegt ist, werden alle aktiven Lese-ACLs in Archivtabellen berücksichtigt. Wenn keine aktiven Lese-ACLs vorhanden sind oder die Eigenschaft auf „falsch“

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	festgelegt ist, gelten die der ursprünglichen Tabelle (Tabelle, aus der die Daten archiviert wurden) für die Archivtabelle. **Hinweis:** In Archivtabellen werden nur Lese-ACLs unterstützt. Andere Vorgänge in Archivtabellen werden intern durch einen Zugriffs-Handler gesteuert.

Plugin für kontextbezogene Sicherheit aktivieren [Aktualisiert in Security Center 1.3]

Aktivieren Sie das Plugin „Contextual Security Plugin“ (*com.glide.role_management*), um die kontextbezogene Sicherheit zu aktivieren, die Datensätze/Informationen mithilfe von Erstellungs-, Lese-, Schreib- und Löschfunktionen sichert.

Nach der Installation und Aktivierung werden die Wörterbuchrollen (vom einfachen Sicherheitsmanager erstellt) nicht mehr getestet. Stattdessen sucht Now Platform in Feldern und Tabellen nach ACL-Regeln. Die Anwendung sichert die Daten mithilfe von ACL-Regeln anstelle von herkömmlichen, rollenbasierten Wörterbuchregeln, die von einem einfachen Sicherheitsmanager implementiert werden. Selbst wenn Sie das Wörterbuchformular konfigurieren und einem Wörterbucheintrag Rollen hinzufügen, werden die Rechte nicht geändert.

Weitere Informationen

Attribut	Beschreibung
Plugin-ID	*com.glide.role_management*
Konfigurationstyp	Systemdefinition > Plugins
Kategorie	Zugriffssteuerung
Zweck	Im Gegensatz zum einfachen Sicherheitsmanager kennt der Kontextsicherheitsmanager die Systemtabellenhierarchie. Sie können möglicherweise andere Sicherheitsregeln für ein Feld haben, je nachdem, wo es in der Hierarchie angezeigt wird.
Empfohlener Wert	Aktiv
Standardwert	Es gibt keinen Standardwert, da dies ein Plugin ist, keine Glide-Eigenschaft.
Sicherheitsrisikobewertung	8.1
Funktionale Auswirkung	(Mittel) Diese Korrektur erzwingt die Funktionsebene von Zugriffssteuerungen, wodurch die Anwendung die Zugriffsbeschränkungen allein auf der ACL-Tabelle bestimmen kann.
Sicherheitsrisiko	(Hoch) Zugriffssteuerungen auf Funktionsebene müssen vor der Ausführung von CRUD-Vorgängen serverseitig erzwungen werden, um Instanzanwendern die entsprechende Zugriffsebene zu gewähren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Referenzen	Contextual Security Manager

Sicherheitsbereich für Playbook für Lizenzen und Berechtigungen erzwingen [Neu in Security Center 1.5]

Verwenden Sie diese Eigenschaft, um festzulegen, ob nur die Zugriffssteuerungslisten (ACLs) im Lizenz- und Erlaubnis-Plugin für die Bestimmung des Zugriffs auf den Bereich verwendet werden oder ob ACLs aus allen Bereichen berücksichtigt werden.

Wenn die Eigenschaft *glide.enforce_security_scope.sn_gsm_lic_prmt* auf den empfohlenen Wert true festgelegt ist, werden nur ACLs innerhalb des Lizenz- und Erlaubnis-Plugins verwendet, um den Zugriff auf den Bereich zu bestimmen. Wenn diese Einstellung auf „false“ konfiguriert ist, werden Daten von Lizenz- und Erlaubnis-Playbooks in Umfangsmastertabellen verfügbar gemacht, da ACLs aus allen Bereichen Zugriff gewährt werden. Um das Datenrisiko zu reduzieren, legen Sie *glide.enforce_security_scope.sn_gsm_lic_prmt* auf den empfohlenen Wert „true“ fest.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.enforce_security_scope.sn_gsm_lic_prmt*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 2,7 • CVSS-Punktzahl: Niedrig • Details zu Sicherheitsrisiken: Wenn Sie diese Einstellung auf den empfohlenen Wert „true“ konfigurieren, werden die Lizenz- und Erlaubnis-Playbooks-Daten in den Umfangs-Master-Tabellen gesichert, indem nur ACLs aus dem Bereich *sn_gsm_lic_prmt* für die Gewährung des Zugriffs berücksichtigt werden. Wenn Sie diese Option auf „false“ festlegen, werden die Lizenz- und Erlaubnis-Playbook-Daten in Umfangsmastertabellen verfügbar gemacht, indem die ACLs aus allen Bereichen für die Gewährung des Zugriffs berücksichtigt werden. Beispielsweise kann der IT-Administrator auf Lizenz- und Erlaubnis-Playbooks zugreifen, wenn diese Einstellung auf „false“ festgelegt ist.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	• Playbook für Lizenzen und Berechtigungen verwenden • Anwendungsbereich

Sicherheitsbereich für Mitarbeiterbereich für HR-Fallverwaltung erzwingen [Neu in Security Center 1.5]

Konfigurieren Sie das Plugin „Mitarbeiterbereich für HR-Fallmanagement“ so, dass Daten in Umfangshaupttabellen nur von Anwendern mit den richtigen Berechtigungen zugänglich sind, und erzwingen Sie das Prinzip der geringsten Berechtigung.

Wenn das Plugin *glide.enforce_security_scope.sn_hr_agent_ws* auf den empfohlenen Wert true konfiguriert ist, werden nur die Zugriffssteuerungslisten (Access Control List, ACL) im Plugin „Mitarbeiterbereich für HR-Fallmanagement“ verwendet, um den Zugriff auf eine Ressource zu bestimmen. Wenn diese Einstellung auf „falsch“ festgelegt ist, sind Daten des Mitarbeiterbereichs für HR-Fallmanagement in Umfangsmastertabellen verfügbar, da den ACLs aus allen Bereichen Zugriff gewährt wird.Beispielsweise kann ein IT-Administrator auf Daten des Mitarbeiterbereichs für HR-Fallverwaltung zugreifen, wenn diese Einstellung auf „falsch“ festgelegt ist. Um dies zu verhindern, legen Sie *glide.enforce_security_scope.sn_hr_agent_ws* auf den empfohlenen Wert „true“ fest. Dadurch wird sichergestellt, dass das Prinzip der geringsten Berechtigung erfüllt ist, da Benutzer nur auf Ressourcen zugreifen können, für die sie berechtigt sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.enforce_security_scope.sn_hr_agent_ws*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 2,7 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn Sie diese Einstellung auf „falsch“ konfigurieren, werden die Daten des Mitarbeiterbereichs für die HR-Fallverwaltung in Tabellen für Umfangsmaster verfügbar gemacht, da den ACLs aus allen Bereichen Zugriff gewährt wird.
Abhängigkeiten und Voraussetzungen	Mitarbeiterbereich für HR-Fallverwaltung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Funktionale Auswirkung	Wenn Sie diese Einstellung auf „wahr“ konfigurieren, wird die Ausführung globaler ACLs für eine Tabelle erzwungen, wenn für sie keine bereichsbezogenen ACLs vorhanden sind.
Referenzen	• https://owasp.org/www-project-proactive-controls/#div-numbering • Fügen Sie eine Komponente hinzu Mitarbeiterbereich

Erzwingen Sie die strikte Validierung des CSRF-Tokens

Verwenden Sie die Eigenschaft *glide.security.csrf.strict.validation.mode*, um die strikte Validierung des CSRF-Tokens zu aktivieren. Wenn das CSRF-Token nicht übereinstimmt, wird die erneute Übermittlung der Anforderung verhindert.

Die Eigenschaft *glide.security.csrf.strict.validation.mode* aktiviert die strikte Validierung des CSRF-Tokens, die die Wiederverwendung von CSRF-Token verhindert. Wenn diese Eigenschaft nicht auf den empfohlenen Wert „wahr“ festgelegt ist, können CSRF-Token wiederverwendet werden, wodurch CSRF-Angriffe erleichtert werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.security.csrf.strict.validation.mode*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Erzwingt die strikte Validierung des CSRF-Tokens und verhindert dessen Wiederverwendung.
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	(Mittel) Websiteübergreifende Anforderungsfälschung stellt ein erhebliches Sicherheitsrisiko dar, das die Integrität der Instanzdaten verletzt. Ein Angreifer kann den CSRF-Angriff auf jeden Instanzbenutzer starten, indem er das Vertrauen des Instanzbenutzers missbraucht. Mithilfe von Social Engineering-Angriffen kann ein Benutzer im Namen des Angreifers eine fehlerhafte Anforderung an die Instanz senden.
Funktionale Auswirkung	(Mittel) Diese Korrektur ermöglicht einen zusätzlichen Validierungsschritt, bevor der Instanzanwender eine Schreibanforderung an die Instanz sendet. Prüft, ob das aktuelle CSRF-Token zuvor verwendet wurde. Falls „Ja“, wird die Übermittlung weiterer Schreibanforderungen verhindert.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	(Mittel) Websiteübergreifende Anforderungsfälschung stellt ein erhebliches Sicherheitsrisiko dar, das die Integrität der Instanzdaten verletzt. Ein Angreifer kann den CSRF-Angriff auf jeden Instanzbenutzer starten, indem er das Vertrauen des Instanzbenutzers missbraucht. Mithilfe von Social Engineering-Angriffen kann ein Benutzer im Namen des Angreifers eine fehlerhafte Anforderung an die Instanz senden.

Kehren Sie zu Konfigurieren Sie den von Ihrem Kunden bereitgestellten Schlüssel, und laden Sie ihn hoch zurück, um Ihren umschlossenen Schlüssel hochzuladen.

Lesezugriff delegierter Entwickler einschränken [Aktualisiert in Security Center 1.3]

Wenn *com.glide.dd_allow_global_access_tables* nicht den empfohlenen Wert wf_activity, wf_activity_definition, wf_workflow, wf_workflow_version, sp_portal, sp_widget und sp_page enthält, können diese Tabellen von einem delegierten Entwickler gelesen werden. Dies könnte dem delegierten Entwickler Lesezugriff auf vertrauliche Informationen gewähren.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*com.glide.dd_allow_global_access_tables*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	wf_activity, wf_activity_definition, wf_workflow, wf_workflow_version, sp_portal, sp_widget, sp_page
Standardwert	wf_activity, wf_activity_definition, wf_workflow, wf_workflow_version, sp_portal, sp_widget, sp_page
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 2,7 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Stellen Sie sicher, dass *com.glide.dd_allow_global_access_tables* auf wf_activity, wf_activity_definition, wf_workflow, wf_workflow_version, sp_portal, sp_widget, sp_page festgelegt ist.

Eingehende E-Mails für gesperrte Anwender deaktivieren

Verwenden Sie die Eigenschaft *glide.pop3.process_locked_out*, um Aktionen für eingehende E-Mails für gesperrte, aktive Benutzer zu steuern.

Legen Sie diese Eigenschaft auf „ **falsch** “ fest, um eingehende E-Mails für gesperrte Anwender zu deaktivieren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Berücksichtigen Sie die Sicherheitsauswirkungen, wenn Sie Benutzer aus nicht vertrauenswürdigen Domänen zulassen, und warum sie gesperrt wurden, bevor Sie zulassen, dass E-Mails von ihnen Aktionen für eingehende E-Mails auslösen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.pop3.process_locked_out*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Diese Eigenschaft steuert Aktionen für eingehende E-Mails für gesperrte Anwender.
Datentyp	boolean
Empfohlener Wert	falsch
Standardwert	falsch
Sicherheitsrisiko	(Hoch) Wenn Sie diese Eigenschaft auf „ **true**“ festlegen, kann es zu einer Offenlegung von Informationen kommen, da eingehende E-Mails von Anwendern mit gesperrten Accounts empfangen würden.
Sicherheitsrisikobewertung	7.5

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Überprüfen Sie die eingehenden Transaktionen noch einmal

Verwenden Sie die Eigenschaft *glide.security.strict.updates*, um die doppelte Überprüfung der Sicherheit bei eingehenden Transaktionen während der Formularübermittlung zu ermöglichen. Wenn Sie diese Eigenschaft auf **true**festlegen, wird eine zusätzliche Ebene der Tabellenvalidierung hinzugefügt, bevor ein Formular im Browser gerendert wird.

Weitere Informationen

Warnung: Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	*glide.security.strict.updates*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Um eine zusätzliche Überprüfungsebene für Benutzerberechtigungen sicherzustellen, bevor das Formular im Browser angezeigt wird.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	8.1
Funktionale Auswirkung	(Niedrig) Diese Korrektur fügt eine zusätzliche Validierungsebene hinzu, um nach Anwenderberechtigungen für die Zieltabelle/-seite in der Instanz zu suchen. Solange die Zugriffssteuerungen in der Kundeninstanz entsprechend festgelegt sind, sollte dies keine Auswirkungen haben.
Sicherheitsrisiko	(Hoch) Sie sollten die Zugriffsanforderung immer überprüfen, wenn Transaktionen zwischen zwei Zonen stattfinden. Dieser Vorgang prüft auf Berechtigungen, wenn das Formular angefordert wird und bevor das Rendern des Formulars erfolgt.
Referenzen	

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Aktivieren Sie ACLs, um Live-Profildetails zu steuern

Verwenden Sie die Eigenschaft *glide.live_profile.details*, um festzulegen, ob ein Anwender alle Detailfelder in einem Live-Profil anzeigen kann, z. B. Unternehmensname und Telefonnummern.

Je nach Einstellung der Eigenschaft *glide.live_profile.details* geschieht Folgendes:

- Wenn der Wert auf Anzeigen festgelegt ist, wird der Zugriff auf die Live-Profilinformationen unabhängig von den für das Anwenderprofil erstellten ACLs gewährt.
- Wenn der Wert auf ACL festgelegt ist, wird der Zugriff auf die Live-Profilinformationen gemäß den für das Anwenderprofil erstellten ACLs eingeschränkt.
- Wenn der Wert auf Ausblenden festgelegt ist, wird der Zugriff auf die Live-Profilinformationen unabhängig von den für das Anwenderprofil erstellten ACLs eingeschränkt.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.live_profile.details*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Der Zweck besteht darin, nur autorisierten Anwendern den Zugriff auf die Details eines Live-Profils (z. B. Unternehmensname, Telefonnummern) zu ermöglichen.
Datentyp	Auswahlliste

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Empfohlener Wert	ACL
Standardwert	ACL
Sicherheitsrisikobewertung	4.3
Funktionale Auswirkung	(Mittel) Wenn die Eigenschaft nicht aktiviert ist, können nicht autorisierte Anwender auf die Live-Profildetails aller anderen Anwender zugreifen.
Sicherheitsrisiko	(Moderat) API-Anforderungen sollten Tabellen-ACLs immer berücksichtigen. Es muss eine Einschränkung angewendet werden, um zu verhindern, dass nicht autorisierte Anwender auf Details eines Live-Profils zugreifen.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

ACLs für Berichtsansicht aktivieren

Verwalten Sie eine Prüfung für report_view-ACLs von veröffentlichten Berichten.

Verwenden Sie die Eigenschaft und *glide.report.report_view.check_published*, um eine Überprüfung der report_view-ACLs für veröffentlichte Berichte zu verwalten. Wenn die Eigenschaft nicht auf den empfohlenen Wert **true**festgelegt ist, wird die Überprüfung von report_view-ACLs auf veröffentlichte Berichte deaktiviert.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.report.report_view.check_published*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregrad-Punktzahl: Hoch • CVSS-Punktzahl: 7,5 • Details zum Sicherheitsrisiko: Wenn die Eigenschaft auf **true**festgelegt ist, wird die Überprüfung von report_view-ACLs auf veröffentlichte Berichte deaktiviert.
Abhängigkeiten und Voraussetzungen	Keine

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

URL-Allow-Liste für ursprungsübergreifende IFrame-Kommunikation aktivieren

Verwenden Sie die Eigenschaft *glide.ui.concourse.onmessage_enforce_same_origin*, um die ursprungsübergreifende Kommunikation zwischen `iframes`zu aktivieren.

`Openframe` kann nur Nachrichten aus vertrauenswürdigen Domänen verarbeiten, die in der Eigenschaft *glide.ui.concourse.onmessage_enforce_same_origin_whitelist* angegeben sind. Weitere Informationen finden Sie unter UTL-Allow-Liste für ursprungsübergreifende IFrame-Kommunikation festlegen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.ui.concourse.onmessage_enforce_same_origin*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Kategorie	Zugriffssteuerung
Zweck	Zum Aktivieren der Aufnahmeliste von vertrauenswürdigen Domänen, damit diese zwischen IFrames für OpenFrame kommunizieren können.
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	4.2
Funktionale Auswirkung	(Mittel) Wenn Sie beabsichtigte Domänen nicht in die Aufnahmeliste aufnehmen, ist die Möglichkeit zum Einbetten anderer Seiten in Now Platform -Instanzen möglicherweise eingeschränkt.
Sicherheitsrisiko	(Hoch) Wenn eine Webseite Ereignishandler enthält, die keine ordnungsgemäße Validierung des Ursprungs durchführen, kann eine Webseite oder ein Skript von einem beliebigen Ursprung mit der Seite kommunizieren. Sie können auch beliebige Funktionen initiieren, die vom Ereignis-Handler ausgeführt werden.
Referenzen	OpenFrame-Übersicht

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Einschränkungen des Anwendungsbereichs erzwingen [Neu in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.record.legacy_cross_scope_access_policy_in_script*, um die Berechtigungen von bereichsbezogenen Apps zu steuern.

Wenn die Eigenschaft *glide.record.legacy_cross_scope_access_policy_in_script* auf „true“ festgelegt ist, können bereichsbezogene Apps APIs aufrufen, die nur für globale Apps verfügbar sein sollten. Diese Eigenschaft umgeht die beabsichtigten Zugriffssteuerungen zum Erstellen und Aktualisieren von Entwicklern für diese bereichsbezogenen Apps.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.record.legacy_cross_scope_access_policy_in_script*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	false
Standardwert	wahr (wenn die Eigenschaft nicht in der Tabelle „sys_properties“ vorhanden ist.)
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 3,5 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf den empfohlenen Wert festgelegt ist, können bereichsbezogene Apps und delegierte Entwickler für diese bereichsbezogenen Apps Datensätze in globalen Tabellen wie Incidents erstellen und aktualisieren.
Abhängigkeiten und Voraussetzungen	Keine

Sicherheitsregeln für die Freigabe von Dashboards erzwingen [Neu in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.cms.dashboards.sharing_with_secure_search*, um zu steuern, ob Benutzer Dashboards freigeben können.

Wenn die Eigenschaft *glide.cms.dashboards.sharing_with_secure_search* nicht auf **true**festgelegt ist, können Benutzer Dashboardgruppen und -rollen freigeben, auf die sie keinen Zugriff haben. Durch Aktivieren dieser Eigenschaft werden Zugriffssteuerungslisten (ACLs) erzwungen, wenn die Tabellen „sys_user“, „sys_user_role“ und „sys_user_group“ während des Dashboard-Freigabeprozesses durchsucht werden. Die übermäßige Freigabe eines Dashboards kann dazu führen, dass Anwender, Gruppen oder Rollen auf Daten zugreifen, für die sie keine Anzeigeberechtigung haben sollten, wodurch möglicherweise vertrauliche Informationen gefährdet werden. Daher wird empfohlen, *glide.cms.dashboards.sharing_with_secure_search* auf „wahr“ zu setzen, damit Dashboards nur für Personen freigegeben werden, die über die entsprechenden Berechtigungen verfügen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.cms.dashboards.sharing_with_secure_search*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 3,5 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf den empfohlenen Wert „true“ festgelegt wird, werden Zugriffssteuerungslisten beim Durchsuchen der Tabellen „sys_user“, „sys_user_role“ und „sys_user_group“ nicht erzwungen. Dies könnte dazu führen, dass Dashboards für nicht autorisierte Benutzer freigegeben werden und vertrauliche Informationen verfügbar gemacht werden.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Zugriffssteuerung
Funktionale Auswirkung	Diese Eigenschaft wendet Sicherheitsregeln auf die Liste der Anwender, Gruppen und Rollen an, die bei der Freigabe von Dashboards sichtbar sind.

Bereichssicherheit für Digitale Dienste für den öffentlichen Bereich erzwingen [Neu in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.enforce_security_scope.sn_gsm*, um zu steuern, wie von der Anwendung „Digitale Dienste für den öffentlichen Bereich“ auf Anwendungsdaten zugegriffen wird.

Mit der Anwendung ServiceNow Digitale Dienste für den öffentlichen Bereich können Sie Anwendungen für den öffentlichen Sektor entwickeln, die digitale Services für Bürger, Unternehmen und Behörden bereitstellen.

Wenn *glide.enforce_security_scope.sn_gsm* auf „false“ festgelegt ist, kann der Zugriff auf die Anwendungsdaten in den globalen Tabellen der App „Digitale Dienste für den öffentlichen Bereich“ basierend auf den Zugriffssteuerungslisten (Access Control Lists, ACLs) dieser globalen Tabellen erfolgen. Wenn diese Eigenschaft auf „true“ festgelegt ist, wird der Zugriff auf Daten in globalen Tabellen nur basierend auf den ACLs ausgewertet, die direkt in der App „Digitale Dienste für den öffentlichen Bereich“ enthalten sind. Das Festlegen dieser Eigenschaft auf „falsch“ kann zur Offenlegung von Informationen durch zu autoritative ACLs führen.

Um dieses Sicherheitsrisiko zu beheben, legen Sie *glide.enforce_security_scope.sn_gsm* auf „wahr“ fest.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.enforce_security_scope.sn_gsm*

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 4.2 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn Sie diese Eigenschaft nicht auf den empfohlenen Wert festlegen, können Informationen durch zu autoritative ACLs offengelegt werden.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Digitale Dienste für den öffentlichen Bereich konfigurieren

Bereichsbezogenen ACL-Zugriff für Playbooks zur Informationsanforderung erzwingen [Neu in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.enforce_security_scope.sn_gsm_info_req*, um den Zugriff auf Playbook-Daten für die Playbook-Funktion zur Informationsanforderung zu steuern.

Die Anwendung Information Request Playbook ermöglicht Endanwendern des öffentlichen Sektors das Übermitteln und Nachverfolgen von Anforderungen für öffentliche Datensätze und bietet Regierungsbeamten einen vordefinierten Prozess für die Bearbeitung und Lösung dieser Anforderungen. Wenn *glide.enforce_security_scope.sn_gsm_info_req* nicht auf „wahr“ festgelegt ist, kann unerwarteter Zugriff auf Playbook-Daten für die Playbooks-Anwendung „Information Request“ gewährt werden. Legen Sie diese Eigenschaft auf „wahr“ fest, um beim Gewähren des Zugriffs nur ACLs aus dem Bereich „sn_gsm_info_req“ zu berücksichtigen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.enforce_security_scope.sn_gsm_info_req*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 4.3 • CVSS-Punktzahl: Mittel

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Details zum Sicherheitsrisiko: Wenn diese Eigenschaft auf „false“ festgelegt ist, werden ACLs aus allen Bereichen berücksichtigt, wenn Zugriff auf Playbook-Daten in der Bereichshaupttabelle gewährt wird. Dadurch würden Playbook-Daten für Informationsanforderungen verfügbar gemacht.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	• Information Request Playbook verwenden • Konfigurieren Sie den Servicekanal „Informationsanforderungen“.

Strikte Erhöhungsberechtigung erzwingen [Neu in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.security.strict_elevate_privilege*, um zu steuern, ob für als privilegiert markierte Rollen manuell erhöht werden müssen, damit dem Benutzer die Fähigkeiten der Rolle gewährt werden.

Legen Sie diese Eigenschaft auf „true“ fest, um eine zusätzliche Sicherheitsvalidierungsebene hinzuzufügen, wenn ein privilegierter Anwender seine Rolle erhöht.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.security.strict_elevate_privilege*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 6,7 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn *glide.security.strict_elevate_privilege* auf „false“ festgelegt ist, werden als privilegiert markierte Rollen bei einer neuen Sitzung eines Administratorbenutzers automatisch erhöht. Sie müssen nicht manuell erhöht werden (mit Ausnahme von security_admin).
Abhängigkeiten und Voraussetzungen	Keine

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Funktionale Auswirkung	Diese Eigenschaft erfordert unbedingt, dass Benutzer mit Administratorrolle bei Bedarf Berechtigungen erhöhen.

AJAXGlideRecord-ACL-Überprüfung erfordern [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.script.secure.ajaxgliderecord*, um eine ACL-Validierung (Access Control Rule) durchzuführen, wenn auf serverseitige Datensätze, z. B. Tabellen, mit GlideAjax-APIs in einem Client-Skript zugegriffen wird.

Von Client-Skripts aus können beliebige Daten vom Server abgefragt werden. Verwenden Sie dazu AJAXGlideRecord (GlideAjax -Client)-API, indem eine Syntax verwendet wird, z. B. ein serverseitiger Glide-Datensatz. Es ist ein leistungsstarkes und nützliches Tool für viele Bereitstellungen.

Wenn Sie Zugriffssteuerungslisten (ACL) auf GlideAjax-API-Aufrufe anwenden, können Sie nur Daten abfragen, auf die der aktuell verbundene Benutzer Zugriff hat. Wenn beispielsweise ein ESS-Benutzer angemeldet ist, der keine Rechte zum Lesen der Tabelle „cmn_location“ hat, schlagen alle Aufrufe der GlideAjax-API für diese Tabelle fehl.

Wenn Now Platform ohne GlideAjax-ACL-Aufrufprüfung ausgeführt wird, kann eine API Informationen zurückgeben, auf die der aktuell angemeldete Benutzer sonst nicht zugreifen könnte.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.script.secure.ajaxgliderecord*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Stellen Sie sicher, dass Sicherheits-ACLs überprüft und validiert werden, auch wenn der Zugriff auf die Datensätze über clientseitige APIs erfolgt.
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	8.1
Funktionale Auswirkung	(Hoch) Diese Korrektur erzwingt die ACL-Beziehung zu serverseitigen Datensätzen, wenn die Anforderungen mithilfe der AJAXGlideRecord-API-Aufrufe gestellt werden. Wenn die ACL-Konfiguration nicht ordnungsgemäß konfiguriert ist, hat dies potenzielle Auswirkungen. Weitere Informationen zu seinen Auswirkungen und zur Identifizierung finden Sie im Artikel Client-seitige GlideRecord-Transaktionen

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	(AJAXGlideRecord) prüfen und überprüfen [KB0550828] in der HI Knowledge Base .
Sicherheitsrisiko	(Hoch) Mithilfe von Client-Skripts können beliebige Daten vom Server über die GlideAjax-API abgefragt werden. Der Zugriff auf serverseitige Ressourcen ist ohne ordnungsgemäße Autorisierung möglich. Die Verwendung der ACL-Validierung hilft der Anwendung, die Anforderung basierend auf der konfigurierten Autorisierung zu validieren.
Workaround	Stellen Sie sicher, dass die richtigen ACLs für Skripteinbindungen, Prozessoren und andere Entitäten erstellt werden, die von einer GlideAjax-API (AJAXGlideRecord) verwendet werden, damit sie mit der richtigen Autorisierung ausgeführt werden kann. Implementieren Sie Methoden wie `canRead ()`, `canWrite()`, `canCreate ()` und `canDelete ()`, um vor dem Zugriff auf Tabellendatensätze mit GlideRecord eine Anwenderautorisierung durchzuführen. Eine andere Methode ist die Verwendung von GlideRecordSecure. Die Klasse wird vom GlideRecord-Server geerbt, der die gleichen Funktionen wie GlideRecord ausführt und außerdem ACLs erzwingt.
Referenzen	ACLs auf AJAXGlideRecord (clientseitiger Glide-Datensatz) anwenden Diese Eigenschaft gehört zu derselben Familie von Eigenschaften, die die Ausführung von Skripts sichern und einschränken, die vom Client stammen: • *glide.script.use.sandbox*: Siehe Sandbox für vom Client generierte Skripts. • *glide.script.allow.ajaxevaluate*: Siehe „AJAXEvaluate aktivieren“

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Erzwingen Sie ACLs auf Feldebene in GlideRecordSandbox

Verwalten Sie ACLs auf Feldebene in GlideRecordSandbox in Ihrer -Instanz.

Verwenden Sie die Eigenschaft] bisund *glide.sandbox.fields.check_acl* , um ACLs auf Feldebene in GlideRecordSandbox zu erzwingen. Ein Beispiel für die Anwendung dieser Eigenschaft ist, wenn ein Benutzer ein Skript bereitstellen kann, wie in *sysparm_query*. Wenn diese Eigenschaft nicht auf den empfohlenen Wert **true**festgelegt ist, können ACL-Einschränkungen umgangen werden, wodurch vertrauliche Daten gefährdet werden können, z. B. *sys_user.user_password*von einem nicht autorisierten Anwender.

⚠ **Warnung:** Der Wert für diese Eigenschaft ist eine Überschreibung ohne DB. Sie kann nicht geändert oder überschrieben werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.sandbox.fields.check_acl*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 7,5 • CVSS-Punktzahl: Hoch • Details zum Sicherheitsrisiko: Wenn Sie diese Eigenschaft auf „ **falsch** “ setzen, können Sie ACL-Einschränkungen umgehen, wodurch vertrauliche Daten verfügbar gemacht werden könnten.
Abhängigkeiten und Voraussetzungen	Keine

Nutzung des Alias für Anmeldeinformationen erzwingen [Neu in Security Center 1.3 und aktualisiert in 1.5]

Erfahren Sie, wie Sie Ihre Anmeldeinformationen vor nicht autorisierter Verwendung schützen, indem Sie die MID-Server-Eigenschaft konfigurieren.

Der MID-Server (Management, Instrumentation und Discovery) ist eine Java-Anwendung, die als Windows-Dienst oder UNIX-Daemon in Ihrem lokalen Netzwerk ausgeführt wird. MID-Server-Eigenschaften werden in der Tabelle [ecc_agent_property] aufgeführt. Sie können in Ihrer Instanz darauf zugreifen, indem Sie zu navigieren **MID-Server** > **Eigenschaften**an. Aliasse für Anmeldeinformationen ermöglichen es einem Administrator, bestimmte Anmeldeinformationen in Discovery-Zeitplänen zu verwenden. Aliasse für Anmeldeinformationen bieten eine präzisere Kontrolle darüber, welche Anmeldeinformationen eine Discovery-Tabelle verwenden darf. Um diese Sicherheitsschwachstelle zu beheben, legen Sie *alias_filtering_behavior* auf „Strikt“ fest, um zu verhindern, dass Anmeldeinformationen mit erhöhten Berechtigungen unnötigerweise verfügbar gemacht werden. Unter MID Server-Eigenschaften finden Sie weitere Details.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*alias_filtering_behavior*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	strict

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Standardwert	los
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 2 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn diese Härtungseinstellung nicht auf „strikt“ festgelegt ist, werden alle Anmeldeinformationen unabhängig von ihren Aliassen für Discovery-Tabellen verwendet, was die Wahrscheinlichkeit eines nicht autorisierten Zugriffs erhöht.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	• MID-Server • Anmeldeinformationsaliasse für Discovery

GroupBy-ACLs erzwingen

Konfigurieren Sie Ihre -Instanz für die Durchführung von ACL-Prüfungen für groupby-Spalten.

Verwenden Sie diese Eigenschaft, um Ihre Instanz für die Durchführung von ACL-Prüfungen für groupby-Spalten zu konfigurieren. Wenn diese Eigenschaft auf den empfohlenen Wert **true**festgelegt ist, wird das Attribut *groupby_acl_check* einer Tabelle so festgelegt, dass groupby-ACLs berücksichtigt werden. Wenn die Eigenschaft auf „ **false**“ festgelegt ist, erfolgt keine ACL-Prüfung für groupby-Spalten in einer Tabelle, was zu Informationsverlusten führen kann.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.security.groupby_acl_check*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 3,7 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn Sie diese Eigenschaft auf „ **falsch** “ setzen, wird die ACL-Prüfung für groupby-Spalten deaktiviert, was zu Informationsverlusten führen kann.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Abhängigkeiten und Voraussetzungen	Keine

Sicherstellen, dass das Erstellen/Löschen von Dashboards eine Zugriffsprüfung erfordert [Neu in Security Center 1.3]

Die Eigenschaft *glide.processors.check_access_before_process* ermöglicht die Erzwingung von Zugriffssteuerungslisten (Access Control List, ACL) zum Erstellen oder Löschen von Dashboards, wenn ein Benutzer angemeldet ist. Diese Eigenschaft muss immer auf „wahr“ festgelegt werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.processors.check_access_before_process*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 6.3 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn Sie diese Eigenschaft deaktivieren, indem Sie sie auf false setzen, wird eine ACL-Umgehung in Dashboards aktiviert. Dies ermöglicht allen authentifizierten Benutzern mit geringen Berechtigungen das Löschen und Hinzufügen von Dashboards.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Diese Eigenschaft steuert die Möglichkeit, neue sys_dashboards zu erstellen und vorhandene Dashboards zu löschen, wenn ein Benutzer nicht über die erforderlichen Zugriffsrechte verfügt. Wenn der Wert auf „false“ festgelegt ist, können Benutzer mit unangemessenen Rollen sys_dashboard-Einträge hinzufügen und löschen (die GlideRecord-Ebene muss jedoch die vorhandenen ACLs erneut überprüfen). Der Wert true schränkt das Hinzufügen und Löschen von Vorgängen für Benutzer ohne die erforderlichen Zugriffsrechte ein.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erzwingen Sie die Validierung des OAuth-Statusparameters

Konfigurieren Sie die Eigenschaft mit demund dem *glide.oauth.state.parameter.required*, um Ihre -Instanz vor CSRF-Angriffen (Cross-Site Request Forgery) zu schützen.

Mit der Eigenschaft *glide.oauth.state.parameter.required*kann der Parameter „State“ in einer OAuth-Anforderung für den Autorisierungscode-Flow erforderlich sein. Der Parameter „State“ ist ein Zeichenfolgenwert, der keine Sonderzeichen enthalten oder leer sein darf. Durch Festlegen dieser Eigenschaft auf „ **true** “ wird sichergestellt, dass ein Angreifer während der Authentifizierung keine CSRF-Angriffe (Cross-Site Request Forgery) ausführen kann. Dadurch wird Ihre Instanz vor Angriffen durch einen Benutzer geschützt, der die Identität eines Benutzers annimmt.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.oauth.state.parameter.required*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 4.2 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Legen Sie diese Eigenschaft auf „ **wahr** “ fest, um sicherzustellen, dass CSRF-Angriffe verhindert werden.
Abhängigkeiten und Voraussetzungen	Keine

Strikten Upload von Anwenderbildern erzwingen

Verwenden Sie die Eigenschaft *glide.security.strict.user_image_upload*, um die Zugriffssteuerung für das Hochladen/Aktualisieren eines Profilbilds zu aktivieren, wenn sie für einen Anwenderdatensatz ausgeführt wird.

Diese Einstellung ermöglicht es einem nicht autorisierten Anwender, ein Bild in das Profil eines anderen Anwenders hochzuladen.

- Wenn Sie diese Eigenschaft auf „ **true**“ festlegen, werden die Tabellen-ACLs beim Hochladen von Fotos erzwungen, sodass nur autorisierte Benutzer ein Bild hochladen können.
- Wenn Sie die Option auf **false**setzen, werden ACLs für Bild-Uploads in das Feld Foto nicht erzwungen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.security.strict.user_image_upload*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Um das Hochladen von Anwenderbildern auf autorisierte Anwender zu beschränken
Empfohlener Wert	wahr
Sicherheitsrisikobewertung	3.7
Funktionale Auswirkung	(Niedrig) Keine Auswirkungen auf die Funktionalität, da autorisierte Anwender weiterhin Bilder in ihr Anwenderprofil hochladen können.
Sicherheitsrisiko	(Niedrig) Wenn Sie diese Eigenschaft auf „ **false**“ festlegen, kann ein authentifizierter Anwender ein Bild ohne Autorisierung in den Account eines anderen Anwenders hochladen.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

E-Mail-Domänen für die Registrierung externer Anwender einschränken [Aktualisiert in Security Center 1.5]

Verwenden Sie die Eigenschaft *sn_ext_usr_reg.allowed_email_domains*, um zulässige externe E-Mail-Domänen aufzulisten.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*sn_ext_usr_reg.allowed_email_domains*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do), Community-Eigenschaften
Kategorie	Zugriffssteuerung
Zweck	Listen Sie E-Mail-Domänen auf, um Anwender-E-Mails für die Registrierung zuzulassen.
Empfohlener Wert	Als nicht leeren Wert festlegen
Konfigurationstyp	Zeichenfolge
Sicherheitsrisiko	(Hoch) Böswillige Akteure könnten die Registrierung mit E-Mail-Adressen aus unerwünschten Domänen durchführen. Stellen Sie sicher, dass *sn_ext_usr_reg.allowed_email_domains* nicht auf einen leeren Wert festgelegt ist.
Sicherheitsrisikobewertung	7.5
Referenzen	Communities

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Plugin für hohe Sicherheit [Aktualisiert in Security Center 1.3]

Wenn Sie das Plugin „Hohe Sicherheit“ aktivieren, erstellt oder aktualisiert es Hunderte verschiedener Konfigurationen, um das Sicherheitsniveau in Ihrer Instanz zu steuern. Diese Konfigurationen entschärfen viele der häufigsten OWASP-Angriffe, indem sie eine strenge Zugriffssteuerung, Eingabevalidierung und Ausgabecodierung ermöglichen.

Diese Konfigurationen umfassen:

- Zugriffssteuerung
- Business-Regeln
- Systemeigenschaften
- UI-Richtlinienaktion
- Skriptaktionen
- Skripteinbindungen

Beispiel

In den Beispielen finden Sie die folgenden Eigenschaften:

Eigenschaft	Thema
glide.ui.escape_all_script	Escape Jelly
glide.security.strict.actions	UI-Aktion vor der Ausführung überprüfen
glide.security.csrf_ previous.allow	Anti-CSRF-Token
glide.security.csrf.strict.validation.mode	Strikte CSRF-Validierung

Weitere Informationen

Attribut	Beschreibung
Plugin-Name	com.glide.high_security
Konfigurationstyp	Systemdefinition > Plugins – Entwicklung
Kategorie	Zugriffssteuerung
Zweck	Dieses Plugin muss aktiviert werden. Sie erhöht die Sicherheitsstufe einer Instanz, wodurch die Angriffsfläche reduziert wird, indem die 10 häufigsten OWASP-Angriffe abgeschwächt werden, einschließlich CSRF, XSS, sichernder Sitzungscookies und Datei-Uploads.
Empfohlener Wert	Aktiv
Sicherheitsrisikobewertung	9.8
Funktionale Auswirkung	(Hoch) Dieses Plugin ermöglicht verschiedene Systemsicherheitskonfigurationen, die sich auch auf die Anwenderoberfläche und die Funktionalität auswirken können.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	(Hoch) Viele Sicherheitskonfigurationen sind unbeabsichtigt offen gelassen, was einige der kritischen Schwachstellen öffnen kann.
Referenzen	Einstellungen für hohe Sicherheit werden aktiviert Strenge Sicherheitseinstellungen

Weitere Informationen zum Aktivieren eines Plugins finden Sie unter Plugins aktivieren

ACLs mit Admin-Aufhebung berücksichtigen

Die Eigenschaft *glide.security.admin.override.accessterm* legt fest, dass Administratoren die ACL-Auswertung nicht überschreiben können, auch wenn die Überschreibung aktiv sein sollte.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.security.admin.override.accessterm*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Steuert, dass Administratoren die ACL-Bewertung nicht überschreiben können.
Datentyp	Boolean
Empfohlener Wert	True
Standardwert	True
Sicherheitsrisiko	(Niedrige) ACLs werden kumulativ ausgewertet. Wenn in einem bestimmten Feld eine Anzahl von ACLs vorhanden ist und die Option Admin-Überschreibungen für eine davon auf „falsch“ (nicht ausgewählt) festgelegt ist, werden die effektiven Administratorüberschreibungen für alle ACLs als „falsch“ betrachtet.
Sicherheitsrisikobewertung	3.8
Referenzen	Regeln für Zugriffssteuerungsliste

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Verhindern, dass sich inaktive Benutzer anmelden [Neu in Security Center 1.5]

Konfigurieren Sie diese Eigenschaft, um zu steuern, ob sich inaktive Anwender bei Ihrer Instanz authentifizieren können.

Legen Sie den Eigenschaftswert *glide.authenticate.only.allow.active.user.login* auf „wahr“ fest (empfohlen). Dadurch wird sichergestellt, dass sich die als inaktiv markierten Anwender in der Tabelle „sys_user“ nicht bei der Instanz anmelden können und gesperrt sind.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die Einstellung auf „false“ konfiguriert ist, können Benutzer weiterhin auf die Instanz und die Daten zugreifen, auf die sie zuvor Zugriff hatten.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.authenticate.only.allow.active.user.login*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 7,5 • CVSS-Punktzahl: Hoch • Details zum Sicherheitsrisiko: Wenn Sie diese Eigenschaft nicht auf den empfohlenen Wert „wahr“ festlegen, könnten inaktive Anwender wie ein gekündigter Mitarbeiter weiterhin auf die Instanz und alle Daten zugreifen.
Abhängigkeiten und Voraussetzungen	Keine

JSONP-Anforderungen auf vertrauenswürdige URLs beschränken [Aktualisiert in Security Center 1.3]

Geben Sie vertrauenswürdige URLs für den AngularJS $http-Service an, um JSONP-Anforderungen zuzulassen oder abzulehnen.

Die Eigenschaft *angular.jsonp.inclusion_list.enabled*gibt vertrauenswürdige URLs für den Service AngularJS $http an, um JSONP-Anforderungen zuzulassen und/oder abzulehnen. Diese Eigenschaft ist erforderlich, da dies einen potenziell grundlegenden Change für Kunden darstellt, sodass sie eine Möglichkeit benötigen, ihre vertrauenswürdigen URLs hinzuzufügen. Wenn diese Eigenschaft nicht auf den empfohlenen Wert „true“ festgelegt ist, sind JSONP-Anforderungen an jede URL zulässig.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*angular.jsonp.inclusion_list.enabled*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Zugriffssteuerung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	• Schweregrad-Punktzahl: Mittel • CVSS-Punktzahl: 5,4 • Details zum Sicherheitsrisiko: Wenn Sie diese Eigenschaft auf „ **falsch** “ setzen, werden JSONP-Anforderungen an jede URL aktiviert.
Abhängigkeiten und Voraussetzungen	Keine

Ausführung von Rohdatenbankabfragen deaktivieren [Aktualisiert in Security Center 1.3]

Steuern Sie, ob ein Anwender SQL-Rohabfragen in der Datenbank ausführen kann.

Mit den Eigenschaftenund *glide.db.allow_unsafe_dbi_execute_sql* können Benutzer SQL-Rohabfragen in der Datenbank ausführen, die Zugriff auf Tabellen und Daten außerhalb von GlideRecord-Einschränkungen gewähren können. Wenn diese Eigenschaft nicht auf den empfohlenen Wert *false*festgelegt ist, ermöglicht dies den Aufruf von *dbi.executeStatement()* von einem Glide-Skript, was zur Ausführung schädlicher SQL-Anweisungen führen kann.

⚠ **Warnung:** Diese Eigenschaft ist sowohl sicher als auch ohne DB-Überschreibung.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.db.allow_unsafe_dbi_execute_sql*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	falsch
Standardwert	falsch
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 7,2 • CVSS-Punktzahl: Hoch • Details zum Sicherheitsrisiko: Wenn Sie diese Eigenschaft nicht auf „ **false** “ setzen, wird der Aufruf von *dbi.executeStatement()* von einem skriptfähigen Glide-Element aktiviert.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Regeln für Zugriffssteuerungsliste

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benutzerkommentare zu Artikeln ausblenden [Neu in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.knowman.show_user_feedback*, um zu steuern, ob Feedback-Kommentare sichtbar sind.

Wenn *glide.knowman.show_user_feedback* nicht auf „nie“ festgelegt ist, sind Feedback-Kommentare zu Knowledge Base-Artikeln (KB) für Anwender mit Rollen in der Glide-Eigenschaft *glide.knowman.show_user_feedback.roles* sichtbar. Da Feedback-Kommentare vertrauliche Informationen enthalten können, soll das Feedback möglicherweise nicht sichtbar sein. Wenn diese Eigenschaft nicht auf „nie“ festgelegt ist, kann dies Auswirkungen auf die Vertraulichkeit haben, wenn vertrauliche Informationen im Feedback offengelegt werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.knowman.show_user_feedback*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Auswahlliste
Empfohlener Wert	nie
Standardwert	onload
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 3,5 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn Sie diese Eigenschaft nicht auf „Nie“ festlegen, können vertrauliche Informationen in Feedback-Kommentaren offengelegt werden.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Zeigt Anwenderkommentare zu KB-Artikeln basierend auf den in der Konfiguration genannten Auswahlmöglichkeiten an.

Standardmäßige Authentifizierung für vom Client aufrufbare Skripteinbindungen anfordern [Aktualisiert in Security Center 1.3]

Standardmäßig sind vom Client aufrufbare Skripteinbindungen, die die Sichtbarkeit nicht explizit festlegen, öffentlich. Fügen Sie bei Bedarf die Eigenschaft *glide.script.ccsi.ispublic* hinzu, um die Datenschutzsteuerung für alle vom Client aufrufbaren Skripteinbindungen zu aktivieren, auf die von öffentlichen Seiten zugegriffen wird.

Wenn Sie diese Eigenschaft hinzufügen, müssen Sie den Wert auf **false** festlegen. Dadurch werden alle vom Client aufrufbaren Skripteinbindungen als privat festgelegt und ihre Sichtbarkeit auf öffentlichen Seiten geändert.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Sie können die Eigenschaft nicht mit dem Wert **true**hinzufügen oder ihren Wert von **false** in **true**ändern. Wenn Sie dies versuchen, wird eine Fehlermeldung angezeigt.

Bei Bedarf können Sie die Datenschutzeinstellung für eine einzelne vom Client aufrufbare Skripteinbindung ändern, indem Sie die Funktion `isPublic()` hinzufügen.

- Die Einstellung „`isPublic()`" hat Vorrang vor der Eigenschaft *`glide.script.ccsi.ispublic`*.
- Wenn Sie beispielsweise `isPublic()` in einem einzelnen Skript auf „ **true** " festlegen, wird es öffentlich gemacht. Dadurch wird die Eigenschaft *`glide.script.ccsi.ispublic`* überschrieben, die alle anderen vom Client aufrufbaren Skripteinbindungen privat macht.

Warnung: Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*`glide.script.ccsi.ispublic`*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Das Festlegen von vom Client aufrufbaren Skripteinbindungen als privat bedeutet, dass Gäste, die auf öffentliche Seiten zugreifen, nicht auf die vom Client aufrufbare Skripteinbindung zugreifen können. Ein nicht angemeldeter Anwender kann kein privates Skript ausführen.
Empfohlener Wert	falsch
Standardwert	falsch
Sicherheitsrisikobewertung	7.5
Funktionale Auswirkung	(Hoch) Wenn die vom Client aufrufbaren Skripteinbindungen als öffentlich gekennzeichnet sind (d. h. diese Eigenschaft fehlt), können nicht authentifizierte Benutzer Client-Skripts ausführen. Fügen Sie die Eigenschaft hinzu, die die Ausführung von Skripts durch einen nicht angemeldeten Benutzer einschränkt.
Sicherheitsrisiko	(Hoch) Wenn Sie diese Eigenschaft nicht hinzufügen, werden clientseitige Skripteinbindungen umgangen, was zu unbeabsichtigten öffentlichen Funktionen führen kann. Wenn das Client-Skript vertrauliche Informationen bereitstellt, kann dies ein nachteiliges potenzielles Sicherheitsrisiko darstellen.
Workaround	Wenn Sie die Eigenschaft *`glide.script.ccsi.ispublic`* auf „ **false** " setzen, werden alle vom Client aufrufbaren Skripteinbindungen privat.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Sie können die Datenschutzeinstellung für eine einzelne vom Client aufrufbare Skripteinbindung ändern, indem Sie die Funktion `isPublic()` hinzufügen. Die Funktion `isPublic` hat Vorrang vor der Eigenschaft *`glide.script.ccsi.ispublic`*. Fügen Sie der Skripteinbindung die folgende Syntax hinzu: `isPublic:function(){return[wahr/falsch];},`

Verhalten von Produktionsinstanz erzwingen [Aktualisiert in Security Center 1.3 und 1.5]

Konfigurieren Sie, ob Ihre Instanz wie eine Produktionsinstanz oder eine Nicht-Produktionsinstanz behandelt werden soll.

Wenn die Eigenschaft *`glide.installation.production`* nicht auf den empfohlenen Wert **true**festgelegt ist, wird die Instanz nicht als Produktionsinstanz behandelt. Daher können zboot und andere potenziell gefährliche Skripts ausgeführt werden. Wenn eine Produktionsinstanz als Instanz außerhalb der Produktion ausgewertet wird, kann dies zu Informationsverlusten oder Denial of Service-Angriffen (DoS) führen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*`glide.installation.production`*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 6.3 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn Sie diesen Eigenschaftswert auf „ **false** “ setzen, wird die Instanz als Instanz außerhalb der Produktion behandelt, wodurch zboot und andere potenziell gefährliche Skripts ausgeführt werden können.
Abhängigkeiten und Voraussetzungen	Keine

Beschränken Sie den Zugriff auf das Hintergrundskript

Konfigurieren Sie die Eigenschaft und *`glide.script_processor.admin`*, um die Rolle festzulegen, die für den Zugriff auf das Modul Skripthintergrund erforderlich ist.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Eigenschaft *glide.script_processor.admin* enthält die erforderliche Rolle für den Zugriff auf das Modul „Skripthintergrund“. Wenn diese Eigenschaft nicht auf den empfohlenen Wert **admin**festgelegt ist, kann jeder Benutzer, unabhängig von seiner Rolle, Hintergrundskripts für die Instanz ausführen. Dadurch können böswillige Akteure das ACL-System umgehen und erhalten vollen Zugriff auf Tabellen.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.script_processor.admin*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	Administrator
Standardwert	Administrator
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 8,8 • CVSS-Punktzahl: Hoch • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf den empfohlenen Wert **„admin** “ festgelegt wird, kann jeder Benutzer Hintergrundskripts in der Instanz ausführen.
Abhängigkeiten und Voraussetzungen	Keine

Beschränken Sie den Zugriff auf E-Mails mit leerer Zieltabelle

Aktivieren Sie die Eigenschaft *glide.email.email_with_no_target_visible_to_all*, um den Zugriff von Anwendern auf E-Mails einzuschränken, mit Ausnahme des jeweiligen Absenders oder Administratoren.

Nicht autorisierte Anwender können auf E-Mails in der Tabelle „sys_email_list“ zugreifen, für die ein Zieldatensatz fehlt. Anstatt ACLs für E-Mail-Einträge zu erzwingen, beschränkt diese Eigenschaft den Zugriff nur auf den E-Mail-Absender und Benutzer mit der Administratorrolle.

ℹ **Hinweis:** E-Mails, die an die Instanz gesendet und von ihr empfangen werden, werden in der Tabelle „sys_email_list“ angezeigt. Allerdings sollten nur empfangene E-Mails, die mit dem Status „Fehler“ und „Ignoriert“ markiert wurden, eine leere Zieltabelle haben.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.email.email_with_no_target_visible_to_all*

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren	Zugriffssteuerung
Zweck	Um zu blockieren, dass der E-Mail-Client E-Mails anzeigt, wenn der Anwender den Zugriff nicht autorisiert.
Empfohlener Wert	falsch
Standardwert	wahr
Sicherheitsrisikobewertung	5.4
Funktionale Auswirkung	(Niedrig) Anwender können keine E-Mails mehr anzeigen, bei denen die Zieltabelle leer ist, es sei denn, sie sind Administratoren oder waren der Absender der E-Mail.
Sicherheitsrisiko	(Mittel) Wenn die Eigenschaft nicht aktiviert ist, können nicht autorisierte Anwender auf alle E-Mails zugreifen, bei denen das Feld „target_table“ leer ist.
Referenzen	Erweiterte E-Mail-Eigenschaften https://support.servicenow.com/kb_view.do?sysparm_article=KB0690043

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Beschränken Sie den Zugriff auf das Plugin für bestimmte IP-Bereiche

Verwenden Sie das Plugin *com.snc.ipauthenticator*, [], um den Zugriff auf bestimmte IP-Bereiche zu beschränken. Sofern kein öffentlicher Zugriff für die Instanz vorgesehen ist, sollten Administratoren den Zugriff auf die ihnen zugewiesenen IP-Netzblöcke beschränken.

Voraussetzungen

Bevor Sie diese Eigenschaft festlegen, müssen Sie das Plugin „Auf dem IP-Adressbereich basierende Authentifizierung “ (com.snc.ipauthenticator) *com.snc.ipauthenticator* aktivieren. Weitere Informationen finden Sie unter Authentifizierung mit IP-Adressbereich und im Abschnitt „Schritte zum Konfigurieren“ (unten).

Weitere Informationen

Attribut	Beschreibung
Plugin-Name	*com.snc.ipauthenticator*
Konfigurationstyp	System Security > IP-Adressen-Zugriffssteuerung
Kategorie	Zugriffssteuerung
Zweck	Um den Bereich der IP-Adressen, die auf die Instanz zugreifen können oder nicht, zur Liste der vertrauenswürdigen und nicht vertrauenswürdigen Domänen hinzuzufügen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Empfohlener Wert	Aktiv
Standardwert	Keine. Dies ist ein Plugin, keine Glide-Eigenschaft. Daher gibt es keinen Standardwert.
Sicherheitsrisikobewertung	5.3
Funktionale Auswirkung	(Niedrig) Für dieses Korrekturelement werden vom Kunden verweigerte IP-Bereiche verwendet. Keine Auswirkung, da der Kunde die Zielliste definiert.
Sicherheitsrisiko	(Niedrig) Die unnötige Offenlegung der Zielinstanz im Internet sollte mithilfe der IP-Zugriffssteuerungsfunktion eingeschränkt werden.
Referenzen	Authentifizierung mit IP-Adressbereich

Schritte zum Konfigurieren von

1. Stellen Sie sicher, dass das Plugin „com.snc.ipauthenticator“ aktiv ist.
2. Navigieren zu **Systemsicherheit** > **IP-Adressen-Zugriffssteuerung**an.
3. Klicken Sie auf **Neu**, um eine Ausschlussliste (Deny) oder eine Aufnahmeliste (Allow) von IP-Adressen zu erstellen.
4. Klicken Sie auf **Absenden**.

Zugriff auf Knowledge Bases beschränken [Neu in Security Center 1.3]

Die Eigenschaft *glide.knowman.block_access_with_no_user_criteria* wird verwendet, um den Lese-/Schreibzugriff von Anwendern auf wissensbasierte Artikel zu steuern.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.knowman.block_access_with_no_user_criteria*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Bewertung mit Schweregrad: 9.1 • CVSS-Punktzahl: Kritisch • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf den empfohlenen Wert true festgelegt ist, kann jeder Anwender eine KB lesen und dazu beitragen.
Abhängigkeiten und Voraussetzungen	Keine

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Funktionale Auswirkung	Verweigert den Zugriff auf eine Knowledge Base, wenn „Kann lesen“ oder „Kann mitwirken“ nicht angegeben ist.

Beschränken Sie die Berechtigungen für das CMDB-Modell

Verwenden Sie die Systemeigenschaft *csm_cmdb_model.customer_visible_flag*, um den Zugriff des Kunden auf Daten in der Tabelle „Produktmodelle“ als zusätzliche Zugriffssteuerung auf das CMDB-Modell zu beschränken.

Legen Sie die Eigenschaft *csm_cmdb_model.customer_visible_flag* auf „ **wahr** “ fest, um das Feld „Sichtbar für Kunden“ für die unten aufgeführten Tabellen zu aktivieren:

- Tabelle „Produktmodelle“ [cmdb_model]
- Tabelle „Softwaremodelle “ [cmdb_software_product_model]
- Tabelle „Anwendungsmodelle “ [cmdb_application_product_model]
- Tabelle „Verbrauchsgütermodelle “ [cmdb_consumable_product_model]
- Tabelle „Anlagenmodelle“ [cmdb_facility_product_model]
- Tabelle „Hardwaremodelle “ [cmdb_hardware_product_model]

Wenn Sie diese Eigenschaft auf „ **true** “ festlegen, werden standardmäßig alle cmdb_model-Werte ausgeblendet.

Legen Sie die Eigenschaft auf „ **falsch** “ fest, um die Spalte/das Attribut „customer_visible“ in der Tabelle „cmdb_model “ nicht zu berücksichtigen und sich auf die cmdb_model-Basis-ACLs zu verlassen, auf die „sn_esm_user“ zugreifen kann.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*csm_cmdb_model.customer_visible_flag*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Wenn dies auf **true true**festgelegt ist, verwendet das System die Einstellung im Feld Sichtbar für Kunden, um den Zugriff auf Produktmodelldaten im Kundenserviceportal zu bestimmen.
Empfohlener Wert	wahr
Standardwert	falsch
Datentyp	Boolean
Sicherheitsrisiko	(Mittel) Jeder Benutzer mit der Rolle „sn_esm_user“ und sofort einsatzbereiten ACLs kann über Berechtigungen für das CMDB-Modell verfügen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Hinweis: Diese Rolle wird in der Regel externen Anwendern zugewiesen. Externen Anwendern könnten widerwillig Berechtigungen für das CMDB-Modell erteilt werden.
Referenzen	Zugriff auf Produktmodelldaten im Customer Service Portal beschränken

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Beschränken Sie den nicht authentifizierten Zugriff auf Anhänge

Verwenden Sie die Eigenschaft *glide.image_provider.security_enabled*, um die Sicherheitseinstellungen für Bilder zu steuern. Bei Festlegung auf **wahr**sind Bilder nur für authentifizierte und autorisierte Benutzer sichtbar. Bei Festlegung auf **false**sind die Bilder für alle sichtbar, die eine URL zum Anhang haben.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.image_provider.security_enabled*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Um den nicht authentifizierten Zugriff auf den Anhang zu verhindern, wenn er im *iix* -Format gerendert wird.
Empfohlener Wert	wahr
Standardwert	wahr
Funktionale Auswirkung	(Niedrig) Keine signifikanten Auswirkungen auf die Funktionalität. Die Anwender-Experience kann etwas beeinträchtigt werden, da der Anwender, der zuvor direkt auf die .iix-Datei zugegriffen hat, sich authentifizieren muss.
Sicherheitsrisiko	(Hoch) Für nicht authentifizierte Anwender muss Einschränkung angewendet werden, da Anhänge möglicherweise vertrauliche Informationen enthalten.
Referenzen	Anhänge werden verwaltet Verfügbare Systemeigenschaften

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugriff auf anwenderdefinierte Journaleinträge beschränken [In Security Center 1.3 aktualisiert]

Verwenden Sie die Eigenschaft *glide.live_feed.custom_journal.acl_check_enabled*, um ACLs in anwenderdefinierten Journalfeldern zu berücksichtigen.

Wenn *glide.live_feed.custom_journal.acl_check_enabled* nicht auf den empfohlenen Wert „true“ festgelegt ist, können alle Benutzer alle Journaleinträge innerhalb der Live-Feed-Funktion sehen. Wenn Sie die Eigenschaft auf „wahr“ setzen, werden ACLs in anwenderdefinierten Journalfeldern berücksichtigt. Dies ist eine vorteilhafte Funktion.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.live_feed.custom_journal.acl_check_enabled*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Um zu steuern, welche Benutzer welche Journaleinträge basierend auf ACLs sehen.
Empfohlener Wert	wahr
Standardwert	wahr
Konfigurationstyp	Boolescher Wert.
Sicherheitsrisiko	(Mittel) Wenn dies auf „wahr“ festgelegt ist, werden nur die anwenderdefinierten Journaleinträge, die ACL übergeben, im Live-Feed angezeigt, andernfalls können alle Anwender alle Journaleinträge sehen.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Lesezugriff auf Flow-Kontext einschränken [Neu in Security Center 1.5]

Verwenden Sie die Eigenschaft *com.snc.process_flow.reporting.require_flow_access*, um zu erzwingen, ob eine zusätzliche Zugriffsprüfung erforderlich ist, damit ein Benutzer eine Flow-Prüfung lesen kann.

Wenn die Eigenschaft *com.snc.process_flow.reporting.require_flow_access* auf den empfohlenen Wert true festgelegt ist, erfolgt eine zusätzliche Zugriffsprüfung für einen Benutzer, der versucht, einen Flow-Kontext zu lesen. Wenn diese Eigenschaft auf „falsch“ festgelegt ist, können geringfügige Informationen offengelegt werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*com.snc.process_flow.reporting.require_flow_access*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Standardwert	wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 2,7 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn Sie diese Eigenschaft auf „falsch“ setzen, wird das vorhandene Verhalten beibehalten. Durch das Festlegen dieser Eigenschaft auf „wahr“ wird die hinzugefügte Sicherheitsebene des Lesezugriffs erzwungen.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Wenn diese Eigenschaft aktiviert ist, wird die Sicherheit beim Lesen von Flow-Kontextdatensätzen erhöht. Die Instanz erzwingt, dass ein Benutzer, der versucht, den Flow-Kontext zu lesen, auch Lesezugriff auf den übergeordneten Flow hat.

Sicherheits-Jump-Start-Plugin aktivieren (ACL-Regeln) [Aktualisiert in Security Center 1.3]

Aktivieren Sie das Plugin „Security Jump Start (ACL Rules)“ (com.snc.system_security *com.snc.system_security*), um mehrere wichtige ACLs zu erstellen, die die Zugriffssteuerungen für einige der wichtigsten Systemtabellen in [Now Platformvalidieren.

Diese Regeln bieten eine Starthilfe für die Sicherung vieler Systemtabellen und erleichtern es einer Organisation, eine Instanz in die Produktion zu bringen. Das Plugin „Security Jump Start (ACL Rules)“ wird automatisch auf allen neuen Instanzen installiert.

Weitere Informationen

Attribut	Beschreibung
Plugin-ID	*com.snc.system_security*
Konfigurationstyp	Systemdefinition > Plugins
Kategorie	Zugriffssteuerung
Zweck	Aktivieren Sie das Plugin „Security Jump Start (ACL Rules)“, um eine ordnungsgemäße Sicherheits-Compliance zu erreichen. Sie stellt einige grundlegende ACLs bereit, die Systemtabellen von Anfang an sichern, anstatt sie manuell für jede Systemtabelle zu erstellen, die mit der Standardbereitstellung einer Instanz einhergeht. Diese ACLs sind hilfreich, wenn die neu erstellte Instanz schnell in die Produktion wechseln muss.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Empfohlener Wert	Aktiv
Standardwert	Keine. Dies ist ein Plugin, keine Glide-Eigenschaft, daher gibt es keinen Standardwert. Das Plugin wird standardmäßig auf zBoot installiert (Zurücksetzungen).
Sicherheitsrisikobewertung	8.1
Funktionale Auswirkung	(Mittel) Es gibt erhebliche funktionale Auswirkungen, wenn dieses Plugin ohne Audit der vorhandenen ACLs in der Instanz installiert wird. Bevor die Korrektur durchgeführt werden kann, sind eine Kontaktaufnahme mit dem Kunden und Definitionen erforderlich.
Sicherheitsrisiko	(Hoch) Die Zugriffssteuerung sollte erzwungen werden, um den unbeabsichtigten Zugriff auf die Instanz zu sperren. ACL-Jumpstart-Regeln wurden erstellt, um einen Ausgangspunkt für das Sichern vieler Systemtabellen zu bieten, damit eine Organisation schnell in die Produktion gehen kann.
Referenzen	Sicherheitshilfe – ACL-Regeln

Schritte zum Konfigurieren von

Wenn dieses Plugin in Ihrer -Instanz nicht aktiviert ist, wenden Sie sich an den ServiceNow Support. Durch die Aktivierung des Plugins an dieser Stelle kann sich der Sicherheitszugriff auf Tabellen ändern, die bereits in einer Produktionsumgebung verwendet werden. Wenn ein Administrator an den neuen ACL-Regeln interessiert ist, die das Plugin bereitstellt, können Sie eine oder mehrere davon bei Bedarf manuell in einer vorhandenen Instanz erstellen. Diese Liste von ACLs kann in diesem Fall als Leitfaden verwendet werden.

Verwendung des Vorgangs zum mehrfachen sicheren Einfügen in der Importsatz-API [Neu in Security Center 1.3]

Verwenden Sie die Eigenschaft *com.glide.import_set_api.insert_multiple_optimize*, um zu steuern, ob *GlideRecordSecure* oder *GlideRecord* für den Vorgang Mehrere einfügen in der Importsatz-API verwendet wird.

Wenn *com.glide.import_set_api.insert_multiple_optimize* auf den empfohlenen Wert „false“ festgelegt ist, wird *GlideRecordSecure* zum Einfügen von Datensätzen verwendet, und Zugriffssteuerungslisten (ACLs) auf Tabellenebene werden ausgewertet. Wenn diese Eigenschaft auf „wahr“ festgelegt ist, wird *GlideRecord* zum Einfügen von Datensätzen verwendet, und ACLs auf Tabellenebene werden nicht ausgewertet. Darüber hinaus müssen Sie sicherstellen, dass die Importsatz-API zum Einfügen mehrerer REST-Endpunkte-ACL (sys_id: 3101b770ff2211105cf343d0653bf182) aktiv ist und dass Benutzer über die Rolle import_transformer verfügen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*com.glide.import_set_api.insert_multiple_optimize*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Empfohlener Wert	falsch
Standardwert	falsch
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 6,5 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf „false“ festgelegt ist, kann ein Benutzer mit geringen Berechtigungen Daten in Tabellen außerhalb des Bereichs seiner privilegierten Rollen einfügen.
Umkehrbares Verhalten	Sowohl sichere Überschreibung als auch Überschreibung ohne DB.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Diese Eigenschaft optimiert die Leistung der Importsatz-API, indem sie GlideRecord zum Speichern von Daten verwendet. Wenn der Parameter festgelegt ist, muss ein Integrationsbenutzer über die Rolle import_transformer verfügen, um auf die API zugreifen zu können.
Referenzen	https://developer.servicenow.com/blog.do?p=/post/gliderecord-vs-gliderecordsecure

Strikte Sicherheit für SOAP-Anforderungen erzwingen [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.soap.strict_security*, um die Sicherheit von Webdiensten zu erzwingen.

Diese Eigenschaft verwendet eine Kombination aus:

- Abfrage/Rückmeldung der Standardauthentifizierung über das HTTP-Protokoll und
- Zugriffssteuerungen auf Systemebene in Kontextsicherheit: Plugin für Rollenmanagement.

Wenn Sie diese Eigenschaft auf **true**festlegen, werden die folgenden Aktionen ausgeführt:

- Wenn der Benutzer über die entsprechende Rolle zum Ausführen des Vorgangs verfügt, prüft er die eingehende SOAP-Anforderung auf Rollenberechtigung, um sie zu validieren. Es tritt während SOAP-Webservice-Aufrufen/-Anforderungen auf, die an Now Platform -Tabellen gestellt werden, wenn CREATE-, READ-, UPDATE- oder DELETE-Vorgänge ausgeführt werden.
- Überprüft die ACLs auf Systemebene, während Daten in Form von SOAP-Daten in der Tabelle abgerufen werden.
- Überprüft die ACLs auf Feldebene für CRUD-Vorgänge, die für ein Feld der Tabelle ausgeführt werden.

ACL-Prüfungen werden nur für standardmäßige Tabellen-API-Aufrufe und nicht für Webservices durchgeführt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.soap.strict_security*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Standardwert	wahr
Empfohlener Wert	wahr
Funktionale Auswirkung	(Hoch) Diese Korrektur erzwingt die Zugriffssteuerung auf Systemebene beim Abrufen von Daten aus Tabellen/Seiten in Form von SOAP-Daten in der Instanz. Wenn derzeit Anwender auf diese Daten zugreifen, ist der Zugriff auf die Daten gemäß den ACL-Regeln eingeschränkt/erlaubt. Informationen zu den Standardrollen mit Zugriffsrechten auf SOAP-Daten finden Sie unter SOAP Web Service .
Sicherheitsrisiko	(Moderat) Wenn keine entsprechende Autorisierung für die eingehenden SOAP-Anforderungen konfiguriert ist, kann ein nicht autorisierter Anwender Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.
Referenzen	Strikte Sicherheit für eingehende SOAP durchsetzen SOAP Web Service

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Erforderliche JMS-Verbindungsfactorys [Neu in Security Center 1.3 und aktualisiert in 1.5]

Die Eigenschaft *mid.property.jms.command.allowed_factory_names* steuert die Verbindungsfactorys des Java Messaging Service (JMS), die der MID Server verwenden kann.

Es ist für einige ausgewählte Factorys vorgesehen, die von Plugins für JMS-Aktivitäten oder -Aktionen benötigt werden. Das Einbeziehen zusätzlicher Hersteller könnte ein Schritt in einer Angriffskette für Schwachstellen wie die JDNI-Einfügung sein, die auf Fähigkeiten beruhen, die ein Angreifer in zulässigen Herstellern nutzen kann. Um die Möglichkeit einer ausgenutzten Schwachstelle zu verhindern, fügen Sie keine Factory-Modelle hinzu, die über die erforderlichen Standardwerte hinausgehen.

Um dieses Sicherheitsrisiko zu beheben, überprüfen Sie die Liste der Namen, die für die MID-Eigenschaft *mid.property.jms.command.allowed_factory_names*angegeben wurden. Stellen Sie sicher, dass zusätzliche Java-Factory-Namen erforderlich sind, die über den Standardwert von connectionFactory, queueConnectionFactory und topicConnectionFactory hinausgehen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*mid.property.jms.command.allowed_factory_names*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Standardwert	*connectionFactory*, *queueConnectionFactory*, *topicConnectionFactory*
Empfohlener Wert	*connectionFactory*, *queueConnectionFactory*, *topicConnectionFactory*
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 4.1 • CVSS-Punktzahl: Mittel • Details zu Sicherheitsrisiken: Wenn das Plugin „MID-Server“ (*com.glideapp.agent*) aktiv ist, überprüfen Sie die Liste der Namen, die für die MID-Eigenschaft *mid.property.jms.command.allowed_factory_names* angegeben wurden. Stellen Sie sicher, dass zusätzliche Factory-Namen erforderlich sind, die über den Standardwert von connectionFactory, queueConnectionFactory und topicConnectionFactory hinausgehen.
Abhängigkeiten und Voraussetzungen	Keine

Zugriffssteuerungsbedingungen für explizite externe Rollen überprüfen [In Security Center 1.5 entfernt]

Es wird empfohlen, das Plugin Explicit Roles zu verwenden, um zu bestimmen, dass alle Benutzer entweder über die Rolle „snc_internal“ für den Zugriff auf interne Ressourcen oder die Rolle „snc_external“ für den Zugriff auf externe Ressourcen verfügen.

Nach der Installation dieses Plugins wird allen vorhandenen Benutzern die Rolle „snc_internal“ zugewiesen, und die vorhandenen Zugriffssteuerungslisten (ACLs) werden mit den Rollenbedingungen gefüllt. Aufgrund der Automatisierungslogik oder des Eingreifens eines Instanzadministrators werden die Rollen „snc_internal“ oder „snc_external“ möglicherweise fälschlicherweise einer ACL hinzugefügt, die bereits eine strengere Rollenanforderung enthält. Da die Auswertung der ACL-Rolle für jeden Anwender mit einer Rolle erfolgt, die einer ACL zugeordnet ist, ist das Hinzufügen von „snc_internal“ oder „snc_external“ möglicherweise zu weit gefasst für den beabsichtigten Zweck einer ACL. Dies kann zu Datenverlust führen, wenn einem Benutzer mit geringen Berechtigungen Zugriff über die ACL gewährt wird.

Beispielsweise wäre es unnötig, dass die Rollen „snc_internal“ und „admin“ derselben ACL innerhalb einer Tabelle zugeordnet werden. Die ACL soll Administratoren Zugriff gewähren. In diesem Fall ist die Rolle „snc_internal“ ein Fehler. Oder die ACL soll allen snc_internal-Benutzern Zugriff gewähren, wodurch die Administratorrolle unnötig wird. Wenn das Plugin „Explicit Roles“ installiert ist, überprüfen Sie die ACLs, die eine Rollenbedingung für „snc_internal“ oder „snc_external“ und gleichzeitig eine Bedingung für eine andere Rolle

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

enthalten. Wenn die Rollen für einen bestimmten Anwendungsfall geeignet sind, sollte das Ergebnis regelmäßig überprüft werden.

Wichtig: In der nächsten ISM-Härtungsbaseline (Version 1.6) wird diese Prüfung durch eine Prüfung mit der Bezeichnung „Prüfungssuite für ACL-Konfiguration für explizite Rollen“ ersetzt. Derzeit führt die Prüfung möglicherweise zu vielen Ergebnissen, um sie überprüfen zu können.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*com.glide.explicit_roles*, *sys_security_acl* und *sys_security_acl_role*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Kein Datentyp
Empfohlener Wert	Kein empfohlener Wert
Standardwert	Kein Standardwert
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 4.2 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Aufgrund der Automatisierung oder des Eingreifens eines Instanzadministrators können die Rollen snc_internal oder snc_external einer ACL hinzugefügt werden, die bereits eine strengere Rollenanforderung enthält. Da die Auswertung der ACL-Rolle für jeden Anwender erfolgt, der eine Rolle enthält, die einer ACL zugeordnet ist, ist das Hinzufügen einer der beiden Rollen für den Zweck einer ACL zu weit gefasst und kann zu Datenverlust führen, wenn einem Anwender mit geringen Berechtigungen Zugriff über die ACL gewährt wird.
Referenzen	Explizite Rollen

Gastanwender für SOAP-Anforderungen festlegen [Aktualisiert in Security Center 1.3]

Konfigurieren Sie diese Eigenschaft, um die Zugriffsebene nicht authentifizierter SOAP-Anforderungen zu steuern.

Diese Eigenschaft steuert die Zugriffsebene nicht authentifizierter SOAP-Anforderungen. Wenn er nicht auf den empfohlenen Wert *soap.guest*oder auf einen Benutzer mit eingeschränkten Berechtigungen festgelegt ist, werden SOAP-Anforderungen im Namen des Benutzers ausgeführt. Wenn diese Eigenschaft leer ist, ermöglicht sie nicht authentifizierten Zugriff auf Vorgänge auf Administrator- oder Wartungsebene, wodurch alle Sicherheitskontrollen innerhalb der Instanz aufgehoben werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*com.glide.soap.guest_user*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	SOAP.Gast
Standardwert	SOAP.Gast
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Bewertung mit Schweregrad: 8,1 • CVSS-Punktzahl: Hoch • Details zum Sicherheitsrisiko: Wenn Sie diese Eigenschaft auf leer setzen, wird ein nicht authentifizierter Zugriff auf Vorgänge auf Administrator- oder Wartungsebene ermöglicht.
Abhängigkeiten und Voraussetzungen	Keine

SNC-Zugriffssteuerungs-Plugin aktivieren [In Security Center 1.3 aktualisiert]

Aktivieren Sie das Plugin „SNC Access Control“ (com.snc.snc_access_control*com.snc.snc_access_control*), um den Zugriff auf Ihre Instanzen durch Mitarbeiter von Kundenservice und Support zu steuern.

Die Standardkonfiguration für Now Platform ermöglicht Kundenservice und Support den Zugriff auf Instanzen über einen internen Prozess, der Anmeldeinformationen für den kurzfristigen Support erstellt. Obwohl jeder Zugriff geprüft wird, ziehen es einige Kunden vor, diesen Zugriff zu kontrollieren.

Mit diesem Plugin können Kundenservice und Support den Zugriff von Kundenservice und Support -Mitarbeitern auf die Instanz sperren. Diese Entscheidung wirkt sich auf Support-SLAs aus, da Sie den Zugriff Now Platform aktivieren müssen, bevor Support-Aktivitäten beginnen können. Weitere Informationen finden Sie unter ServiceNow-Zugriffssteuerung.

Weitere Informationen

Attribut	Beschreibung
Plugin-Name	*com.snc.snc_access_control*
Konfigurationstyp	Systemdefinition > Plugins
Kategorie	Zugriffssteuerung
Zweck	Verbietet Mitarbeitern Kundenservice und Support den Zugriff auf die Instanz
Empfohlener Wert	Aktiv

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Standardwert	Keine. Dies ist ein Plugin, keine Glide-Eigenschaft, daher gibt es keinen Standardwert. Das Plugin wird standardmäßig nicht installiert.
Erforderliche Rolle	Der Kundenadministrator kann dieses Plugin nicht aktivieren. Es muss explizit angefordert werden, da es erweiterte Berechtigungen zum Aktivieren des Plugins erfordert.
Sicherheitsrisikobewertung	8.2
Funktionale Auswirkung	(Niedrig) Wenn dieses Plugin inaktiv ist, können alle Kundenservice und Support -Mitarbeiter auf die Instanz des Kunden zugreifen. Durch Aktivieren des Plugins kann der Kunde den Zugriff auf autorisierte Mitarbeiter von Kundenservice und Support beschränken.
Sicherheitsrisiko	(Hoch) Unnötige Offenlegung des Instanzzugriffs für eine größere Gruppe von Personen.
Referenzen	ServiceNow-Zugriffssteuerung

Schritte zum Konfigurieren von

1. Um das Plugin anzufordern, führen Sie die Schritte in Die Zugriffssteuerung ServiceNow wird aktiviertaus. Kunden müssen das Plugin „SNC Access Control“ (com.snc.snc_access_control) von HI anfordern.
2. Führen Sie zum Aktivieren der SNC-Zugriffssteuerung die Schritte in Die Zugriffssteuerung für ServiceNow wird konfiguriertaus. Konfigurieren Sie einen Zugriffssteuerungsdatensatz, um einen oder mehrere Kundenservice und Support Mitarbeiter anzugeben, die berechtigt sind, sich bei Ihrer -Instanz anzumelden.

API und Webservice

Die API- und Webservice-Kategorie stellt sicher, dass Anwendungen über ein angemessenes Management von Authentifizierung, Autorisierung und Sitzungen verfügen, alle Eingaben validieren, die eine Vertrauensgrenze überschreiten, und Sicherheitskontrollen für alle API-Typen enthalten.

Spezifische Steuerungen in dieser Kategorie beziehen sich auf die Eingabevalidierung nach Servicetyp, z. B. XDS-Schemavalidierung für SOAP Web Services oder Denial of Service-Schutz für graphQL-APIs.

SOAP-Inhaltstyp validieren [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.soap.require_content_type_xml*, um die Validierung eines Inhaltstyps als Text/XML zu aktivieren und vor ungültigen SOAP-Anforderungen zu schützen.

- Bei Festlegung auf **true**validiert Now Platform den Inhaltstyp als Text/XML und schützt vor ungültigen SOAP-Anforderungen.
- Bei Festlegung auf „ **false**“ ist jeder Inhaltstypwert zulässig.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnung: Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.soap.require_content_type_xml*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	Vor ungültigen SOAP-Anforderungen schützen
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	8.8
Funktionale Auswirkung	(Niedrig) Diese Korrektur ermöglicht die Validierung des SOAP-Inhaltstyps für alle eingehenden SOAP-Anforderungen. • Wenn Sie für eingehende Anforderungen einen anderen Inhaltstyp als Text/XML verwenden, kann dies zu einem potenziellen Fehler bei SOAP-Transaktionen führen. • Wenn Sie nicht den richtigen MIME-Typ verwenden, kann dies zu Störungen bei Integrationen von Drittanbietern führen.
Sicherheitsrisiko	(Mittel) Bei der Annahme eingehender SOAP-Anforderungen wird eine entsprechende Validierung durchgeführt, um sicherzustellen, dass der relevante Inhaltstyp als Teil der Anforderung definiert wird. Sie schränkt die ungültigen SOAP-Antworten ein, die als Sicherheitsrisiko angesehen werden können.
Referenz	Inhaltstypen

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Autorisierung für PDF-Anforderungen erfordern [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.basicauth.required.pdf*, um festzulegen, ob für eingehende PDF-Anforderungen eine Standardauthentifizierung erforderlich sein soll.

Weitere Informationen

Warnung: Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Eigenschaftsname	*glide.basicauth.required.pdf*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	Um die Standardauthentifizierung für PDF-Anforderungen zu erzwingen.
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	7.5
Funktionale Auswirkung	(Niedrig) Diese Korrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Standardauthentifizierung und Zugriffssteuerung auf Systemebene. • Es führt diese Authentifizierung durch, während Daten aus Tabellen/Seiten in Form von PDF-Daten in der Instanz abgerufen werden. • Sie schränkt alle Gastanwender ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Anwender erstellen, die Zugriff auf diesen Inhalt benötigen, mit den erforderlichen Zugriffssteuerungsberechtigungen. Weitere Informationen finden Sie unter Webservice-Importsätze .
Sicherheitsrisiko	(Hoch) Wenn keine entsprechende Autorisierung für die eingehenden PDF-Anforderungen konfiguriert ist, kann ein nicht autorisierter Anwender Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Authentifizierung für Ereignismanagement-HTTP-Prozessor erforderlich [Neu in Security Center 1.3]

Erfahren Sie, wie Sie eine sichere Standardauthentifizierung für eingehende Amazon Simple Notification Service-(SNS-)Anforderungen einrichten, wenn das Plugin „Ereignismanagement“ (*com.glideapp.itom.snac*) aktiviert ist.

Wenn die Eigenschaft *glide.basicauth.required.evtmgmthttpprocessor* nicht auf den empfohlenen Wert **true**festgelegt ist und das Plugin „Ereignismanagement“ (*com.glideapp.itom.snac*) aktiv ist, ist die Standardauthentifizierung für alle eingehenden Anforderungen von Amazon Simple Notification Service (SNS) nicht erforderlich. Dies kann zu nicht authentifiziertem Zugriff auf Instanzdaten führen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um dieses Sicherheitsrisiko zu beheben, stellen Sie sicher, dass *glide.basicauth.required.evtmgmthttpprocessor* auf „**true** “ festgelegt und *com.glideapp.itom.snac* aktiv ist.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.basicauth.required.evtmgmthttpprocessor*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	API und Webservice
Sicherheitsrisiko	• Schweregrad-Punktzahl: 7 • CVSS-Punktzahl: Hoch • Details zum Sicherheitsrisiko: Wenn *glide.basicauth.required.evtmgmthttpprocessor* nicht auf den empfohlenen Wert „true“ festgelegt und das Plugin *com.glideapp.itom.snac* „ nicht aktiviert wird, wird die Standardauthentifizierung für eingehende SNS-Anforderungen nicht aktiviert. Dies kann zu nicht authentifiziertem Zugriff auf Instanzdaten führen.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	• https://docs.aws.amazon.com/sns/latest/dg/welcome.html • Zugriffssteuerung
Funktionale Auswirkung	Wenn *glide.basicauth.required.evtmgmthttpprocessor* nicht auf den empfohlenen Wert „True“ festgelegt ist und das Plugin „Ereignismanagement“ (com.glideapp.itom.snac) aktiv ist, ist die Standardauthentifizierung nicht für alle eingehenden Amazon Web Services-SNS-Anforderungen erforderlich. Dies kann zu nicht authentifiziertem Zugriff auf Instanzdaten führen.

Autorisierung für SOAP-Anforderungen erfordern [Aktualisiert in Security Center 1.3 und 1.5]

Verwenden Sie die Eigenschaft *glide.basicauth.required.soap*, um festzulegen, ob für eingehende SOAP-Anforderungen eine Standardautorisierung erforderlich sein soll.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Warnung: Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	*glide.basicauth.required.soapglide.soap.require_ws_secur*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	Zum Erzwingen der Autorisierung von SOAP-Anforderungen.
Empfohlener Wert	wahr
Sicherheitsrisikobewertung	8.1
Funktionale Auswirkung	(Mittel) Diese Korrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Standardauthentifizierung und Zugriffssteuerung auf Systemebene. • Es führt diese Authentifizierung durch, während es Daten aus Tabellen/Seiten in Form von SOAP-Daten in der Instanz abruft. • Sie schränkt alle Gastanwender ein, die derzeit auf diese Daten zugreifen. • Erstellen Sie einen Account für einen Anwender, der Zugriff auf diesen Inhalt benötigt, mit den erforderlichen Berechtigungen für die Zugriffssteuerung. Weitere Informationen finden Sie unter SOAP-Webservice- und MID-Server-Authentifizierung, Anmeldeinformationen und SOAP-Anforderungen .
Sicherheitsrisiko	(Mittel) Ohne entsprechende Autorisierung für die Datenquellen-SOAP-Anforderungen kann ein nicht autorisierter Anwender auf vertrauliche Inhalte/Daten in der Zielinstanz zugreifen.
Referenzen	Authentifizierung

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Autorisierung für Entlade-Anforderungen erfordern [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.basicauth.required.unl* (useUnloadFormat), um festzulegen, ob für eingehende Entladeanforderungen eine Standardauthentifizierung erforderlich sein soll.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.basicauth.required.unl*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	Zum Erzwingen der Standardauthentifizierung bei Entladeanforderungen.
Empfohlener Wert	wahr
Sicherheitsrisikobewertung	7.5
Funktionale Auswirkung	(Mittel) Diese Korrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Standardauthentifizierung und Zugriffssteuerung auf Systemebene. Diese Authentifizierung wird beim Abrufen von Daten aus Tabellen/Seiten in Form von Entladedaten in der Instanz durchgeführt.
Sicherheitsrisiko	(Hoch) Wenn keine entsprechende Autorisierung für die Entladeanforderungen für Datenquellen konfiguriert ist, kann ein nicht autorisierter Anwender Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten. Stellen Sie sicher, dass *glide.basicauth.required.unl* in sys_properties_table vorhanden und auf „wahr“ festgelegt ist.
Referenzen	Authentifizierung

Autorisierung für CSV-Anforderungen erfordern [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.basicauth.required.csv*, um festzulegen, ob eingehende CSV-Anforderungen (Comma-Separated Values) eine Standardauthentifizierung erfordern sollen.

Weitere Informationen

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	*glide.basicauth.required.csv*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	Um die Standardauthentifizierung für CSV-Anforderungen zu erzwingen.
Empfohlener Wert	wahr

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisikobewertung	7.5
Funktionale Auswirkung	(Niedrig) Diese Korrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Standardauthentifizierung und Zugriffssteuerung auf Systemebene. • Es führt diese Authentifizierung durch, während Daten aus Tabellen/Seiten in Form von CSV-Daten in der Instanz abgerufen werden. • Sie schränkt alle Gastanwender ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Anwender erstellen, die Zugriff auf diesen Inhalt benötigen, mit den erforderlichen Zugriffssteuerungsberechtigungen. Weitere Informationen finden Sie unter Daten aus einer CSV-formatierten Datei abrufen .
Sicherheitsrisiko	(Hoch) Wenn keine entsprechende Autorisierung für die eingehenden CSV-Anforderungen konfiguriert ist, kann ein nicht autorisierter Anwender Zugriff auf vertrauliche Inhalte und Daten in der Zielinstanz erhalten. Stellen Sie sicher, dass *glide.basicauth.required.csv* in der Tabelle „sys_properties“ vorhanden und auf „wahr“ festgelegt ist.
Referenzen	Webservice – Sicherheit

Autorisierung für Excel-Anforderungen erfordern [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.basicauth.required.excel*, um festzulegen, ob für eingehende Excel-Anforderungen eine Standardauthentifizierung erforderlich sein soll.

Weitere Informationen

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	*glide.basicauth.required.excel*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	Um die Standardauthentifizierung für Excel-Anforderungen zu erzwingen.
Empfohlener Wert	wahr
Sicherheitsrisikobewertung	7.5

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Funktionale Auswirkung	(Niedrig) Diese Korrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Standardauthentifizierung und Zugriffssteuerung auf Systemebene. • Es führt diese Authentifizierung durch, während Daten aus Tabellen/Seiten in Form von Excel-Daten in der Instanz abgerufen werden. • Sie schränkt alle Gastanwender ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Anwender erstellen, die Zugriff auf diesen Inhalt benötigen, mit den erforderlichen Zugriffssteuerungsberechtigungen.
Sicherheitsrisiko	(Hoch) Wenn keine entsprechende Autorisierung für die eingehenden Excel-Anforderungen konfiguriert ist, kann ein nicht autorisierter Anwender Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Autorisierung für Importanforderungen erfordern [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.basicauth.required.importprocessor*, um festzulegen, ob für eingehende Importanforderungen eine Standardauthentifizierung erforderlich sein soll.

Weitere Informationen

Warnung: Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	*glide.basicauth.required.importprocessor*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	Erzwingen der Standardauthentifizierung bei Importanforderungen.
Empfohlener Wert	wahr
Sicherheitsrisikobewertung	5.3
Funktionale Auswirkung	(Niedrig) Diese Korrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Standardauthentifizierung und Zugriffssteuerung auf Systemebene.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Diese Authentifizierung wird beim Importieren von Datenquellen in die Instanztabellen/-seiten durchgeführt. • Sie schränkt alle Gastanwender ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Anwender erstellen, die Zugriff auf diesen Inhalt benötigen, mit den erforderlichen Zugriffssteuerungsberechtigungen. Weitere Informationen finden Sie unter Daten aus einer CSV-formatierten Datei abrufen .
Sicherheitsrisiko	(Moderat) Wenn keine entsprechende Autorisierung für die Datenquellen-Importanforderungen konfiguriert ist, kann ein nicht autorisierter Anwender Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.
Referenzen	Sicherheit von SOAP-Webservices SOAP-Webservice

Autorisierung für JSONv2-Anforderung erfordern [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.basicauth.required.jsonv2*, um festzulegen, ob für eingehende JSONv2-Anforderungen eine Standardautorisierung erforderlich sein soll.

Weitere Informationen

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	*glide.basicauth.required.jsonv2*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	Zum Erzwingen der Autorisierung von JSONv2-Anforderungen.
Sicherheitsrisikobewertung	7.5
Empfohlener Wert	wahr
Funktionale Auswirkung	(Mittel) Diese Korrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Standardauthentifizierung und Zugriffssteuerung auf Systemebene.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Diese Authentifizierung wird durchgeführt, während Daten aus Tabellen/Seiten in Form von JSON-Daten in der Instanz abgerufen werden. • Sie schränkt alle Gastanwender ein, die derzeit auf diese Daten zugreifen. • Erstellen Sie einen Account für einen Anwender, der Zugriff auf diesen Inhalt benötigt, mit den erforderlichen Berechtigungen für die Zugriffssteuerung. Weitere Informationen finden Sie unter JSONv2-Webservice JSONv2-Webservice .
Sicherheitsrisiko	(Hoch) Wenn keine entsprechende Autorisierung für die JSON-Anforderungen der Datenquelle konfiguriert ist, kann ein nicht autorisierter Anwender auf vertrauliche Inhalte/Daten in der Zielinstanz zugreifen.
Referenzen	Authentifizierung Basic Authentication für eingehende JSONv2-Anforderungen anfordern

Autorisierung für WSDL-Anforderung erfordern [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.basicauth.required.wsdl*, um festzulegen, ob für eingehende WSDL-Anforderungen (Web Services Description Language) eine Standardauthentifizierung erforderlich sein soll.

Hinweis: Wenn Sie keine Standardauthentifizierung für eingehende WSDL-Anforderungen vorschreiben möchten, müssen Sie die Regeln für die Zugriffssteuerung (ACL) ändern, um Gastbenutzern den Zugriff auf WSDL-Inhalt zu ermöglichen.

Weitere Informationen

Warnung: Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	*glide.basicauth.required.wsdl*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	Um die Standardauthentifizierung für WSDL-Anforderungen zu erzwingen.
Empfohlener Wert	wahr
Sicherheitsrisikobewertung	4.3

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Funktionale Auswirkung	(Niedrig) Diese Korrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Standardauthentifizierung und Zugriffssteuerung auf Systemebene. • Diese Authentifizierung wird durchgeführt, während Daten aus Tabellen/Seiten in Form von WSDL-Daten in der Instanz abgerufen werden. • Sie schränkt alle Gastanwender ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Anwender erstellen, die Zugriff auf diesen Inhalt benötigen, mit den erforderlichen Zugriffssteuerungsberechtigungen.
Sicherheitsrisiko	(Mittel) Wenn keine entsprechende Autorisierung in den WSDL-Webservices konfiguriert ist, kann ein nicht autorisierter Anwender Zugriff auf vertrauliche WSDL-Inhalte/-Daten in der Zielinstanz erhalten.
Referenzen	Webservice – Sicherheit

Autorisierung für XML-Anforderungen erfordern [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.basicauth.required.xml*, um anzugeben, ob für eingehende XML-Anforderungen eine Standardauthentifizierung erforderlich sein soll.

Weitere Informationen

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	*glide.basicauth.required.xml*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	Erzwingen der Standardauthentifizierung für XML-Anforderungen.
Sicherheitsrisikobewertung	7.5
Empfohlener Wert	wahr
Funktionale Auswirkung	(Niedrig) Diese Korrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Standardauthentifizierung und Zugriffssteuerung auf Systemebene.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Es führt diese Authentifizierung durch, während es Daten aus Tabellen/Seiten in Form von XML-Daten in der Instanz abruft. • Sie schränkt alle Gastanwender ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Anwender erstellen, die Zugriff auf diesen Inhalt benötigen, mit den erforderlichen Zugriffssteuerungsberechtigungen. Weitere Informationen finden Sie unter XML-Parser-Schritt .
Sicherheitsrisiko	(Hoch) Wenn keine entsprechende Autorisierung für die eingehenden XML-Anforderungen konfiguriert ist, kann ein nicht autorisierter Anwender Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.
Referenzen	Authentifizierung

Berechtigung für XML-Ausgabeanforderungen anfordern

Konfigurieren Sie diese Eigenschaft so, dass für alle eingehenden XMLOutputProcessor-Anforderungen eine Standardautorisierung erforderlich ist.

Wenn die Eigenschaft *glide.basicauth.required.xmloutputprocessor* nicht auf den empfohlenen Wert **true**festgelegt ist, ist für eingehende XMLOutputProcessor-Anforderungen keine Standardautorisierung erforderlich. Dies könnte zu einer nicht authentifizierten Offenlegung von Informationen durch die Instanz führen.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.basicauth.required.xmloutputprocessor*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	API und Webservice
Sicherheitsrisiko	• Schweregrad-Punktzahl: 7,5 • CVSS-Punktzahl: Hoch

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Details zum Sicherheitsrisiko: Wenn Sie die Eigenschaft nicht auf den empfohlenen Wert „ **true** “ festlegen, können vertrauliche Informationen aus der Instanz verloren gehen.
Abhängigkeiten und Voraussetzungen	Keine

Autorisierung für XSD-Anforderungen erfordern

Verwenden Sie die Eigenschaft *glide.basicauth.required.xsd*, um festzulegen, ob für eingehende XSD-Anforderungen (XML-Schemadefinition) eine Standardauthentifizierung erforderlich sein soll.

Weitere Informationen

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	glide.basisauth.erforderlich.xsd*glide.basicauth.required.xsd*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	Um die Standardauthentifizierung für XSD-Anforderungen zu erzwingen.
Empfohlener Wert	wahr
Sicherheitsrisikobewertung	5.3
Funktionale Auswirkung	(Niedrig) Diese Korrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Standardauthentifizierung und Zugriffssteuerung auf Systemebene. • Es führt diese Authentifizierung durch, während Daten aus Tabellen/Seiten im Formular von XSD-Daten in der Instanz abgerufen werden. • Sie schränkt alle Gastanwender ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Anwender erstellen, die Zugriff auf diesen Inhalt benötigen, mit den erforderlichen Zugriffssteuerungsberechtigungen. Weitere Informationen finden Sie unter Nicht interaktive Sitzungen .
Sicherheitsrisiko	(Moderat) Wenn keine entsprechende Autorisierung für die eingehenden XSD-Anforderungen konfiguriert

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	ist, kann ein nicht autorisierter Anwender Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.
Referenzen	Authentifizierung

Autorisierung für Skriptanforderungen erfordern

Verwenden Sie die Eigenschaft *glide.basicauth.required.scriptedprocessor*, um festzulegen, ob für eingehende Skriptanforderungen eine Standardauthentifizierung erforderlich sein soll.

Weitere Informationen

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	*glide.basicauth.required.scriptedprocessor*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	Erzwingen der Standardauthentifizierung für Skriptanforderungen.
Empfohlener Wert	wahr
Sicherheitsrisikobewertung	7.2
Funktionale Auswirkung	(Mittel) Diese Korrektur erzwingt die Authentifizierung in Form von Standardautorisierung. • Diese Authentifizierung wird bei der Verarbeitung von Skriptanforderungen in der Instanz durchgeführt. • Sie schränkt alle Gastanwender ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Anwender erstellen, die Zugriff auf diesen Inhalt benötigen, mit den erforderlichen Zugriffssteuerungsberechtigungen.
Sicherheitsrisiko	(Hoch) Ohne entsprechende Konfiguration der Autorisierung für eingehende Skriptanforderungen greift ein nicht autorisierter Anwender auf vertrauliche Inhalte/Daten in der Zielinstanz zu.
Referenzen	Authentifizierung

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Autorisierung für SCHEMA-Anforderungen erfordern [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.basicauth.required.schema*, um eine Standardautorisierung für alle Anforderungen an den eingehenden Tabellenschemaprozessor zu erfordern.

Der Schebma-Prozessor für eingehende Tabellen verarbeitet eingehende Schemaanforderungen für die Plattform.

Legen Sie *glide.basicauth.required.schema* auf den empfohlenen Wert „ **wahr** “ fest, um eine Standardautorisierung für alle Anforderungen an den eingehenden Tabellenschemaprozessor anzufordern. Legen Sie den Wert auf **„falsch“ fest**, um keine Standardautorisierung für alle Anforderungen an den eingehenden Tabellenschemaprozessor zu erfordern.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.basicauth.required.schema*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	Um eine Standardautorisierung für alle Anforderungen des eingehenden Tabellenschemaprozessors anzufordern.
Empfohlener Wert	Wahr (Standardwert).
Konfigurationstyp	Boolean
Sicherheitsrisiko	(Mittel) Wenn die Authentifizierung von diesem Prozessor ausgelassen wird, führt dies zu nicht authentifiziertem Zugriff auf Instanzdaten.

Autorisierung für RSS-Anforderungen erfordern [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.basicauth.required.rss*, um festzulegen, ob für eingehende RSS-Anforderungen eine Standardauthentifizierung erforderlich sein soll.

Weitere Informationen

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	*glide.basicauth.required.rss*

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	Um die Standardauthentifizierung für RSS-Anforderungen zu erzwingen.
Empfohlener Wert	wahr
Sicherheitsrisikobewertung	7.5
Funktionale Auswirkung	(Niedrig) Diese Korrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Standardauthentifizierung und Zugriffssteuerung auf Systemebene. • Diese Authentifizierung wird bei der Verarbeitung von RSS-Anforderungen in der Instanz durchgeführt. • Sie schränkt alle Gastanwender ein, die derzeit auf diese Daten zugreifen. Gegebenenfalls müssen Sie möglicherweise ein neues Konto für Anwender erstellen, die Zugriff auf diesen Inhalt benötigen, mit den erforderlichen Zugriffssteuerungsberechtigungen. Weitere Informationen finden Sie unter RSS-Feed-Generator .
Sicherheitsrisiko	(Hoch) Wenn keine entsprechende Autorisierung für die eingehenden RSS-Anforderungen konfiguriert ist, kann ein nicht autorisierter Anwender Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.
Referenzen	RSS-Basic Authentication

Autorisierung für API-Anforderungen erfordern [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.basicauth.required.api*, um die Sicherheit für die Standardautorisierung für eingehende REST-Anforderungen zu erhöhen.

Legen Sie die Eigenschaft *glide.basicauth.required.api* auf „ **wahr** “ fest, um eine Autorisierung für alle REST-Anforderungen zu erfordern. Legen Sie die Eigenschaft auf **„false“ fest**, um die Autorisierung für alle REST-Anforderungen zu umgehen.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.basicauth.required.api*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Kategorie	API und Webservice
Zweck	Standardberechtigung für eingehende REST-Anforderungen.
Empfohlener Wert	Wahr (Standard)
Konfigurationstyp	Zeichenfolge
Sicherheitsrisiko	(Hoch) Wenn „glide.basicauth.required.api“ nicht auf den empfohlenen Wert „wahr“ festgelegt ist, wird die Standardauthentifizierung für die API-Anforderung deaktiviert. Dies führt zu nicht authentifiziertem Zugriff auf Instanzdaten.
Sicherheitsrisikobewertung	8.6

Architektur, Design und Bedrohungsmodellierung

Diese umfassende Steuerung befasst sich mit allgemeinen Designüberlegungen und Schlüsselelementen zur Implementierung einer sicheren Anwendung. Dies umfasst die Mandanten der Verfügbarkeit, der Vertraulichkeitsverarbeitungsintegrität, der Nachweisbarkeit und des Datenschutzes. Darüber hinaus sind Elemente eines sicheren Software-Entwicklungslebenszyklus enthalten.

Zertifikatbasierte Authentifizierung nicht erzwungen [Neu in Security Center 1.3]

Die Eigenschaft *glide.authenticate.mutual.enabled* ermöglicht die zertifikatbasierte Authentifizierung, eine Art der gegenseitigen Authentifizierung für eingehende REST-Verbindungen zu REST- und SOAP-APIs in Now Platform.

Die gegenseitige Authentifizierung stellt Vertrauen zwischen Server und Client her, indem SSL-Zertifikate (Secure Socket Layer) ausgetauscht werden, um das Zertifikat mit einer vertrauenswürdigen Zertifizierungsstelle zu validieren. Dies ermöglicht die Überprüfung, ob eine vertrauenswürdige Quelle eine Verbindung zu Now Platformherstellt. Wenn diese Instanz nicht auf den empfohlenen Wert „true“ festgelegt ist, ist eine Instanz möglicherweise angreifbar für Man-in-the-Middle-Angriffe (MitM).

Um diese Sicherheitsbedrohung zu beheben, aktivieren Sie die gegenseitige Authentifizierung für eingehende Webservices. Wenn Sie das Plugin für die zertifikatsbasierte Authentifizierung (*com.glide.auth.mutual)* für Now Platform] zum ersten Mal installieren, folgen Sie den Anweisungen unter Richten Sie die zertifikatbasierte Authentifizierung ein. Stellen Sie außerdem sicher, dass die Eigenschaft *glide.authenticate.mutual.enabled* auf „true“ festgelegt ist, um das Plugin zu aktivieren.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.authenticate.mutual.enabled*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Standardwert	wahr
Kategorie	Architektur, Design und Bedrohungsmodellierung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 5.3 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf den empfohlenen Wert true festgelegt ist, validiert die zertifikatsbasierte Authentifizierung keine Zertifikate mit einer vertrauenswürdigen Zertifizierungsstelle. Dies erhöht die Wahrscheinlichkeit, dass ein böswilliger Akteur eine Instanz mit MitM-Angriffen angreift.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	• https://csrc.nist.gov/glossary/term/man_in_the_middle_attack • Zertifikatbasierte Authentifizierung • Konfigurieren der gegenseitigen Authentifizierung

Identitätswechsel bei ACL-Bewertung in HR-App überprüfen [Neu in Security Center 1.3 und aktualisiert in 1.5]

Verwenden Sie die Eigenschaft *sn_hr_core.impersonateCheck*, um zu verhindern, dass ein Benutzer die Identität eines anderen Benutzers annimmt und auf dessen HR-Informationen zugreift.

Eine sichere Einstellung verhindert, dass ein Administrator die HR-Informationen eines anderen Anwenders sieht, während er die Identität von anwendet. Eine unsichere Einstellung für diese Eigenschaft ermöglicht es einem Administrator, die Identität eines Anwenders anzunehmen und mit dem Zugriff des Anwenders, dessen Identität angenommen wurde, auf HR-Daten wie Umfrageergebnisse oder Audit-Datensätze zuzugreifen. Aufgrund der Art dieser Art von Daten (z. B. Informationen, die nur für den Anwender selbst verfügbar sein sollten, z. B. E-Mail) wird dies nicht empfohlen. Wenn *sn_hr_core.impersonateCheck* auf „wahr“ festgelegt wird, wird nur dann der Zugriff auf HR-Informationen ermöglicht, wenn der Anwender nicht die Identität eines anderen Anwenders annimmt.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*sn_hr_core.impersonateCheck*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	falsch

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Kategorie	Architektur, Design und Bedrohungsmodellierung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 2,7 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Eine unsichere Einstellung für diese Eigenschaft ermöglicht es einem Administrator, die Identität eines Anwenders anzunehmen und mit dem Zugriff des Anwenders, dessen Identität angenommen wurde, auf HR-Daten wie Umfrageergebnisse oder Audit-Datensätze zuzugreifen.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Wenn diese Eigenschaft auf „true“ festgelegt ist, kann ein Administrator während des Identitätswechsels die HR-Informationen eines anderen Anwenders nicht einsehen. Bei Festlegung auf „falsch“ kann ein Administrator die Identität eines Benutzers annehmen und mit dem Zugriff des Benutzers, der die Identität eines Benutzers angenommen hat, auf HR-Daten wie Umfrageergebnisse oder Audit-Datensätze zugreifen. Aufgrund der Art dieser Art von Daten (z. B. Informationen, die nur für den Anwender selbst verfügbar sein sollten, wie eine E-Mail) wird dies nicht empfohlen. Wenn Sie sn_hr_core.impersonateCheck auf „wahr“ setzen, wird nur dann der Zugriff auf HR-Informationen ermöglicht, wenn der Anwender nicht die Identität eines anderen Anwenders annimmt.

Deaktivieren Sie nicht authentifizierte veröffentlichte Berichte

Deaktivieren Sie diese Eigenschaft, um zu verhindern, dass der Anwender Berichte veröffentlicht oder auf sie zugreift. Diese Eigenschaft deaktiviert die Funktion für veröffentlichte Berichte in der Berichterstellung.

Aktivieren Sie das Veröffentlichen von Berichten, indem Sie *glide.report.published_reports.enabled* auf **true** setzen.

Sicherheit für Berichte erzwingen ist konform, wenn *glide.report.published_reports.enabled* auf „ **falsch**“ festgelegt ist.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.report.published_reports.enabled*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Architektur, Design und Bedrohungsmodellierung
Zweck	Deaktiviert die Funktion „Veröffentlichte Berichte“ in der Berichterstellung.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Typ	wahr | falsch
Empfohlener Wert	**false**
Sicherheitsrisikobewertung	6.5
Funktionale Auswirkung	(Mittel) Der Anwender kann keine Berichte veröffentlichen.
Sicherheitsrisiko	(Mittel) Wenn diese Eigenschaft nicht aktiviert ist, können Anwender möglicherweise auf Berichte zugreifen oder diese veröffentlichen, die vertrauliche Daten enthalten. Durch das Veröffentlichen eines Berichts wird eine URL erstellt, über die alle Benutzer auf den Bericht zugreifen können, auch Personen, die keine Benutzer von sind. Wenn jemand zur URL navigiert, wird der Bericht mit aktuellen Daten aus der Instanz generiert.
Referenzen	Berichte veröffentlichen

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Erzwingen Sie Feld-ACLs für eingehende Abfrageanforderungen

Verwalten Sie, wie eingehende Abfragen in Ihrer Instanz validiert werden.

Verwenden Sie die Eigenschaft *glide.report.report_view.check_published*, um zu überprüfen, wie eingehende Abfragen in Ihrer Instanz validiert werden. Wenn die Eigenschaft auf den empfohlenen Wert **true**festgelegt ist, werden Feld-ACLs auf eingehende Abfragen geprüft und abgelehnt, wenn der Benutzer nicht autorisiert ist. Wenn die Eigenschaft auf **false**festgelegt ist, werden ACLs nicht auf eingehende Abfragen geprüft und weiterhin ausgeführt, was zur Offenlegung von Informationen an nicht autorisierte Parteien führen kann.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.export.query.enforce_field_acl*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Architektur, Design und Bedrohungsmodellierung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 4.4 • CVSS-Punktzahl: Mittel

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Details zum Sicherheitsrisiko: Wenn diese Eigenschaft auf „ **false**“ festgelegt ist, werden ACLs nicht auf eingehende Abfragen überprüft, die zur Offenlegung von Informationen führen können.
Abhängigkeiten und Voraussetzungen	Keine

Erzwingen Sie Lese-ACLs in Berichtsansichten

Verwalten Sie, wie Lese-ACLs in Ihrer Instanz erzwungen werden.

Verwenden Sie die Eigenschaft *glide.report.report_view.read_acl*, um die Lese-ACL (Tabellenebene) für Berichtsfunktionen zu erzwingen, wenn für die Tabelle oder das Feld keine Berichtsansichts-ACL vorhanden ist. Wenn diese Eigenschaft nicht auf „ **erzwingen**“ festgelegt ist, können ACLs umgangen werden, was zu einem Verlust vertraulicher Informationen führt.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.report.report_view.read_acl*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	erzwingen
Standardwert	erzwingen
Kategorie	Architektur, Design und Bedrohungsmodellierung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 7.1 • CVSS-Punktzahl: Hoch • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf „ **Erzwingen** “ festgelegt wird, können ACLs umgangen werden.
Abhängigkeiten und Voraussetzungen	Keine

Zulässige ServiceNow interne IP-Adressen definieren [Aktualisiert in Security Center 1.3 und 1.5]

Verwenden Sie die Eigenschaft *glide.ip.authenticate.strict*, um IP-Bereiche anzugeben, die eingehende Verbindungen in einer Instanz herstellen können.

Wenn *glide.ip.authenticate.strict* auf truefestgelegt ist, können nur die in *glide.ip.authenticate.allow.secured*angegebenen IP-Bereiche eingehende Verbindungen in einer Instanz herstellen. Diese Eigenschaft enthält eine Liste nur der wichtigen internen ServiceNow-IP-Bereiche (sicheres VPN, DC).

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn *glide.ip.authenticate.allow.secured* nicht auf den empfohlenen Wert „10.0.0.0/8, 37.98.232.0/21, 103.23.64.0/22, 149.96.0.0/17, 149.96.0.0/16, 199.91.136.0/21, 148.139. 0.0/16, 127.0.0.1, 0:0:0:0:0:0:0:1", kann es nicht vertrauenswürdigen Quellen außerhalb von ServiceNow DataCenter und sicherem VPN gestattet werden, auf sensible Überwachungsendpunkte in Instanzen zuzugreifen.

⚠ **Warnung:** Der Wert für diese Eigenschaft ist eine Überschreibung ohne DB. Sie kann nicht geändert oder überschrieben werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.ip.authenticate.strict*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Architektur, Design und Bedrohungsmodellierung
Zweck	Ermöglicht ServiceNow-Mitarbeitern, nur über einen gesicherten Satz von IP-Bereichen auf die Instanz zuzugreifen
Empfohlener Wert	wahr
Sicherheitsrisikobewertung	4.3
Funktionale Auswirkung	(Niedrig) Wenn diese Eigenschaft nicht aktiviert ist, können ServiceNow-Mitarbeiter über alle IP-Bereiche auf die Instanz des Kunden zugreifen. Durch Aktivieren der Eigenschaft wird der Zugriff auf einen sicheren Satz von IP-Bereichen (sicheres VPN, DC) eingeschränkt. **Hinweis:** Wenn Sie diese Eigenschaft auf `true`festlegen, verwendet Now Platform eine restriktivere Eigenschaft *glide.ip.authenticate.allow.secured* anstelle der Eigenschaft IP-Beschränkung für die Leistungsüberwachung (*glide.ip.authenticate.allow.secured*) für eine Reihe von IP-Bereichen, die auf die Instanz zugreifen können.
Sicherheitsrisiko	(Niedrig) Unnötige Offenlegung des Instanzzugriffs für eine größere Gruppe von Personen.
Referenz	Authentifizierung mit IP-Adressbereich

Hinweis: Die Regel „Alle verweigern“ muss der IP-Zugriffssteuerung hinzugefügt werden, um den Zugriff von IPs einzuschränken, die nicht der IP-Zugriffssteuerung hinzugefügt wurden. Alle erforderlichen zulässigen IPs müssen dann der IP-Zugriffssteuerung hinzugefügt werden.

Legacy-JQuery-Verhalten deaktivieren [in Security Center 1.3 aktualisiert]

glide.jquery.legacy wird verwendet, um zu verhindern, dass ältere vorab gepatchte JQuery-Versionen verwendet werden, die zu nicht gepatchten Schwachstellen in der Bibliothek führen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Legen Sie *glide.jquery.legacy* auf den empfohlenen Wert „ **false** “ fest, um zu verhindern, dass ältere vorab gepatchte JQuery-Versionen verwendet werden, die nicht gepatchte Schwachstellen in der Bibliothek einführen. Legen Sie den Wert auf „ **true** “ fest, um vorab gepatchte JQuery-Versionen zuzulassen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.jquery.legacy*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Architektur, Design und Bedrohungsmodellierung
Zweck	Um potenzielle Sicherheitsrisiken durch Angriffe auf Schwachstellen zu verhindern, die in veralteten JQuery-Bibliotheksversionen erkannt wurden.
Empfohlener Wert	Falsch
Konfigurationstyp	Boolean
Sicherheitsrisiko	(Hoch) Verhindern, dass ältere vorab gepatchte JQuery-Versionen verwendet werden, die nicht gepatchte Schwachstellen in der Bibliothek einführen. Die Systemeigenschaft ist eine Ausfallsicherung für den Fall, dass Organisationen bei der Ausführung ihrer anwenderdefinierten Implementierungen auf die nicht gepatchten Versionen von Angular JS angewiesen sind.
Sicherheitsrisikobewertung	7.1

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Verhalten der Vorgängerversion für die Umgrenzung des GlideRecord-Bereichs deaktivieren [Neu in Security Center 1.3]

Die Eigenschaft *glide.record.legacy_cross_scope_access_policy_in_script* deaktiviert Bereichsbegrenzung, sodass bereichsbezogene Apps auf globale Skriptschnittstellen zugreifen können. Es wurde als Patch für den bereichsübergreifenden Zugriff von GlideRecord erstellt.

GlideRecord bietet bereichsübergreifenden Erstellungs- und Aktualisierungszugriff auf Tabellen, die nicht mit dieser Zugriffsebene konfiguriert wurden. Um zu verhindern, dass Anwendungen von Kunden beschädigt werden, wenn dieses bereichsbezogene Zugriffsverhalten gepatcht wurde, wurde die Eigenschaft *glide.record.legacy_cross_scope_access_policy_in_script* erstellt. Wenn diese Eigenschaft auf „true“ festgelegt ist, greift der bereichsübergreifende Zugriff auf das veraltete Verhalten zurück, das unsicher ist.

Diese Eigenschaft deaktiviert Bereichsbegrenzung, sodass bereichsbezogene Apps auf globale Skriptschnittstellen zugreifen können. Durch das Erzwingen der Bereichsbegrenzung wird sichergestellt, dass Anwendungen nur auf Ressourcen zugreifen können, die explizit gewährt wurden oder innerhalb des festgelegten Bereichs liegen. Dadurch wird das Prinzip der geringsten Berechtigung durchgesetzt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.record.legacy_cross_scope_access_policy_in_script*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	falsch
Standardwert	wahr (wenn die Eigenschaft nicht in der Tabelle „sys_properties“ vorhanden ist.)
Kategorie	Architektur, Design und Bedrohungsmodellierung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 5 • CVSS-Punktzahl: Mittel • Details zu Sicherheitsrisiken: Durch die Umfangsdefinition wird sichergestellt, dass Anwendungen nur auf Ressourcen mit explizitem Zugriff oder innerhalb ihres Bereichs zugreifen können, wobei das Prinzip der geringsten Rechte (Least-Privilege-Prinzip) gilt. Das Deaktivieren dieser Funktion kann Auswirkungen auf Vertraulichkeit, Verfügbarkeit und Integrität haben.
Abhängigkeiten und Voraussetzungen	Keine

Legacy-AngularJS-Verhalten deaktivieren [in Security Center 1.3 aktualisiert]

Verwenden Sie die Eigenschaft *glide.angular.legacy*, um sich vor potenziellen Sicherheitsrisiken zu schützen, die durch Angriffe auf Schwachstellen entstehen, die in veralteten AngularJS-Bibliotheksversionen erkannt wurden.

Legen Sie *glide.angular.legacy* auf den empfohlenen Wert „ **false** “ fest, um zu verhindern, dass ältere vorab gepatchte AngularJS-Versionen verwendet werden. Legen Sie die Eigenschaft auf „ **true** “ fest, um ältere vorab gepatchte AngularJS-Versionen zu verwenden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.angular.legacy*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Architektur, Design und Bedrohungsmodellierung
Zweck	Die Systemeigenschaft ist eine Ausfallsicherung für den Fall, dass Organisationen bei der Ausführung ihrer anwenderdefinierten Implementierungen auf die nicht gepatchten Versionen von Angular JS angewiesen sind.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Empfohlener Wert	Falsch
Konfigurationstyp	Boolean
Sicherheitsrisiko	(Hoch) Die Verwendung älterer Versionen von AngularJS kann möglicherweise zu Sicherheitsrisiken durch Angriffe auf Schwachstellen führen, die in veralteten AngularJS-Bibliotheksversionen erkannt wurden.
Sicherheitsrisikobewertung	7.1

Autorisierung für Daten-Broker-REST-API erfordern [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.basicauth.required.databrokerrestapiprocessor*, um die Standardautorisierung für alle eingehenden Daten-Broker-REST-API-Anforderungen zu erfordern.

Wenn diese Eigenschaft auf **true**festgelegt ist, wird die Autorisierung angewendet. Wenn sie auf **false**festgelegt ist, wird keine Autorisierung verwendet, was dazu führen könnte, dass vertrauliche Informationen aus Ihrer Instanz verloren gehen.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.basicauth.required.databrokerrestapiprocessor*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Architektur, Design und Bedrohungsmodellierung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 8,6 • CVSS-Punktzahl: Hoch • Details zum Sicherheitsrisiko: Wenn die Eigenschaft auf „ **false**“ festgelegt ist, wird die API-Authentifizierung nicht angewendet, sodass ein böswilliger Akteur auf vertrauliche Daten zugreifen kann.
Abhängigkeiten und Voraussetzungen	Keine

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardmäßig mit leeren ACLs verweigern [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.sm.default_mode*, um das Standardverhalten des Sicherheitsmanagers zu steuern, wenn festgestellt wird, dass vorhandene ACL-Regeln Teil von ACL-Regeln der Platzhaltertabelle sind.

Wenn das Plugin „Strenge Sicherheitseinstellungen“ (com.glide.high_security) während der Erstinstallation der Instanz aktiviert wird, erstellt es diese Eigenschaft, und es werden Platzhalter-ACL-Regeln aktiviert. Um rollenbasierten Zugriff auf Systemtabellen bereitzustellen, steuern diese Regeln eine erhebliche Anzahl von ACLs und die meisten gängigen datensatzbasierten Vorgänge:

- Lesen
- Schreiben
- Erstellen
- Löschen

Wenn Sie das Plugin „Hohe Sicherheit“ mit aktivierter standardmäßiger Ablehnungsoption nicht verwenden, sind viele Tabellen nicht geschützt. Now Platform verwendet ein standardmäßiges Deny-Sicherheitsmodell, das verhindert, dass Benutzer ohne Administratorrechte auf Objekte zugreifen, wenn sie eine übereinstimmende ACL-Regel erfüllen. Mit diesem Modell werden viele Angriffsvektoren entfernt, z. B. unsichere Skripts.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.sm.default_mode*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Architektur, Design und Bedrohungsmodellierung
Zweck	Die beste Sicherheitsmethode besteht darin, den Zugriff auf die Tabellen durch einen nicht autorisierten Benutzer einzuschränken. • Wenn für Tabellen keine ACL-Regeln vorhanden sind, stellt diese Eigenschaft sicher, dass mindestens Platzhalter-ACLs für jeden CRUD-Vorgang validiert werden, der für die Tabelle/das Feld ausgeführt wird. • Diese Regeln schränken die Lese-, Schreib-, Erstellungs- und Löschvorgänge für alle Tabellen ein, es sei denn, der Benutzer verfügt über die Administratorrolle oder erfüllt die Anforderungen einer anderen Tabellen-ACL-Regel.
Empfohlener Wert	verweigern
Funktionale Auswirkung	(Hoch) Wenn Sie diese Eigenschaft auf **Allow**festlegen, erlauben die ACL-Regeln der Platzhaltertabelle

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	CRUD-Vorgänge für alle Tabellen, es sei denn, es sind bestimmte ACL-Regeln für Tabellen vorhanden, um solche Vorgänge einzuschränken. **Hinweis:** Dieses Plugin ist nicht für vorhandene Instanzen vorgesehen, da es den Sicherheitszugriff auf Tabellen ändern könnte, die bereits in einer Produktionsumgebung verwendet werden.
Sicherheitsrisiko	8.8
Referenzen	Standardmäßige Verweigerungseigenschaft

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Authentifizierung

Die Authentifizierungskategorie deckt die Hauptelemente der modernen Authentifizierung ab, mit denen bestätigt wird, dass eine Entität und ihre Ansprüche zuverlässig und korrekt sind, gegen Identitätswechsel abgesichert sind und das Abfangen von Passwörtern verhindern.

Der ASVS-Standard basiert auf der Spezifikation NIST 800-63b (https://pages.nist.gov/800-63-3/sp800-63b.html) für diesen Abschnitt.

Zur Authentifizierung gehören Passwortrichtlinien, Kontrollen und Speicherung, ordnungsgemäße Implementierung von Authentifikatoren und ordnungsgemäße Implementierung von Out-of-Band- oder einmaligen Verifizierungen.

Rollenbasierte Multifaktor-Authentifizierung aktivieren [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.authenticate.multifactor*, um die rollenbasierte Multifaktor-Authentifizierung (MFA) für alle Benutzer zu erzwingen, die bestimmten Rollen zugewiesen sind.

Erzwingen Sie die Multifaktor-Authentifizierung basierend auf den Rollen, die dem Anwender zugewiesen sind. Wenn einem Anwender in der Liste der Multifaktor-Rollen die Rollen „admin“, „security_admin“ oder „user_admin“ zugewiesen wurden, wird MFA erzwungen.

- Legen Sie diese Eigenschaft auf **„wahr** “ fest, um die rollenbasierte Multifaktor-Authentifizierung für alle Anwender zu erzwingen, die bestimmten Rollen zugewiesen sind.
- Legen Sie diese Eigenschaft auf „ **falsch** “ fest, um die rollenbasierte Multifaktor-Authentifizierung für alle Anwender zu deaktivieren, die bestimmten Rollen zugewiesen sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.authenticate.multifactor*

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Erzwingen Sie die rollenbasierte Multifaktor-Authentifizierung für alle Anwender, die bestimmten Rollen zugewiesen sind.
Typ	wahr/falsch
Empfohlener Wert	`true`
Sicherheitsabhängigkeiten	Aktivieren **Sie die rollenbasierte Multifaktor-Authentifizierung** in der **Tabelle Multifaktor-Kriterien**.
Sicherheitsrisikobewertung	7.2
Funktionale Auswirkung	(Mittel) Durch Aktivieren dieser Eigenschaft verbessert sich die Experience des Anwenders. Sie dient als zusätzliche Schutz- und Sicherheitsebene gegen kompromittierte Anmeldeinformationen.
Sicherheitsrisiko	(Mittel) Wenn diese Eigenschaft nicht aktiviert ist, besteht das Risiko eines nicht autorisierten Zugriffs auf vertrauliche Daten.
Referenzen	Konfigurieren Sie rollenbasierte Multifaktor-Kriterien

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Accountwiederherstellung aktivieren [In Security Center 1.3 und 1.5aktualisiert]

Die Eigenschaft `glide.sso.acr.enabled` steuert die Funktion zur Accountwiederherstellung.

Legen Sie `glide.sso.acr.enabled` auf den empfohlenen Wert „ **wahr** “ fest, um eine Accountwiederherstellung nach Anwender-ID zu ermöglichen. Legen Sie den Wert auf „ **falsch** “ fest, um die Accountwiederherstellung nach Anwender-ID nicht zuzulassen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.sso.acr.enabled`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Steuert die Accountwiederherstellung nach Anwender-ID-Funktion.
Empfohlener Wert	Wahr (Standard)
Konfigurationstyp	Boolean
Sicherheitsrisiko	Kritisch (Wenn diese Eigenschaft nicht aktiviert ist, können Anwender ihren Account nicht nach Anwender-ID wiederherstellen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisikobewertung	9.1
Referenzen	Weitere Informationen finden Sie unter Accountwiederherstellung (ACR).

Verschleierung der klassischen mobilen App-UI vorschreiben [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.ui.m.blur_ui_when_backgrounded*, um alle Felder aus dem Snapshot zu verschleiern, da das Bild während des Hintergrundprozesses gespeichert wird.

Auf Android-Geräten erstellt das Android-Betriebssystem einen Screenshot zur Verwendung im Menü für aktuelle Aufgaben, wenn die Anwendung im Hintergrund ausgeführt wird. Benutzer können auch manuelle Screenshots der Anwendung erstellen, die öffentlich auf dem Gerät gespeichert werden.

Auf iOS-Geräten können Anwendungen mit dem iOS-Betriebssystem auch Bilddateien speichern. Diese Datei stellt den letzten Bildschirm dar, den der Anwender sieht, wenn die Anwendung in den Hintergrund verschoben wird. Der Zweck besteht zwar darin, eine bessere Anwender-Experience zu bieten, stellt jedoch auch ein Sicherheitsrisiko dar, da die Bilder als PNG-Bilddateien gespeichert werden.

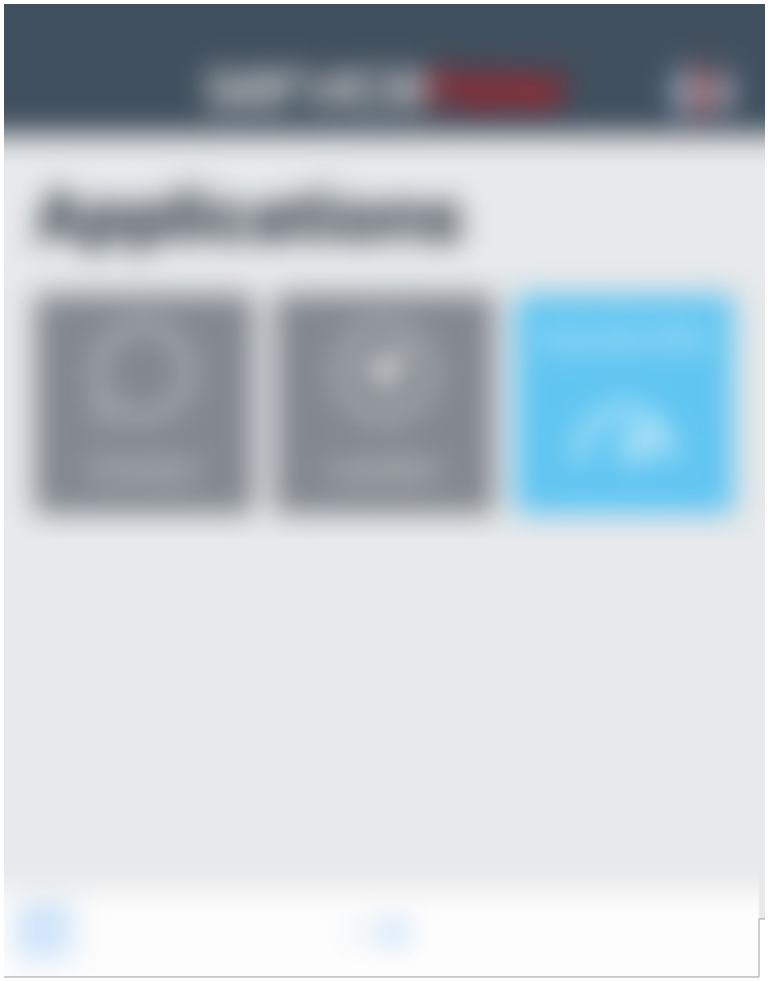
Hinweis: Diese Einstellung oder Konfiguration gilt pro Instanz, daher muss der Anwender eine Verbindung zur Instanz mit der konfigurierten Eigenschaft herstellen.

Informationen zum Verschleiern aller Felder aus dem Snapshot in der ServiceNow Classic-App finden Sie unter Option zum Unscharfmachen von Apps konfigurieren, um die Sicherheit zu verbessern .

Beispiel

Wenn Sie diese Eigenschaft auf true] festlegen, wird die Hintergrundanwendung bfür iOS-Geräte verschleiert und für Android-iOS-Geräte gesperrt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Weitere Informationen

Attribut	Beschreibung
Eigenschafts-/Plugin-Name	*glide.ui.m.blur_ui_when_backgrounded*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Dient zum Verschleiern aller Felder des Snapshots, da das Bild während des Hintergrundprozesses gespeichert wird.
Empfohlener Wert	wahr
Sicherheitsrisikobewertung	2.4
Funktionale Auswirkung	(Niedrig) Wenn die Eigenschaft *glide.ui.m.blur_ui_when_backgrounded*] auf truefestgelegt ist, verwenden die nativen Apps den auf dem Server definierten Parameter, um den Bildschirm unscharf zu machen, wenn die App in den Hintergrund verschoben wird.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Die von iOS- und Android-Geräten aufgenommenen Screenshots werden unscharf, wenn die App in den Hintergrund verschoben wird. • Die Anwender-Experience kann beeinträchtigt werden, da der Inhalt nicht angezeigt wird, wenn die App im Hintergrund ausgeführt wird.
Sicherheitsrisiko	(Mittel) Ein gefährdetes Gerät (mit Jailbreak) würde einem Angreifer vollständigen Zugriff auf das Dateisystem ermöglichen, d. h. auf Dateien/Snapshots mit eingebetteten vertraulichen Informationen.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Passwortlose Authentifizierung deaktivieren

Verwenden Sie die Eigenschaft *glide.login.no_blank_password*, um zu verhindern, dass sich Anwender mit leeren Passwörtern bei der NOW Platform anmelden, oder indem Sie das Feld **Passwort** leer lassen.

Selbst wenn der Administrator absichtlich einen leeren Wert oder ein leeres Passwort in Benutzerdatensätzen zuweist, kann sich ein Anwender nicht anmelden, ohne einen Wert im Feld **Passwort** anzugeben.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.login.no_blank_password*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um eine starke Authentifizierung sicherzustellen, da der Anwendername innerhalb einer Organisation manchmal leicht zu erraten ist.
Empfohlener Wert	wahr
Funktionale Auswirkung	(Niedrig) Vorgänge sollten keine leeren Passwörter verwenden, da dies als kritisches Sicherheitsrisiko angesehen wird. Wenn jedoch ein gültiger Fall für eine solche Verwendung vorliegt, besteht die Möglichkeit eines Ausfalls. Anwender mit leeren Passwörtern können sich nicht bei der Instanz anmelden.
Sicherheitsrisiko	(Hoch) Ein Angreifer kann sich bei der Instanz mit den Standardanwendernamen oder einer bestimmten Person/Gruppe (normalerweise Vorname.Nachname) ohne Passwort anmelden. Dies wird als kritisches Sicherheitsrisiko angesehen, da ein öffentlicher Benutzer dadurch die Vertraulichkeit und Integrität der Instanzdaten verletzen könnte.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Passwortrichtlinie bei der Anmeldung nicht anwenden

Verwalten Sie, wie die Passwortkomplexität in Ihrer Instanz gehandhabt wird.

Verwenden Sie die Eigenschaft und *glide.apply.password_policy.on_login*, um die Passwortkomplexität zu verwalten. Wenn diese Eigenschaft auf **„false“**festgelegt ist, wird während der Anmeldung keine Passwortkomplexität erzwungen. Wenn auf „ **wahr**“ festgelegt, wird Passwortkomplexität erzwungen, was zu Problemen mit der Compliance mit Organisationsrichtlinien führen kann. Anstatt die Passwortkomplexität zu erzwingen, schlägt der Application Security Verification Standard (ASVS) vor, eine Mindestlänge von12 Zeichen für das Passwort zu erzwingen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.apply.password_policy.on_login*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	falsch
Standardwert	falsch
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 4.4 • CVSS-Punktzahl: Mittel • Details zu Sicherheitsrisiken: Das Festlegen dieser Eigenschaft auf „ **wahr** “ kann die Passwortkomplexität erzwingen und zu Compliance-Problemen der Organisation führen.
Abhängigkeiten und Voraussetzungen	Keine

Aktivieren Sie eine Passwortvalidierungsprüfung für die Deny-Liste

Verwalten Sie die Passwörter der Deny-Liste in der Tabelle „Ausgeschlossene Passwörter“.

Verwenden Sie die Eigenschaft *glide.enable.blacklist_password*, um Passwörter auf der Deny-Liste zu überwachen. Wenn die Eigenschaft auf **true**festgelegt ist, wird das Passwort des Benutzers mit einer Liste von Passwörtern auf der Deny-Liste verglichen, um zu verhindern, dass er ein Passwort aus einer Reihe von Passwörtern mit Verstößen verwendet. Der Administrator kann die Liste verwalten, indem er Passwörter in die Tabelle „Ausgeschlossene Passwörter“ einfügt.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.enable.blacklist_password*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Authentifizierung
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Ausschließen von Passwörtern über Passwortrichtlinien in Ihrer Instanz

Captcha für die Registrierung externer Anwender aktivieren [Aktualisiert in Security Center 1.5]

sn_ext_usr_reg.captchaEnabled steuert, ob CAPTCHA für die Registrierung externer Anwender validiert wird.

Legen Sie *sn_ext_usr_reg.captchaEnabled* auf den empfohlenen Wert „ **wahr** “ fest, um automatische Angriffe auf die Kontoerstellung zu verhindern, die CAPTCHA für die Registrierung externer Anwender erfordern. Legen Sie den Wert auf „ **falsch** “ fest, um CAPTCHA für die Registrierung externer Anwender nicht zu erfordern.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*sn_ext_usr_reg.captchaEnabled*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Diese Eigenschaft wird verwendet, um die CAPTCHA-Validierung während der Registrierung externer Anwender in Portalen wie CSP und Community zu aktivieren oder zu deaktivieren. Dies wird auch in Store-Apps wie VAM und CSM Gast-Walkup verwendet, um Captcha zu aktivieren/deaktivieren.
Empfohlener Wert	True
Konfigurationstyp	Boolean
Sicherheitsrisiko	(Niedrig) Die Eigenschaft steuert die CAPTCHA-Aktivierung bei der Registrierung externer Anwender. Ein unidealer Wert kann zu einer Sicherheitsschwachstelle führen.
Sicherheitsrisikobewertung	3.7

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktivieren Sie CAPTCHA bei der Passwortzurücksetzung

Verwenden Sie die Eigenschaft *password_reset.captcha.ignore*, um das Erfordernis einer CAPTCHA-Abfrage zu aktivieren oder zu deaktivieren, wenn ein Benutzer sein Passwort zurücksetzt.

Legen Sie *password_reset.captcha.ignore* auf den empfohlenen Wert „ **falsch** “ fest, um eine CAPTCHA-Abfrage zum Zurücksetzen des Passworts eines Anwenders zu erfordern. Legen Sie den Wert auf „ **wahr** “ fest, um die CAPTCHA-Option für die Passwortzurücksetzung zu ignorieren.

CAPTCHAs helfen, Automatisierungsangriffe zu verhindern, indem sie den Anwender zu einer Abfrageantwort auffordern, die von automatisierten Systemen nicht einfach beantwortet werden kann. Wenn CAPTCHA deaktiviert ist, kann ein Angreifer während automatisierter Angriffe auf die Funktion zum Zurücksetzen des Passworts erfolgreicher sein.

Hinweis: Diese Eigenschaft wird nur für die Automatisierung der Passwortzurücksetzung verwendet.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*password_reset.captcha.ignore*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Diese Eigenschaft wird verwendet, um die CAPTCHA-Validierung während der Passwortzurücksetzung zu aktivieren oder zu deaktivieren.
Empfohlener Wert	falsch
Konfigurationstyp	Boolean
Sicherheitsrisiko	(Moderat) Ein unidealer Wert kann zu einer Sicherheitsschwachstelle führen.
Sicherheitsrisikobewertung	5.5

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Aktivieren Sie E-Mail-OTP für die Multifaktor-Authentifizierung

Verwalten Sie, wie die Zwei-Faktor-Authentifizierung auf Ihre Instanz angewendet wird.

Verwenden Sie die Eigenschaft [bisund *glide.authenticate.multifactor.email.otp.enabled*, um zu steuern, ob ein Token für die Zwei-Faktor-Authentifizierung per E-Mail gesendet wird. E-Mail wird als schwacher MFA-Faktor betrachtet, auf den sich ein Angreifer unter Umgehung der MFA mit größerer Wahrscheinlichkeit Zugriff verschafft. Durch Festlegen dieser Eigenschaft auf „ **false**“ wird das Risiko reduziert, dass ein Angreifer die MFA umgeht, wenn er das Passwort eines Anwenders gefährdet hat.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.authenticate.multifactor.email.otp.enabled*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	falsch
Standardwert	wahr
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 3,1 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn Sie diese Eigenschaft auf **„false** “ festlegen, verringert sich das Risiko, dass ein böswilliger Akteur die Zwei-Faktor-Authentifizierung umgeht.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Mehrstufige Authentifizierung mit E-Mail

Richtlinienprüfungen für die Passwortzurücksetzung aktivieren

Verwenden Sie die Eigenschaft **„glide.enable.password_policy“**, um Prüfungen der Passwortrichtlinie zu aktivieren, wenn ein Benutzer sein Passwort über die Anwenderoberfläche ändert.

Um zu definieren, welche Passwortrichtlinie verwendet werden soll, sobald diese Eigenschaft aktiviert ist, siehe Passwortrichtlinien für Ihre Instanz aktivieren.

Hinweis: **glide.enable.password_policy** gilt nicht, wenn ein Administrator ein Passwort ändert oder einen Anwender über ein Skript hinzufügt.

Warnung: Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.enable.password_policy*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Zum Anwenden der Passwortrichtlinie zum Zeitpunkt der Passwortänderung.
Empfohlener Wert	true (für Passwörter mit höherer Sicherheit)

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisikobewertung	7.4
Funktionale Auswirkung	(Mittel) Wenn Sie die Eigenschaft auf „true“ setzen, werden Passwortrichtlinienprüfungen aktiviert, wenn ein Benutzer sein Passwort zurücksetzt.
Sicherheitsrisiko	(Mittel) Ohne eine Passwortrichtlinie kann ein Anwender ein schwaches Passwort erstellen, was die Wahrscheinlichkeit erhöht, dass ein Angreifer Zugriff auf die Instanz erhält.

Schritte zum Konfigurieren von

Wenn Sie diese Einstellung auf der Seite „Konfiguration der Härtungscompliance“ im Instanz-Sicherheitszentrum konfigurieren:

1. Wählen Sie unter **Mittel**die Option **Management**von Sitzungen aus.
2. **Wählen Sie in der Einstellung Richtlinienprüfung für Passwortzurücksetzung aktivieren** die Option **Mittel** für Passwörter mit mittlerer Stärke oder **Stark** für robustere Passwörter mit höherer Stärke aus. Wenn Sie eine dieser Optionen auswählen, wird die Eigenschaft **„glide.enable.password_policy“** auf „true“ festgelegt und ein Workflow gestartet, der Ihre Passwortrichtlinie automatisch aktualisiert.

Darüber hinaus können Sie die Systemeigenschaft *glide.apply.password_policy.on_login* festlegen, um Prüfungen der Passwortrichtlinie zum Zeitpunkt der Anmeldung zu ermöglichen.

Richtlinienbasierten Sitzungszugriff für Mobilgeräte aktivieren [Neu in Security Center 1.5]

Verwenden Sie das Plugin „The Zero Trust – Richtlinienbasierter Sitzungszugriff“, um zu steuern, ob die Rollen von Anwendern, die sich über eine mobile App authentifizieren, eingeschränkt werden.

Mit dem Plugin „Zero Trust – Richtlinienbasierter Sitzungszugriff“ können Sicherheitsadministratoren den Benutzerzugriff in einer Sitzung basierend auf Parametern wie IP-Adresse, Standort, Provider-Attribute und Benutzerattribute mit adaptiven Authentifizierungsrichtlinien reduzieren. Wenn dieses Plugin aktiviert oder auf „wahr“ festgelegt ist, werden die Rollen von Anwendern, die sich über ein Mobilgerät authentifizieren, gemäß den Richtlinien des Plugins eingeschränkt. Instanzadministratoren möchten möglicherweise den Zugriff mit hohen Berechtigungen einschränken, wenn sich Anwender über ein Mobilgerät authentifizieren, da dies auf eine unsichere Umgebung für vertrauliche Vorgänge hinweisen könnte.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.authenticate.session_access.mobile.enabled*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	wahr

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 4,7 • CVSS-Punktzahl: Mittel • Details zu Sicherheitsrisiken: Wenn diese Härtungseinstellung auf „true“ festgelegt ist, wird der richtlinienbasierte Sitzungszugriff auf die Instanz für mobile Anmeldungen erzwungen, und für Anwender, die nicht aus einer vertrauenswürdigen Umgebung stammen oder keine vertrauenswürdigen Geräte verwenden, werden die Rollen von reduziert Berechtigungen. „Wahr“ ist die sichere Einstellung. Wenn diese Einstellung auf „falsch“ konfiguriert ist, wird der richtlinienbasierte Sitzungszugriff deaktiviert, und die Anwender verfügen weiterhin über vollständige Rollen, einschließlich der Rollen mit hohen Berechtigungen wie „admin“.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Wenn der Administrator die Richtlinie für den Sitzungszugriff in der Instanz konfiguriert hat, werden die Rollen von Benutzern nach der mobilen Anmeldung reduziert, wenn sie nicht aus einer vertrauenswürdigen Umgebung stammen oder kein vertrauenswürdiges Gerät verwenden.
Referenzen	Adaptive Authentifizierung

Aktivieren Sie SSL in der LDAP-Authentifizierung

Verwalten Sie die Verschlüsselung von LDAP-Authentifizierungsanforderungen in Ihrer -Instanz.

Verwenden Sie die Eigenschaft und *`glide.ldap.use.ssl`*, um die TLS-Verschlüsselung für LDAP-Authentifizierungsanforderungen zu aktivieren oder zu deaktivieren, die über das Netzwerk gesendet werden. Wenn diese Eigenschaft nicht auf den empfohlenen Wert **true**festgelegt ist, ist die LDAP-Authentifizierung anfällig für Man-in-the-Middle-Angriffe.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*`glide.ldap.use.ssl`*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Authentifizierung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	• Bewertung mit Schweregrad: 8,1 • CVSS-Punktzahl: Hoch • Details zu Sicherheitsrisiken: Wenn Sie diese Eigenschaft auf „ **false**“ setzen, wird die LDAP-Authentifizierung für einen Man-in-the-Middle-Angriff angreifbar.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	LDAP-Integration

Ablaufdauer des Links zur Registrierung externer Anwender minimieren [Aktualisiert in Security Center 1.3 und 1.5]

Verwalten Sie die Anzahl der Tage, an denen auf einen Registrierungslink zugegriffen werden kann.

Verwenden Sie die Eigenschaft *sn_ext_usr_reg.Reg_link_expiration_days*, um zu verwalten, wer auf einen Registrierungslink zugreifen kann. Wenn für den Link der empfohlene Wert **3**festgelegt ist, kann ein Registrierungslink von einer anderen Person als dem vorgesehenen Benutzer verwendet werden, wenn der Link zu einem späteren Zeitpunkt erkannt wird.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*sn_ext_usr_reg.Reg_link_expiration_days*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Ganzzahl
Empfohlener Wert	3
Standardwert	3
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregrad-Punktzahl: Mittel • CVSS-Punktzahl: 6,6 • Details zum Sicherheitsrisiko: Wenn Sie diese Eigenschaft nicht auf die Ganzzahl 3 festlegen, kann dies dazu führen, dass der Registrierungslink von einem unbeabsichtigten Anwender verwendet wird.
Abhängigkeiten und Voraussetzungen	Keine

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fehlgeschlagene Anmeldungsversuche werden verwaltet

Es sind zwei Skriptaktionen verfügbar, mit denen ein Site-Administrator verwalten kann, wie oft ein Benutzer ein falsches Passwort eingeben kann, bevor er von Now Platformgesperrt wird. Sie können eine dieser Skriptaktionen aktivieren, um fehlgeschlagene Anmeldungsversuche zu verwalten.

Weitere Informationen

Attribut	Beschreibung
Eigenschafts-/Plugin-Name	N/V
Konfigurationstyp	Systemrichtlinie > Skriptaktionen
Kategorie	Authentifizierung
Zweck	Um eine strikte Richtlinie für fehlgeschlagene Anmeldungsversuche zu erzwingen, um das Brute-Forcing von Anmeldeinformationen zu vermeiden.
Empfohlener Wert	Aktiv
Sicherheitsrisikobewertung	7.3
Funktionale Auswirkung	(Niedrig) Diese Korrektur würde es dem Administrator der Instanz ermöglichen, böswilligen Anwenderzugriff zu überwachen und zu melden. Keine Auswirkung auf die Funktionalität, nur Änderung der Anwender-Experience.
Sicherheitsrisiko	(Moderat) Wenden Sie eine definierte Protokollierungs- und Auditstrategie an, damit Sie verdächtige Aktivitäten rechtzeitig erkennen und entsprechende Maßnahmen ergreifen können.

Schritte zum Konfigurieren von

1. Navigieren zu **Systemrichtlinie** > **Skriptaktionen.**
2. Suchen Sie nach dem Namen *`*SNC User`*.
3. Um die Verwaltung fehlgeschlagener Anmeldungsversuche zu ermöglichen, ändern Sie den Status Aktiv der Skriptaktionen *`SNC User Lockout Check with Auto Unlock`* oder *`SNC User Lockout Check`* von **false** in **true**.
4. Um den Zähler für fehlgeschlagene Anmeldungen nach einer erfolgreichen Anmeldung zurückzusetzen, können Sie die Skriptaktion *`SNC User Clear`* aktivieren.

Zeitüberschreitungsdauer beim Entsperren bei fehlgeschlagener Anmeldung maximieren [Aktualisiert in Security Center 1.3]

Es sind zwei Skriptaktionen verfügbar, mit denen ein Site-Administrator verwalten kann, wie oft ein Benutzer ein falsches Passwort eingeben kann, bevor er von Now Platformgesperrt wird. Sie können eine dieser Skriptaktionen aktivieren, um fehlgeschlagene Anmeldungsversuche zu verwalten.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.user.unlock_timeout_in_mins*
Konfigurationstyp	Systemrichtlinie > Skriptaktionen
Kategorie	Authentifizierung
Zweck	Um eine strikte Richtlinie für fehlgeschlagene Anmeldungsversuche zu erzwingen, um das Brute-Forcing von Anmeldeinformationen zu vermeiden.
Empfohlener Wert	Aktiv
Funktionale Auswirkung	(Niedrig) Diese Korrektur würde es dem Administrator der Instanz ermöglichen, böswilligen Anwenderzugriff zu überwachen und zu melden. Keine Auswirkung auf die Funktionalität, nur Änderung der Anwender-Experience.
Sicherheitsrisiko	(Moderat) Wenden Sie eine definierte Protokollierungs- und Auditstrategie an, damit Sie verdächtige Aktivitäten rechtzeitig erkennen und entsprechende Maßnahmen ergreifen können.

Schritte zum Konfigurieren von

1. Navigieren zu **Systemrichtlinie** > **Skriptaktionen.**
2. Suchen Sie nach dem Namen **SNC User*.
3. Um die Verwaltung fehlgeschlagener Anmeldungsversuche zu ermöglichen, ändern Sie den Status Aktiv der Skriptaktionen *SNC User Lockout Check with Auto Unlock* oder *SNC User Lockout Check* von **false** in **true**.
4. Um den Zähler für fehlgeschlagene Anmeldungen nach einer erfolgreichen Anmeldung zurückzusetzen, können Sie die Skriptaktion *SNC User Clear* aktivieren.

Verschleierung der Mobile-App-UI erfordern [Aktualisiert in Security Center 1.3]

Konfigurieren Sie die Eigenschaft mit demund *glide.sg.blur_ui_when_backgrounded*so, dass die Anwenderoberfläche der App unscharf ist, wenn die App im Hintergrund ausgeführt wird.

Wenn diese Eigenschaft nicht auf den empfohlenen Wert **true**festgelegt ist, ist die Anwenderoberfläche der mobilen App bei Ansicht über den App-Umschalter sichtbar. Die Anwenderoberfläche ist auch dann sichtbar, wenn die App im Hintergrund ausgeführt wird, was für Endanwender ein geringeres Maß an Sicherheit und Vertraulichkeit bietet.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.sg.blur_ui_when_backgrounded*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Datei und Ressourcen
Sicherheitsrisiko	• Schweregrad-Punktzahl: 2,4 • CVSS-Punktzahl: Niedrig • Details zu Sicherheitsrisiken: Wenn Sie den Wert auf „ **true** “ festlegen, wird ein höheres Maß an Vertraulichkeit und Datenschutz auf dem lokalen Gerät erreicht, indem die Anwenderoberfläche unscharf dargestellt wird, wenn die App im Hintergrund ausgeführt wird.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Verschleierung der mobilen Anwenderoberfläche

Benachrichtigen Sie Anwender während des Prozesses zum Zurücksetzen/Ändern des Passworts

Verwenden Sie die Eigenschaft für, damit Endanwender Passwörter mithilfe eines Selfservice-Prozesses zurücksetzen oder ändern können.

Diese Eigenschaft ermöglicht es einem Endanwender, ein Passwort mithilfe eines Selfservice-Prozesses zurückzusetzen oder zu ändern. Alternativ kann Ihre Organisation einen Prozess implementieren, bei dem ein Service Desk-Mitarbeiter Passwörter für Endanwender zurücksetzen muss. Wenn ein Prozess zum Ändern und/oder Zurücksetzen des Passworts Anwender nicht über die Passwortaktualisierung benachrichtigt, kann ein böswilliger Akteur diesen Anwender möglicherweise ohne sein Wissen für seinen Account sperren. Dies würde dem böswilligen Akteur mehr Zeit für böswillige Aktivitäten geben. Stellen Sie sicher, dass der Prozess zum Zurücksetzen des Passworts Anwender benachrichtigt, wenn das Passwort geändert oder zurückgesetzt wird.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*pwd_process.change, pwd_process.reset*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Authentifizierung
Sicherheitsrisiko	• Bewertung mit Schweregrad: 8,1 • CVSS-Punktzahl: Hoch

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Details zum Sicherheitsrisiko: Ein böswilliger Akteur kann einen Anwender ohne dessen Wissen für seinen Account sperren, wenn nach dem Zurücksetzen des Passworts keine Benachrichtigung an ihn gesendet wird.
Abhängigkeiten und Voraussetzungen	Keine

Entfernen Sie die Anmeldeinformationen von der Willkommensseite

Ändern Sie den Standardinhalt auf der Willkommensseite, um die Standardanmeldeinformationen zu entfernen.

Zwei **Anmeldedatensätze** werden als Teil der Demodaten für das CMS-Plugin installiert.

Hinweis: Wenn Sie die Demodaten für eine Instanz nicht installieren, sind diese Datensätze nicht vorhanden. In diesem Fall gilt die Konfiguration als sicherheitskonform gemäß den empfohlenen Sicherheitspraktiken.

Weitere Informationen

Attribut	Beschreibung
Name	*How to login*
Konfigurationstyp	Tabelle: sys_home
Kategorie	Authentifizierung
Zweck	Zum Entfernen von Standardanmeldeinformationen von der Willkommensseite, die mit Demodaten hinzugefügt wurden.
Empfohlener Wert	Falsch oder NULL, wenn keine Demodaten verwendet wurden.
Standardwert	Keine. Dies ist eine Tabellenkonfiguration, keine Glide-Eigenschaft. Daher ist kein Wert für den Standardwert vorhanden.
Konfigurationstyp	Boolean
Sicherheitsrisiko	(Moderat) Demodaten werden für das CMS-Plugin bereitgestellt, das zwei Standardpasswörter enthält, die auf der Willkommensseite enthalten sind. Wenn dies nicht entfernt wird, könnte ein nicht autorisierter Angreifer Zugriff auf die Instanz erhalten.
Referenzen	https://support.servicenow.com/kb_view.do?sysparm_article=KB0550107 Willkommensseiten

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Max. SMS pro Tag für die Passwortzurücksetzung minimieren [Aktualisiert in Security Center 1.3]

Verwalten Sie die maximale Anzahl an SMS-Codes, die pro Tag vom Anwender zur Verifizierung gesendet werden.

Die Eigenschaftund *password_reset.sms.max_per_day* stellt die maximale Anzahl von SMS-Codes dar, die täglich von einem Benutzer zur Verifizierung gesendet werden können.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*password_reset.sms.max_per_day*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer
Empfohlener Wert	10
Standardwert	10
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 5,9 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf den empfohlenen Wert von **10** oder weniger festgelegt ist, ist es einfacher, den SMS-Code mit Brute-Force zu erzwingen.
Abhängigkeiten und Voraussetzungen	Keine

Ablaufdauer für die Anforderung einer Passwortzurücksetzung minimieren [Aktualisiert in Security Center 1.3]

password_reset.request.expiry gibt den Zeitraum in Minuten an, in dem ein Benutzer den Prozess zum Zurücksetzen des Passworts durchführen muss.

Hinweis: Die Einstellung für die Eigenschaft *password_reset.request.expiry* hat Vorrang vor der Einstellung für die Eigenschaft *glide.pwd_reset.onetime.token.validity*, die standardmäßig einen 12-Stunden-Wert hat.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*password_reset.request.expiry*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Zweck	Gibt den Zeitraum in Minuten an, in dem ein Benutzer den Prozess zum Zurücksetzen des Passworts durchführen muss.
Empfohlener Wert	Legen Sie eine Ganzzahl von **10** oder weniger fest. Der Standardwert ist 10.
Konfigurationstyp	Ganzzahlwerte
Sicherheitsrisiko	(Mittel) Wenn die Eigenschaft nicht auf den empfohlenen Wert von 10 oder weniger festgelegt ist, erhöht dies die Möglichkeit für andere, die Anforderung zu erraten und zu verwenden und zu versuchen, das Passwort zurückzusetzen.
Sicherheitsrisikobewertung	4.2
Referenzen	Konfigurieren Sie Eigenschaften für die Passwortzurücksetzung

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Maximale Versuchsanzahl für die Anforderung einer Passwortzurücksetzung minimieren [Aktualisiert in Security Center 1.3]

password_reset.request.max_attempt wird verwendet, um die maximale Anzahl der Fehlversuche zu steuern, die ein Benutzer durchführen kann, um sein Passwort zurückzusetzen oder zu ändern, bevor er für einen bestimmten Zeitraum gesperrt wird.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*password_reset.request.max_attempt*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Gibt die maximale Anzahl der fehlgeschlagenen Versuche zum Zurücksetzen des Passworts an, bevor der Anwender für den Prozess zum Zurücksetzen des Passworts gesperrt wird. Der Sperrzeitraum wird durch den Wert in *password_reset.request.max_attempt_window* bestimmt.
Empfohlener Wert	Legen Sie dies auf einen positiven ganzzahligen Wert kleiner als drei fest. Der Standardwert ist **3**. Wenn Sie den Grenzwert für den oberen Bereich der Eigenschaft bestimmen, berücksichtigen Sie die Aufgabe, die der Benutzer ausführt.
Konfigurationstyp	Positive ganzzahlige Werte
Sicherheitsrisiko	(Hoch) Wenn die Eigenschaft nicht auf den empfohlenen Wert „**3**“ oder einen anderen angemessen kleinen Wert festgelegt ist, kann ein

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Brute-Force-Angriff auf den Prozess zum Zurücksetzen des Passworts durchgeführt werden.
Sicherheitsrisikobewertung	7.5
Referenzen	Konfigurieren Sie Eigenschaften für die Passwortzurücksetzung

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Fensterdauer bei maximalen Versuchen für die Anforderung einer Passwortzurücksetzung minimieren [Aktualisiert in Security Center 1.3]

Die Eigenschaft *password_reset.request.max_attempt_window* steuert die Anzahl der Minuten, die ein Benutzer warten muss, um sein Passwort zurückzusetzen oder zu ändern, nachdem die maximale Anzahl von Fehlversuchen überschritten wurde, die mit der Eigenschaft *password_reset.request.max_attempt* festgelegt wurde.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*password_reset.request.max_attempt_window*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Gibt den Sperrzeitraum in Minuten an, nachdem die maximale Anzahl erfolgloser Versuche zum Zurücksetzen des Passworts erreicht wurde.
Empfohlener Wert	1440
Standardwert	1440
Konfigurationstyp	Positive ganzzahlige Werte
Sicherheitsrisiko	(Hoch) Wenn die Eigenschaft nicht auf den empfohlenen Wert von 1440 oder weniger festgelegt ist, kann es möglich sein, Account-Brute-Force auszuführen, da der Account nach einer maximalen Anzahl falscher Authentifizierungsversuche nicht gesperrt wird.
Sicherheitsrisikobewertung	7.5
Referenzen	Konfigurieren Sie Eigenschaften für die Passwortzurücksetzung

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Wiederholungsfensterdauer für die Anforderung einer Passwortzurücksetzung maximieren [Aktualisiert in Security Center 1.3]

Die Eigenschaft *password_reset.request.retry_window* steuert die Anzahl der Minuten, bis die Anzahl der Versuche zum Zurücksetzen des Passworts aktualisiert wird.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*password_reset.request.retry_window*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Gibt die Zeit in Minuten an, nach der die Anzahl der Passwortversuche von der letzten Anforderung aktualisiert wird, bevor die Anzahl der Wiederholungen auf Null zurückgesetzt wird.
Empfohlener Wert	Legen Sie dies auf einen positiven ganzzahligen Wert von **mindestens 1440** fest. Der Standardwert beträgt **1440** Minuten.
Konfigurationstyp	Positive ganzzahlige Werte.
Sicherheitsrisiko	(Hoch) Wenn die Eigenschaft nicht auf den empfohlenen Wert von 1440 oder mehr festgelegt ist, kann es möglich sein, Account-Brute-Force gegen Prozess zum Zurücksetzen des Passworts auszuführen.
Sicherheitsrisikobewertung	7.5
Referenzen	Konfigurieren Sie Eigenschaften für die Passwortzurücksetzung

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Fensterdauer bei erfolgreicher Anforderung einer Passwortzurücksetzung minimieren [Aktualisiert in Security Center 1.3]

Die Eigenschaft *password_reset.request.success_window* steuert die Anzahl der Minuten, die ein Benutzer warten muss, um sein Passwort erneut zurückzusetzen oder zu ändern, nachdem das Passwort erfolgreich zurückgesetzt wurde. Der Anwender wird für die angegebene Dauer daran gehindert, das Passwort erneut zurückzusetzen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*password_reset.request.success_window*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Sie gibt den Zeitraum in Minuten an, den ein Benutzer nach dem erfolgreichen Zurücksetzen des Passworts warten muss, um das Passwort erneut zurückzusetzen.
Empfohlener Wert	1440
Standardwert	1440
Konfigurationstyp	Positive ganzzahlige Werte

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	(Hoch) Wenn die Eigenschaft nicht auf den empfohlenen Wert von maximal 1440 festgelegt ist, erhöht dies die Wahrscheinlichkeit, dass jemand anderes die Funktion zum Zurücksetzen des Passworts missbraucht, um sich nicht autorisierten Zugriff auf ein Anwenderkonto zu verschaffen.
Sicherheitsrisikobewertung	4.9
Referenzen	Konfigurieren Sie Eigenschaften für die Passwortzurücksetzung

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Fensterdauer beim Entsperren für Anforderung zum Zurücksetzen des Passworts maximieren [Aktualisiert in Security Center 1.3]

Die Eigenschaft *password_reset.request.unlock_window* steuert die Anzahl der Minuten, die ein Benutzer nach der letzten erfolgreichen Aktion zum Entsperren eines Accounts warten muss, um eine Zurücksetzungsanforderung zu starten.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*password_reset.request.unlock_window*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Sie gibt den Zeitraum in Minuten an, den ein Benutzer nach dem erfolgreichen Zurücksetzen des Passworts warten muss, um das Passwort erneut zurückzusetzen.
Empfohlener Wert	1440
Standardwert	1440
Konfigurationstyp	Positive ganzzahlige Werte
Sicherheitsrisiko	(Hoch) Wenn die Eigenschaft nicht auf den empfohlenen Wert von 1440 oder höher festgelegt ist, erhöht sie die Möglichkeit eines böswilligen Akteurs, mit automatischen Tools Brute-Force-Passwortzugriff durchzuführen.
Sicherheitsrisikobewertung	5.9
Referenzen	Konfigurieren Sie Eigenschaften für die Passwortzurücksetzung

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SMS- Komplexität bei der Passwortzurücksetzung maximieren [Aktualisiert in Security Center 1.3]

Die Eigenschaft *password_reset.sms.default_complexity* steuert die erforderliche Mindestgröße für die SMS-Codeüberprüfung, die beim Zurücksetzen des Passworts erforderlich ist.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*password_reset.sms.default_complexity*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Gibt die Größe der SMS-Codeüberprüfung an, die beim Zurücksetzen des Passworts erforderlich ist.
Empfohlener Wert	6
Standardwert	4
Konfigurationstyp	Ganzzahliger Wert größer als null
Sicherheitsrisiko	(Niedrig) Wenn die Eigenschaft nicht auf den empfohlenen Wert festgelegt ist, wird ein schwaches SMS-Validierungstoken verwendet. Dies erhöht die Wahrscheinlichkeit, dass Token erraten werden, was zu einer Account-Übernahme führen könnte.
Sicherheitsrisikobewertung	3.8

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

SMS-Ablaufzeit bei Passwortzurücksetzung minimieren [Aktualisiert in Security Center 1.3]

Steuern Sie die Anzahl der verbleibenden Minuten, bis der SMS-Code abläuft.

Die Eigenschaftund *password_reset.sms.expiry* gibt die Anzahl der Minuten an, bis der SMS-Code abläuft.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*password_reset.sms.expiry*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer
Empfohlener Wert	5
Standardwert	5
Kategorie	Authentifizierung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 5,6 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf den empfohlenen Wert von **5** oder weniger festgelegt ist, erhöht sich die Wahrscheinlichkeit, dass ein böswilliger Akteur den SMS-Code errät und zum Zurücksetzen des Passworts verwendet.
Abhängigkeiten und Voraussetzungen	Keine

Fensterdauer bei SMS-Pause für Passwortzurücksetzung maximieren [Aktualisiert in Security Center 1.3]

Verwalten Sie die Zeitdauer in Minuten, die ein Anwender warten muss, bevor er einen neuen Code zur Passwortzurücksetzung anfordern kann.

Wenn diese Eigenschaft nicht auf den empfohlenen Wert von mindestens **2** Minuten festgelegt ist, kann ein böswilliger Anwender in einem kurzen Zeitfenster viele Passwortzurücksetzungscodes initiieren. Dies erhöht die Wahrscheinlichkeit, dass ein schlechter Akteur den SMS-Zurücksetzungscode vorhersagt.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*password_reset.sms.pause_window*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer
Empfohlener Wert	2
Standardwert	2
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 4,8 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Stellen Sie sicher, dass *password_reset.sms.pause_window* auf mindestens 2 festgelegt ist.
Abhängigkeiten und Voraussetzungen	Keine

Verzögerungsdauer für die Verifizierung der Verifizierung der Passwortzurücksetzung maximieren [Aktualisiert in Security Center 1.3]

Konfigurieren Sie die Verzögerung in Millisekunden, die ein Anwender warten muss, bevor eine neue Anforderung zur Passwortzurücksetzung gesendet wird.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein böswilliger Akteur könnte versuchen, Brute-Force-Anmeldeinformationen mithilfe von Automatisierungstools wie Bots zu erzwingen, gegen die die **Verzögerungseigenschaft der Verifizierung der Passwortzurücksetzung** verteidigt. Der Eigenschaftswert stellt die Verzögerung in Millisekunden dar, die ein Benutzer warten muss, bevor er eine Anforderung zum Zurücksetzen des Passworts stellen kann. Wenn diese Eigenschaft nicht auf den empfohlenen Wert von **mindestens 1000** festgelegt ist, ist die Anmeldung anfälliger für Brute-Force-Angriffe.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*password_reset.verification.delay*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	1000
Standardwert	1000
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 5,9 • CVSS-Punktzahl: Mittel • Details zu Sicherheitsrisiken: Wenn Sie den Eigenschaftswert auf weniger als 1000 festlegen, wird Ihre Anmeldung anfälliger für Brute-Force-Angriffe.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Passwort für einen Benutzer konfigurieren

SAML-Dauer von „notBefore“ und „notOnOrAfter“ minimieren [Aktualisiert in Security Center 1.3 und 1.5]

Konfigurieren Sie diese Eigenschaft, um einen Toleranzzeitraum hinzuzufügen, in dem SAML-Anforderungen und -Antworten als gültig betrachtet werden.

Diese Eigenschaft fügt einen Toleranzzeitraum hinzu, während dessen SAML-Anforderungen und -Antworten als gültig betrachtet werden. Der Eigenschaftswert stellt die Anzahl der Sekunden dar, die den Einschränkungen *NotBefore* und *NotOnOrAfter* hinzugefügt werden sollen, um Zeitunterschiede zwischen der Uhr des Identitätsanbieters (IdP) und der Uhr des Service Providers (SP) zu berücksichtigen. Diese Einschränkungen schützen vor Replay-Angriffen, indem sie Anforderungen ablehnen, die nicht innerhalb des angegebenen Zeitrahmens gestellt werden. Wenn sich die IdP- und SP-Uhren erheblich unterscheiden, kann die Netzwerklatenz dazu führen, dass die SAML-Anforderung nicht autorisiert ist.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.authenticate.sso.saml2.clockskew*

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	Weniger als 60
Standardwert	180
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 7,5 • CVSS-Punktzahl: Hoch • Details zum Sicherheitsrisiko: Das Festlegen des Eigenschaftswerts auf oder höher als 60 kann verhindern, dass die Einschränkungen gegen Wiederholungsangriffe schützen.
Abhängigkeiten und Voraussetzungen	Keine

Erstellen von Anwendern aus eingehenden E-Mails deaktivieren [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.user.trusted_domain*, um die kommagetrennte Liste der vertrauenswürdigen Domänen anzugeben, die bei der Erstellung von Anwendern aus eingehenden E-Mails verwendet wird.

Ein Administrator kann eine E-Mail-Eigenschaft so festlegen, dass Benutzer automatisch aus eingehenden E-Mails erstellt werden. Wenn diese Eigenschaft auf den unsicheren Wert festgelegt ist, erstellt die Instanz automatisch Anwender aus eingehenden E-Mails. Jeder erstellte Anwender hat das gleiche hartcodierte Standardpasswort, was das Umgehen der Authentifizierung durch Brute-Force erleichtert.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.pop3readerjob.create_caller*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Empfohlener Wert	falsch
Standardwert	falsch
Sicherheitsrisikobewertung	5.4
Funktionale Auswirkung	(Mittel) Sobald diese Eigenschaft konfiguriert ist, akzeptiert die Instanz nur E-Mails von vertrauenswürdigen Domänen. Wenn Sie die Domäne nicht in die Liste der vertrauenswürdigen Domänen aufnehmen, hat dies Auswirkungen auf Gastbenutzer, da Konten automatisch erstellt werden.
Sicherheitsrisiko	(Mittel) Wenn die Eigenschaft nicht aktiviert ist, kann ein Angreifer eine E-Mail-Spoofing-/Spam-Kampagne

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	verwenden, um mehrere E-Mails zu senden, was zur Erstellung weiterer unnötiger Gastbenutzer führt.
Referenzen	Konfiguration für eingehende E-Mails

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Rollenbasierte Multifaktor-Authentifizierung aktivieren [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.authenticate.multifactor*, um die rollenbasierte Multifaktor-Authentifizierung (MFA) für alle Benutzer zu erzwingen, die bestimmten Rollen zugewiesen sind.

Erzwingen Sie die Multifaktor-Authentifizierung basierend auf den Rollen, die dem Anwender zugewiesen sind. Wenn einem Anwender in der Liste der Multifaktor-Rollen die Rollen „admin“, „security_admin“ oder „user_admin“ zugewiesen wurden, wird MFA erzwungen.

- Legen Sie diese Eigenschaft auf **„wahr** “ fest, um die rollenbasierte Multifaktor-Authentifizierung für alle Anwender zu erzwingen, die bestimmten Rollen zugewiesen sind.
- Legen Sie diese Eigenschaft auf „ **falsch** “ fest, um die rollenbasierte Multifaktor-Authentifizierung für alle Anwender zu deaktivieren, die bestimmten Rollen zugewiesen sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.authenticate.multifactor*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Erzwingen Sie die rollenbasierte Multifaktor-Authentifizierung für alle Anwender, die bestimmten Rollen zugewiesen sind.
Typ	boolean
Empfohlener Wert	*true*
Standardwert	falsch
Sicherheitsabhängigkeiten	Aktivieren **Sie die rollenbasierte Multifaktor-Authentifizierung** in der **Tabelle Multifaktor-Kriterien**.
Sicherheitsrisikobewertung	7.2
Funktionale Auswirkung	(Mittel) Durch Aktivieren dieser Eigenschaft verbessert sich die Experience des Anwenders. Sie dient als zusätzliche Schutz- und Sicherheitsebene gegen kompromittierte Anmeldeinformationen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	(Mittel) Wenn diese Eigenschaft nicht aktiviert ist, besteht das Risiko eines nicht autorisierten Zugriffs auf vertrauliche Daten.
Referenzen	Konfigurieren Sie rollenbasierte Multifaktor-Kriterien

Legen Sie die minimale Passwortlänge fest

Legen Sie die Mindestlänge für ein Benutzerpasswort in Ihrer Instanz fest.

Die Eigenschaftund *set.password.length* definiert die Mindestlänge, die für ein Passwort erforderlich ist, und wird verwendet, um die Compliance anhand der aktuellen Passwortrichtlinie zu bewerten. Der Eigenschaftswert ist eine Ganzzahl mit einem empfohlenen Mindestwert von **12**. Die Verwendung einer kürzeren Länge kann zu Compliance-Fehlern gegenüber empfohlenen Vorschriften führen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*set.password.length*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer
Empfohlener Wert	12
Standardwert	12
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 5,9 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Das Festlegen der Eigenschaft auf einen Wert kleiner als 12 kann zu Compliance-Problemen führen und erhöht das Risiko, dass ein Angreifer Passwörter erfolgreich mit Brute-Force erzwingt.
Abhängigkeiten und Voraussetzungen	Keine

Legen Sie die OTP-Lebensdauer für die Passwortzurücksetzung auf maximal 12 Stunden fest

Steuern Sie die Dauer des Links in der E-Mail zum Zurücksetzen des Passworts.

Diese Eigenschaft lässt den Link in der E-Mail zum Zurücksetzen des Passworts nach der in der Eigenschaft „Bestanden“ angegebenen Anzahl von Stunden ablaufen. Die Gültigkeit eines Passwortzurücksetzungstokens sollte so kurz wie möglich gehalten werden, ohne die normale Anwender-Experience zu beeinträchtigen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.pwd_reset.onetime.token.validity*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer
Empfohlener Wert	12
Standardwert	12
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 5,6 • CVSS-Punktzahl: Mittel • Details zu Sicherheitsrisiken: Eine lange Gültigkeit des Passwortzurücksetzungstokens erhöht die Wahrscheinlichkeit, dass ein böswilliger Akteur eine Account-Übernahme durchführt.
Abhängigkeiten und Voraussetzungen	Keine

Einmalige Lebensdauer der Verifizierung außerhalb des Bereichs minimieren [Aktualisiert in Security Center 1.3]

Verwalten Sie die Zeitdauer für Verifizierungen außerhalb des Bereichs.

Eine Out-of-Band-Verifizierung ist eine alternative Bereitstellungsmethode für einmalige Codesituationen. Beispiel: Zurücksetzen eines Multifaktor-Tokens. Wenn diese Methode von Administratoren im Plugin Multifaktor-Authentifizierung (MFA) aktiviert wird, wird ein einmaliger Code per E-Mail zugestellt. Legen Sie fest, dass die einmaligen Out-of-Band-Verifizierungen nach 10 Minuten ablaufen, um das Gültigkeitsfenster zu begrenzen. Ein größeres Zeitfenster lässt mehr Zeit, bis der Code durch illegale Mittel wie Phishing, Social Engineering oder Side-Surfing-Angriffe gefährdet ist.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.multifactor.onetime.code.validity*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer
Empfohlener Wert	10
Standardwert	10
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 3,9 • CVSS-Punktzahl: Niedrig

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Details zu Sicherheitsrisiken: Legen Sie fest, dass die einmaligen Verifizierungen außerhalb des Bereichs nach 10 Minuten ablaufen. Alles, was länger dauert, erhöht das Risiko, dass der Code durch einen böswilligen Akteur kompromittiert wird.
Abhängigkeiten und Voraussetzungen	Multifaktor-Authentifizierung (MFA)
Referenzen	

Anforderungen für Geräteverschlüsselung und Passcode erzwingen [Neu in Security Center 1.3]

Die Eigenschaft *glide.sg.device_encryption_enabled* erzwingt die Verschlüsselung nach dem Federal Information Processing Standard (FIPS 140-2). Verschlüsselung und Passcode für Mobilgeräte stellen sicher, dass ein nicht autorisierter Benutzer nicht auf den Inhalt eines Geräts zugreifen kann, auch wenn das Gerät physisch erworben wurde.

Wenn *glide.sg.device_encryption_enabled* auf „wahr" festgelegt ist, überprüft die mobile ServiceNow-App, ob die Geräteverschlüsselung und der Gerätepasscode aktiviert sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.sg.device_encryption_enabled*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 4.2 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn Verschlüsselung oder Passcode nicht aktiviert ist, kann sich der Anwender nicht mobil bei der Instanz anmelden
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Wenn diese Eigenschaft auf „wahr" festgelegt ist, überprüft die mobile App, ob die Geräteverschlüsselung aktiviert ist. Wenn die Verschlüsselung nicht aktiviert ist, können sich Anwender nicht auf Mobilgeräten bei der aktuellen Instanz anmelden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Captcha für Walk-Up Experience der Kundenservice-Anwendung für Gäste anfordern [Neu in Security Center 1.3 und aktualisiert in 1.5]

Das Captcha für die Walk-Up Experience für Gäste verhindert, dass nicht authentifizierte Gastbenutzer Buchungen erstellen, indem von Anwendern eine Captcha-Verifizierung verlangt wird.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*sn_guest_walkup_cs.captcha.enabled*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 3,7 • CVSS-Punktzahl: Niedrig • Details zu Sicherheitsrisiken: Wenn Captcha nicht aktiviert ist, kann dies zur automatisierten Erstellung von Spam-Terminen führen, um das System zu überfordern oder alle verfügbaren Buchungsplätze zu füllen, was zu einem Denial of Service-Angriff (DoS) führt.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Diese Eigenschaft aktiviert oder deaktiviert das Captcha in den Walk-up-Check-in-Widgets für CSM-Gäste. Standardmäßig ist sie auf „true“ festgelegt.

SMS-Codebenachrichtigung für die Registrierung und Verifizierung aktivieren [Aktualisiert in Security Center 1.3]

Die Eigenschaftund *password_reset.sms.use_notify* steuert die Verwendung von SMS-Codebenachrichtigungen für die Passwortzurücksetzung.

Wenn die Eigenschaft *password_reset.sms.use_notify* auf den empfohlenen Wert **true**festgelegt ist, wird der Benutzer aufgefordert, das Passwort mithilfe der SMS-Verifizierung und der Registrierung neuer Geräte zurückzusetzen. Dies ist sicherer als E-Mail.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*password_reset.sms.use_notify*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 3,7 • CVSS-Punktzahl: Niedrig • Details zu Sicherheitsrisiken: Wenn Sie diese Eigenschaft auf „**falsch** “ setzen, wird E-Mail zur Standardmethode für die Passwortwiederherstellung. Diese Methode ist weniger sicher als SMS.
Abhängigkeiten und Voraussetzungen	Keine

Geschäftslogik

Diese Kategorie befasst sich mit der Logik und dem Flow, die bzw. den für jede Anwendung eindeutig sind, mit allgemeinen Sicherheitsprinzipien. Stellt insbesondere sicher, dass die beabsichtigte Reihenfolge des Geschäftslogik-Flows nicht umgangen werden kann, dass Grenzwerte zum Erkennen und Verhindern automatisierter Angriffe vorhanden sind und dass Schutzmaßnahmen gegen Spoofing, Manipulation, Offenlegung von Informationen und Angriffen zur Erhöhung von Berechtigungen vorhanden sind.

Im Folgenden sind einige Sicherheitskontrollen aufgeführt, die ein Administrator konfigurieren kann, um den nicht autorisierten Zugriff auf vertrauliche Entitäten in der Now Platform einzuschränken.

Maximale Anzahl von Kommentaren pro Anwender und Tag begrenzen

Konfigurieren Sie die Eigenschaft *sn_kb_social_qa.max_comments_per_user_daily*, um die Anzahl der QA-Kommentare pro Tag zu beschränken.

Wenn diese Eigenschaft nicht auf den empfohlenen Wert von **500** oder weniger festgelegt ist, gibt es keine Beschränkung der Anzahl von QA-Kommentaren pro Tag, was zu einer Erschöpfung der Ressourcen führen könnte.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*sn_kb_social_qa.max_comments_per_user_daily*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer
Empfohlener Wert	500
Standardwert	500
Kategorie	Geschäftslogik

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 3,7 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn Sie den empfohlenen Wert dieser Eigenschaft nicht auf 500 oder weniger festlegen, werden QA-Kommentare pro Tag nicht begrenzt, was zu einer Erschöpfung der Ressourcen führen kann.
Abhängigkeiten und Voraussetzungen	Keine

Begrenzen Sie die maximalen Abonnements pro Anwender und Tag

Konfigurieren Sie die Eigenschaft und *sn_kb_social_qa.max_subscriptions_per_user_daily*, um die maximale Anzahl von Abonnements zu begrenzen, die ein Benutzer an einem Tag abonnieren kann.

Wenn diese Eigenschaft nicht auf den empfohlenen Wert von **500** oder weniger festgelegt ist, gibt es keine Beschränkung der maximalen Anzahl von F&A-Fragen, die ein Anwender an einem Tag abonnieren kann. Diese Einschränkung kann zu einer Erschöpfung der Ressourcen führen und die Verfügbarkeit Ihrer Instanz beeinträchtigen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*sn_kb_social_qa.max_subscriptions_per_user_daily*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer
Empfohlener Wert	500
Standardwert	500
Kategorie	Geschäftslogik
Sicherheitsrisiko	• Schweregrad-Punktzahl: 3,7 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Legen Sie den Eigenschaftswert auf maximal 500 fest, um eine Erschöpfung der Ressourcen zu verhindern.
Abhängigkeiten und Voraussetzungen	Keine

SMTP-Empfängermenge minimieren [Aktualisiert in Security Center 1.3]

glide.email.smtp.max_recipients gibt die maximale Anzahl von Empfängern an, die die Instanz in der Zeile **An:** für eine einzelne E-Mail-Benachrichtigung auflisten kann.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Legen Sie *glide.email.smtp.max_recipients* auf den empfohlenen Wert von **100 oder weniger fest**. Benachrichtigungen, die diese Grenze überschreiten, erstellen stattdessen doppelte E-Mail-Benachrichtigungen, die an eine Teilmenge der Empfängerliste adressiert sind. Jede E-Mail-Benachrichtigung hat dieselbe maximale Anzahl an Empfängern.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.email.smtp.max_recipients*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Geschäftslogik
Zweck	Wenn diese Eigenschaft auf einen unsicheren Wert über dem Standardwert 100 festgelegt ist, kann in der Instanz ein Denial of Service auftreten.
Empfohlener Wert	100
Standardwert	100
Konfigurationstyp	Ganzzahl
Sicherheitsrisiko	(Moderat) Benachrichtigungen, die diese Grenze überschreiten würden, erstellen stattdessen doppelte E-Mail-Benachrichtigungen, die an eine Teilmenge der Empfängerliste adressiert sind.
Sicherheitsrisikobewertung	4.9

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Validiert den Remote-Host

Legen Sie die Eigenschaft auf „true“ fest, um zu verhindern, dass böswillige Akteure interne Port-Scans in Ihrem Netzwerk verwenden.

Wenn die Eigenschaft *glide.update_set.remote.check_host* nicht auf den empfohlenen Wert **true**festgelegt ist, ermöglicht die Testfunktion der Remote-Instanz Teamentwicklung das Scannen interner Ports. Dies ist eine Methode, mit der böswillige Akteure Schwachstellen in einem Netzwerk erkennen können. Dann ist es möglich, alle offenen Ports auf einem bestimmten Host aufzulisten und in einigen Fällen Antwortdaten abzurufen, was zu Informationsverlusten oder nicht autorisiertem Datenzugriff führen kann.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.update_set.remote.check_host*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Geschäftslogik
Sicherheitsrisiko	• Schweregrad-Punktzahl: 6.3 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn Sie die Eigenschaft nicht auf den empfohlenen Wert „ **wahr** “ festlegen, können böswillige Akteure möglicherweise interne Port-Scans verwenden, um sich Zugriff auf nicht autorisierte Daten zu verschaffen.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB0755132 Remote-Instanzen definieren

Kommunikation

Diese Steuerung stellt die ordnungsgemäße Verschlüsselung mit sicheren Algorithmen und Ziffern sicher. Dies umfasst sicherzustellen, dass die empfohlene Version von TLS für Client-Konnektivität verwendet wird, die Verwendung von sicheren Verschlüsselungssammlungen, die Verwendung vertrauenswürdiger und signierter Zertifikate, sicherzustellen, dass Verbindungen zwischen Komponenten verschlüsselt werden, und die Protokollierung von Verbindungsfehlern.

Zertifikatvertrauen erzwingen [In Security Center 1.3 aktualisiert und in 1.5 entfernt]

Standardmäßig ist die Eigenschaft *com.glide.communications.trustmanager_trust_all* auf **false**festgelegt. Now Platform vertraut nur Zertifikaten, die anhand des JVM-Zertifikatspeichers verifiziert werden können. Selbst- und unternehmenssignierte Zertifikate sind nicht vertrauenswürdig.

Hinweis: Die Werte für diese Eigenschaften sind und können nach der Änderung nicht mehr geändert werden (sie können nicht rückgängig gemacht werden). Ändern Sie aus Sicherheitsgründen diesen Eigenschaftswert nicht. Wenn Sie weitere Fragen haben, wenden Sie sich an Kundenservice und Support.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*com.glide.communications.trustmanager_trust_all*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Kategorie	Kommunikation
Zweck	Erzwingen der Zertifikatvalidierung für ausgehende Anforderungen.
Empfohlener Wert	falsch
Sicherheitsrisikobewertung	6.6
Funktionale Auswirkung	(Mittel) Diese Korrektur erzwingt eine strikte Validierung für das Feld „Zertifizierungsstelle“ (Zertifizierungsstelle). Wenn das Zertifikat von einer vertrauenswürdigen Entität (CA) ausgestellt wurde, akzeptiert die Instanz das Zertifikat zur weiteren Verwendung.
Sicherheitsrisiko	(Mittel) Aus Vertraulichkeits- und Integritätsgründen sollte die Anwendung die Zertifizierungsstelle des Zertifikats validieren, bevor das Zertifikat für Transaktionsvorgänge verwendet wird.
Referenzen	Zertifikate Verifizierung des Hostnamens des HTTP-Clients

Ausgehende SSLv2-/SSLv3-Verbindungen deaktivieren [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.outbound.sslv3.disabled*, um den MID-Server zur Verwendung von TLS bei ausgehenden Verbindungen wie REST- und SOAP-Anforderungen zu zwingen. Normalerweise wird für ausgehende Verbindungen einer Instanz die Verwendung von TLS anstelle von SSL erzwungen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.outbound.sslv3.disabled*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Kommunikation
Zweck	Erzwingen der Verwendung von TLS für alle ausgehenden Verbindungen von der ServiceNow-Instanz.
Empfohlener Wert	wahr
Standardwert	Phase
Sicherheitsrisikobewertung	6.5
Funktionale Auswirkung	(Mittel) Diese Korrektur erzwingt die Verwendung der TLS-Protokollversion bei der Kommunikation über HTTPS. Wenn von Kunden/Benutzern der Instanz Geräte verwendet werden, die keine TLS-Kommunikation unterstützen, kann ein Ausfall auftreten.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	(Moderat) Legacy-Versionen von SSL haben sich bei der Verwendung für die Implementierung der sicheren HTTP-Shell aufgrund clientseitiger Angriffe, einschließlich BEAST und SSL-Heart-Bleed, als unsicher erwiesen.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Keine Demozertifikate für aktive SAML-Konfigurationen verwenden [Aktualisiert in Security Center 1.5]

Steuern Sie, ob Demozertifikate in SAML-Konfigurationen für die Produktion verwendet werden.

Die von ServiceNow bereitgestellten Demozertifikate sollten nicht in SAML-Konfigurationen für die Produktion verwendet werden, da sie allen Instanzen mit einer bekannten Passphrase gemeinsam sind. Wenn eine der SAML-Eigenschaften, die einen Zertifikatschlüsselspeicher verwenden, aktiv ist (*require_signed_authnrequest*, *require_signed_logoutrequest*oder *encrypt_assertion*), sollten die Demodaten nicht verwendet werden. Da Demodaten von allen Instanzen gemeinsam genutzt werden, gibt es keine Integritätsgarantie für Anforderungen, die mit gemeinsam genutzten Zertifikaten signiert wurden. Daher könnte jede vom IdP verschlüsselte Nachricht von einem böswilligen Akteur entschlüsselt werden, wenn sie abgefangen wird.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.authenticate.sso.saml2.keystore*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	sys_id eines anwenderdefinierten Schlüsselspeichers
Standardwert	leere Zeichenfolge
Kategorie	Kommunikation
Sicherheitsrisiko	• Schweregrad-Punktzahl: 3,9 • CVSS-Punktzahl: Niedrig
Abhängigkeiten und Voraussetzungen	Keine

OCSP-Prüfung bei Netzwerkfehler erzwingen [Neu in Security Center 1.3]

Erfahren Sie, wie Sie die Eigenschaft *com.glide.communications.httpclient.ocsp_allow_network_error*konfigurieren, um zu verhindern, dass böswillige Akteure OCSP-Prüfungen (Online Certificate Status Protocol) umgehen.

Wenn *com.glide.communications.httpclient.ocsp_allow_network_error*nicht auf den empfohlenen Wert „false“ festgelegt ist und bei der OCSP-Prüfung (Online Certificate

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Status Protocol) ein Netzwerkfehler auftritt (z. B. Zeitüberschreitung oder Problem beim Abrufen der Sperrinformationen), wird die OCSP-Sicherheitsprüfung umgangen und berücksichtigt erfolgreich. Dies könnte es einem Angreifer mit einem widerrufenen Zertifikat ermöglichen, die Public Key Infrastructure (PKI) und das Vertrauen in digitale Zertifikate zu brechen, die für das Web von grundlegender Bedeutung sind. Die Verwendung widerrufener Zertifikate ist häufig ein Indikator für böswillige Aktivitäten, es sei denn, die Server sind nicht synchron.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*com.glide.communications.httpclient.ocsp_allow_network_e*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	falsch
Standardwert	wahr
Kategorie	Kommunikation
Sicherheitsrisiko	• Schweregrad-Punktzahl: 5,9 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf „falsch“ festgelegt wird, kann ein böswilliger Akteur die OCSP-Sicherheitsprüfung umgehen.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Diese Eigenschaft bestimmt, ob eine Anforderung an die Online Certificate Status Protocol(OCSP)-URI von Authority Information Access (AIA) im Falle eines Verbindungs- oder Zeitüberschreitungsfehlers zu „Bestanden“ oder „Nicht bestanden“ führt. Bei Festlegung auf „falsch“ kann der Widerrufstatus des vorgelegten Serverzertifikats nicht validiert werden und führt zu einem Kommunikationsfehler mit diesem Endpunkt. Wenn ein Netzwerkfehler auftritt, wenn die Eigenschaft auf den Standardwert true festgelegt ist, wird das Zertifikat unter Zurücknahmeaspekten als gültig behandelt.

Zertifikatkette und Hostname verifizieren [Neu in Security Center 1.3]

Konfigurieren Sie die Eigenschaft *com.glide.communications.httpclient.verify_hostname*, um Man-in-the-Middle-Angriffe zu verhindern, indem Sie sicherstellen, dass der Zertifizierungsverifizierungsprozess ausgeführt wird.

Wenn *com.glide.communications.httpclient.verify_hostname* nicht auf „**true**“ festgelegt ist, kann dies Man-in-the-Middle-Angriffe ermöglichen, bei denen die Kommunikation zwischen zwei Parteien abgefangen wird. Durch Festlegen dieser Eigenschaft

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

auf „falsch“ wird der Zertifikatverifizierungsprozess deaktiviert. Um diese Sicherheitsbedrohung zu beheben, legen Sie *com.glide.communications.httpclient.verify_hostname* auf „ **wahr** “ fest, um zu verhindern, dass der HTTP-Client eine Verbindung zu einem potenziell schädlichen Hostnamen herstellt.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*com.glide.communications.httpclient.verify_hostname*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Kommunikation
Sicherheitsrisiko	• Schweregrad-Punktzahl: Hoch • CVSS-Punktzahl: 7,4 • Details zu Sicherheitsrisiken: Wenn Sie *com.glide.communications.httpclient.verify_hostname* nicht auf den empfohlenen Wert „true“ festlegen, wird Ihre Instanz möglicherweise angreifbar für Man-in-the-Middle-Angriffe.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Überprüft den Hostnamen und die Zertifikatkette, die von Remote-SSL-Hosts (Secure Socket Layer) dargestellt werden. Legen Sie diese Eigenschaft auf „true“ fest, um sich vor MITM-Angriffen (Man-in-the-Middle) zu schützen. **Hinweis:** Diese Eigenschaft überschreibt die Eigenschaft *com.glide.communications.trustmanager_trust_all*,.

Zertifikatwiderrufung verifizieren [Neu in Security Center 1.3]

Die Eigenschaft *com.glide.communications.httpclient.verify_revoked_certificate* überprüft den Widerruf des Zertifikats während des TLS-Handshakes (Transport Layer Security), um sicherzustellen, dass Sicherheitsprüfungen nicht umgangen werden.

Wenn *com.glide.communications.httpclient.verify_revoked_certificate* nicht auf den empfohlenen Wert **true**festgelegt ist, wird die Zertifikatwiderrufung während des TLS-Handshake nicht geprüft. TLS verschlüsselt über das Internet gesendete Daten, um sicherzustellen, dass böswillige Akteure keine vertraulichen Informationen wie Passwörter oder Kreditkartennummern sehen können. Das Umgehen des TLS-Handshake stellt ein Sicherheitsrisiko dar, da ein Angreifer mit einem widerrufenen Zertifikat die Bereitstellung eines gültigen Zertifikats vernachlässigen kann und die Public Key Infrastructure (PKI) und das Vertrauen in das digitale Zertifikat verletzt werden.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*com.glide.communications.httpclient.verify_revoked_certi*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Kommunikation
Sicherheitsrisiko	• Schweregrad-Punktzahl: 6,5 • CVSS-Punktzahl: Mittel • Details zu Sicherheitsrisiken: Wenn *com.glide.communications.httpclient.verify_revoked_cert* nicht auf den empfohlenen Wert „wahr“ festgelegt wird, wird die Zertifikatwiderrufung während des TLS-Handshake nicht überprüft.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Diese Eigenschaft muss auf „true“ festgelegt werden, um sicherzustellen, dass eine TLS-Sitzung (Transport Layer Security) mit einem authentifizierten Endpunkt gestartet wird. Wenn diese Eigenschaft auf „false“ festgelegt ist, wird das Zertifikat nicht überprüft, was die Sicherheit der Instanz gefährden könnte.

Automatische Übersetzung

Konfiguration

Die Kategorie Konfiguration stellt sicher, dass Anwendungen über eine sichere Build-Umgebung und gesicherte Bibliothekskomponenten von Drittparteien verfügen. Insbesondere muss sichergestellt werden, dass eine Build- und Bereitstellungspipeline wiederholbar ist, automatisierte Tests durchgeführt und verhindert wird, dass bekannte Sicherheitsprobleme bereitgestellt werden. Dies beinhaltet, Abhängigkeiten auf dem neuesten Stand und frei von bekannten Schwachstellen zu halten.

Inhaltstypoptionen automatisch festlegen [In Security Center 1.3.3 entfernt]

Konfigurieren Sie die Eigenschaft Inhaltstypoptionen automatisch festlegen in Ihrer Instanz, um MIME-Verwirrungsangriffe zu verhindern.

Verwenden Sie diese Eigenschaft, um den HTTP-Header der X-Content-Type-Options-Antwort zu steuern. Der X-Content-Type-Options-Antwort-HTTP-Header wird vom Server verwendet, um anzugeben, dass die in den Content-Type-Headern angegebenen MIME-Typen befolgt werden sollen. Wenn diese Eigenschaft auf falsefestgelegt ist, kann ein Angreifer MIME-Verwirrungsangriffe durchführen. if auf wahr gesetzt, dann verhindert dieser Header, dass der Browser Dateien als etwas anderes als den Inhaltstyp in den HTTP-Headern interpretiert.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnung: Der Wert für diese Eigenschaft ist eine Überschreibung ohne DB. Sie kann nicht geändert oder überschrieben werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.security.header.auto_set_x_content_type_options*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Konfiguration
Sicherheitsrisiko	• Schweregrad-Punktzahl: 7,3 • CVSS-Punktzahl: Hoch • Details zum Sicherheitsrisiko: Wenn Sie diese Eigenschaft auf „ **false** “ setzen, kann ein Angreifer MIME-Verwirrungsangriffe durchführen.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Systemeigenschaft hinzufügen

Cache-Steuerung – HTTP-Headerwert [In Security Center 1.3 aktualisiert]

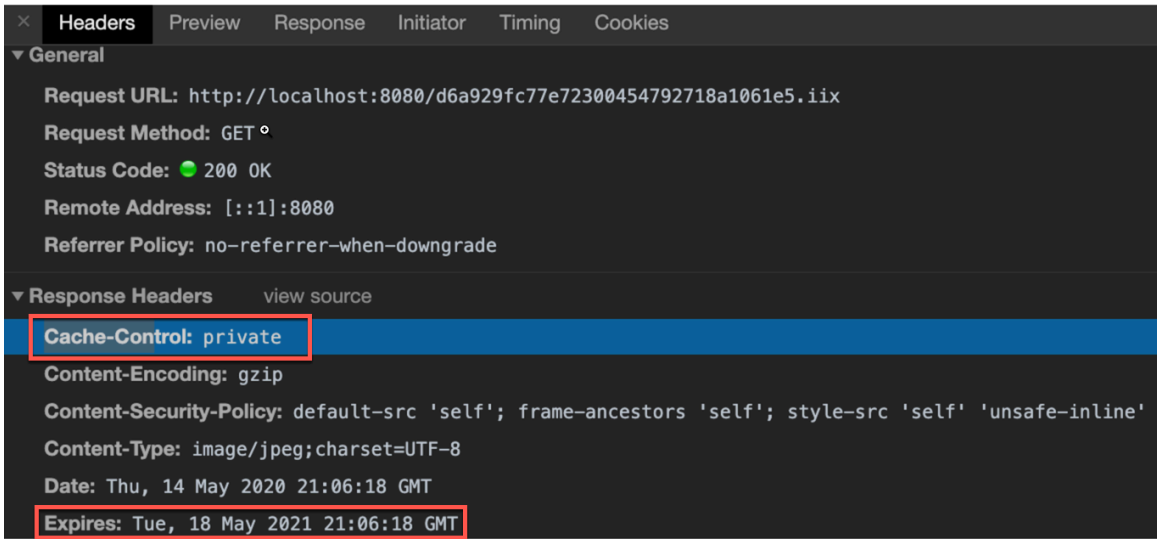
Verwenden Sie die Eigenschaft *glide.http.cache_control*, um den Standardwert für die Cachesteuerung in den HTTP-Antwortheadern festzulegen, die von Now Platform gesendet werden, wenn statische Inhaltsdaten für eine Seite angefordert werden. Beispiele für statische Inhalte sind Bilder, CSS und JavaScript, die von innerhalb einer Seite gerendert werden.

Die Eigenschaft *glide.http.cache_control* legt den Standardwert für Cache-Steuerung in HTTP-Antwortheadern auf **private** oder **öffentlich**fest. Der Standardwert ist **private**.

Wert	Beschreibung
Privat	Statische Inhalte können auf Browserebene (Client-Ebene) zwischengespeichert werden, nicht jedoch auf Proxyserverebene.
Öffentlich	Statische Inhalte können auf Browserebene (Client) und auch auf Proxyserverebene zwischengespeichert werden.

Der Wert Expires in den HTTP-Antwortheadern steuert, wann der statische Inhalt abläuft. Er hat einen Standardwert von 369 Tagen. Um den Standardwert manuell zu überschreiben, verwenden Sie die Eigenschaft *glide.http.expire.days*.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis: Mit der Eigenschaft *glide.http.cache* können Sie festlegen, ob das Festlegen der Werte für Cache-Steuerung und Ablauf in HTTP-Antwortheadern aktiviert oder deaktiviert werden soll. Der Standardwert ist **true**, wodurch Sie Folgendes festlegen können:

- Cache-Steuerungswert standardmäßig unter Verwendung der Eigenschaft *glide.http.cache_control*.
- Läuft standardmäßig mit der Eigenschaft *glide.http.expire.days* ab.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.http.cache_control*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Konfiguration
Zweck	Zum Konfigurieren des HTTP-Antwort-Header-Werts „Cache-Steuerung“ für statischen Inhalt.
Empfohlener Wert	Privat
Standardwert	Privat
Sicherheitsrisikobewertung	4.3
Funktionale Auswirkung	(Mittel) Legt den Standardwert für „Cache-Control“ in einem HTTP-Antwortheader fest.
Sicherheitsrisiko	(Hoch) Wenn Sie diese Eigenschaft auf „ **public**“ festlegen, können Instanzen mit CDN/Proxys statischen Inhalt zwischenspeichern und ohne Authentifizierung rendern. • **„privat“** ist eine geeignetere Einstellung für Instanzen mit CDN-/Proxy-Setup. • Wenn für die Instanz kein CDN/Proxy eingerichtet ist, sollten beide Werte geeignet sein.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Chatserver-Debugging deaktivieren

Aktivieren oder deaktivieren Sie die Systemprotokolle Ihrer Instanz, indem Sie diese Eigenschaft konfigurieren.

Verwenden Sie die Eigenschaft *glide.cs.debug*, um zu verwalten, wie Ihre Instanz Systemprotokolle behandelt. Wenn die Eigenschaft auf den empfohlenen Wert **false**festgelegt ist, sind Systemprotokolle nicht aktiviert. Wenn sie auf **true**festgelegt ist, sind Systemprotokolle aktiviert. Legen Sie die Eigenschaft nur dann auf „ **true** “ fest, wenn Sie eine Problembehandlung durchführen möchten, und deaktivieren Sie sie dann, wenn Sie fertig sind. Das Aktivieren von Systemprotokollen kann dazu führen, dass viele Nachrichten generiert werden, was die Systemprotokolle überlasten könnte. Protokollnachrichten könnten versehentlich vertrauliche Informationen verfügbar machen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.cs.debug*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	falsch
Standardwert	falsch
Kategorie	Konfiguration
Sicherheitsrisiko	• Schweregrad-Punktzahl: 2,3 • CVSS-Punktzahl: Niedrig • Details zu Sicherheitsrisiken: Das Aktivieren von Systemprotokollen kann dazu führen, dass viele Nachrichten generiert werden, die das System mit Protokollnachrichten überlasten könnten, die versehentlich vertrauliche Informationen offenlegen.
Abhängigkeiten und Voraussetzungen	Keine

Debugging von gesperrten Formularelementen deaktivieren

Hier ist die Beschreibung für *glide.security.explain.write.locks*.

Legen Sie *glide.security.explain.write.locks* auf den empfohlenen Wert „ **falsch** “ fest, um die Anzeige von Erklärungen für gesperrte Formularelemente zu verhindern. Legen Sie den Wert auf **„true“ fest**, um die Erklärung der gesperrten Formularelemente anzuzeigen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.security.explain.write.locks*

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Konfiguration
Zweck	Beschränkt das Anzeigeverhalten von SecurityDebugger ohne Abhängigkeit von anderen Eigenschaften.
Empfohlener Wert	falsch
Standardwert	falsch
Konfigurationstyp	Boolean
Sicherheitsrisiko	(Niedrig) Verhindert die Anzeige der Erklärung für gesperrte Formularelemente. Dadurch wird die Anwendung etwas sicherer, da vom Sicherheits-Debugger weniger Informationen bereitgestellt werden.
Sicherheitsrisikobewertung	3,5

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Multisso-Debugging deaktivieren

Die Eigenschaft *glide.authenticate.multisso.debug* steuert die Debug-Protokollierung für Multi-SSO.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.authenticate.multisso.debug*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Konfiguration
Zweck	Deaktiviert Multi-SSO-Debugging.
Empfohlener Wert	falsch
Standardwert	falsch
Konfigurationstyp	Boolean
Sicherheitsrisiko	(Hoch) Legen Sie die Eigenschaft auf den empfohlenen Wert „falsch“ fest. Andernfalls ist MultiSSO-Debugging aktiviert, was zu einem unbeabsichtigten Verlust vertraulicher Informationen führen könnte.
Sicherheitsrisikobewertung	4.0
Referenzen	Eigenschaften, Tabellen und Skripts für Mehrfachanbieter-SSO

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Klonen von Zielen nicht zulassen [Neu in Security Center 1.3]

Konfigurieren Sie die Eigenschaft *glide.db.clone.allow_clone_target*, um zu verhindern, dass Ihre -Instanz als Klonziel verwendet wird.

Wenn *glide.db.clone.allow_clone_target* nicht auf den empfohlenen Wert „false“ festgelegt ist, kann die Instanz als Klonziel oder als Datensatz verwendet werden, der die Instanz-URL und die zum Klonen verwendeten Anmeldeinformationen angibt. Von einem Systemklon sprechen Sie, wenn der gesamte Inhalt einer Datenbank von einer Instanz in eine andere kopiert wird. Dies stellt ein Sicherheitsrisiko dar, da die Instanzdatenbank beim Klonvorgang überschrieben werden kann, was zu Datenverlust und fehlender Datenintegrität führt. Stellen Sie als Korrektur sicher, dass *glide.db.clone.allow_clone_target* auf „false“ festgelegt ist.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.db.clone.allow_clone_target*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	falsch
Standardwert	wahr
Kategorie	Konfiguration
Sicherheitsrisiko	• Schweregrad-Punktzahl: 5,9 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn Sie diese Eigenschaft nicht auf den empfohlenen Wert „false“ setzen, kann die Instanz als Klonziel verwendet werden. Dies stellt ein Sicherheitsrisiko dar, da die Instanzdatenbank beim Klonen überschrieben werden kann.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	• Systemklon • Erstellen Sie ein Klonziel
Funktionale Auswirkung	Diese Eigenschaft bietet einen zusätzlichen Schutz, der verhindert, dass eine Produktionsinstanz geklont wird. Der Standardwert ist für Produktionsinstanzen „falsch“ und für Test- und Entwicklungsumgebungsinstanzen wie „dev“ oder „qa“ „wahr“. Um die Verwendung einer Instanz als Klonziel zu aktivieren, legen Sie diese Eigenschaft auf „wahr“ fest.

Anzeige der Stapelablaufverfolgung für SOAP-Fehler deaktivieren

Verwalten Sie, wie Stack Traces in Ihrer Instanz angezeigt werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie die Eigenschaft *glide.soapfault.display_stack_trace*, um Stack Traces in Ihrer Instanz zu verwalten. Wenn diese Eigenschaft auf „ **false**“ konfiguriert ist, können vertrauliche Informationen offengelegt werden. Wenn sie auf „ **true**“ festgelegt ist, wird kein Stack Trace angezeigt.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.soapfault.display_stack_trace*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	falsch
Standardwert	falsch
Kategorie	Konfiguration
Sicherheitsrisiko	• Schweregrad-Punktzahl: 4.3 • CVSS-Punktzahl: Mittel • Details zu Sicherheitsrisiken: Wenn Sie diese Eigenschaft auf **„falsch** “ setzen, können vertrauliche Informationen aus dem Stack Trace verfügbar gemacht werden.
Abhängigkeiten und Voraussetzungen	Keine

Beschränken Sie den Zugriff auf die Leistungsüberwachung

Verwenden Sie die Eigenschaft *glide.security.diag_txns_acl*, um den Zugriff auf „stats.do“, „threads.do“, „thread_pool_stats“ und „replication.do“ über eine nicht authentifizierte Verbindung zu steuern.

Wenn Sie diese Eigenschaft auf „ **true**“ festlegen, ermöglicht die Eigenschaft *glide.security.diag_txns_acl* nur den Zugriff auf Folgendes durch das Administratorkonto:

- https://<instancename>.servicenow.com/stats.do
- https://<instancename>.servicenow.com/threads.do
- https://<instancename>.servicenow.com/replication.do
- https://<instancename>.servicenow.com/thread_pool_stats.do

Ohne diese Einstellung zu aktivieren, ist es weiterhin möglich, über eine nicht authentifizierte Verbindung auf diese Ressourcen zuzugreifen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.security.diag_txns_acl*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Kategorie	Konfiguration
Zweck	Beschränken Sie den Zugriff auf Konfigurationsseiten auf das Administratorkonto
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	5.3
Funktionale Auswirkung	(Niedrig) Diese Korrektur erzwingt, dass nur der Administratoraccount zu Protokollierungs- und Problembehandlungszwecken Zugriff auf die vertraulichen Anwendungsdaten erhält.
Sicherheitsrisiko	(Moderat) Sensible Daten wie Serverdetails, Threads und Prozesse, die auf dem Server ausgeführt werden, sollten für Endanwender ohne entsprechende Berechtigungen niemals sichtbar oder zugänglich sein.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Aktualisierte Version des MultiSSO-Plugins aktivieren [In Security Center 1.3 und 1.5aktualisiert]

Vergewissern Sie sich, dass Sie v2 des MultiSSO-Plugins verwenden und dass die Option auf „true“ festgelegt ist, um Sicherheitsschwachstellen zu reduzieren.

Wenn das MultiSSO-Plugin in Ihrer Instanz aktiviert ist, sollte die Version v2 und der Wert auf „ **true**“ festgelegt sein. Die Versionen vor MultiSSOv2, einschließlich SAML 1.1 und SAML 2.0, entsprechen nicht den Sicherheitsstandards, da sie OpenSAML-Bibliotheksversionen mit bekannten allgemeinen Schwachstellen und Gefährdungen (CVEs) verwenden. Wenn es sich bei den bekannten CVEs um Sicherheitsbedrohungen in veralteten OpenSAML-Bibliotheken handelt, könnte dies einem böswilligen Akteur ermöglichen, Nachrichten zu fälschen und die Authentifizierung durch Wrapping-Angriffe auf XML-Signaturen zu umgehen, die Identität von Entitäten anzunehmen oder Man-in-the-Mate-Angreifern zu ermöglichen, sich nicht autorisierten Zugriff auf eine Instanz zu verschaffen .

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.authenticate.multissov2_feature.enabled*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Konfiguration
Sicherheitsrisiko	• Schweregrad-Punktzahl: 5 • CVSS-Punktzahl: Mittel

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Details zu Sicherheitsrisiken: Wenn Sie die Eigenschaft auf „ **false** “ setzen, verwenden Sie frühere Versionen von MultiSSOv2, welche OpenSAML-Bibliotheken mit Sicherheitsschwachstellen verwenden. Dies könnte es böswilligen Akteuren ermöglichen, Nachrichten zu fälschen.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB0756504

Sichere Referrer-Richtlinie erzwingen [Neu in Security Center 1.3]

Verwenden Sie die Eigenschaft *com.glide.security.referrerpolicy*, um sicherzustellen, dass der HTTP-Header „Referrer-Richtlinie“ die entsprechende Datenebene an jede Seite ServiceNow® sendet, um Datenverluste zu vermeiden.

Wenn die Eigenschaft *com.glide.security.referrerpolicy* auf Standard festgelegt ist, wird sichergestellt, dass der HTTP-Header „Referrer-Policy“ mit der entsprechenden Ebene an gesendeten Informationen verwaltet wird, speziell auf die Anforderungsseite Now Platform® zugeschnitten. Dies verhindert nicht autorisierte Datenverluste, auf die von anderen Teilen der vollständigen URL aus zugegriffen werden könnte, z. B. vom Pfad und der Abfragezeichenfolge.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*com.glide.security.referrerpolicy*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	Standard
Standardwert	Standard
Kategorie	Konfiguration
Sicherheitsrisiko	• Schweregrad-Punktzahl: 4.3 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Stellen Sie sicher, dass die Eigenschaft *com.glide.security.referrerpolicy* auf Standard festgelegt ist, um zu verhindern, dass nicht autorisierte Daten verloren gehen.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Referrer-Richtlinie

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Funktionale Auswirkung	Diese Eigenschaft steuert, wie viele Informationen über den Referrer-Header gesendet werden, wenn eine Anforderung von einer Seite gesendet wird: • Standard: Die Instanz übernimmt die Header der Referrer • Same-Origin: Vollständige Referrer-URL innerhalb der Instanz/gleicher Domäne und keine Referrer-URL an externe Herkunft senden • Ursprung: Es wird nur der Ursprung als Empfehlungsgeber innerhalb und außerhalb des Ursprungs gesendet • Origin-when-cross-origin: Senden Sie die vollständige Referrer-URL innerhalb der Instanz/derselben Domäne und nur den Ursprung außerhalb des Ursprungs

Implementieren Sie den Sicherheitsheader „x-frame-options: SAMEORIGIN“ [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.set_x_frame_options*, um den X-Frame-Options-Antwortheader für alle UI-Seiten auf SAMEORIGIN festzulegen.

Verwenden Sie den HTTP-Antwortheader „X-Frame-Options“, um anzugeben, ob der Browser eine Seite in `<frame>` oder `<iframe>`rendern darf. Websites können diese Funktion verwenden, um Clickjacking-Angriffe zu vermeiden, indem sichergestellt wird, dass ihr Inhalt nicht in andere Websites eingebettet wird. Ein Angreifer könnte Ihre Seite in seine eigene Seite einbetten und Ihre Seitenelemente in böswillige Absichten überführen. Der Endanwender hält die Seite möglicherweise für legitim, da sie Ihrer Seite ähnelt. Der Endanwender kann wie üblich auf Elemente klicken, um schädliche Skripts oder Elemente auszuführen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.set_x_frame_options*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Konfiguration
Zweck	Zur Abwehr von ClickJacking-Angriffen.
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	7.1
Funktionale Auswirkung	(Niedrig) Diese Korrektur erzwingt die Einschränkung für das Rendern einer Now Platform -Anwendung in einer Drittparteianwendung in Form eines iFrame. Wenn Sie über eine solche Integration verfügen, wird

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	die Anwendung in der angepassten Drittanbieter-App nicht gerendert.
Sicherheitsrisiko	(Mittel) Mit der Richtlinie „Same Origin“ können Sie verhindern, dass eine Domäne ein Skript oder eine Ressource aus einer anderen Domäne abruft. Alle modernen Browser unterstützen diese Funktionalität. Die Richtlinie validiert die Verbindung basierend auf Protokoll, Port und Host. CORS (Cross Origin Request) ist eine Änderung der Richtlinie für gleiche Herkunft, die den Zugriff auf Ressourcen/Skripts aus einer anderen Domäne ermöglicht, wenn sie explizit als Teil des Headerwerts angegeben wird. • In diesem Fall steuert der X-Frame-Options-Header, ob die Anwendung Now Platform auf der Website des Drittanbieters gerendert werden kann. • Reduziert das sensible Risiko, da der Eigenschaftswert, wenn er auf **SAMEORIGIN** festgelegt ist, das Rendern nicht ermöglicht.
Referenzen	Verfügbare Systemeigenschaften iFrames konfigurieren

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Schreibzugriff erfordern, um auf die Seite „Element hinzufügen“ des Servicekatalogs zuzugreifen [Neu in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.sc.request.add_item_write_access*, um zu verhindern, dass nicht autorisierte Vorgänge an Katalogelementen ausgeführt werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.sc.request.add_item_write_access*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Konfiguration
Sicherheitsrisiko	• Schweregrad-Punktzahl: 4.3 • CVSS-Punktzahl: Mittel • Details zu Sicherheitsrisiken: Wenn die Eigenschaft *glide.sc.request.add_item_write_access* auf „false“ festgelegt ist, kann jeder angemeldete

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Benutzer auf die UI-Seite „Katalogelement hinzufügen“ zugreifen. Dies kann dazu führen, dass nicht autorisierte Vorgänge an Katalogelementen ausgeführt werden. Um dieses Sicherheitsrisiko zu beheben, legen Sie diese Eigenschaft auf „wahr“ fest.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Wenn die Eigenschaft „wahr“ ist, muss der Benutzer im Kontext der UI-Seite Schreibzugriff auf den Datensatz haben.

Xframe-Optionen festlegen, um das Einbetten von Websites von Drittanbietern zu verhindern [Aktualisiert in Security Center 1.3]

Konfigurieren Sie diese Eigenschaft, um zu verhindern, dass der Inhalt einer Webanwendung in die Website eines Drittanbieters eingebettet wird.

Wenn diese Eigenschaft nicht auf den empfohlenen Wert **DENY** oder **SAMEORIGIN festgelegt**ist, kann der Inhalt einer Webanwendung mithilfe eines **ALLOW-FROM-** URI in eine Drittanbieterwebsite eingebettet werden. Sie ermöglicht es nicht vertrauenswürdigen Websites von Drittparteien, Angriffe wie Clickjacking zu ermöglichen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*com.glide.cs.embed.xframe_options*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	gleicher Herkunft
Standardwert	gleicher Herkunft
Kategorie	Konfiguration
Sicherheitsrisiko	• Schweregrad-Punktzahl: 3,1 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn Sie diese Eigenschaft nicht auf den empfohlenen Wert festlegen, kann der Inhalt einer Webanwendung in die Website eines Drittanbieters eingebettet werden, was Angriffe wie Click-Jacking ermöglicht.
Abhängigkeiten und Voraussetzungen	Keine

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenschutz

Die Datenschutzkategorie behandelt die Elemente Vertraulichkeit, Integrität und Verfügbarkeit (CIA) von Daten.

Die CIA-Komponenten sind:

- Vertraulichkeit: Daten sind während der Übertragung und im Ruhezustand vor nicht autorisiertem Zugriff geschützt.
- Integrität: Daten werden vor nicht autorisierter Erstellung, Löschung oder Änderung geschützt.
- Verfügbarkeit: Daten sind bei Bedarf zugänglich.

„Anwendernamen speichern“ entfernen

Verwenden Sie die Eigenschaft *glide.ui.forgetme*, um das Kontrollkästchen Anwendernamen speichern von der **Anmeldeseite** zu entfernen, um zu verhindern, dass Anmeldeinformationen zwischengespeichert werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.ui.forgetme*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Datenschutz
Zweck	Um sicherzustellen, dass keine Authentifizierungsinformationen zwischengespeichert werden.
Sicherheitsrisikobewertung	3,5
Empfohlener Wert	wahr
Standardwert	wahr
Funktionale Auswirkung	(Niedrig) Diese Korrektur würde die Anwender-Experience ändern, indem sie automatisch aus der Instanz abgemeldet werden, wenn ihre Sitzung abläuft. Der Ablauf der Sitzung hängt ausschließlich von dem in der Systemeigenschaft festgelegten Wert ab, wie in Benutzersitzungen verwalten beschrieben.
Sicherheitsrisiko	(Niedrig) Wenn Sie bei der **Anmeldung** das Kontrollkästchen „Anwendernamen speichern“ aktivieren, wird ein zusätzliches Cookie auf dem Computer des Benutzers gespeichert. • Sein Zweck besteht darin, die Sitzung für die nachfolgenden Besuche des angemeldeten Anwenders automatisch wiederherzustellen. • Dies stellt ein Sicherheitsrisiko dar, da die Benutzersitzung aktiv bleiben kann, bis sie sich absichtlich abmeldet. Die Wahrscheinlichkeit eines Angriffs in diesem Szenario erhöht sich, wenn der

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Endanwender den Browser unbeaufsichtigt gelassen hat oder wenn er durch einen anderen Angriff gefährdet ist.
Referenzen	Kontrollkästchen „Anwendernamen speichern“ entfernen

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen

Löschen der Zwischenablage anfordern, wenn die mobile Anwendung im Hintergrund ausgeführt wird [Neu in Security Center 1.3]

Die Eigenschaft *glide.sg.clear_pasteboard_when_backgrounded* steuert, ob Text, der aus der mobilen ServiceNow-App kopiert wurde, im Clipper und auf der Zwischenablage beibehalten wird, nachdem die App im Hintergrundmodus ausgeführt wurde.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.sg.clear_pasteboard_when_backgrounded*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Datenschutz
Sicherheitsrisiko	• Schweregrad-Punktzahl: 3,5 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf den empfohlenen Wert true festgelegt ist, können vertrauliche Informationen an die Android- oder iOS-Zwischenablage weitergegeben werden, wo sie anderen Anwendungen auf dem Gerät zur Verfügung stehen können.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Diese Eigenschaft löscht die Zwischenablage zum Kopieren und Einfügen, wenn die ServiceNow-App in den Hintergrund verschoben wird.

Aktualisierungen von HR-Fällen auf persönliche E-Mails beschränken [Neu in Security Center 1.3 und aktualisiert in 1.5]

Verwenden Sie die Eigenschaft *sn_hr_core.restrict_guest_email*, um zu steuern, ob ein Benutzer mit seiner persönlichen E-Mail-Adresse auf einen HR-Fall antworten kann.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die Eigenschaft *sn_hr_core.restrict_guest_email* nicht auf „true“ festgelegt ist, kann ein Benutzer von einem persönlichen Konto aus eine E-Mail senden, die auf den HR-Fall verweist, der in die Arbeitsnotizen aufgenommen werden soll. Dies kann zu geringfügigen Problemen mit der Vertraulichkeit oder Integrität führen, wenn die persönliche E-Mail gefährdet ist oder die Kommunikation unsicher ist. Ein Administrator möchte möglicherweise die Möglichkeit von Anwendern einschränken, von ihrer persönlichen E-Mail aus auf HR-Fälle zu antworten, da sie nicht sicher sein können, ob der Anwender auf das persönliche E-Mail-Konto zugreift.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*sn_hr_core.restrict_guest_email*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Datenschutz
Sicherheitsrisiko	• Schweregrad-Punktzahl: 3,5 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf „wahr“ festgelegt ist, kann dies zu geringfügigen Vertraulichkeits- oder Integritätsproblemen führen, wenn die persönliche E-Mail gefährdet ist oder unsicher kommuniziert.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Diese Eigenschaft steuert, ob eine Antwort von einer persönlichen E-Mail-Adresse einen HR-Fall aktualisiert. Bei Festlegung auf „wahr“ wird jede Antwort von einer persönlichen E-Mail den Fallnotizen hinzugefügt. Bei „falsch“ werden der Fall und die Notizen nicht aktualisiert.

OAuth-Parameter auf Post-Text beschränken [Neu in Security Center 1.3]

Die Eigenschaft *glide.oauth.allow.parameters.in.post.body.only* steuert die Akzeptanz von Zugriffstoken durch die eingehende OAuth-Authentifizierung. Zugriffstoken sind vertraulich und sollten nur akzeptiert werden, wenn sie sich in einem POST-Anforderungstext befinden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.oauth.allow.parameters.in.post.body.only*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Datenschutz
Sicherheitsrisiko	• Schweregrad-Punktzahl: 7,4 • CVSS-Punktzahl: Hoch • Details zum Sicherheitsrisiko: Wenn *glide.oauth.allow.parameters.in.post.body.only* nicht auf den empfohlenen Wert „true“ festgelegt ist, könnten sich Zugriffstoken im GET-Anforderungsparameter befinden, die in Client-Infrastrukturprotokollen verbleiben können und möglicherweise zu einer Account-Übernahme führen, wenn diese Protokolle offengelegt werden.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	• OAuth 2.0 • Verwalten Sie OAuth-Token
Funktionale Auswirkung	Stellt sicher, dass der Prozessor „oauth_token.do“ ausschließlich POST-Textparameter als Eingabe für alle unterstützten Gewährungstypen akzeptiert.

Fehlerbehandlung und -protokollierung

Die Kategorie für Fehlerbehandlung und Protokollierung befasst sich mit der Qualität und Ausführlichkeit protokollierter Informationen, die für Stakeholder verfügbar gemacht werden.

Dies beinhaltet sicherzustellen, dass Protokolle und Fehlermeldungen keine vertraulichen Informationen erfassen, Daten gemäß Klassifizierung korrekt schützen und eine angemessene Lebensdauer haben. Darüber hinaus bezieht sich diese Kategorie auf die angemessene Fehlerbehandlung und die Nichtoffenlegung sensibler Fehler für Endanwender, z. B. ausführliche Stack Traces für nicht behandelte Ausnahmen mit Sicherheitsauswirkungen.

Deaktivieren Sie die Protokollierung für Anwender mit geringen Berechtigungen in der Skript-Sandbox

Verwalten Sie die Fähigkeit des Glide-Systems, in der Sandbox-Umgebung ausgeführte Skripts zu protokollieren.

Verwenden Sie die Eigenschaft *glide.security.sandbox_no_logging*, um die Fähigkeit des Glide-Systems zur Protokollierung von in der Sandbox-Umgebung ausgeführten Skripts zu steuern. Wenn *glide.security.sandbox_no_logging* auf „ **false**“ festgelegt ist, ist die Protokollierung für Benutzer mit geringeren Berechtigungen verfügbar, die Sandbox-Skripts verwenden. Dies stellt eine potenzielle Sicherheitsschwachstelle dar, da Anwender mit geringen Berechtigungen Protokolle einschleusen können, die es einem böswilligen Akteur ermöglichen, einen Angriff zu verschleiern. Konfigurieren Sie die Eigenschaft auf „ **true**“, um

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zu verhindern, dass Benutzer mit niedrigeren Berechtigungen, die ein Skript in einer Sandbox verwenden, über Protokollierungsfunktionen verfügen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.security.sandbox_no_logging*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Fehlerbehandlung und -protokollierung
Sicherheitsrisiko	• Schweregradpunktzahl: 2.2 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn Sie diese Eigenschaft auf „ **falsch** “ setzen, wird die Protokollierung für Anwender mit geringeren Berechtigungen aktiviert, was es einem böswilligen Akteur ermöglichen könnte, einen Angriff zu verschleiern.
Abhängigkeiten und Voraussetzungen	Keine

Sicheres Cookie-Debugging deaktivieren

Verwalten Sie die Protokollnachrichten im Zusammenhang mit Cookies in Ihrer Instanz.

Verwenden Sie die Eigenschaft und *glide.secure_cookie.debug*, um Ihre Protokollnachrichten im Zusammenhang mit Cookies zu verwalten. Wenn diese Eigenschaft auf **false**festgelegt ist, werden keine Protokollnachrichten angezeigt. Wenn sie auf **true**festgelegt ist, werden Nachrichten in den Klassen `SecureUserCookie` und `Cookie` protokolliert. Dies könnte dazu führen, dass in Ihrer Instanz vertrauliche Informationen verfügbar gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.secure_cookie.debug*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	falsch
Standardwert	falsch
Kategorie	Fehlerbehandlung und -protokollierung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 4.2 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn Sie diese Eigenschaft auf „ **wahr** “ konfigurieren, können vertrauliche Informationen verfügbar gemacht werden.
Abhängigkeiten und Voraussetzungen	Keine

SQL-Fehlermeldungen deaktivieren [In Security Center 1.3 aktualisiert]

Verwenden Sie die Eigenschaft *glide.db.loguser*, um die Darstellung von SQL-Fehlermeldungen in einem Browser zu deaktivieren.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.db.loguser*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Fehlerbehandlung und -protokollierung
Zweck	Um die Anzeige von SQL-Fehlermeldungen im Browser zu deaktivieren.
Typ	boolean
Empfohlener Wert	falsch
Standardwert	wahr
Sicherheitsrisikobewertung	3.1
Funktionale Auswirkung	(Niedrig) Diese Korrektur deaktiviert das Rendern von SQL-Fehlermeldungen. Es gibt keine Auswirkungen auf Funktionen.
Sicherheitsrisiko	(Mittel) Es sollten keine vertraulichen SQL-Informationen, die einem Angreifer helfen könnten, als Teil der Fehlermeldung auf einer Webseite angezeigt werden.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

MID-Audit-Protokoll aktivieren [Neu in Security Center 1.3 und aktualisiert in 1.5]

Das Audit-Protokoll für MID-Server-Befehle zeichnet Details wie den Befehlsnamen, den Befehlshash, den Namen der verwendeten Anmeldeinformationen und den Ausführungsstatus auf.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nach der Aktivierung können Audit-Protokolle von Benutzern mit der Rolle agent_security_admin in der Tabelle ecc_agent_command_audit_log oder durch Navigieren zu angezeigt werden **MID-Server** > **Befehlsauditprotokolle**an.

Legen Sie *mid.log.command_audit.enable* in der Tabelle „ecc_agent_property“ auf „true“ fest, um die Überwachung für vom MID-Server ausgeführte Befehle zu aktivieren.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*mid.log.command_audit.enable*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Fehlerbehandlung und -protokollierung
Sicherheitsrisiko	• Schweregradpunktzahl: 2.2 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Im Falle einer Sicherheitsuntersuchung kann diese Tabelle von Incident-Antwortteams verwendet werden, um die auf dem MID-Server ausgeführten Befehle zu prüfen. Ohne dieses Protokoll sind möglicherweise nicht genügend Details vorhanden, um auf Situationen wie die nicht autorisierte Kontoverwendung zu reagieren.
Abhängigkeiten und Voraussetzungen	Keine

Plugin „Protected Tables“ aktivieren [Neu in Security Center 1.3]

Verwenden Sie die Eigenschaft *com.glide.security.protected_table.enabled*, um zu verhindern, dass Benutzer mit höheren Berechtigungen Protokolltabellen manipulieren.

Wenn die Eigenschaft *com.glide.security.protected_table.enabled* auf **true**festgelegt ist, wird das Plugin für geschützte Tabellen verwendet, um zu verhindern, dass Benutzer mit höheren Berechtigungen in einer Instanz Protokolltabellen manipulieren. Die folgenden Protokolltabellen verfügen über besondere Schutzmaßnahmen, wenn diese Eigenschaft auf „ **true**“ festgelegt ist:

- syslog (keine DB-Überschreibung)
- syslog_transaction
- sys_outbound_http_log
- sysevent
- sys_audit

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sys_push_notification
- opened_table_configuration (keine DB-Überschreibung)

Die Integrität von Protokollen ist wichtig, um schädliche Aktivitäten in einer Instanz durch einen Kundenadministrator zu ermitteln.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*com.glide.security.protected_table.enabled*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Fehlerbehandlung und -protokollierung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 4,5 • CVSS-Punktzahl: Mittel • Details zu Sicherheitsrisiken: Wenn *com.glide.security.protected_table.enabled* nicht auf den empfohlenen Wert „true“ festgelegt wird, können Benutzer mit höheren Berechtigungen in einer Instanz Protokolltabellen manipulieren.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Systemprotokolle

Alle Felder für ausgehende HTTP-Anforderungen protokollieren [Entfernt in Security Center v1.3.2]

Konfigurieren Sie die Eigenschaft bis *glide.outbound_http.security.log.allow.all.fields* auf „falsch“, um zu verhindern, dass sensible ausgehende HTTP-Felder im Nur-Text-Format protokolliert werden.

Wenn diese Eigenschaft nicht auf den empfohlenen Wert **false**festgelegt ist, werden sensible ausgehende HTTP-Felder möglicherweise im Nur-Text-Format protokolliert. Dies kann den Sicherheitsstatus Ihres Unternehmensnetzwerks beeinträchtigen, da ausgehende Anforderungen mit vertraulichen Daten und Anmeldeinformationen im unverschlüsselten Nur-Text-Format protokolliert und von Benutzern mit geringeren Berechtigungen angezeigt werden können.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.outbound_http.security.log.allow.all.fields*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Datentyp	integer
Empfohlener Wert	30
Standardwert	30
Kategorie	Fehlerbehandlung und -protokollierung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 6,8 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf „ **falsch** “ festgelegt wird, erhöht sich die Wahrscheinlichkeit, dass sensible ausgehende Felder im Nur-Text-Format protokolliert werden, was ein Sicherheitsrisiko darstellt.
Abhängigkeiten und Voraussetzungen	Keine

HTML-Bereinigung protokollieren

Konfigurieren Sie die Eigenschaft *glide.html_sanitize.discarded_log.enable*, um zu bestimmen, ob HTML-Bereinigungsereignisse in Ihrer Instanz protokolliert werden.

Wenn diese Eigenschaft nicht auf den empfohlenen Wert **true**festgelegt ist, werden HTML-Bereinigungsereignisse nicht in der Tabelle *sys_log* protokolliert. Fehlende Protokollierung kann sich negativ auf die automatisierten Sicherheitserkennungs- und Untersuchungsfunktionen Ihrer Instanz auswirken.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.html_sanitize.discarded_log.enable*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Fehlerbehandlung und -protokollierung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 2,4 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf den empfohlenen Wert **true**festgelegt ist, werden HTML-Bereinigungsereignisse nicht in der Tabelle *sys_log* protokolliert, was sich auf die automatisierten Sicherheitserkennungs- und Untersuchungsfunktionen auswirken könnte.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	HTML-Bereinigung aktivieren

Sitzungsaudit-Ereignisse protokollieren [Neu in Security Center 1.3]

Legen Sie die Eigenschaft *glide.authenticate.session_access.log_audit_event* auf **true**fest, damit Audit-Ereignisse für Sitzungen in der Tabelle *sys_session_access_audit* erstellt werden.

Das Protokollieren von Informationen über den Sitzungszugriff hilft Ihnen bei der Analyse von Cybersicherheitsangriffen. Zu den protokollierten Informationen gehören Anwender, Sitzungs-ID (nicht vertraulich), IP-Adresse, Rollen und Richtlinien.

Hinweis: Die Systemeigenschaft *glide.authenticate.session_access.log_audit_event* ist spezifisch für den Zero Trust-Zugriff. Weitere Informationen finden Sie unter Zero Trust-Zugriff.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.authenticate.session_access.log_audit_event*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Fehlerbehandlung und -protokollierung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 6.3 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf den empfohlenen Wert „wahr“ festgelegt wird, wird die Protokollierung von Ereignissen verhindert. Dies könnte verhindern, dass Sie im Falle eines Cyberangriffs böswillige Akteure finden.
Abhängigkeiten und Voraussetzungen	Keine

Protokollieren Sie den Identitätswechsel des Anwenders

Konfigurieren Sie *glide.sys.log_impersonation*, um zu steuern, ob Ereignisse, die die Identität von Benutzern annehmen, in Ihrer Instanz protokolliert werden.

Wenn diese Eigenschaft nicht auf den empfohlenen Wert **true**festgelegt ist, werden Ereignisse, bei denen die Identität von Benutzern angenommen wird, nicht mehr protokolliert. Das Ausbleiben der Protokollierung kann sich auf die automatisierten Sicherheitserkennungs- und Untersuchungsfunktionen in Ihrer Instanz auswirken.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.sys.log_impersonation*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Fehlerbehandlung und -protokollierung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 6,4 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf „ **true**“ festgelegt ist, werden Ereignisse, die die Identität von Anwendern annehmen, nicht mehr protokolliert, was sich auf die Sicherheitserkennungs- und Untersuchungsfunktionen Ihrer Instanz auswirken könnte.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Identität von Benutzern annehmen

Deaktivieren Sie ausführliche SQL-Fehlermeldungen für den Importprozessor

Konfigurieren Sie diese Eigenschaft, um zu steuern, ob ausführliche SQL-Fehlermeldungen angezeigt werden.

Wenn die Eigenschaft auf „ **false**“ festgelegt ist, wird eine ausführliche SQL-Fehlermeldung angezeigt, die vertrauliche Informationen offenlegen kann. Um dies zu vermeiden, legen Sie die Eigenschaft auf **„true“** fest, um eine generische Nachricht anzuzeigen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.import.error_message.generic*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Fehlerbehandlung und -protokollierung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 3,1 • CVSS-Punktzahl: Niedrig

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Details zum Sicherheitsrisiko: Wenn Sie die Eigenschaft auf „ **falsch** “ setzen, werden ausführliche SQL-Nachrichten aktiviert, die zu Informationsverlusten führen können.
Abhängigkeiten und Voraussetzungen	Keine

Datei und Ressourcen

Die Kategorie „Datei und Ressourcen“ stellt sicher, dass Anwendungen Daten in nicht vertrauenswürdigen Dateien sicher verarbeiten und nicht vertrauenswürdige Daten aus nicht vertrauenswürdigen Quellen mit eingeschränkten Berechtigungen an einem geeigneten Ort speichern.

Dies umfasst Steuerungen wie das Vermeiden von Denial of Service durch große oder unerwartete Dateitypen, das Validieren des Dateityps und das Verhindern eines Pfaddurchlaufs.

Download infizierter Dateien nicht zulassen

Verwalten Sie diese Eigenschaft, um zu steuern, ob Stack Traces in Ihrer Instanz angezeigt werden.

Wenn die Eigenschaft *com.glide.snap.infected_download_allowed* auf „true“ festgelegt ist, können Benutzer weiterhin nicht gescannte Anhänge herunterladen, falls der Antivirus-Service ausfällt oder nicht erreichbar ist. In dieser Situation besteht für Benutzer möglicherweise das Risiko, dass sie eine schädliche Datei herunterladen und dadurch ihren Desktop infizieren, insbesondere wenn auf dem Gerät kein anderer Endpunktschutz installiert ist.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*com.glide.snap.infected_download_allowed*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	falsch
Standardwert	falsch
Kategorie	Datei und Ressourcen
Sicherheitsrisiko	• Schweregrad-Punktzahl: 6,7 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn Sie diese Eigenschaft nicht auf den empfohlenen Wert „falsch“ festlegen, kann Ihre Instanz dem Herunterladen schädlicher Dateien ausgesetzt sein.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Abhängigkeiten und Voraussetzungen	Keine

Bewertung und Filterung von E-Mail-Spam aktivieren [Aktualisiert in Security Center 1.3]

Installieren Sie das Plugin „E-Mail-Filter“ (*com.glide.email_filter*), um die E-Mail-Filterung innerhalb der Instanz zu installieren. Diese Filterung identifiziert vorhandene Header, sodass Sie basierend auf dem zugeordneten Header entscheiden können, was mit der E-Mail geschehen soll.

Jede über E-Mail-Server Now Platform gesendete Nachricht wird auf die Wahrscheinlichkeit geprüft, Spam zu sein.

Hinweis: Wenn eine Instanz einen privaten E-Mail-Server verwendet, ist dieses Thema nicht anwendbar. Weitere Informationen finden Sie unter Bewertung und Filterung von E-Mail-Spam.

Voraussetzungen

Vor dem Festlegen dieser Eigenschaft:

Legen Sie die Eigenschaft *glide.email.read.active* auf „Wahr“ fest. Weitere Informationen finden Sie unter Verwendung eigenen POP3-Servers aktivieren .

Weitere Informationen

Attribut	Beschreibung
Plugin-Name	*com.glide.email_filter*
Konfigurationstyp	Systemdefinition > Plugins
Kategorie	Datei und Ressourcen
Zweck	Um Filterung zu erzwingen, um Spam von E-Mails zu vermeiden.
Empfohlener Wert	Aktiv
Standardwert	Keine. Dies ist ein Plugin, keine Glide-Eigenschaft, daher gibt es keinen Standardwert.
Sicherheitsrisikobewertung	8.1
Funktionale Auswirkung	E-Mails (niedrig) werden im Rahmen der Spam-Bewertung niemals in der Instanz gefiltert, blockiert oder unter Quarantäne gestellt. Er wird nur bewertet und dann an die Instanz gesendet. Alle Filter werden innerhalb der Instanz mit dem Plugin „E-Mail-Filter“ durchgeführt.
Sicherheitsrisiko	(Mittel) E-Mail-Filter ermöglichen Administratoren die Verwendung eines Bedingungsgenerators oder eines bedingten Skripts, um anzugeben, wann böswillige eingehende E-Mails von bekannten/unbekannten Absendern ignoriert werden sollen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Referenzen	E-Mail-Filter https://support.servicenow.com/kb_view.do?sysparm_article=KB0549426

Weitere Informationen zum Aktivieren von Plugins finden Sie unter Plugins aktivieren .

Antivirenprüfung aktivieren

Die Eigenschaft *com.glide.snap.enable_scan* aktiviert die Antivirus-Scan-Funktion.

Legen Sie *com.glide.snap.enable_scan* auf den empfohlenen Wert „ **wahr** “ fest, um die Virenprüfung zu aktivieren.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*com.glide.snap.enable_scan*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Datei und Ressourcen
Zweck	Um das Scannen auf Viren für eine bestimmte Instanz zu aktivieren oder zu deaktivieren
Empfohlener Wert	wahr
Standardwert	wahr
Datentyp	boolean
Sicherheitsrisiko	(Hoch) Antivirus-Scans tragen zum Schutz Ihrer Instanz vor Virusinfektionen bei, die durch Dateianhänge zu Ihren Systemdatensätzen (z. B. Incidents, Probleme und Storys) eingeführt werden können.
Sicherheitsrisikobewertung	7.7

Herunterladbare Dateitypen in statischen Inhalten beschränken [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.ui.strict_customer_uploaded_static_content*, um Einschränkungen für die Dateitypen zu aktivieren, die heruntergeladen werden können, wenn sie mit der Funktion „Datei hochladen“ hochgeladen wurden.

Sie verwenden diese Eigenschaft mit der Eigenschaft *glide.ui.strict_customer_uploaded_content_types*, die eine durch Kommas getrennte Liste mit eingeschränkten herunterladbaren Dateitypen erstellt. Weitere Informationen finden Sie unter Herunterladbare Dateitypen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnung: Der Wert für diese Eigenschaft ist eine Überschreibung ohne DB. Sie kann nicht geändert oder überschrieben werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.ui.strict_customer_uploaded_static_content*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Datei und Ressourcen
Zweck	Um sicherzustellen, dass sichere Dateitypen aus der Anwendung heruntergeladen werden dürfen.
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	3.1
Funktionale Auswirkung	(Niedrig) Diese Korrektur erzwingt die Einschränkung von Dateidownloads basierend auf den Werten, die in der Eigenschaft *glide.ui.strict_customer_uploaded_content_types* angegeben sind. Weitere Informationen finden Sie unter Herunterladbare Dateitypen.
Sicherheitsrisiko	(Niedrig) Dateidownload-Einschränkungen sollten auf alle nicht vertrauenswürdigen Benutzereingabequellen angewendet werden.

Anhangsgröße in Trainings- und Vorhersage-Flows für GraphQL-Endpunkte begrenzen [Neu in Security Center 1.3 und aktualisiert in 1.5]

Die Eigenschaft *glide.platform_ml_di.max_attachment_size_graphql* steuert die maximal zulässige Größe für die Rückgabe von Anhängen in GraphQL-Endpunkten von Trainings- oder Vorhersage-Flows.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.platform_ml_di.max_attachment_size_graphql*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer
Empfohlener Wert	5,242,880
Standardwert	5.242.880
Kategorie	Datei und Ressourcen
Sicherheitsrisiko	• Schweregrad-Punktzahl: 4.3 • CVSS-Punktzahl: Mittel

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf den empfohlenen Wert von 5.242.880 oder weniger festgelegt ist, kann die Rückgabe großer Dateien zu einem Denial of Service (DoS) führen.
Abhängigkeiten und Voraussetzungen	Keine

Anhangsgröße in Trainings- und Vorhersage-Flows begrenzen [Neu in Security Center 1.3 und aktualisiert in 1.5]

Die Eigenschaft *glide.platform_ml_di.max_attachment_size* steuert die maximal zulässige Größe für die Rückgabe von Anhängen in Trainings- und Vorhersage-Flows.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.platform_ml_di.max_attachment_size*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer
Empfohlener Wert	4,000,000
Standardwert	4.000.000
Kategorie	Datei und Ressourcen
Sicherheitsrisiko	• Schweregrad-Punktzahl: 4.3 • CVSS-Punktzahl: Mittel • Details zu Sicherheitsrisiken: Wenn *glide.platform_ml_di.max_attachment_size* nicht auf den empfohlenen Wert von 4.000.000 oder weniger festgelegt ist, kann die Rückgabe großer Dateien einen Denial-of-Service-Angriff (DoS) verursachen.
Abhängigkeiten und Voraussetzungen	Keine

Größe des HTTP-Antworttexts begrenzen [Neu in Security Center 1.3 und aktualisiert in 1.5]

Konfigurieren Sie die Eigenschaften *glide.http.response.get_body.limit.enabled* und *glide.http.response.get_body.limit*, um Ihre Instanz vor *OutOfMemoryExceptions* zu schützen.

Die Eigenschaften *glide.http.response.get_body.limit.enabled* und *glide.http.response.get_body.limit* wurden eingeführt, um neue Funktionen zu aktivieren, die verhindern, dass *OutOfMemoryExceptions* als Ergebnis einer zu großen Anforderungsantwort ausgelöst werden. *„OutOfMemoryExceptions"* können Denial-of-

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Service-Angriffe (DoS) sowie andere Probleme verursachen, die Angreifern dabei helfen können, eine Instanz zu gefährden.

Um Ihre Instanz vor diesen Sicherheitsschwachstellen zu schützen, stellen Sie sicher, dass *glide.http.response.get_body.limit.enabled* auf „true“ festgelegt ist und *glide.http.response.get_body.limit* nicht mehr als 524.288.000 Megabyte (500 MB) beträgt.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.http.response.get_body.limit.enabled* und *glide.http.response.get_body.limit*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Datei und Ressourcen
Sicherheitsrisiko	• Schweregrad-Punktzahl: 6,4 • CVSS-Punktzahl: Mittel • Details zu Sicherheitsrisiken: Wenn Sie diese Eigenschaften nicht auf die empfohlenen Werte festlegen, kann Ihre Instanz angreifbar für *OutOfMemoryExceptions* und Denial-of-Service-Angriffe werden.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Diese Eigenschaft verringert das Risiko einer *OutOfMemoryException*, wenn ein Kunde versehentlich eine große Datei in den Arbeitsspeicher lädt.

Beschränken Sie die maximale Anzahl von Anhängen in E-Mails

Konfigurieren Sie die Anzahl der eingehenden E-Mail-Anhänge in Ihrer -Instanz.

Die Eigenschaftund *glide.email.inbound.max_attachment_count* steuert die maximale Anzahl eingehender E-Mail-Anhänge in Ihrer Instanz. Wenn diese Eigenschaft nicht auf den empfohlenen Wert von **30** oder weniger festgelegt ist, können eingehende E-Mails zu einer Verschlechterung der Instanzleistung führen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.email.inbound.max_attachment_count*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Datentyp	integer
Empfohlener Wert	30
Standardwert	30
Kategorie	Datei und Ressourcen
Sicherheitsrisiko	• Schweregrad-Punktzahl: 5.3 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Das Festlegen des Eigenschaftswerts auf mehr als 30 kann zu Verschlechterungsproblemen führen.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	E-Mail-Eigenschaften

Zulässige Anhangsgröße minimieren [Aktualisiert in Security Center 1.3]

Konfigurieren Sie die Eigenschaft *com.glide.attachment.max_size*, um die maximal zulässige Größe für einen hochgeladenen Anhang zu steuern.

Diese Eigenschaft steuert die maximale Größe eines hochgeladenen Anhangs. Wenn diese Eigenschaft nicht auf den empfohlenen Wert von **1024** oder weniger festgelegt ist, kann die Plattform große Dateien akzeptieren, die den Speicher füllen und zu einem Denial of Service-Angriff (DoS) führen könnten.

Hinweis: Die tatsächliche Anhangsgröße wird berechnet, indem 1024 x 1024 mit dem Wert der Eigenschaft multipliziert wird. Wenn der Wert der Eigenschaft **1024**ist, beträgt die maximal zulässige Größe für einen Anhang 1 GB.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*com.glide.attachment.max_size*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer
Empfohlener Wert	1024
Standardwert	4096
Kategorie	Datei und Ressourcen
Sicherheitsrisiko	• Schweregrad-Punktzahl: 6,5 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn diese Eigenschaft nicht auf **1024** oder einen kleineren Wert festgelegt ist, kann die Plattform große Dateien akzeptieren, die zu einem DoS-Angriff führen können.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Eigenschaften der Anhangsbeschränkungen

Validiert den Datei-MIME-Typ im SOAP-Webservice „AttachmentCreator“ [Neu in Security Center 1.3]

Die Eigenschaft *glide.attachment.enforce_security_validation* bestimmt, ob MIME-Dateien (Multifunktions-Internet-Mail-Erweiterungen) einer Validierung unterzogen werden.

Wenn *glide.attachment.enforce_security_validation* nicht auf den empfohlenen Wert **true**festgelegt ist, finden keine Validierung für MIME-Dateien statt, sodass schädliche Dateien mit falschen Dateierweiterungen hochgeladen werden können. Wenn diese Eigenschaft auf festgelegt ist, werden die Dateien mit der **richtigen**Dateierweiterung hochgeladen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.attachment.enforce_security_validation*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Datei und Ressourcen
Sicherheitsrisiko	• Schweregrad-Punktzahl: 7,5 • CVSS-Punktzahl: Hoch • Details zum Sicherheitsrisiko: Wenn die Eigenschaft auf „false“ festgelegt ist, finden beim Hochladen keine Validierungen für MIME-Dateien statt. Dies könnte es ermöglichen, schädliche Dateien zu verschleiern, indem ihre Dateierweiterung geändert wird.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	https://developer.mozilla.org/en-US/docs/Web/HTTP/Basics_of_HTTP/MIME_types/Common_types
Funktionale Auswirkung	Legen Sie diese Härtungseinstellung auf „wahr“ fest, um MIME-Typ- und Dateierweiterungsvalidierungen für hochgeladene Dateianhänge auszuführen. Wenn diese Eigenschaft auf „falsch“ festgelegt ist, werden keine Validierungen ausgeführt. Diese Eigenschaft ist standardmäßig auf „true“ festgelegt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Böswilliger Code

Die Kategorie „Böswilliger Code“ stellt sicher, dass nach Möglichkeit geprüft wird, ob Ihr Code frei von Schwachstellen und unerwünschten Funktionen ist.

Dies beinhaltet die Sicherstellung einer sicheren und ordnungsgemäßen Behandlung schädlicher Aktivitäten, keine zeitbasierten Angriffe, keine ausgehende Kommunikation an nicht vertrauenswürdige Ziele und dass kein nicht autorisierter oder von Angreifern kontrollierter Code enthalten ist. Diese Kategorie enthält Audit- oder Drittparteibibliotheken aus der Anwendungscodebasis.

Blockieren Sie gerootete Mobilgeräte oder Mobilgeräte mit Jailbreak

Sichern Sie Ihre Instanz, indem Sie nicht autorisierte Zugriffe von Geräten mit Jailbreak verhindern.

Verwenden Sie die Eigenschaft *glide.sg.allow_rooted_jailbroken_device*, um Ihre Instanz vor nicht autorisiertem Zugriff durch Geräte mit Jailbreak zu schützen. Wenn ein Anwender versucht, sich mit einer mobilen App bei einer Instanz zu authentifizieren, während diese Eigenschaft auf „ **false**“ festgelegt ist, erhält er die folgende Warnung: `Auf diesem Gerät wurde anscheinend ein Jailbreak durchgeführt, daher kann es nicht für den Zugriff auf diese Instanz verwendet werden. Wenden Sie sich an Ihren ServiceNow-Administrator.` Die App ist eingefroren, während die Warnmeldung angezeigt wird. Die einzige Möglichkeit, diese Meldung zu schließen, ist das Auswählen **von Abmelden**. Wenn diese Eigenschaft auf „ **true** “ festgelegt ist, authentifizieren sich Benutzer bei einer Instanz mit einem Gerät, das einen Jailbreak durchgeführt hat.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.sg.allow_rooted_jailbroken_device*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	falsch
Standardwert	falsch
Kategorie	Böswilliger Code
Sicherheitsrisiko	• Schweregrad-Punktzahl: 4,5 • CVSS-Punktzahl: Mittel • Details zu Sicherheitsrisiken: Der Mangel an Sicherheit bei Geräten mit Jailbreak macht sie zu einem Hauptziel für böswillige Akteure. Wenn nicht autorisierte Personen auf Unternehmensdaten zugreifen, kann dies die Sicherheitslage eines Unternehmensnetzwerks schwächen.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Zugriffssteuerung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Codesignatur für Anwendungskonfigurationsdaten und -skripts aktivieren [Entfernt in Security Center 1.3]

Verwalten Sie Codesignatur für Anwendungskonfigurationsdaten und Skripts in Ihrer -Instanz.

Codesignatur kann die Sicherheit verbessern, indem vertrauliche Anwendungskonfigurationsdaten und Skripts validiert werden, bevor sie verwendet werden. Die Codesignatur erstellt digitale Signaturen für die Daten, die später überprüft werden, um die Authentizität und Integrität der Daten zu bestätigen. Diese Überprüfung verhindert, dass in der Instanz schädliche Daten oder Skripts verwendet werden, was zu einer vollständigen Gefährdung der Instanz führen kann.

Verwenden Sie die Eigenschaft] bisund *com.snc.kmf.signature.validation.flag*, um die Codesignatur für Anwendungskonfigurationsdaten und -skripts zu verwalten. Wenn diese Eigenschaft auf „ **true**“ festgelegt werden soll, wird Codesignatur für Anwendungskonfigurationsdaten und Skripts aktiviert.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*com.snc.kmf.signature.validation.flag*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Böswilliger Code
Sicherheitsrisiko	• Schweregrad-Punktzahl: 6 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn Sie diese Eigenschaft auf „ **true** “ setzen, wird die Codesignatur aktiviert, die zur Verbesserung der Sicherheit beiträgt, indem vertrauliche Anwendungskonfigurationsdaten und Skripts validiert werden.
Abhängigkeiten und Voraussetzungen	Keine

Management von Anwendersitzungen

Diese Kategorie befasst sich mit der Sicherheit des Anwendungsstatus für einen Anwender. Sitzungen sollten für jede Person eindeutig sein, nicht erraten oder geteilt werden können und nach Phasen der Inaktivität oder wenn sie nicht benötigt werden, für ungültig erklärt werden. Dies umfasst Faktoren wie Cookie-Attribute für Cookies-basierte Sitzungen, die Generierung von Sitzungstoken und den Speicher sowie Anforderungen für die erneute Verbundauthentifizierung.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Absolute Zeitüberschreitungsdauer für Sitzung minimieren [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.ui.user_cookie.max_life_span_in_days*, um eine maximale Lebensdauer für Anwendercookies festzulegen, die erstellt werden, wenn sich Anwender mit **aktiviertem** Kontrollkästchen „Anwendernamen speichern“ anmelden. Wenn das **Cookie** abläuft, werden Benutzer, die das Kontrollkästchen „Anwendernamen speichern“ aktiviert, müssen sich erneut bei der Instanz authentifizieren.

Dadurch kann das Benutzercookie für die Dauer angegebener Tage gültig sein, beginnend mit der ersten Ausgabe des Cookies. Der Standardwert beträgt 30 Tage, und die maximale Obergrenze liegt bei 365 Tagen.

Hinweis: Informationen zum Erzwingen einer maximalen Sitzungsdauer für aktive Benutzersitzungen finden Sie unter Benutzersitzungen verwalten .

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.ui.user_cookie.max_life_span_in_days*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Management von Anwendersitzungen
Zweck	Um zu erzwingen, dass Benutzer, die das Kontrollkästchen **Anwendernamen** speichern aktiviert haben, sich nach bestimmten Tagen erneut authentifizieren.
Empfohlener Wert	Weniger als oder gleich 30
Standardwert	30 Tage
Funktionale Auswirkung	(Mittel) Diese Eigenschaft erzwingt die obligatorische erneute Anmeldung, indem jede Art von Cookie-Rotation nach einem bestimmten Zeitrahmen vermieden wird.
Sicherheitsrisikobewertung	4.2
Sicherheitsrisiko	(Mittel) Dass Anwendercookies für unbestimmte Zeit aktiv sind, stellt ein Sicherheitsrisiko dar und sollte bei einer zeitbasierten Konfiguration ablaufen.
Referenzen	Verfügbare Systemeigenschaften Anwendernamen speichern

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Ausnahmerollen für Zeitüberschreitung bei aktiver Sitzung definieren [Neu in Security Center 1.3]

Die Eigenschaft *glide.active.session.timeout.exception.roles* steuert die Rollen, die von einer Zeitüberschreitungsgrenze für aktive Sitzungen befreit sind.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Zeitüberschreitung für aktive Sitzungen stellt sicher, dass eine gekaperte Sitzung nicht unbegrenzt verwendet werden kann, ohne dass die Authentifizierungsinformationen erneut angegeben werden. Um dieses Sicherheitsrisiko zu beheben, stellen Sie sicher, dass die Eigenschaft *glide.active.session.timeout.exception.roles* auf **„edge_encryption, mid_server“ festgelegt ist**.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.active.session.timeout.exception.roles*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	„edge_encryption“, „mid_server“.
Standardwert	„edge_encryption“, „mid_server“.
Kategorie	Management von Anwendersitzungen
Sicherheitsrisiko	• Schweregrad-Punktzahl: 7.1 • CVSS-Punktzahl: Hoch • Details zum Sicherheitsrisiko: Berücksichtigen Sie nur eine Ausnahme für die Zeitüberschreitungsgrenze für aktive Sitzungen für interne Integrationskontorollen. Wenn für eine Rolle eine Ausnahme von der Sitzungszeitüberschreitung gewährt wird und diese Rolle einem Benutzer zugewiesen wird, der Opfer eines Hijacking-Angriffs auf die Sitzung wird, kann ein Angreifer sich weiterhin unbegrenzt bei dieser Sitzung authentifizieren. Dies kann die Auswirkungen eines Security Incident erhöhen, da ein Angreifer mehr Zeit hat, ein gekapertes Konto auszunutzen.
Abhängigkeiten und Voraussetzungen	Keine

Aktivieren Sie UserCookie Version 3.1

Verwalten Sie die Version von UserCookie, die in Ihrer Instanz aktiviert ist, um die Speicherung des geheimen Schlüssels im Quellcode zu sichern.

UserCookie v3 wird nur generiert, wenn die Eigenschaft *glide.ui.secure.cookies.use_kmf* deaktiviert ist. UserCookie v3 ist nicht sicher, da der geheime Schlüssel für Hash-basierte Nachrichtenauthentifizierungscodes (HMAC) im Quellcode gespeichert wird, der für alle Kunden identisch ist. Ein böswilliger Akteur kann einen geheimen Schlüssel verwenden, um zu versuchen, Benutzersitzungen zu kapern. Um dieses Sicherheitsrisiko zu beheben, stellen Sie sicher, dass die Eigenschaft *glide.ui.secure.cookies.use_kmf* auf „ **wahr** “ festgelegt ist, die UserCookie v3.1 verwendet. Der geheime Schlüssel wird in einem sicheren Speicher wie KMF gespeichert.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.ui.secure.cookies.use_kmf*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Management von Anwendersitzungen
Sicherheitsrisiko	• Schweregrad-Punktzahl: 7.1 • CVSS-Punktzahl: Hoch • Details zum Sicherheitsrisiko: Die Einstellung auf „ **false** “ stellt eine Sicherheitsschwachstelle dar, die durch den geheimen Schlüssel für Hash-basierte Nachrichtenauthentifizierungscodes (HMAC) verursacht wird, der im Quellcode gespeichert ist.
Abhängigkeiten und Voraussetzungen	Keine

Passwortzurücksetzung für API-Anforderungen erzwingen

Verwalten Sie, wie die Funktion zum Zurücksetzen des Passworts auf Ihre Instanz funktioniert.

Wenn ein Anwender für **Passwort muss zurückgesetzt**werden gekennzeichnet ist, muss er beim nächsten Authentifizierungsversuch ein neues Passwort eingeben. Diese Eigenschaft steuert, ob die Passwortzurücksetzung vor dem Ausführen von API-Aufrufen obligatorisch ist. Wenn diese Eigenschaft nicht auf den empfohlenen Wert **true**festgelegt ist, können Anwenderaccounts, die als **Passwort muss zurückgesetzt** werden gekennzeichnet sind, können weiterhin Vorgänge ausführen, indem sie die Tabellen-API über die Standardauthentifizierung abfragen. Diese Sicherheitsschwachstelle kann zu Informationsverlust führen, wenn ein inaktives Konto gefährdet wird.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.authenticate.api.user.reset_password.mandatory*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Management von Anwendersitzungen

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	• Bewertung mit Schweregrad: 8,1 • CVSS-Punktzahl: Hoch • Details zu Sicherheitsrisiken: Das Festlegen dieser Eigenschaft auf „ **falsch** “ kann zu Informationsverlust führen, wenn ein inaktives Konto gefährdet wird.
Abhängigkeiten und Voraussetzungen	Keine

Kennzeichnung für „Nur-HTTP-Cookie“ aktivieren [In Security Center 1.3 aktualisiert]

Verwenden Sie die Eigenschaft *glide.cookies.http_only*, um das HTTPOnly-Attribut für vertrauliche Cookies zu aktivieren.

Verwenden Sie das Attribut HTTPOnly, um Angriffe wie websiteübergreifendes Skripting zu verhindern, da es keinen Zugriff auf das Cookie mit einem clientseitigen Skript wie JavaScript zulässt. Dadurch werden die Risiken von websiteübergreifendem Skripting nicht eliminiert, es werden jedoch einige Angriffsvektoren eliminiert.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.cookies.http_only*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Management von Anwendersitzungen
Zweck	Um das Risiko eines clientseitigen Skriptzugriffs auf das geschützte Cookie zu minimieren.
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	8
Funktionale Auswirkung	(Niedrig) Diese Korrektur fügt Sitzungscookies eine zusätzliche HTTPOnly-Kennzeichnung hinzu und schützt sie so vor Diebstahl. • Wenn Sie über eine anwenderdefinierte Funktionalität verfügen, für die JavaScript erforderlich ist, um auf das Cookie des Anwenders zuzugreifen, wird diese Funktionalität beeinträchtigt. Unter normalen Umständen sollte dies nicht der Fall sein.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Now Platform übernimmt die Sitzungsverwaltung, und es darf keinen Grund dafür geben, dass ein benutzerdefiniertes Skript auf die Cookies des Benutzers zugreift.
Sicherheitsrisiko	(Moderat) Sitzungscookies in der Anwendung authentifizieren einen Endanwender und stellen implizite Zugriffsberechtigungen für die Anwendung bereit. Das heißt, sie müssen vor Diebstahl oder Export geschützt werden. Nur-HTTP-Kennzeichnungen schützen die Sitzungscookies vor JavaScript-Einschleusungen oder websiteübergreifenden Skripting-Schwachstellen, die sie stehlen.
Referenzen	Verfügbare Systemeigenschaften

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Anzahl der gleichzeitigen interaktiven Sitzungen minimieren [Aktualisiert in Security Center 1.3]

Verwenden Sie diese Eigenschaft mit dem Plugin „Gleichzeitige Sitzungen begrenzen“, um die Anzahl der aktiven Sitzungen zu steuern, die von einem Benutzer geöffnet werden können.

Verwenden Sie die Eigenschaft „Maximale Anzahl **gleichzeitiger interaktiver Sitzungen für Glide-Authentifizierung** “ mit dem Plugin „ **Gleichzeitige Sitzung begrenzen** “ (*com.glide.limit.concurrent.sessions*), um die Anzahl der aktiven Sitzungen zu steuern, die für einen Benutzer geöffnet sind. Der empfohlene Wert ist **1**. Dadurch wird die Anzahl der geöffneten Sitzungen verringert (eine höhere Anzahl erhöht die Wahrscheinlichkeit, dass eine Sitzung gekapert wird).

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.authenticate.max.concurrent.interactive.sessions*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer
Empfohlener Wert	1
Standardwert	1
Kategorie	Management von Anwendersitzungen
Sicherheitsrisiko	• Schweregrad-Punktzahl: 3,7 • CVSS-Punktzahl: Niedrig

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Details zum Sicherheitsrisiko: Wenn Sie den Standardwert der Eigenschaft auf größer als 1 setzen, erhöht sich die Wahrscheinlichkeit eines Hijacking-Angriffs auf Sitzungen.
Abhängigkeiten und Voraussetzungen	Das Plugin „ **Gleichzeitige interaktive Sitzungen** “ (*com.glide.limit.concurrent.sessions*) muss aktiviert sein.
Referenzen	Begrenzen Sie gleichzeitige Sitzungen

Gleichzeitige Sitzungen über alle Knoten hinweg begrenzen [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.authenticate.limit.concurrent.sessions.across.all.nodes* mit dem Plugin „Gleichzeitige Sitzungen begrenzen“, um die Anzahl der auf allen Knoten nachverfolgten Sitzungen zu verwalten.

Wenn das Plugin Begrenzen Sie gleichzeitige Sitzungen „ aktiv ist, kann die Anzahl der offenen Sitzungen pro Benutzer begrenzt werden. Stellen Sie sicher, dass, wenn dieses Plugin aktiv ist, die Eigenschaft (**Glide-Authentifizierung für gleichzeitige Sitzungen auf allen Knoten beschränken**) auf „ **wahr** “ festgelegt ist, damit die Anzahl der offenen Sitzungen für alle Knoten und nicht für einen einzelnen Anwendungsknoten nachverfolgt wird. Wenn diese Eigenschaft auf **false**festgelegt ist, können mehrere Sitzungen auf mehreren Knoten geöffnet sein, was die Wahrscheinlichkeit eines Hijacking-Angriffs auf Sitzungen erhöht.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.authenticate.limit.concurrent.sessions.across.all.n*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Management von Anwendersitzungen
Sicherheitsrisiko	• Schweregrad-Punktzahl: 3,7 • CVSS-Punktzahl: Niedrig • Details zu Sicherheitsrisiken: Wenn Sie das Plugin „ **Gleichzeitige Sitzungen** begrenzen“ verwenden, können Sie durch Festlegen dieser Eigenschaft auf „ **falsch** “ mehrere Sitzungen auf mehreren Knoten öffnen, was die Wahrscheinlichkeit einer Sicherheitsschwachstelle wie eines Hijacking-Angriffs auf Sitzungen erhöht.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Begrenzen Sie gleichzeitige Sitzungen

Plugin „Gleichzeitige Sitzungen begrenzen“

Konfigurieren Sie das Plugin „com.glide.limit.concurrent.sessions“, um das Risiko eines Hijacking-Angriffs auf Sitzungen in Ihrer Instanz zu reduzieren.

Mit diesem Plugin kann ein Administrator die Anzahl der aktiven Sitzungen pro Anwender und/oder Rolle begrenzen. Es wird empfohlen, dieses Plugin zu aktivieren und zu konfigurieren, um die Wahrscheinlichkeit eines Hijacking-Angriffs auf Sitzungen zu reduzieren. Wenn dieses Plugin aktiviert und konfiguriert ist, gibt es ein Limit für die Anzahl offener Sitzungen, die Opfer eines Hijacking-Angriffs werden können.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*com.glide.limit.concurrent.sessions*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Plugin
Empfohlener Wert	com.glide.limit.gleichzeitige.sitzungen aktiviert und konfiguriert
Standardwert	com.glide.limit.gleichzeitige.sitzungen aktiviert und konfiguriert
Kategorie	Management von Anwendersitzungen
Sicherheitsrisiko	• Schweregrad-Punktzahl: 3,7 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn dieses Plugin nicht aktiv ist, besteht eine erhöhte Wahrscheinlichkeit eines Hijacking-Angriffs auf Sitzungen.
Abhängigkeiten und Voraussetzungen	Keine

Lebensdauer aktiver Sitzungen von Gästen begrenzen [Neu in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.guest.active.session.life_span*, um die Dauer der HTTP-Sitzungen eines aktiven Gasts zu steuern.

Die Eigenschaft *glide.guest.active.session.life_span* erzwingt eine maximale Lebensdauer für aktive Gast-HTTP-Sitzungen, unabhängig von der Inaktivität ihrer Sitzung oder der Zeit, die ein Benutzer inaktiv ist, bevor seine Sitzung abläuft und geschlossen wird. Der konfigurierte Wert wird in Minuten angegeben. Ein Wert von Null deaktiviert das Timeout für aktive Sitzungen. Ein höherer Wert könnte es einem Angreifer ermöglichen, länger in einer gestohlenen Sitzung zu bleiben, was die Wahrscheinlichkeit eines Security Incidents erhöht.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Eigenschaft ist auf Gastbenutzer beschränkt, die geringe Berechtigungen für den Zugriff auf eine Instanz haben.

Um diese Sicherheitsschwachstelle zu beheben, legen Sie *glide.guest.active.session.life_span* auf einen Wert größer als 0 und kleiner oder gleich 720 fest.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.guest.active.session.life_span*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer
Empfohlener Wert	1–720 (Minuten)
Standardwert	0
Kategorie	Management von Anwendersitzungen
Sicherheitsrisiko	• Schweregrad-Punktzahl: 4.2 • CVSS-Punktzahl: Mittel • Details zu Sicherheitsrisiken: Wenn Sie die maximale Lebensdauer auf einen hohen Wert setzen, haben böswillige Akteure mehr Zeit für eine Instanz, falls sie eine Sitzung stehlen.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Diese Konfiguration erzwingt die maximale Lebensdauer für aktive Gast-HTTP-Sitzungen unabhängig von der inaktiven Zeitüberschreitung. Der konfigurierte Wert wird in Minuten angegeben. Ein Wert von Null deaktiviert das Timeout für aktive Sitzungen. Die maximale Lebensdauer muss größer sein als die inaktive Zeitüberschreitung *glide.guest.session_timeout* (Standard: 30 Minuten).

Gleichzeitige interaktive Sitzungen begrenzen [Aktualisiert in Security Center 1.3]

Verwalten Sie die Anzahl der interaktiven Sitzungen in Ihrer -Instanz.

Verwenden Sie die Eigenschaft [bisund *glide.authenticate.limit.concurrent.interactive.sessions*, um die Anzahl der interaktiven Sitzungen in einer Instanz zu verwalten. Diese Eigenschaft ist für die Verwendung mit dem Plugin Begrenzen Sie gleichzeitige Sitzungen(com.glide.limit.gleichzeitige.sitzungen) vorgesehen. Wenn das Plugin aktiv ist und die Eigenschaft auf **false**festgelegt ist, kann ein Benutzer eine beliebige Anzahl gleichzeitiger interaktiver Sitzungen in einer Instanz haben. Eine größere Anzahl offener Sitzungen bedeutet eine höhere Wahrscheinlichkeit eines Hijacking-Angriffs auf eine Sitzung.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.authenticate.limit.concurrent.interactive.sessions*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Management von Anwendersitzungen
Sicherheitsrisiko	• Schweregrad-Punktzahl: 3,7 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn das Plugin aktiv ist und die Eigenschaft auf **„false**“ festgelegt ist, kann ein Benutzer eine beliebige Anzahl gleichzeitiger interaktiver Sitzungen haben, was die Wahrscheinlichkeit eines Hijacking-Angriffs auf Sitzungen erhöht.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Gleichzeitige interaktive Sitzungen begrenzen [Aktualisiert in Security Center 1.3]

Lebensdauer aktiver Sitzungen von Integrationen begrenzen [Neu in Security Center 1.3]

Die Eigenschaft *glide.integrations.active.session.life_span* erzwingt die maximale Lebensdauer für aktive Gast-HTTP-Sitzungen unabhängig von der inaktiven Zeitüberschreitung. Der konfigurierte Wert wird in Minuten angegeben. Ein Wert von Null deaktiviert das Timeout für aktive Sitzungen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.integrations.active.session.life_span*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer
Empfohlener Wert	0 bis 720
Standardwert	0
Kategorie	Management von Anwendersitzungen
Sicherheitsrisiko	• Schweregrad-Punktzahl: 4.2 • CVSS-Punktzahl: Mittel

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Details zum Sicherheitsrisiko: Eine höhere maximale Lebensdauer könnte es einem Angreifer ermöglichen, länger in einer gestohlenen Sitzung zu verharren, was den Umfang eines Security Incidents erhöht. Diese Eigenschaft ist auf Integrationen beschränkt, die geringe Berechtigungen für den Zugriff auf eine Instanz haben. Legen Sie die Glide-Eigenschaft *glide.integrations.active.session.life_span* auf einen Wert von 0 und kleiner oder gleich 720 fest.
Abhängigkeiten und Voraussetzungen	Keine

Intervall für mobiles Aktualisierungstoken für richtlinienbasierten Sitzungszugriff beschränken [Neu in Security Center 1.5]

Verwenden Sie die Eigenschaft *glide.authenticate.session_access.mobile.refresh_token_interval*, um die Zeitspanne zu steuern, nach der die erneute Authentifizierung eines Mobilgerätbenutzers erzwungen wird.

Anwender werden nur dann zur erneuten Authentifizierung aufgefordert, wenn der Administrator die Attribute für den Identitätsanbieter in der Sitzungsrichtlinie konfiguriert hat (Attribute können bei jeder Anmeldung variieren) und sich der Anwender mit Single Sign-on (SSO) authentifiziert. Der Standardwert stellt die Zeit in Sekunden dar, die einem Benutzer zur Verfügung steht, bevor er erneut authentifiziert wird. Ein höherer Standardwert bietet einem böswilligen Akteur im Falle eines Hijacking-Angriffs auf eine Sitzung mehr Zeit für den Sitzungszugriff.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.authenticate.session_access.mobile.refresh_token_i*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer
Empfohlener Wert	1800 (Sekunden)
Standardwert	1800 (Sekunden)
Kategorie	Management von Anwendersitzungen
Sicherheitsrisiko	• Schweregrad-Punktzahl: 4.3 • CVSS-Punktzahl: Mittel • Details zum Sicherheitsrisiko: Wenn die ZTA-Richtlinie in der Instanz aktiviert ist, werden Anwender, die SSO während der mobilen Anmeldung verwenden, gezwungen, sich nach dem Standardwert von 1800 Sekunden (30 Minuten) abzumelden und

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	erneut anzumelden. Wenn ein höherer Wert verwendet wird, werden Anwender gezwungen, diese verstrichene Zeit zu warten.
Abhängigkeiten und Voraussetzungen	Zero Trust: Richtlinienbasierter Sitzungszugriff
Funktionale Auswirkung	Diese Einstellung steuert die Zeit in Sekunden nach der Anmeldung, während der Anwender gezwungen werden, sich von Mobilgeräten abzumelden, wenn sie Single Sign-on für die Authentifizierung verwenden und der Administrator die Attribute „Provider identifizieren“ in der Sitzungszugriffsrichtlinie konfiguriert hat.

Lebensdauer aktiver Sitzungen von UI begrenzen [Neu in Security Center 1.3]

Die Eigenschaft *glide.ui.active.session.life_span* erzwingt die maximale Lebensdauer für aktive und authentifizierte HTTP-Sitzungen unabhängig von der inaktiven Zeitüberschreitung.

Der konfigurierte Wert wird in Minuten angegeben. Ein Wert von Null deaktiviert das Timeout für aktive Sitzungen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.ui.active.session.life_span*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer
Empfohlener Wert	1-720
Standardwert	0
Kategorie	Management von Anwendersitzungen
Sicherheitsrisiko	• Schweregrad-Punktzahl: 4.2 • CVSS-Punktzahl: Mittel • Details zu Sicherheitsrisiken: Eine höhere maximale Lebensdauer könnte es einem Angreifer ermöglichen, länger in einer gestohlenen Sitzung zu bleiben, was die Wahrscheinlichkeit eines Security Incidents erhöht.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Erzwingt die maximale Lebensdauer für aktive und authentifizierte HTTP-Sitzungen unabhängig von der inaktiven Zeitüberschreitung. Der konfigurierte Wert wird in Minuten angegeben. Ein Wert von Null deaktiviert das Timeout für aktive Sitzungen. Die maximale Lebensdauer muss

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	größer als die Zeitüberschreitung bei Inaktivität „glide.ui.session_timeout“ (Standard: 30 Minuten) sein.

Inaktive Sitzungen proaktiv für ungültig erklären [Neu in Security Center 1.3]

Die Eigenschaft *glide.active.session.timeout.invalidate.session* steuert, ob eine Timeout-Sitzung vor dem Tomcat-Server proaktiv für ungültig erklärt wird.

Wenn *glide.active.session.timeout.invalidate.session* nicht auf „ **true**“ festgelegt ist, kann es ein kurzes Zeitintervall geben, in dem eine Sitzung mit Zeitüberschreitung nicht für ungültig erklärt wird (mindestens 60 Sekunden, abhängig von der Warteschlangengröße). Wenn eine Sitzung gekapert wird, kann ein Angreifer während dieses kurzen Zeitraums möglicherweise eine Sitzung verwenden. Um dieses Sicherheitsrisiko zu beheben, legen Sie *glide.active.session.timeout.invalidate.session* auf „ **true**“ fest.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.active.session.timeout.invalidate.session*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Management von Anwendersitzungen
Sicherheitsrisiko	• Schweregrad-Punktzahl: 4,6 • CVSS-Punktzahl: Mittel • Details zu Sicherheitsrisiken: Wenn Sie diese Eigenschaft nicht auf den empfohlenen Wert „wahr“ festlegen, kann dies dazu führen, dass eine Sitzung mit Zeitüberschreitung nicht validiert wird. Dies erhöht die Wahrscheinlichkeit, dass ein böswilliger Akteur eine Sitzung kapert.
Abhängigkeiten und Voraussetzungen	Keine

HTTP-Sitzungs-Bezeichner rotieren

Verwenden Sie die Eigenschaft *glide.ui.rotate_sessions*, um die Rotation der HTTP-Sitzungsbezeichner zu aktivieren und so Sicherheitsschwachstellen zu reduzieren.

Wenn sich die Sitzungs-ID eines nicht authentifizierten Benutzers nach der Authentifizierung nicht ändert, ist eine Webanwendung angreifbar für einen Angriff zur Sitzungskorrektur . Ein böswilliger Benutzer könnte eine nicht authentifizierte Sitzung starten und dem Opfer die zugehörige Sitzungs-ID geben. Sobald sich das Opfer authentifiziert hat, gibt der böswillige Anwender diese authentifizierte Sitzung jetzt frei.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.ui.rotate_sessions*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Management von Anwendersitzungen
Zweck	Um eine sicherere Sitzungsauthentifizierung zu erreichen.
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	8.8
Funktionale Auswirkung	(Mittel) Diese Korrektur hat die SessionID geändert, wenn der Anwender von einer nicht authentifizierten Seite zu authentifizierten Seiten navigiert. • Wenn Sie einen Proxy verwenden oder die SessionID bei der ersten Anmeldung eines Anwenders oder aus anderen Gründen codieren, kann dies eine potenzielle Auswirkung auf die Funktionalität haben. • Wenn Sie das SAML 2.0-Plugin für die Single Sign-on-Authentifizierung verwenden, kann dies die gemeinsame Nutzung von Sitzungsinformationen zwischen der Instanz und dem Identitätsanbieter beeinträchtigen. In diesem Fall können Sie diese Eigenschaft auf „falsch“ festlegen.
Sicherheitsrisiko	Die (mäßige) SessionID wird zum Verarbeiten und Authentifizieren des Instanzanwenders verwendet, indem der Sitzungsstatus im Browser verwaltet wird. Daher gilt die SessionID als vertrauliche Daten und sollte standardmäßig sicher sein. Die Sitzungsrotation ist eine Sicherheitskontrolle, die die Änderung der Sitzungs-ID erzwingt, wenn der Anwender von nicht authentifizierten Seiten zu authentifizierten Seiten navigiert.
Referenzen	Authentifizierung mit SAML

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Anzahl der gleichzeitigen interaktiven Sitzungen minimieren [Aktualisiert in Security Center 1.3]

Verwenden Sie diese Eigenschaft mit dem Plugin „Gleichzeitige Sitzungen begrenzen“, um die Anzahl der aktiven Sitzungen zu steuern, die von einem Benutzer geöffnet werden können.

Verwenden Sie die Eigenschaft „Maximale Anzahl **gleichzeitiger interaktiver Sitzungen für Glide-Authentifizierung** “ mit dem Plugin „ **Gleichzeitige Sitzung begrenzen**

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

“ (*com.glide.limit.concurrent.sessions*), um die Anzahl der aktiven Sitzungen zu steuern, die für einen Benutzer geöffnet sind. Der empfohlene Wert ist **1**. Dadurch wird die Anzahl der geöffneten Sitzungen verringert (eine höhere Anzahl erhöht die Wahrscheinlichkeit, dass eine Sitzung gekapert wird).

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.authenticate.max.concurrent.interactive.sessions*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	integer
Empfohlener Wert	1
Standardwert	1
Kategorie	Management von Anwendersitzungen
Sicherheitsrisiko	• Schweregrad-Punktzahl: 3,7 • CVSS-Punktzahl: Niedrig • Details zum Sicherheitsrisiko: Wenn Sie den Standardwert der Eigenschaft auf größer als 1 setzen, erhöht sich die Wahrscheinlichkeit eines Hijacking-Angriffs auf Sitzungen.
Abhängigkeiten und Voraussetzungen	Das Plugin „ **Gleichzeitige interaktive Sitzungen** “ (*com.glide.limit.concurrent.sessions*) muss aktiviert sein.
Referenzen	Begrenzen Sie gleichzeitige Sitzungen

Zeitüberschreitungsdauer der Sitzungsaktivität minimieren [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.ui.session_timeout*, um den Zeitüberschreitungswert der Aktivität in Minuten anzugeben.

Das Festlegen dieser Eigenschaft hat mehrere funktionale Auswirkungen:

- Je länger die angegebene Sitzungsüberschreitung ist, desto mehr Arbeitsspeicher wird während einer Verarbeitungssitzung verwendet. Das Basissystem verwendet eine standardmäßige Apache Tomcat-Zeitüberschreitungsdauer von 30 Minuten.
- Der Now Platform meldet Benutzer weiterhin mit „Anwendernamen speichern“ ab. Nach 30 Minuten Inaktivität in der Anwendung meldet die Plattform den Benutzer automatisch ab, es sei denn, das Kontrollkästchen „Anwendernamen speichern“ auf der **Anmeldeseite** ist aktiviert. Der Unterschied von besteht darin, dass sie sich nicht erneut anmelden müssen, um fortzufahren.
- Wenn auf den Homepages von Anwendern Anzeigen oder Inhalte vorhanden sind, die automatisch aktualisiert werden, kann diese Zeitüberschreitung möglicherweise nie erreicht werden.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.ui.session_timeout*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Management von Anwendersitzungen
Zweck	Zum Erzwingen der Zeitüberschreitung bei Sitzung.
Empfohlener Wert	Vom Anwender angegebene Zeitüberschreitung in Minuten. Der empfohlene Wert beträgt 60 Minuten, dieser Wert kann jedoch je nach Funktionalität und Sicherheitsanforderung variieren. Legen Sie diesen Wert nicht auf mehr als einen Tag fest.
Sicherheitsrisikobewertung	7.5
Funktionale Auswirkung	(Mittel) Diese Korrektur erzwingt das rechtzeitige Ablaufen des Anwenderaccounts. Keine Auswirkungen auf die Funktionalität, jedoch die Anwender-Experience wird geändert.
Sicherheitsrisiko	(Hoch) Wenn Anwendersitzungen für unbestimmte Zeit aktiv sind, stellen sie ein Sicherheitsrisiko dar und sollten bei einer zeitbasierten Konfiguration ablaufen.
Referenzen	Verwalten Sie Benutzersitzungen

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Zeitüberschreitungsdauer des Sitzungsfensters minimieren [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.ui.user_cookie.life_span_in_days*, um den Ablaufzeitraum für das „Anwendernamen speichern“-Cookie festzulegen. Der Standardwert beträgt 15 Tage, und die maximale Obergrenze beträgt 30 Tage.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.ui.user_cookie.life_span_in_days*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Management von Anwendersitzungen
Zweck	Um den standardmäßigen Ablauf des **„Anwendernamen-** Cookies speichern“ zu aktivieren.
Datentyp	Ganzzahl
Empfohlener Wert	15
Standardwert	15
Sicherheitsrisikobewertung	4.9

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Funktionale Auswirkung	(Mittel) Diese Eigenschaft wird vom Endanwender aktiviert, wenn der Endanwender auf der **Anmeldeseite** das Kontrollkästchen Anwendernamen speichern aktiviert und sich bei Now Platformanmeldet.
Sicherheitsrisiko	(Mittel) Dass Anwendercookies für unbestimmte Zeit aktiv sind, stellt ein Sicherheitsrisiko dar und sollte bei einer zeitbasierten Konfiguration ablaufen.
Referenzen	Verfügbare Systemeigenschaften Anwendernamen speichern

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Gespeicherte Kryptografie

Diese Kategorie konzentriert sich auf die Verschlüsselung der gespeicherten Daten. Sie umfasst mehrere Schlüsselaspekte, z. B. die Verwendung etablierter Algorithmen und kryptografischer Module, die Sicherstellung der ordnungsgemäßen Generierung von Pseudozufallswerten, die Implementierung der Verschlüsselung auf Grundlage der Datenklassifizierung und die sichere Speicherung und Isolierung von Schlüsselmaterial.

Glide KMF-Verschlüsseler aktivieren [In Security Center 1.3.2 entfernt]

Verwalten Sie die für Password2-Felder verwendeten Verschlüsselungsprogramme in Ihrer -Instanz.

Verwenden Sie die Eigenschaft] bisund *glide.kmf.encrypter.enabled*, um den KMF-Verschlüsseler als Standardverschlüsseler für Password2-Felder festzulegen. Diese Eigenschaft stellt sicher, dass anstelle eines veralteten Verschlüsselers starke und konforme Verschlüsselungsstandards verwendet werden. Um sicherzustellen, dass der KMF-Verschlüsseler anstelle des Legacy-Verschlüsselers verwendet wird, legen Sie diese Eigenschaft auf **wahr**fest.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.kmf.encrypter.enabled*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Gespeicherte Kryptografie
Sicherheitsrisiko	• Schweregrad-Punktzahl: 4,9 • CVSS-Punktzahl: Mittel

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Details zum Sicherheitsrisiko: Durch Festlegen dieser Eigenschaft auf „ **wahr** “ wird sichergestellt, dass der KMF-Verschlüsseler anstelle des Legacy-Verschlüsselers verwendet wird.
Referenzen	Password2-Verschlüsselung mit dem Key Management Framework (KMF)

Validierung, Bereinigung und Codierung

Validierung, Bereinigung und Codierung behandeln die Validierung der Eingabe, um Schwachstellen wie websiteübergreifendes Skripting (Cross-Site Scripting, XSS), SQL-Einschleusung und andere Angriffe zu verhindern.

Diese Steuerung stellt sicher, dass Eingabevalidierung und Ausgabecodierung vorhanden und ordnungsgemäß konfiguriert sind, z. B. Codierung oder Escape-Zeichen für Ausgabedaten. Diese Kategorie umfasst auch Prüfungen für Elemente wie Deserialisierung von Objekten, Sandboxing bei Bedarf und positive Validierung durch Allow-Listen.

Zugriff auf skriptfähige GlideSystemUserSession-API beschränken [Aktualisiert in Security Center 1.3]

Die vom Client aufrufbare skriptfähige GlideSystemUserSessionSandbox-API macht die Methoden addErrorMessageNoSanitization und addInfoMessageNoSanitization von GlideSystemUserSession für die Javascript-Sandbox verfügbar. Dadurch können alle Anwender diese Methode per Skript aufrufen.

Bei Festlegung auf **true**darf eine Benutzersitzung in einer Sandbox Informations- oder Fehlermeldungen ohne Bereinigung aufrufen. Beim Aufruf der Nachricht wird eine Warnung protokolliert. Bei Festlegung auf **false**ist der Anruf nicht zulässig.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.sandbox.usersession.allow_unsanitized_messages`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Diese Eigenschaft verhindert, dass nicht bereinigte Informations- oder Fehlermeldungen in einer Anwendersitzung mit einer Sandbox aufgerufen werden.
Typ	boolean
Empfohlener Wert	falsch
Standardwert	wahr

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisikobewertung	8.1
Funktionale Auswirkung	(Hoch) Wenn Sie die Eigenschaft auf den Wert „falsch“ festlegen, werden keine Nachrichten erstellt oder protokolliert, wenn diese Funktionen aufgerufen werden.
Sicherheitsrisiko	(Hoch) Ohne entsprechende Bereinigung kann auf potenziell gefährliche Inhalte zugegriffen werden, und die nicht bereinigte Fehlerfunktion ist für das Skript verfügbar.
Referenzen	Zugriffssteuerung

JavaScript-Tags in eingebettetem HTML deaktivieren [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.ui.security.codetag.allow_script*, um die Unterstützung für das Einbetten von HTML-JavaScript-Code zu deaktivieren, der mit dem [code]-Tag erstellt wurde.

Now Platform entschärft viele Einschleusungs- und websiteübergreifende Angriffe durch die Implementierung von Escaping- und Codierungstechniken. Daher können Anwender keine HTML-formatierten Eingaben für Journalfelder schreiben und übermitteln. Journalfelder können jedoch Text, der in Code-Tags eingeschlossen ist, als HTML rendern. Stellen Sie sicher, dass die Eigenschaft *glide.ui.security.codetag.allow_script* in der Tabelle „sys_properties“ vorhanden und auf „falsch“ festgelegt ist.

- Es ist jedoch ein Sicherheitsrisiko verbunden. Bei Festlegung auf **wahr**können böswillige Anwender schädlichen HTML-JavaScript-Code schreiben, der nach dem Rendern von Journalfeldern in einem anderen Client-Browser ausgeführt werden kann.
- Legen Sie diese Eigenschaft auf „ **falsch** “ fest, damit Administratoren verhindern können, dass Journalfelder HTML-JavaScript-Code rendern, indem sie die Unterstützung für das `[code]` -Tag deaktivieren.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.ui.security.codetag.allow_script*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Schützt vor websiteübergreifendem Skripting und der Ausführung böswilliger Skripts
Empfohlener Wert	falsch
Standardwert	falsch
Sicherheitsrisikobewertung	8.8

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Funktionale Auswirkung	(Mittel) Diese Korrektur erzwingt JavaScript-Escaping auf der Anwenderoberfläche und rendert die codierten Ergebnisse für den Anwender. Sie kann basierend auf der Interaktion des Instanzanwenders mit den resultierenden Daten Auswirkungen auf die Funktionalität haben.
Sicherheitsrisiko	(Hoch) Die Eingabevalidierung muss in der Anwendung erfolgen, um sich gegen websiteübergreifende Skripting-Angriffe zu schützen. Diese Angriffe ermöglichen die Ausführung fremder Skripts in der Anwendersitzung im Kontext des angemeldeten Browsers. Angreifer können damit Sitzungsinformationen und vertrauliche Daten stehlen.
Referenzen	Beschränken Sie das CODE-Tag in Journalfeldern Journalfeldeinträge als HTML rendern Strenge Sicherheitseinstellungen

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Sicherheitsmanager für gehärtetes Java aktivieren [Neu in Security Center 1.3]

Die Eigenschaft *glide.security.manager* enthält den Java-Klassennamen des aktuellen Java-Sicherheitsmanagers.

Warnung: Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.security.manager*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	*com.glide.sys.security.ContextualSecurityManager*
Standardwert	*com.glide.sys.security.ContextualSecurityManager*
Kategorie	Validierung, Bereinigung und Codierung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 7,2 • CVSS-Punktzahl: Hoch • Details zum Sicherheitsrisiko: Wenn *glide.security.manager* nicht auf den empfohlenen Wert *com.glide.sys.security.ContextualSecurityManager* festgeleg

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	ist, verwendet die Instanz möglicherweise einen veralteten Java-Sicherheitsmanager, für den die erwarteten Härtungsrichtlinien fehlen. Ohne diese Härtung könnte ein böswilliger Akteur mit Skriptausführungszugriff die Remoteausführung von Code in der Instanz erhalten.
Abhängigkeiten und Voraussetzungen	Keine

HTML-Bereinigung erzwingen [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *com.glide.security.check_unsanitized_html*, um das Bereinigungsverhalten von translated_html-Feldern auf globaler Ebene für Feldzuweisungen zu erzwingen.

HTML ist einer der Typen, die den Wörterbuchfeldern zugewiesen werden können. Durch das Zuweisen von HTML-Feldern an einen beliebigen Feldtyp erhalten Sie die Funktionalität zum Formatieren von Inhalten mithilfe von HTML-Tags (z. B. `<p>`, `<a href>`, `<b>`, `<font>`, `<img>`). Um böswillige Aktivitäten zu verhindern, können bestimmte HTML-Tags mithilfe einer Sperrliste deaktiviert werden. Diese Eigenschaft verhindert, dass unzulässige Tags in „translated_html"-Feldern in Ihrer Instanz verwendet werden.

- Legen Sie diese Eigenschaft auf „ **erzwingen** " fest, um das Bereinigungsverhalten von translated_html-Feldern zu erzwingen.
- Legen Sie die Eigenschaft auf „ **deaktiviert** " fest, um die HTML-Bereinigung zu deaktivieren und blockierte HTML-Tags in „translated_html"-Feldern zuzulassen.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*com.glide.security.check_unsanitized_html*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Verhindert die Verwendung unsicherer HTML-Tags zum Schutz vor Angriffen wie websiteübergreifendem Skripting.
Typ	Zeichenfolge
Empfohlener Wert	erzwingen
Standardwert	erzwingen
Sicherheitsrisikobewertung	7.3
Funktionale Auswirkung	(Mittel) Diese Korrektur erzwingt die HTML-Bereinigung auf der Anwenderoberfläche und rendert übersetzte HTML-Felder für den Anwender. Dies kann

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Auswirkungen auf die Lesbarkeit und Formatierung haben.
Sicherheitsrisiko	(Hoch) Die Eingabevalidierung muss in der Anwendung erfolgen, um sich gegen websiteübergreifende Skripting-Angriffe zu schützen. Diese Angriffe ermöglichen die Ausführung fremder Skripts in Anwendersitzungen im Kontext des angemeldeten Browsers. Angreifer können damit Sitzungsinformationen und vertrauliche Daten stehlen.
Referenzen	HTML-Bereinigung

Vom Client generierte Skripts-Sandbox erzwingen [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.script.use.sandbox*, um das Skript-Sandboxing zu aktivieren.

Es gibt zwei Fälle in Now Platform, die es dem Client ermöglichen, Skripts zur Bewertung an den Server zu senden:

Filter oder Abfragen

Es ist zulässig, einen Filter an den Server zu senden, z. B. `assigned_to=JavaScript:getMyGroups()`.

System-API

Ein API-Aufruf ermöglicht es dem Client, beliebige Skripts auf dem Server auszuführen und eine Antwort zu erhalten.

Wenn Sie Skript-Sandboxing aktivieren, wird das an einem dieser beiden Einstiegspunkte ausgewertete Skript in einer Sandbox mit reduzierten Rechten und mit den folgenden Eigenschaften ausgeführt:

- Nur die als vom Client aufrufbar markierten Business-Regeln sind in der Sandbox verfügbar.
- In der Sandbox sind nur Skripteinbindungen verfügbar, die als vom Client aufrufbar markiert sind.
- Bestimmte API-Aufrufe (weitgehend, aber nicht vollständig, beschränkt auf Aufrufe, die den direkten DB-Zugriff betreffen) sind nicht zulässig.
- Sie können in der Sandbox keine Daten einfügen, aktualisieren oder löschen. Beispielsweise werden alle Aufrufe von `current.update()` ignoriert. Wenn Sie Now Platform ausführen, ohne Skript-Sandboxing zu aktivieren, gelten keine dieser Einschränkungen.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.script.use.sandbox*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Zweck	Erzwingt die Validierung für die clientseitigen JavaScript-Abfragen, die für die Plattform gestartet werden
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	9.8
Funktionale Auswirkung	(Kritisch) Diese Korrektur erzwingt die Validierung für die clientseitigen JavaScript-Abfragen, die für Now Platformgestartet werden. Es kann potenziell Auswirkungen haben, wenn der Kunde Anpassungen verwendet hat, die hartcodierte JavaScript-Abfragen zur Durchführung von CRUD-Vorgängen enthalten.
Sicherheitsrisiko	(Kritisch) Now Platform bietet über JavaScript-Abfragen eine Vielzahl von Features und Funktionen. Ohne entsprechende Autorisierung und Validierung besteht jedoch die Möglichkeit, dass ein Angreifer nicht autorisierte Vorgänge auf der Plattform durchführt.
Referenzen	Sandbox-Eigenschaft für Skript konfigurieren *glide.script.use.sandbox* gehört zu derselben Familie von Eigenschaften, die die Ausführung von Skripts sichern und einschränken, die vom Client stammen: • *glide.script.allow.ajaxevaluate*: Siehe „AJAXEvaluate aktivieren“ • *glide.script.secure.ajaxgliderecord*: Siehe Aktivieren der AJAXGlideRecord-ACL-Überprüfung:

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Eingehende E-Mail-Bilder in Anhänge konvertieren [In Security Center 1.3 aktualisiert und in 1.5 entfernt]

Verwenden Sie die Eigenschaft *glide.email.inbound.convert_html_inline_attachment_references*, um anzugeben, ob eingehende HTML-E-Mails so konvertiert werden sollen, dass E-Mail-Bilder in der HTML-Textvorschau der E-Mail angezeigt werden.

Folgendes geschieht, wenn die Systemeigenschaft *glide.email.inbound.convert_html_inline_attachment_reference* auf „false“ festgelegt ist:

- In Now Platformwerden anstelle der empfangenen Bilder defekte CID-Links (Inhalts-ID) angezeigt. Das Format, in dem das E-Mail-Bild angezeigt wird, hängt von der Eigenschaftseinstellung zum Zeitpunkt des Empfangs der E-Mail ab, nicht von der aktuellen Eigenschaftseinstellung.
- Der im Anhang empfangene „böswillige“ Inhalt wird im HTML-Code der E-Mail nicht referenziert. Der Anhang selbst wird in der Tabelle „sys_attachment“ gespeichert.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Bei der Verarbeitung eingehender E-Mails werden die HTML-Daten der E-Mail nicht aktualisiert, um den gespeicherten Speicherort des Anhangs in der Tabelle „sys_attachment“ widerzuspiegeln. Dies hat folgende Auswirkungen:
  - Inline-Bilder werden in der E-Mail-Anzeige im Aktivitätsformatierer nicht angezeigt.

    Hinweis: Um dieses Problem mit dem Aktivitätsformatierer zu beheben, überprüfen Sie zunächst, ob keine Sicherheitsbedenken bestehen. Legen Sie dann die Systemeigenschaft *glide.email.inbound.convert_html_inline_attachment_reference* auf „ **true** “ fest, damit zukünftige empfangene E-Mails die erforderliche HTML-URL enthalten, um auf das Bild zu verweisen. Durch das Ändern der Eigenschaft werden bereits empfangene E-Mails nicht aktualisiert. Der neue Wert wirkt sich nur auf eingehende E-Mails aus, die nach dem Ändern der Eigenschaft empfangen wurden.

  - Inline-Bilder werden nicht angezeigt, wenn die E-Mail in der HTML-Vorschau der E-Mail angezeigt wird.
  - Beim Anfügen von „email.body_htm“ in eingehenden Aktionen zwischen Code-Tags fehlen die Bilder.

Voraussetzungen

Legen Sie vor dem Festlegen dieser Eigenschaft die Eigenschaft *glide.email.read.active* auf „wahr“ fest. Weitere Informationen finden Sie unter Die Verwendung Ihres eigenen POP3-Servers aktivieren .

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.email.inbound.convert_html_inline_attachment_refere*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Um das Rendern von Bildern in der HTML-Textvorschau einzuschränken.
Empfohlener Wert	falsch
Sicherheitsrisikobewertung	5.4
Funktionale Auswirkung	(Mittel) Sobald diese Eigenschaft konfiguriert ist, kann der Anwender die Bildvorschau nicht im E-Mail-Text anzeigen.
Sicherheitsrisiko	(Mittel) Wenn die Eigenschaft nicht aktiviert ist, kann ein Angreifer ein schädliches Bild mit Malware senden.
Referenzen	E-Mail-Eigenschaften Konfiguration für eingehende E-Mails

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AJAXEvaluate deaktivieren

Verwenden Sie *glide.script.allow.ajaxevaluate*, um die System-API vor Schwachstellen bei der Clientskriptausführung über AJAX-Aufrufe zu schützen.

Zum Bearbeiten der Eigenschaft ist eine Hochstufung auf die Rolle „security_admin“ erforderlich.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.script.allow.ajaxevaluate*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Um zu verhindern, dass ein Benutzer Skripts mit Administratorrechten ausführt
Empfohlener Wert	falsch
Standardwert	falsch
Konfigurationstyp	Boolean
Funktionale Auswirkung	(Mittel) Diese Korrektur erzwingt das Abschalten des AJAXEvaluate-Prozessors. Es kann sich auf die Funktionalität auswirken, wenn Sie den AJAX-Auswertungsprozessor explizit als Teil von anwenderdefinierten Skripts verwenden.
Sicherheitsrisiko	(Hoch) Der AjaxEvaluator-Prozessor führt Client-Skripts in der Sandbox aus. Es gibt jedoch mehrere zusätzliche Eigenschaften, die es ermöglichen, den Umfang der Aktivitäten in der Sandbox zu erweitern oder vollständig zu deaktivieren.
Sicherheitsrisikobewertung	7.3
Referenzen	Diese Eigenschaft gehört zu derselben Familie von Eigenschaften, die die Ausführung von Skripts sichern und einschränken, die vom Client stammen: • *glide.script.use.sandbox*: Siehe Sandbox für vom Client generierte Skripts. • *glide.script.allow.ajaxevaluate*: Siehe „AJAXEvaluate aktivieren“

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Entitätserweiterung im XMLDocument2-Streaming-Parser deaktivieren [Aktualisiert in Security Center 1.5]

Wenn Anpassungen keine Entitätserweiterung erfordern, verwenden Sie die Eigenschaft *glide.stax.allow_entity_resolution*, um die externe Entitätserweiterung vollständig zu deaktivieren. Die XML-Datei schließt die Analyse ab, enthält jedoch keine internen oder externen Entitäten.

- Wenn Sie diese Eigenschaft auf **true**festlegen, versuchen alle externen Entitäten, abhängig von der Einstellung in der Eigenschaft *glide.stax.whitelist_enabled*, die betreffenden Entitäten aufzulösen oder zu erweitern.
- Wenn Sie diese Eigenschaft auf **false**festlegen, werden alle Auflösungen und Erweiterungen von Entitäten blockiert. Weitere Informationen finden Sie unter Validierung von XMLdoc2-Entitäten mit weißer Liste.

Voraussetzungen

Vor dem Festlegen dieser Eigenschaft:

- Legen Sie die Eigenschaften *glide.xml.entity.whitelist.enabled*und *glide.stax.whitelist_enabled*auf „wahr“ fest. Weitere Informationen finden Sie unter Validierung von XMLdoc/XMLUtil-Entitäten mit weißer Liste und Validierung von XMLdoc2-Entitäten mit weißer Liste .
- Definieren Sie eine Liste von kommagetrennten FQDNs in der Eigenschaft *glide.xml.entity.whitelist*, den einzigen URLs, die über die Verarbeitung von XML-Entitäten erreicht werden können. Eigenschaft. Weitere Informationen finden Sie unter Verarbeitung externer XML-Entitäten – weiße Liste.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.stax.allow_entity_resolution*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Diese Korrektursteuerung muss aktiviert sein, um sich gegen einen Angriff der XML-Entitätserweiterung/ Billion Leign zu schützen.
Empfohlener Wert	falsch
Standardwert	wahr
Funktionale Auswirkung	(Niedrig) Wenn die Anpassung die Entitätserweiterung verwendet, blockiert Now Platform möglicherweise die weitere Verarbeitung.
Sicherheitsrisiko	(Kritisch) Ein Angreifer kann diese Schwachstelle nutzen, um Daten exponentiell zu erweitern, wodurch schnell alle Systemressourcen verbraucht werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Workaround	Wenn die Anpassung eine Entitätserweiterung erfordert, legen Sie diese Eigenschaft auf „true“ fest, und befolgen Sie die in XMLdoc2-Entitätsvalidierungdokumentierten Schritte mit weißer Liste .

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen

Weitere Informationen zu OWASp-Ressourcen finden Sie unter OWASp .

URL für externen Inhalt deaktivieren

Verwalten Sie mit Connect-Chat, wie externe Link-Metadaten in Ihrer Instanz verwendet werden.

Verwenden Sie die Eigenschaft *glide.ui.url.external.content*, um externe Link-Metadaten in Ihrer -Instanz zu verwalten. Wenn die Eigenschaft auf den empfohlenen Wert **false**festgelegt ist, werden keine externen Link-Metadaten gerendert. Bei Festlegung auf „ **wahr** “ ruft Connect-Chat externe Link-Metadaten aus Quellen wie YouTube oder Nachrichtenartikeln ab, um umfangreichere Nachrichten darzustellen. Dies kann zu SSRF-Angriffen (Server Side Request Forgery) führen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.ui.url.external.content*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	falsch
Standardwert	wahr
Kategorie	Validierung, Bereinigung und Codierung
Sicherheitsrisiko	• Bewertung mit Schweregrad: 8,1 • CVSS-Punktzahl: Hoch • Details zu Sicherheitsrisiken: Wenn Sie diese Eigenschaft auf „ **true** “ setzen, ist Ihre Instanz möglicherweise SSRF-Angriffen (Server Side Request Forgery) ausgesetzt.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Connect-Chat

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingeschränkt herunterladbare MIME-Typen definieren [Aktualisiert in Security Center 1.3]

Die Eigenschaft *glide.ui.attachment.download_mime_types* erzwingt, dass die angegebene Liste gefährlicher Dateitypen auf den Client heruntergeladen und nicht inline im Browser angezeigt wird.

Wenn der MIME-Typ einer Datei in *glide.ui.attachment.download_mime_types* vorhanden ist, wird ein Download erzwungen. Beispiel: Das Herunterladen von Text/HTML erzwingt, dass eine HTML-Datei als Datei auf den Client heruntergeladen und nicht inline im Browser angezeigt wird, wodurch ein XSS-Angriff verhindert wird.

Um eine Liste vorhandener MIME-Typen anzuzeigen, `geben Sie / sys_attachment_icon_rule_list.do ein`. Sie können jeden dieser MIME-Typen aktivieren, um die Sicherheits-Compliance-Anforderungen in Now Platformzu erfüllen.

Hinweis: Zum Bearbeiten der Eigenschaft ist die Rolle „security_admin“ erforderlich.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.ui.attachment.download_mime_types*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Durch ordnungsgemäßes Verwalten der Liste gefährlicher Dateitypen, die nicht im Browser angezeigt werden können, werden Cross Site Scripting-Angriffe (XSS) verhindert.
Empfohlener Wert	Liste der anwendbaren MIME-Typen oder der empfohlene Wert: `text/html,image/svg,image/svg+xml,application/xml`
Standardwert	Liste der anwendbaren MIME-Typen für den Standardwert: `text/html,image/svg,image/svg+xml,application/xml`
Konfigurationstyp	Zeichenfolge: Beliebige, durch Kommas getrennte Werte von Anwendungs-MIME-Typen.
Funktionale Auswirkung	(Niedrig) Diese Korrektur erzwingt die Leistung von Validierungsprüfungen, bevor eine Aktion ausgeführt wird, wenn Sie in einer Anwendung Now Platform auf einen Anhang klicken. Es gibt keine potenziellen Auswirkungen, aber die Anwender-Experience wird geändert.
Sicherheitsrisiko	(Moderat) Angreifer können MIME-Typen missbrauchen und unbeabsichtigte Skriptinhalte im Anhang auf der Seite des Opfers platzieren, um vertrauliche Informationen zu erfassen. Die Möglichkeit, über XSS zu verfügen, kann dazu führen, dass eine problemlose Ausweitung von Berechtigungen auf höhere Rollen wie „Administrator“ erreicht werden kann, in denen mehr seitliche Bewegung möglich ist.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Füllen Sie im aktuellen Kontext die Eigenschaft mit einer Liste von kommagetrennten MIME-Anhangtypen aus, die nicht inline im Browser gerendert werden sollen.
Sicherheitsrisikobewertung	6.3
Zugehörige Eigenschaften	• *glide.ui.attachment.force_download_all_mime_types* • *glide.ui.attachment.tables_ignore_force_download*
Referenzen	Download der MIME-Typen erzwingen.

Eingebetteten HTML-Code deaktivieren [In Security Center 1.3 aktualisiert]

Verwenden Sie die Eigenschaft *glide.ui.security.allow_codetag*, um die Unterstützung für das Einbetten von HTML-Code zu deaktivieren, der mit dem Tag [code] erstellt wurde.

Now Platform entschärft viele Einschleusungs- und websiteübergreifende Angriffe durch die Implementierung von Escaping- und Codierungstechniken. Daher können Anwender keine HTML-formatierten Eingaben für Journalfelder schreiben/senden. Journalfelder können jedoch Text, der in Code-Tags eingeschlossen ist, als HTML rendern.

- Es ist jedoch ein Sicherheitsrisiko verbunden. Bei Festlegung auf `wahr`können böswillige Anwender schädlichen HTML JS-Code schreiben, der nach dem Rendern von Journalfeldern in einem anderen Client-Browser ausgeführt werden kann.
- Legen Sie diese Eigenschaft auf „ `falsch` “ fest, damit Administratoren verhindern können, dass Journalfelder HTML-Code rendern, indem sie die Unterstützung für das `[code]` -Tag deaktivieren.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.security.allow_codetag
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Schützen Sie sich vor websiteübergreifendem Skripting und der Ausführung schädlicher Skripts
Empfohlener Wert	falsch
Standardwert	wahr
Sicherheitsrisikobewertung	4.2
Funktionale Auswirkung	(Mittel) Diese Korrektur erzwingt die HTML-Codierung auf der Anwenderoberfläche und rendert die codierten Ergebnisse für den Anwender. Diese Eigenschaft ist standardmäßig auf „ `true` “ festgelegt. In diesem Status zeigt Ihre Instanz

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	gerenderten HTML-Code in Journalfeldern und Formularen an. Wenn diese Eigenschaft auf „`false`“ festgelegt ist, wird HTML nicht ordnungsgemäß gerendert, und HTML-Tags werden möglicherweise in Journalfeldern in Formularen angezeigt. Dies kann sich nachteilig auf die Funktionalität und die Benutzerinteraktionen mit den resultierenden Daten auswirken.
Sicherheitsrisiko	(Mittel) Die Eingabevalidierung muss in der Anwendung erfolgen, um sich gegen websiteübergreifende Skripting-Angriffe zu schützen. Diese Angriffe ermöglichen die Ausführung fremder Skripts in einer Benutzersitzung im Kontext des angemeldeten Browsers. Angreifer können damit Sitzungsinformationen und vertrauliche Daten stehlen.

HTML-Bereinigung in Virtual Agent aktivieren [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *`com.glide.cs.html.sanitizer.enabled`*, um HTMLSanitizerService zu aktivieren.

Weitere Informationen

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	*`com.glide.cs.html.sanitizer.enabled`*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Verhindert Cross Site Scripting- und HTML-Einschleusungsangriffe auf die Anwendung.
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	8
Funktionale Auswirkung	(Hoch) Diese Korrektur erzwingt den HTML-Ausgabecodierungsmechanismus, bevor die Anwenderdaten an den Anwender zurückgegeben werden. Wenn der Kunde Anpassungen vorgenommen hat, die das Rendern des HTML-Attributs oder der Inhaltsdaten umfassen, wirkt sich dies auf die Funktionalität aus.
Sicherheitsrisiko	(Hoch) Benutzereingaben sollten sicher behandelt werden, wenn die Daten in der Anwendung gespeichert und verarbeitet werden. Dadurch

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	werden clientseitige Cross Site Scripting-Angriffe durch Ausgabecodierung der Daten reduziert.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Jelly JS-Interpolationsschutz aktivieren

Verwenden Sie die Eigenschaft *glide.ui.jelly.js_interpolation.protect*, um sicherzustellen, dass JavaScript-Code, der auf einer Jelly-Seite ausgeführt werden soll, mithilfe der Jelly-Interpolation vor der Einschleusung geschützt ist.

Wenn Sie die Eigenschaft auf „ **true**“ festlegen, durchläuft eine Anwendung eine Jelly-Skriptstruktur (verschachtelt). Es umschließt potenziell gefährliche Jelly-Ausdrücke mit einem Filter, der:

- Codiert aus Sicherheitsgründen ein Escape-Zeichen für die Ergebnisse, oder
- Wenn ihre Sicherheit nicht garantiert werden kann, generiert eine SecurityException, da der Ausdruck, der ausgewertet wurde, ein mögliches Sicherheitsproblem darstellt.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.ui.jelly.js_interpolation.protect*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Zur Abwehr von Angriffen mit böswilliger Codeausführung, die mit Jelly Injection auftreten können.
Empfohlener Wert	wahr
Standardwert	falsch
Sicherheitsrisikobewertung	9
Funktionale Auswirkung	(Hoch) Diese Eigenschaft ermöglicht eine bestmögliche Schätzung, ob ein Ausdruck in Anführungszeichen gesetzt ist. Möglicherweise wird ein berechtigter Ausdruck falsch angegeben. In diesem Fall muss ein Ausdruck möglicherweise manuell als sicher markiert werden.
Sicherheitsrisiko	(Moderat) Die JEXL-Injektion ist eine für Now Platform eindeutige Form der Eingabeinjektion, die sowohl zu websiteübergreifender Anforderungsfälschung als auch zu Codeausführung führen kann. Durch das vollständige Deaktivieren des Schutzes können möglicherweise viele P1-Sicherheitsschwachstellen geöffnet werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Workaround	Um einen Ausdruck manuell als sicher zu markieren, fügen Sie dem Jelly-Ausdruck das SAFE-Präfix hinzu: `${SAFE:sysparm_input};` Das blinde Hinzufügen von SAFE zu jedem Ausdruck ist die falsche Herangehensweise, da dies zu einer Sicherheitsschwachstelle führen kann. • Fügen Sie einem Ausdruck nur dann SAFE hinzu, wenn Sie garantieren können, dass der Ausdruck keine Eingaben vom Client enthält. • Wenn dies der Fall ist, kann ein böswilliger Client die Auswertung von privilegiertem JavaScript verursachen.
Referenzen	Jelly Tags Strenge Sicherheitseinstellungen

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Aktivieren Sie den Jelly JS-Interpolationsschutz für geschachtelte Ausdrücke

Verwalten Sie den Interpolationsschutz in Ihrer -Instanz.

Verwenden Sie die Eigenschaft und *glide.ui.jelly.js_interpolation.protect_nested_expressions*, um den Interpolationsschutz zu verwalten. Der Interpolationsschutz stellt sicher, dass Jelly-Ausdrücke, wenn sie in JavaScript verwendet werden, als sicher eingestuft werden müssen, indem sie entweder unter bestimmte Kategorien fallen oder im Ausdruck selbst als SAFE gekennzeichnet sind. Wenn diese Minderung nicht aktiviert ist, kann ein böswilliger Akteur einen GET-Parameter an eine Jelly-Seite senden und veranlassen, dass der Inhalt dieses Parameters als serverseitiges JavaScript mit Administratorrechten ausgewertet wird. Wenn diese Eigenschaft nicht auf den empfohlenen Wert **true**festgelegt ist, sind in JavaScript interpolierte schädliche Jelly-Ausdrücke zulässig, und ein Anwender kann Code mithilfe einer Jelly-Vorlage ausführen.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.ui.jelly.js_interpolation.protect_nested_expressio*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	falsch

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Kategorie	Validierung, Bereinigung und Codierung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 9 • CVSS-Punktzahl: Kritisch • Details zum Sicherheitsrisiko: Wenn die Eigenschaft auf **„false“** festgelegt ist, sind schädliche Jelly-Ausdrücke zulässig.
Abhängigkeiten und Voraussetzungen	Keine

Relative Links erzwingen

Verwenden Sie die Eigenschaft *glide.cms.catalog_uri_relative*, um relative Links vom URI-Parameter für `/ess/catalog.do`zu erzwingen.

- Bei Festlegung auf **true**werden nur relative URLs über die Seite „ `/ess/catalog.do` “ unter Verwendung des Parameters *uri* zugelassen.
- Bei Festlegung auf **„falsch“** sind alle URLs zulässig, was auch Verknüpfungen zu externen, nicht autorisierten Inhalten zulassen kann.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.cms.catalog_uri_relative*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Um Versuche einzuschränken, externe, nicht autorisierte Inhalte zu verknüpfen.
Empfohlener Wert	wahr
Standardwert	falsch
Sicherheitsrisikobewertung	2.6
Funktionale Auswirkung	(Niedrig) Diese Korrektur erzwingt die Validierung auf der Katalogseite, sodass nur relative URLs zulässig sind. Vorhandene Links zu externen Webanwendungen werden beschädigt.
Sicherheitsrisiko	(Hohe) absolute URLs können ein Sicherheitsrisiko darstellen, wenn sie als Teil von Parametern oder Feldwerten verwendet werden und so die Quellseite auf eine von Angreifern kontrollierte Website umleiten.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erzwingen Sie die Prüfung der URL-Allow-Liste

Verwenden Sie die Eigenschaft *glide.security.url.whitelist*, um eine zusätzliche Validierungsebene hinzuzufügen, um sicherzustellen, dass eine eingeführte externe URL Teil der URLs auf der Aufnahmeliste sein muss.

Eine offene Umleitung tritt auf, wenn eine angreifbare Webseite zu einer nicht vertrauenswürdigen und böswilligen Seite umgeleitet wird, die den Benutzer gefährden kann. Offene Umleitungsangriffe gehen mit einem Phishing-Angriff einher, da der geänderte angreifbare Link mit der ursprünglichen Website identisch ist, was die Erfolgswahrscheinlichkeit des Phishing-Angriffs erhöht.

Diese Eigenschaft gilt in den folgenden Fällen:

- `/logout.do?sysparm_goto_url={Externe URL}`
- `/cms_login_redirect.do?sysparm_goto_url={Externe URL}`

Benutzer werden zu einer externen vertrauenswürdigen Site weitergeleitet, nachdem sie sich von der Instanz abgemeldet haben:

- `/logout_redirect.do?sysparm_url={Externe URL}`
- `/saml_redirector.do?sysparm_uri={Externe URL}`

Wenn SAML aktiviert ist, wird eine Abmelde-URL eines Identitätsanbieters (IDP) aufgerufen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.security.url.whitelist*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Dient zur Implementierung einer sicheren URL-Umleitung während der Anmeldung, Abmeldung oder anderen Umleitungen. Diese Eigenschaft mindert einen der OWASP-Top-10-Angriffe namens „Ungültige Umleitungen und Weiterleitungen“.
Typ	Zeichenfolge
Standardwert	wahr
Empfohlener Wert	wahr
Wert	Die genehmigten URLs Ihrer Organisation [Ein definierter FQDN (vollständig qualifizierter Domänenname)] z. B. http://www.servicenow.de]
Sicherheitsrisikobewertung	8.3
Funktionale Auswirkung	(Mittel) Diese Korrektur erzwingt die Validierung auf der Abmeldeseite. Dies kann sich auf einen Benutzer einer Instanz mit einer SSO/SAML-Konfiguration auswirken.
Sicherheitsrisiko	(Hoch) Die clientseitige offene Umleitung kann es Angreifern ermöglichen, Opfer/Anwender auf die vom

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Angreifer kontrollierte Website umzuleiten, und wird als Sicherheitsrisiko angesehen.
Referenzen	Fehler und Korrekturen für Multi-SSO (SAML 2.0).

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Excel-Formeln codieren [In Security Center 1.3 aktualisiert]

Verwenden Sie die Eigenschaft *glide.export.escape_formulas*, um die Excel-Injektion, auch bekannt als Formelinjektion, zu verhindern.

Eine Excel-Einschleusung tritt auf, wenn Websites nicht vertrauenswürdige Einträge in Excel-Dateien einbetten. Wenn Sie eine Tabellenkalkulationsanwendung wie Microsoft Excel oder LibreOffice Call verwenden, um eine Datei zu öffnen, werden alle Zellen, die mit +, -, = oder @ beginnen, als Formel interpretiert. Wenn Sie die Eigenschaft *glide.export.escape_formulas* auf **true**festlegen, wird Zeichenfolgenwerten, die mit +, -, = oder @ beginnen, beim Exportieren in CSV-, XLS- oder XLSX-Dateien ein einzelner Apostroph vorangestellt.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.export.escape_formulas*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Um die Anwendung gegen die Excel- oder Formelinjektion zu verhindern.
Empfohlener Wert	wahr
Standardwert	falsch
Sicherheitsrisikobewertung	6.5
Funktionale Auswirkung	(Niedrig) Böswillig erstellte Formeln können für einen Hijacking-Angriff auf den Computer des Benutzers verwendet werden, indem Schwachstellen in der Tabellenkalkulationssoftware ausgenutzt werden.
Sicherheitsrisiko	(Moderat) Böswillige Formeln stellen auch dann ein Risiko dar, wenn die Einbettungstabelle keine vertraulichen Informationen enthält, da sie dazu verwendet werden können, den Computer des Betrachters zu gefährden.
Workaround	Erwägen Sie als Alternative, nach Möglichkeit alle nachfolgenden Leerzeichen zu entfernen und alle vom Client bereitgestellten Daten auf alphanumerische Zeichen zu beschränken.
Referenzen	Verfügbare Systemeigenschaften

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

HTML in Listenansichten codieren [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.ui.escape_html_list_field*, um HTML-Escape-Zeichen für HTML-Felder in einer Listenansicht zu erzwingen.

HTML ist einer der Typen, die den Wörterbuchfeldern zugewiesen werden können. Durch das Zuweisen von HTML-Feldern an einen beliebigen Feldtyp erhalten Sie die Funktionalität zum Formatieren von Inhalten mithilfe von HTML-Codes (z. B. `<p>`, `<a href>`, `<b>`, `<font>`, `<img>`). Ein böswilliger Anwender kann HTML-Code in das Formularfeld einschleusen, um unerwünschte Skripts in verschiedenen Client-/Benutzersitzungen auszuführen.

- Legen Sie diese Eigenschaft auf „ **falsch** “ fest, um ein HTML-Escaping auszuführen, bevor die Datensätze/Felder im Browser gerendert werden, wenn die Tabelle als Listenansicht angezeigt wird.
- Wenn dies auf **true**festgelegt ist und Sie diese Spalte in einer Listenansicht auswählen, wenn Sie eine Tabellen- oder Datensatzliste anzeigen, werden diese HTML-formatierten Felder möglicherweise angezeigt.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.ui.escape_html_list_field*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Um die Anwendung gegen websiteübergreifende Skripting-Angriffe zu schützen
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	8.8
Funktionale Auswirkung	(Mittel) Diese Korrektur erzwingt die HTML-Codierung in der Anwenderoberfläche auf HTML-Parser-Ebene und gibt dem Anwender daher codierte Ergebnisse zurück. Sie kann basierend auf der Interaktion des Instanzanwenders mit den resultierenden Daten Auswirkungen auf die Funktionalität haben.
Sicherheitsrisiko	(Hoch) Die Eingabevalidierung muss in der Anwendung erfolgen, um sich gegen websiteübergreifende Skripting-Angriffe zu schützen. Diese Angriffe ermöglichen die Ausführung fremder Skripts in Anwendersitzungen im Kontext des angemeldeten Browsers. Angreifer können damit Sitzungsinformationen und vertrauliche Daten stehlen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Referenzen	Strenge Sicherheitseinstellungen

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

JavaScript mit Escape-Zeichen versehen

Verwenden Sie die Eigenschaft *glide.html.escape_script*, um in HTML-Feldern während Listenansichten Escape-Zeichen für JavaScript-Tags (`<script></script>`) zu erzwingen.

HTML ist einer der Typen, die den Wörterbuchfeldern zugewiesen werden können. Durch das Zuweisen von HTML-Feldern an einen beliebigen Feldtyp wird dem Anwender die Möglichkeit gegeben, den Inhalt mithilfe von HTML-Codes zu formatieren (z. B. `<p>`, `<a href>`, `<b>`, `<font>`, `<img>`). Wenn Sie *glide.html.escape_script* auf **false**setzen, werden die Tags (`<script></script>`) möglicherweise angezeigt, wenn Sie diese Spalte in einer Listenansicht auswählen, während Sie eine Tabellen- oder Datensatzliste anzeigen.

Ein böswilliger Angreifer kann JavaScript-Code einfügen, indem er ihn in die Tags (`<script></script>`) einbettet. Der Angreifer kann einen Vorteil ausnutzen, indem er einen ausgefeilten JS-Vektor einschleust, der ausgeführt werden kann, wenn ein Benutzer den Tabellendatensatz öffnet.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.html.escape_script*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Verhinderung von Cross Site Scripting-Angriffen auf eine Anwendung
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	8.8
Funktionale Auswirkung	(Mittel) Diese Korrektur erzwingt JavaScript-Escaping in der Anwenderoberfläche und rendert codierte Ergebnisse für den Anwender. Dies kann sich je nach Interaktion des Instanzbenutzers mit den resultierenden Daten auf die Funktionalität auswirken
Sicherheitsrisiko	(Hoch) Die Eingabevalidierung muss in der Anwendung erfolgen, um sich gegen websiteübergreifende Skripting-Angriffe zu schützen. Diese Angriffe ermöglichen die Ausführung fremder Skripts in einer Anwendersitzung im Kontext des

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	angemeldeten Browsers. Angreifer können damit Sitzungsinformationen und vertrauliche Daten stehlen.
Referenzen	Verfügbare Systemeigenschaften Strenge Sicherheitseinstellungen

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Escape-Zeichen für Jelly-Skript [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.ui.escape_all_script*, um das Escape-Zeichen für alle in Jelly eingefügten Skripts zu erzwingen.

Versieht alle in enthaltenen JS- und HTML-Zeichenfolgen mit Escape-Zeichen<j:jelly> `...` </j:jelly> bevor sie in den Ausgabestream geschrieben werden, wodurch mehrere XSS-Probleme verhindert werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.ui.escape_all_script*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Kategorie	Validierung, Bereinigung und Codierung

Zweck	Wenn die Eigenschaft nicht auf **true**festgelegt ist, müssen Entwickler für jedes anwenderdefinierte Jelly-Skript mehrere Schritte ausführen, um XSS-Probleme zu vermeiden. Diese Schritte umfassen das Auffinden der Jelly-Variablen, die an den Ausgabestream gesendet werden, um sie auf Webseiten zu rendern, und das Ausführen von Escape-Zeichen für jedes der folgenden Tags:
	
	`$ – {JS: Ausdruck}`
	
	`$ – {HTML: Ausdruck}`
	
	ODER
	
	`$ – {JS, HTML: Ausdruck}`

Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	7.3
Funktionale Auswirkung	(Mittel) Diese Korrektur erzwingt Jelly-Escaping auf Parser-Ebene. Sie kann sich auf die Funktionalität der

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Benutzerinteraktion mit den resultierenden Daten auswirken.
Sicherheitsrisiko	(Hoch) Die Eingabevalidierung muss für alle Anwendereingaben erfolgen, die in der Anwendung eingegeben werden. Auf diese Weise können Einschleusungsangriffe auf die Plattform verteidigt und geschützt werden.
Workaround	Die Anwenderoberfläche kann betroffen sein, da einige der Skripts und HTML-Tags, die für das Rendern auf einer Webseite entwickelt wurden, fehlerhaft erscheinen können. Diese Korrektur sendet die codierte Ausgabeseite zum Rendern an den Browser. Anstelle von „`meine Zeichenfolge hier`"könnte beispielsweise „`<u>meine</u>` Zeichenfolge hier" angezeigt werden, da das Tag `<u>` ordnungsgemäß mit Escape-Zeichen versehen wurde. In diesem Fall fügen Sie dem Jelly-Ausdruck das Präfix „NOESC" hinzu, um ein Escape-Zeichen für JS zu verhindern. Beispiel: • Vor: ($[jvar_context_menus]); • Nach: `($[NOESC:jvar_context_menus]);` • Vor: $[jvar_ui_policy_scripts] • Nach: `$[NOESC:jvar_ui_policy_scripts]`
Referenzen	Strenge Sicherheitseinstellungen Jelly Tags

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Skripts in Scratchpad codieren [In Security Center 1.3 aktualisiert]

Erfahren Sie, wie Scratchpad-Faktoren die Sicherheitslage Ihrer Instanz berücksichtigen und wie Sie sie verwalten, damit keine schädlichen Skripts darauf ausgeführt werden können.

Mit dem Scratchpad können Sie auf einfache Weise Informationen auf dem Server festlegen, auf die Sie im Browser zugreifen können. Ein Administrator kann ein Skript für alles erstellen, was darin enthalten sein soll, einschließlich beliebiger Datensätze. Wenn diese Eigenschaft nicht auf den empfohlenen Wert **true**festgelegt ist, können bösartige Skripts wie bei einer websiteübergreifenden Skripting-Schwachstelle ausgeführt werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.ui.escape_scratchpad*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Validierung, Bereinigung und Codierung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 6,5 • CVSS-Punktzahl: Mittel • Details zu Sicherheitsrisiken: Wenn die Eigenschaft nicht auf den empfohlenen Wert **true**festgelegt ist, können bösartige Skripts wie bei einer websiteübergreifenden Skripting-Schwachstelle ausgeführt werden.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Workflow-Verwaltung

XML-Markup codieren [In Security Center 1.3 aktualisiert]

Verwenden Sie die Eigenschaft *glide.ui.escape_text*, um das Escape-Zeichen für XML-Werte auf Parser-Ebene zu erzwingen, bevor Sie sie an den Browser des Clients übertragen.

Site-übergreifendes Skripting tritt auf, wenn ein Angreifer schädliches JavaScript in einen Einstiegspunkt einschleust. Die Plattform/Anwendung kann das schädliche JavaScript nicht mit Escape-Zeichen versehen, bevor sie zur Ausführung an den Browser des Opfers übertragen wird. Escape-Zeichen bedeutet in diesem Kontext Folgendes:

- **&** --> `&`
- **<** --> `<`
- **>** --> `>`
- **"** --> `"`
- **'** --> `'`
- **/** --> `/`

Beispiel: <![CDATA[<script> `alert('XSS-Angriff');`</script>]]>

Escape-Zeichen: <script>alert('XSS Attack');</script>

Stellen Sie sicher, dass die Eigenschaft *glide.ui.escape_text* in der Tabelle „sys_properties“ vorhanden und auf „wahr“ festgelegt ist.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.ui.escape_text*

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Das Codieren von XML stellt sicher, dass Browser das schädliche JavaScript, das in nicht vertrauenswürdigen Daten eingebettet ist, nicht analysieren und als JavaScript ausführen. • Ein böswilliger Anwender kann einen XSS-Angriff versuchen, um entweder die Sitzung anderer Anwender zu kapern oder den Anwender auf eine schädliche Website umzuleiten. • Die NOW Platform enthält Code zum Sichern von Cookies. Um ihn jedoch mit Escape-Zeichen zu versehen, muss diese Eigenschaft auf **true**festgelegt sein.
Empfohlener Wert	wahr
Sicherheitsrisikobewertung	8.8
Funktionale Auswirkung	(Mittel) Diese Korrektur erzwingt die XML-Codierung auf XML-Parser-Ebene in der Anwenderoberfläche. Sie rendert die codierten Ergebnisse für den Benutzer, was je nach Interaktion des Instanzbenutzers mit den resultierenden Daten Auswirkungen auf die Funktionalität haben kann.
Sicherheitsrisiko	(Hoch) Die Eingabevalidierung muss in der Anwendung erfolgen, um sich gegen websiteübergreifende Skripting-Angriffe zu schützen. Diese Angriffe ermöglichen die Ausführung fremder Skripts in einer Anwendersitzung im Kontext des angemeldeten Browsers. Angreifer können damit Sitzungsinformationen und vertrauliche Daten stehlen.

Workaround	Nachdem Sie diese Eigenschaft auf **true**festgelegt haben, wird das Rendern für die HTML-Tags in der Katalogelementbeschreibung oder im Hilfetext der Katalogelementvariablen angehalten. Sie können möglicherweise für einige Felder keine HTML-Formatierung verwenden.
	
	Wenn jedoch die Eigenschaft *glide.ui.escape_text* deaktiviert ist, wird allen JEXL-Ausdrücken ein Ausgabecodierer vorangestellt:
	
	`${JS:Ausdruck}`
	
	`${HTML:Ausdruck}`
	
	oder
	
	`${JS,HTML:Ausdruck}`

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Escape-XML-Antwort

Verwalten Sie, wie XML-Escape-Zeichen in Ihrer Instanz behandelt werden.

Verwenden Sie diese Eigenschaft, um zu verwalten, ob XML-Antworten mit Escape-Zeichen versehen werden. Wenn die Eigenschaft auf den empfohlenen Wert „ **false**“ festgelegt ist, werden XML-Antworten nicht mit Escape-Zeichen versehen, was zu einem XML-Einschleusungsangriff führen kann. Das Einfügen von unbeabsichtigtem XML-Inhalt in eine XML-Nachricht kann die beabsichtigte Logik einer Anwendung ändern.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.soaprequest.unescape_xml_response*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	falsch
Standardwert	falsch
Kategorie	Validierung, Bereinigung und Codierung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 6,4 • CVSS-Punktzahl: Mittel • Details zu Sicherheitsrisiken: Wenn Sie diese Eigenschaft auf „ **falsch** “ setzen, wird XML-Escaping deaktiviert, was zu einem XML-Einschleusungsangriff führen kann.
Abhängigkeiten und Voraussetzungen	Keine

HTML-Bereinigung aktivieren [In Security Center 1.3 aktualisiert]

Verwenden Sie die Eigenschaft *glide.html.sanitize_all_fields*, um die HTMLSanitizer-Skripteinbindung zu aktivieren, die HTML-Eingaben basierend auf den in einem Skript konfigurierten Attributen auf der Ausschluss- und Aufnahmeliste bereinigt.

Die für Dictionary/Fields verfügbaren Feldtypen sind HTML und Übersetztes HTML. Mit diesen HTML-Eingabefeldern können Anwender Eingaben im HTML-Format schreiben, z. B.:

`<h1>Test</h1>`) unter Verwendung der einfachsten HTML-Tags wie `<img>`, `<a href …>`und `<iframe>`.

Sie kann einem böswilligen Angreifer die Möglichkeit geben, bösartige Vektoren mit HTML-Tags einzuschleusen, z. B.:

```
[<IMG SRC=" &#14; JavaScript:alert('XSS');">][<IMG
onmouseover="alert('xss')">],[a href="" onclick=alert(/xss/)].
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.html.sanitize_all_fields*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Verhindert Cross Site Scripting- und HTML-Einschleusungsangriffe auf die Anwendung
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	8.8
Funktionale Auswirkung	(Hoch) Diese Korrektur erzwingt den HTML-Ausgabecodierungsmechanismus, bevor die Anwenderdaten an den Anwender zurückgegeben werden. Wenn der Kunde Anpassungen vorgenommen hat, die das Rendern des HTML-Attributs oder der Inhaltsdaten umfassen, wirkt sich dies auf die Funktionalität aus.
Sicherheitsrisiko	(Hoch) Anwendereingaben sollten sicher behandelt werden, wenn die Daten in der Anwendung gespeichert und verarbeitet werden. Dies reduziert clientseitige Cross Site Scripting-Angriffe durch Ausgabecodierung der Daten.
Workaround	Diese Eigenschaft bereinigt alle HTML-Felder im System. Wenn Sie die HTML-Bereinigung für einzelne Felder aktivieren müssen, finden Sie weitere Informationen unter Bereinigung einzelner Felder aktivieren. Sie können auch die Aufnahme- oder Ausschlussliste konfigurieren, um HTML-Tags und Attribute gemäß den Richtlinien Ihrer Organisation zu bereinigen.
Referenzen	HTML-Bereinigung aktivieren HTML-Bereinigung

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Zulässige Java-Pakete einschränken [Aktualisiert in Security Center 1.3]

Durch die Konfiguration dieser Eigenschaften wird verhindert, dass gefährliche APIs für die Skript-Engine verfügbar gemacht werden.

Konfigurieren Sie die Systemtabellen, und installieren Sie das empfohlene Plugin entsprechend.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die Tabellen *sys_whitelist_member* und *sys_whitelist_package* keine leeren Werte sind, können gefährliche APIs für die Skript-Engine verfügbar gemacht werden. Einträge entsprechen dem Java-Namespace, die nicht von den Sicherheitsteams von ServiceNow genehmigt wurden.

Installieren Sie das Tool zum Entfernen von Paketaufrufen. Details siehe Tool zum Entfernen von Paketenaufrufen.

Wenden Sie sich an Kundenservice und Support, um diese Tabellen zu bearbeiten.

Weitere Informationen

Attribut	Beschreibung
Tabelle, Plugin-Name	Tabellen: • *sys_whitelist_member* • *sys_whitelist_package* Plugin: com.glide.script.packages_call_removal
Konfigurationstyp	Tabellarische Konfiguration, Plugins
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Vor gefährlichen APIs schützen, die für die Skript-Engine verfügbar gemacht werden.
Empfohlener Wert	Leer
Standardwert	Keine. Dies ist eine Tabellenkonfiguration und keine Glide-Eigenschaft, daher gibt es keinen Standardwert.
Konfigurationstyp	Tabellenliste, Plugin
Sicherheitsrisiko	(Hoch) Gefährliche APIs sind möglicherweise für die Skript-Engine verfügbar gemacht. Diese unterstützten APIs führen wahrscheinlich zu Instabilität und Ungewissheit innerhalb der Instanz.
Sicherheitsrisikobewertung	8.2

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Tool zum Entfernen von Paketenaufrufen

Aktivieren und starten Sie das Plugin Packages Call Entfernung Tool (*com.glide.script.packages_call_removal*), und überlegen Sie dann, ob jede der vorgeschlagenen Änderungen abgeschlossen oder abgelehnt werden soll.

Das Tool zum Entfernen von Paketenaufrufen ist ein Plugin, das:

- Durchsucht Skripts nach Paketaufrufen für Now Platform Java-Klassen.
- Schlägt Änderungen vor, um sie durch bevorzugte GlideScriptable-Namen zu ersetzen.
- Erleichtert die Skriptänderungen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn es sich bei diesem Datensatz um einen Basissystemdatensatz handelt, wird das Element durch Verwendung der Empfehlung des Tools als „customer_update“ markiert. Es kann jedoch dennoch nützlich sein, dieses Tool zu verwenden, da es Pakete,xxx-Aufrufe kennzeichnet.

Das Tool zum Entfernen von Paketaufrufen meldet möglicherweise einige Paketaufrufe, die in „`sa_mapping_ext_commands`“ und „`sa_custom_operation`“verwendet werden. Diese Paketaufrufe gehören zum MID-Server. Da es keine Klassen gibt, wird der Code im MID-Server ausgeführt. Wenn Sie im Abschnitt „Fehler“ einen der folgenden aufgelisteten Paketaufrufe finden, markieren Sie ihn als Abgelehnt (Ignoriert). Das Tool meldet diesen Paketaufruf nicht erneut.

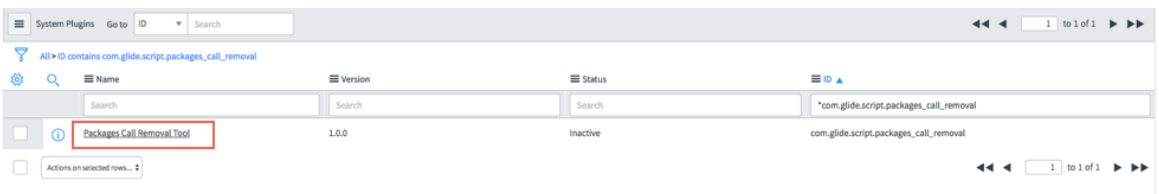
- `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_content);`
- `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(Dateiname);`
- `Packages.com.snc.sw.commands.HttpCallHandler`
- `Packages.com.snc.sw.dto.ProviderType.SSH`

Weitere Informationen

Attribut	Beschreibung
Plugin-Name	com.glide.script.packages_call_removal
Konfigurationstyp	Systemdefinition > Plugins
Zweck	Entfernen/Ersetzen nicht autorisierter Paket-/Mitgliedsaufrufe durch zulässige Glide-Namen (GlideScriptable), die nur autorisierten Zugriff auf Daten ermöglichen.
Empfohlener Wert	Aktiv
Funktionale Auswirkung	(Niedrig) Diese Korrektur würde die Paketaufrufe durch *`GlideScriptable`* APIs ersetzen und kann sich auf die Anpassungen auswirken, die Paketaufrufe enthalten. Das Tool ersetzt Paketaufrufe nicht automatisch. Stattdessen werden Vorschläge bereitgestellt, die in der Tabelle „packages_call_item“ gespeichert sind. Ihr Administrator kann dann entscheiden, ob er den vorgeschlagenen Change akzeptiert oder ablehnt.
Sicherheitsrisiko	(Mittel) Clientseitige API-Aufrufe, die zum Abruf von Daten oder zum Objektzugriff auf dem Server führen, gelten unter Sicherheitsaspekten als gefährlich. Sie sollten für die Autorisierung und Einschränkung des Zugriffs auf vertrauliche Objekte validiert werden.

Schritte zum Konfigurieren von

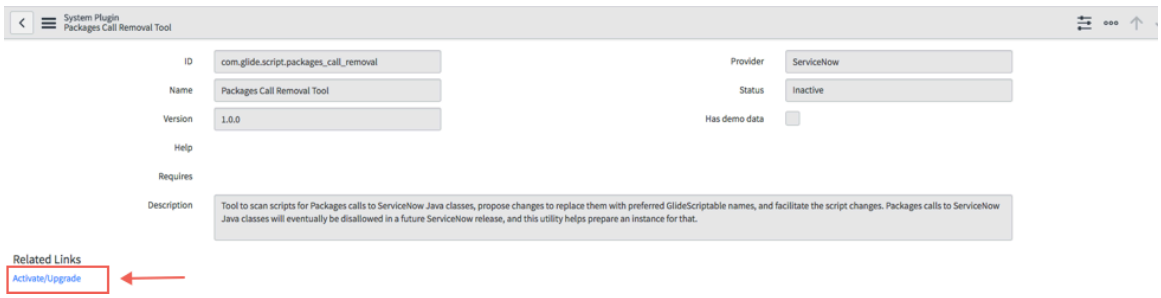
1. Navigieren zu **Systemdefinition** > **Plugins**



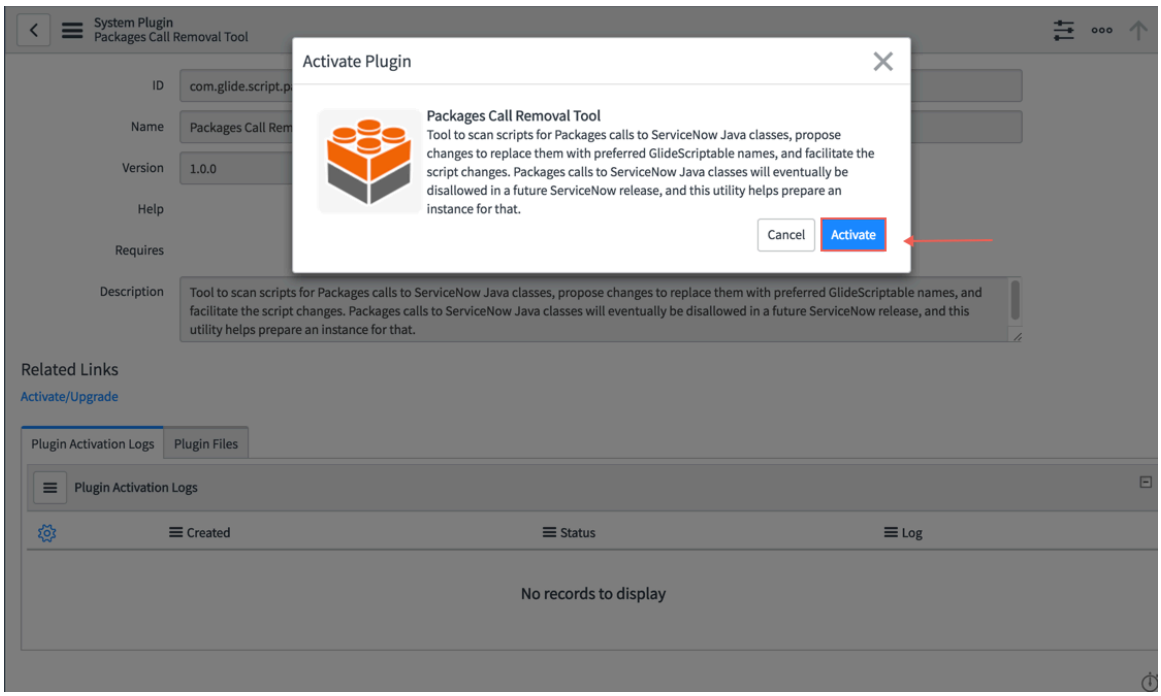
Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Suchen Sie nach der Plugin-ID = *com.glide.script.packages_call_removal*.



3. Klicken Sie auf **Aktivieren/Upgrade**, um das Plugin zu aktivieren.



4. Um Aufrufe von Aufnahmelistenpaketen und Aufnahmelistenmitglieder zu überprüfen, führen Sie die in den Abschnitten „Schritte zum Konfigurieren“ in den folgenden Themen beschriebenen Aktionen aus:
   - Überprüft die Anrufe von Allow-Listenmitgliedern
   - Überprüft die Allow-Liste der Paketaufrufe

Anfänglicher eindeutiger LDAP-Namen löschen [Aktualisiert in Security Center 1.3]

Verwenden Sie diese Eigenschaft, um den eindeutigen Namen eines LDAP-Server-Datensatzes zu verwalten.

Diese Eigenschaft steuert den eindeutigen Namen eines LDAP-Serverdatensatzes, der beim Ausführen eines sofort einsatzbereiten Korrekturskripts eingefügt wird. Wenn die Option auf den empfohlenen Wert „“ oder leer festgelegt ist, können LDAP-Serverdaten von einem Benutzer mit geringeren Berechtigungen aufgelistet werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.ldap.initial.dn*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	leer
Standardwert	leer
Kategorie	Validierung, Bereinigung und Codierung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 2,7 • CVSS-Punktzahl: Niedrig • Details zu Sicherheitsrisiken: Wenn Sie den Eigenschaftswert auf „“ oder leer festlegen, könnten LDAP-Serverdaten für einen Anwender mit geringeren Berechtigungen zugänglich sein.
Abhängigkeiten und Voraussetzungen	Keine

Strikte Sicherheit von Sitzungscookies erzwingen [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.ui.secure_cookies*, um ordnungsgemäß formatierte Cookies anzufordern

Wenn Sie die Eigenschaft auf „true“ festlegen, lehnt Ihre Instanz eine Sitzung ab, wenn das zugehörige Cookie nicht das erwartete Format aufweist.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.ui.secure_cookies*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Um eine sicherere Sitzungsauthentifizierung zu erreichen.
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	8.8

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Funktionale Auswirkung	(Niedrig) Wenn die Eigenschaft auf „true“ festgelegt ist, werden falsch formatierte Cookies abgelehnt. Wenn ein solches Cookie abgelehnt wird, muss sich der Benutzer erneut anmelden.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Schwellenwert für Entitätserweiterung minimieren [Aktualisiert in Security Center 1.3]

Verwenden Sie die Eigenschaft *glide.xmlutil.max_entity_expansion*, um die maximale Entitätserweiterungsgrenze in eine kleinere Zahl zu ändern.

Now Platform verarbeitet keine weiteren Entitätserweiterungen, die größer als der in dieser Eigenschaft angegebene zulässige Grenzwert sind.

Hinweis: 500 ist das von Now Platformfestgelegte Standardminimum, was als sicherer Schwellenwert gilt.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.xmlutil.max_entity_expansion*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Diese Korrektursteuerung muss aktiviert sein, um sich gegen XML-Entitätserweiterungs-/Billion-Lach-Angriffe zu schützen.
Empfohlener Wert	3000
Standardwert	100000
Sicherheitsrisikobewertung	5.3
Funktionale Auswirkung	(Niedrig) Wenn die Anpassung eine große Entitätserweiterung verwendet, blockiert Now Platform möglicherweise die weitere Verarbeitung.
Sicherheitsrisiko	(Mittel) Ein Angreifer kann diese Schwachstelle nutzen, um Daten exponentiell zu erweitern, wodurch schnell alle Systemressourcen verbraucht werden.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Hochgeladene MIME-Typen einschränken [in Security Center 1.3 aktualisiert]

Verwenden Sie die Eigenschaft *glide.security.file.mime_type.validation*, um die Überprüfung des MIME-Typs für Uploads zu aktivieren. Sie können die MIME-Typvalidierung für Dateianhänge aktivieren (setzen Sie die Eigenschaft auf **wahr**) oder deaktivieren (setzen Sie sie auf **falsch**).

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Voraussetzungen

Legen Sie vor dem Festlegen dieser Eigenschaft die Eigenschaft *glide.attachment.extensions* fest. Nur die in *glide.attachment.extensions* angegebenen Erweiterungen werden während des Uploads auf den MIME-Typ überprüft. Weitere Informationen finden Sie unter Dateierweiterungen einschränken .

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.security.file.mime_type.validation*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Erzwingen der Überprüfung von MIME-Typ/magischen Bytes während Datei-Uploads.
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	5.4
Funktionale Auswirkung	(Mittel) Diese Korrektur aktiviert die Verifizierung des MIME-Typs für die Anhänge zur Anwendung. Keine Auswirkungen auf die Funktionalität, es sei denn, beim Hochladen der Dateien liegt eine böswillige Absicht vor, da diese Validierung lediglich überprüft, ob die Synchronisierung zwischen dem MIME-Typ und den Daten fehlerhaft ist.
Sicherheitsrisiko	(Mittel) Um Schwachstellen wie Dateieinschluss und das Hochladen schädlicher Dateien zu reduzieren, sollte die Verifizierung des MIME-Typs aktiviert sein.
Referenzen	Anhänge werden verwaltet

Weitere Informationen zum Konfigurieren von Eigenschaften für die Härtung finden Sie unter Härtungseinstellungen für die Instanzsicherheit.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Externe XML-Entitäten einschränken [in Security Center 1.3 aktualisiert]

Verwenden Sie die Eigenschaft *glide.security.file.mime_type.validation*, um die Überprüfung des MIME-Typs für Uploads zu aktivieren. Sie können die MIME-Typvalidierung für Dateianhänge aktivieren (setzen Sie die Eigenschaft auf **wahr**) oder deaktivieren (setzen Sie sie auf **falsch**).

Voraussetzungen

Legen Sie vor dem Festlegen dieser Eigenschaft die Eigenschaft *glide.attachment.extensions* fest. Nur die in *glide.attachment.extensions* angegebenen Erweiterungen werden während des Uploads auf den MIME-Typ überprüft.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnung: Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.xml.entity.whitelist*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Diese Korrektursteuerung muss aktiviert sein, um sich gegen XXE-Angriffe zu schützen.
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	5.4
Funktionale Auswirkung	(Niedrig) Wenn die Anpassung eine externe Entität verwendet, die nicht in der Eigenschaft *glide.xml.entity.whitelist* aufgeführt ist, blockiert die NOW Platform möglicherweise die weitere Verarbeitung.
Sicherheitsrisiko	(Kritisch) Ein Angreifer kann die DTD verwenden, um beliebige HTTP-Anforderungen einzubeziehen, die der Server ausführen könnte. Dies könnte zu weiteren Angriffen führen, die die Vertrauensstellung des Servers zu anderen Entitäten nutzen.

XMLdoc2-Entitätsvalidierung mit allowlistDisable-Entitätserweiterung erfordern [Aktualisiert in Security Center 1.3]

Wenn Anpassungen keine Entitätserweiterung erfordern, verwenden Sie die Eigenschaft *glide.xmlutil.max_entity_expansion*, um die externe Entitätserweiterung vollständig zu deaktivieren. Die XML-Datei schließt die Analyse ab, enthält jedoch keine internen oder externen Entitäten.

- Wenn Sie diese Eigenschaft auf **true**festlegen, versuchen alle externen Entitäten, abhängig von der Einstellung in der Eigenschaft *glide.stax.whitelist_enabled*, die betreffenden Entitäten aufzulösen oder zu erweitern.
- Wenn Sie diese Eigenschaft auf **false**festlegen, werden alle Auflösungen und Erweiterungen von Entitäten blockiert. Weitere Informationen finden Sie unter XMLdoc2-Entitätsvalidierung mit Allow-Liste.

Voraussetzungen

Vor dem Festlegen dieser Eigenschaft:

- Legen Sie die Eigenschaften *glide.xml.entity.whitelist.enabled*und *glide.stax.whitelist_enabled*auf „wahr“ fest. Weitere Informationen finden Sie unter XMLdoc/XMLUtil-Entitätsvalidierung mit Allow-Liste und XMLdoc2-Entitätsvalidierung mit Allow-Liste.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Definieren Sie eine Liste von kommagetrennten FQDNs in der Eigenschaft *glide.xml.entity.whitelist*, den einzigen URLs, die über die Verarbeitungseigenschaft für XML-Entitäten erreicht werden können. Weitere Informationen finden Sie unter Verarbeitung externer XML-Entitäten – Allow-Liste.

Warnung: Dies ist eine Safe-Harbor-Eigenschaft. Das bedeutet, dass der Wert nicht geändert werden kann, nachdem er geändert wurde. Er kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.stax.whitelist_enabled*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Diese Korrektursteuerung muss aktiviert sein, um sich gegen einen Angriff der XML-Entitätserweiterung/ Billion Leign zu schützen.
Empfohlener Wert	wahr
Standardwert	falsch
Sicherheitsrisikobewertung	9.8
Funktionale Auswirkung	(Niedrig) Wenn die Anpassung die Entitätserweiterung verwendet, blockiert Now Platform möglicherweise die weitere Verarbeitung.
Sicherheitsrisiko	(Kritisch) Ein Angreifer kann diese Schwachstelle nutzen, um Daten exponentiell zu erweitern, wodurch schnell alle Systemressourcen verbraucht werden.
Workaround	Wenn die Anpassung eine Erweiterung der Entität erfordert, legen Sie diese Eigenschaft auf „true“ fest, und befolgen Sie die in XMLdoc2-Entitätsvalidierung mit Allow-Listedokumentierten Schritte.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Weitere Informationen zu OWASp-Ressourcen finden Sie unter OWASp .

Legen Sie eine Sicherheitsrichtlinie für sichere Inhalte für SVG-Dateien fest [Neu in Security Center 1.3]

Die Eigenschaft *com.glide.csp.self_script_src_svg* fügt dem HTTP Content-Security-Policy-Header die Direktive „ **script-src None** “ hinzu, wenn über die Dateierweiterung „Translation Memory Index“ (IIX) auf skalierbare SVG-Dateien zugegriffen wird.

Die Eigenschaft *com.glide.csp.self_script_src_svg* verhindert, dass schädliche Dateianhänge, die Cross Site Scripting-Angriffe (XSS) speichern, in einer Instanz ausgeführt werden. Ohne diese Richtlinie könnte ein böswilliger Akteur einen Anwender dazu veranlassen, beliebigen JavaScript-Code in seinem Webbrowser auszuführen, was zu Sicherheitsschwachstellen wie Datenexfilterung und Sitzungsübernahme führen könnte.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*com.glide.csp.self_script_src_svg*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Validierung, Bereinigung und Codierung
Sicherheitsrisiko	• Schweregrad-Punktzahl: 7.1 • CVSS-Punktzahl: Hoch • Details zum Sicherheitsrisiko: Wenn Sie diese Eigenschaft nicht auf den empfohlenen Wert „true“ festlegen, kann dies dazu führen, dass ein Anwender beliebigen JavaScript-Code eines ungültigen Akteurs ausführt.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Diese Eigenschaft verhindert, dass SVG-Dateien (scalable vector graphics, skalierbare Vektorgrafiken) auf externe Skripts zugreifen.

Log Export Service (LES)

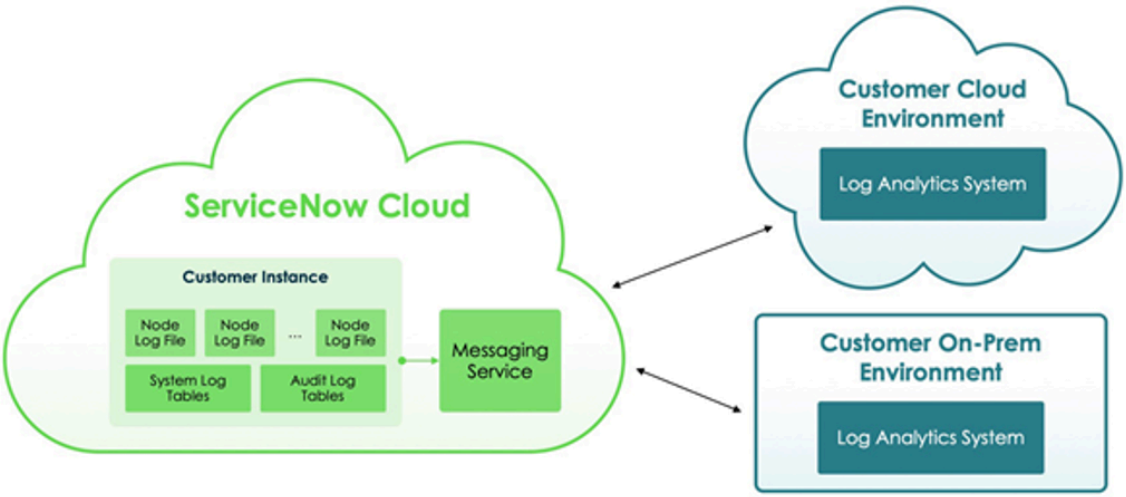
Log Export Service Mit (LES) können Sie Ihre Instanzsystem- und Anwendungsprotokolle nahtlos in Ihre Analysetools für Unternehmenssicherheit exportieren. Der Service bietet eine hoch skalierbare Integration mit Analysetools nahezu in Echtzeit, die einfach einzurichten und zu warten ist.

Mit dem -Integrationstool können Sie Ihre Analyselösungen für Folgendes nutzen:

- Erkennen Sie ServiceNow Sicherheitsbedrohungen, und analysieren Sie Security Incidents
- Beheben Sie Probleme, und optimieren Sie die Leistung der App ServiceNow .
- Überwachen und optimieren Sie die Anwender-Experience von ServiceNow .

LES nutzt eine Now Platform -Fähigkeit namens Hermes Messaging-Service, einen auf Apache Kafka] erstellten Multi-Mandanten-, Multi-Cluster-, Datentransport- und Warteschlangenservice, mit dem Ihre Instanz große Mengen von Kafka-Ereignissen produzieren und verbrauchen kann. Apache Kafka ist eine Open-Source-Datenstreaming-Plattform, die einen zentralen Integrationspunkt für den geschäftssystemübergreifenden Datenaustausch in Ihrem Unternehmen bietet.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



LES leitet eine Kopie der Protokollereignisse, sobald sie generiert werden, an Hermes Messaging-Serviceweiter.

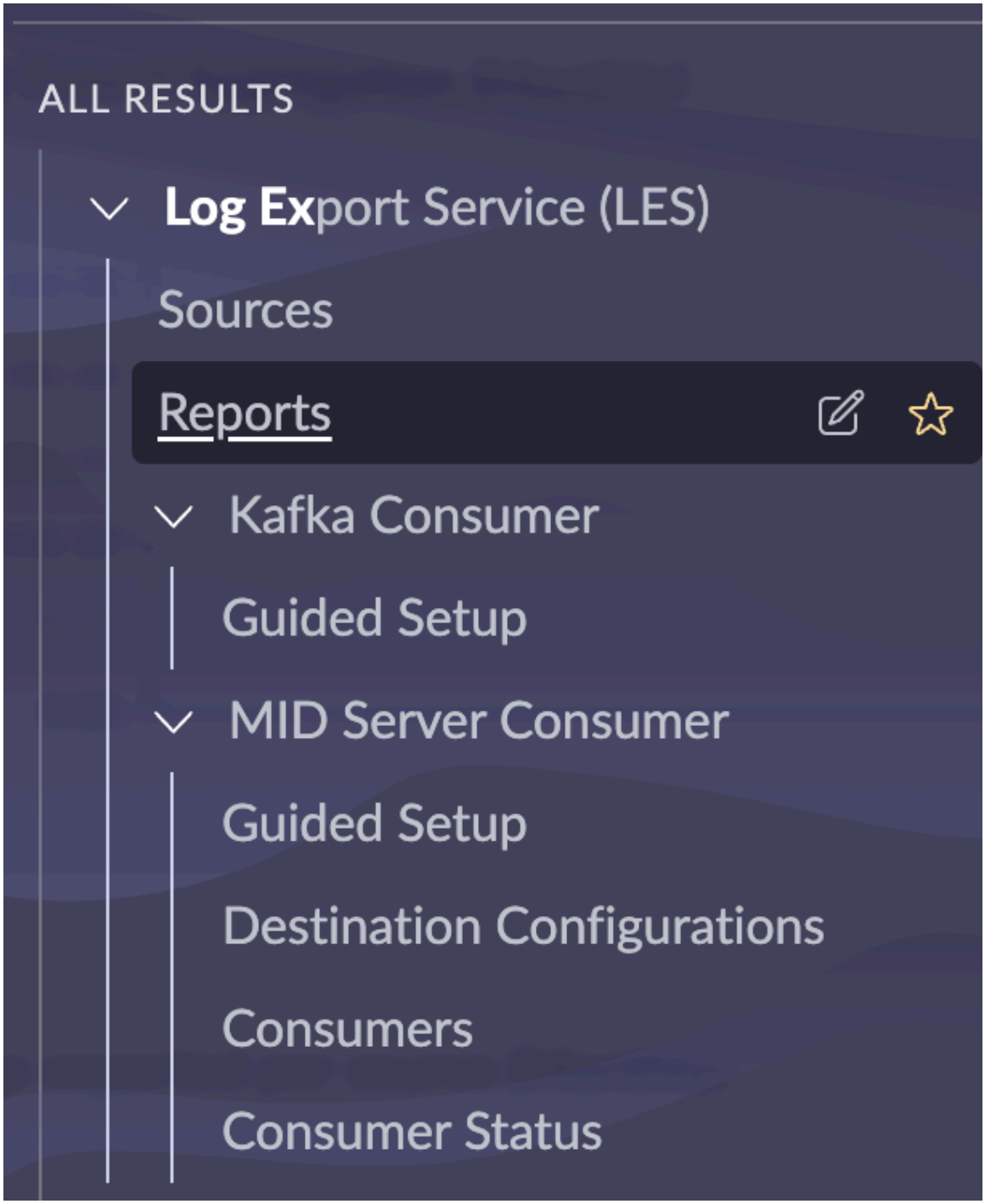
Hermes Messaging-Service ist ein auf Apache Kafka] erstellter Multi-Mandanten-, Multi-Cluster-, Datentransport- und Warteschlangenservice, mit dem Ihre -Instanz große Mengen von Kafka-Ereignissen produzieren und verbrauchen kann. Hermes Messaging-Service ist eine Now Platform-Fähigkeit, die als Teil von Stream Connect für Apache Kafka , Log Export Service (LES) und Instanzübergreifende Datenreplikation (IDR) verfügbar ist.

Die externen Protokollanalysesysteme, entweder in der Cloud oder lokal, können die Protokollereignisse aus Hermes Messaging-Serviceverwenden und verarbeiten. LES bietet drei Konnektivitätsoptionen zum Verwenden der Protokolle:

- Dedizierter MID-Server: Ein dedizierter MID-Server wird lokal oder in der Cloud installiert, der automatisch eine Verbindung zu Hermes Messaging-Serviceherstellt, Protokollereignisse kontinuierlich daraus abruft und sie dann über eine REST-Verbindung an Protokollanalysetools weiterleitet.
- Nutzen Sie den Kafka-Connector aus Ihrer Log Analytics-Lösung (z. B. Splunk): Ein Kafka-Connector des Log Analytics-Produkts Ihrer Wahl wird lokal oder in der Cloud installiert und stellt automatisch eine Verbindung zu Hermes Messaging-Serviceher, ruft kontinuierlich Protokollereignisse ab und veröffentlicht sie dann an Log Analytics-Tools zu übergeben.
- Direkt aus Ihrem Kafka-System: Ihr Kafka-System stellt eine direkte Verbindung mit dem Hermes Messaging-Service her und verwendet seine nativen Kafka-Protokollbefehle und Konnektivität, um Protokollereignisse daraus abzurufen.

Zum Konfigurieren und Verwalten von LES müssen Sie es aus ServiceNow Storeinstallieren. Die LES-Anwendung bietet Geführte Setups, die Sie bei der Installation des Service unterstützen, Seiten zum Konfigurieren des Service (Protokollquellen, Verbraucher und Ziele) und Berichte zum Verständnis der Protokollerstellung und -nutzung.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis: Sie können auch eine neue Quellkonfiguration erstellen. Weitere Informationen finden Sie unter Erstellen Sie eine Protokollquellenkonfiguration.

Log Export Service Rollen

Log Export Service wird mit diesen Rollen installiert.

Anwendungsadministrator [sn_logstoanalytics.admin]

Weitere Informationen zum Verwalten von Abonnements pro Benutzer finden Sie unter Verwalten von Abonnements pro Benutzer in Abonnement-Management , und wenden Sie sich an Ihren -Kundenbetreuer.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Rolle wird zusammen mit der Anwendung LES installiert und ermöglicht auch Nicht-Administratoren die Verwendung der Anwendung.

Enthält die Rollen

Liste der Rollen, die in der Rolle enthalten sind.

Keine.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Erweitert

Gibt an, ob die Rolle eine erhöhte Rolle ist. Erhöhte Rollen werden keinen Anwendern oder Gruppen zugewiesen und müssen durch eine Erhöhung verwendet werden. Einzelheiten finden Sie unterAuf eine privilegierte Rolle hochstufen.

Nein.

Besondere Überlegungen

Keine.

Systemadministrator [admin]

Weitere Informationen zum Verwalten von Abonnements pro Benutzer finden Sie unter Verwalten von Abonnements pro Benutzer in Abonnement-Management , und wenden Sie sich an Ihren -Kundenbetreuer.

Die Administratorrolle ist für das Setup der LES-Store-Anwendung erforderlich.

Enthält die Rollen

Liste der Rollen, die in der Rolle enthalten sind.

- sn_templated_snip.template_snippet_admin
- sn_employee.admin
- taxonomy_admin
- sn_ace.ace_user
- sn_hr_sp.esc_admin

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Erweitert

Gibt an, ob die Rolle eine erhöhte Rolle ist. Erhöhte Rollen werden keinen Anwendern oder Gruppen zugewiesen und müssen durch eine Erhöhung verwendet werden. Details finden Sie unter Auf eine privilegierte Rolle hochstufen.

Nein.

Besondere Überlegungen

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Keine.

Protokollquellen

Log Export Service (LES) kann Protokollquellen aus einigen Systemprotokolltabellen, der Audit-Tabelle und Anwendungsknoten-Protokolldateien exportieren.

Die folgenden Protokollquellen können von LES exportiert werden.

- Systemprotokolltabellen
  - syslog-Tabelle: Zeigen Sie Warnungen und Fehler für Instanzprozesse, Datensätze und nicht kritische Ereignisse an, z. B. die Auslastung des Arbeitsspeichers auf dem Servercomputer
  - Tabelle „syslog_transaction“: Zeigt alle Browseraktivitäten für eine Instanz an
  - Tabelle „sys_outbound_http_log“: Zeigt alle Anforderungen und Antworten für ausgehende Webservices wie REST und SOAP an
- Audit-Tabelle: Verwenden Sie die sys_audit-Tabellenansicht, um Änderungen an den für die Audit ausgewählten Tabellen vorzunehmen
- Protokolldateien für Anwendungsknoten: Verwenden Sie die localhost-Protokolldateien, um Anwendungsknotenfehler anzuzeigen. Ihre Instanz verfügt über mehrere Knoten, und jeder Knoten enthält mehrere Protokolldateien.

Weitere Informationen zu Schema und Zweck der oben genannten Protokollquellen finden Sie unter Systemprotokolle.

Erstellen Sie eine Protokollquellenkonfiguration

Durch Erstellen einer Protokollquellenkonfiguration können Sie die weiterzuleitenden Protokolle regulieren und Filter dafür festlegen.

Vorbereitungen

Erforderliche Rolle: admin oder sn_logstoanalytics.admin

Prozedur

1. Navigieren zu **Alle** > **Protokollexportservice**an.
   Eine Liste der Quellkonfigurationen wird angezeigt.
2. Wählen Sie **Neu** aus, wenn Sie eine neue Quellkonfiguration erstellen möchten.
   Sie können auch eine vorhandene Quellkonfiguration auswählen, wenn Sie sie ändern möchten.
   Das Quellformular wird angezeigt.
3. Füllen Sie die Felder im Formular aus.

Quellformular

Felder	Beschreibung
Quelltyp	Arten von Protokollquellen ◦ Knotenprotokoll ◦ Tabelle Weitere Informationen finden Sie unter Protokollquellen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder	Beschreibung
Protokollebene	Ein Satz von Standardprotokollierungsebenen, die zur Steuerung der Protokollierungsausgabe verwendet werden können. Gemäß der Konvention leitet jede Ebene Protokolle mit gleichem oder höherem Schweregrad weiter. **Hinweis:** Dieses Feld ist nur sichtbar, wenn eine der folgenden Bedingungen erfüllt ist. ◦ Wenn Sie „Knotenprotokoll“ als Quelltyp auswählen ◦ Wenn Sie Tabelle als Quelltyp auswählen und die Tabelle syslog ist
Akzeptiert	Gibt das Format an, in dem die Protokolle an Hermes weitergeleitet werden. Sie können entweder als JSON oder als Nur-Text gesendet werden.
Tabelle	Auswahl der Tabelle für Tabellentypprotokolle. **Hinweis:** Dieses Feld ist nur sichtbar, wenn Sie Tabelle als Quelltyp auswählen.
Filtertyp	Bedingungen für die selektive Weiterleitung von Protokollen. **Hinweis:** Dieses Feld ist nur sichtbar, wenn Sie entweder „syslog“ oder „sys_audit“ als Tabelle auswählen.

4. Wählen Sie Absenden aus, um eine neue **Quellkonfiguration** zu erstellen.

Erstellen Sie mehrere Themen in der LES-Quelltabelle

Verwenden Sie Nachrichten für jeden Quelltyp unabhängig voneinander, indem Sie ein eindeutiges Thema pro Quelltyp erstellen.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Fügen Sie die Systemeigenschaft sn_logstoanalytics.kafka.multi_topics hinzu, und legen Sie sie auf true fest.
   Sie ist standardmäßig auf False festgelegt.
2. Erstellen Sie einen neuen Quelldatensatz.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn Sie einen neuen Quelltyp erstellen, wird ein eindeutiges Thema dafür erstellt.

Die Themennamen haben das Suffix als Quelltyp. Beispiel: sn_logstoanalytics.node_log hat „node_log“ als Quelltyp.

3. Wahlweise: Erstellen Sie ein anderes Thema für eine andere Quelle als in den vorherigen Schritten.

Hinweis: Wenn sn_logstoanalytics.kafka.multi_topics auf „falsch“ festgelegt ist, ist die Möglichkeit zum Erstellen mehrerer Themen in der Quelltabelle deaktiviert.

Hinweis: Diese Funktion ist nicht mit dem MID-Server-Verbraucher (LES v2) kompatibel. Sie müssen Ihren eigenen Verbraucher (LES v1) verwenden.

Kafka-Verbraucher

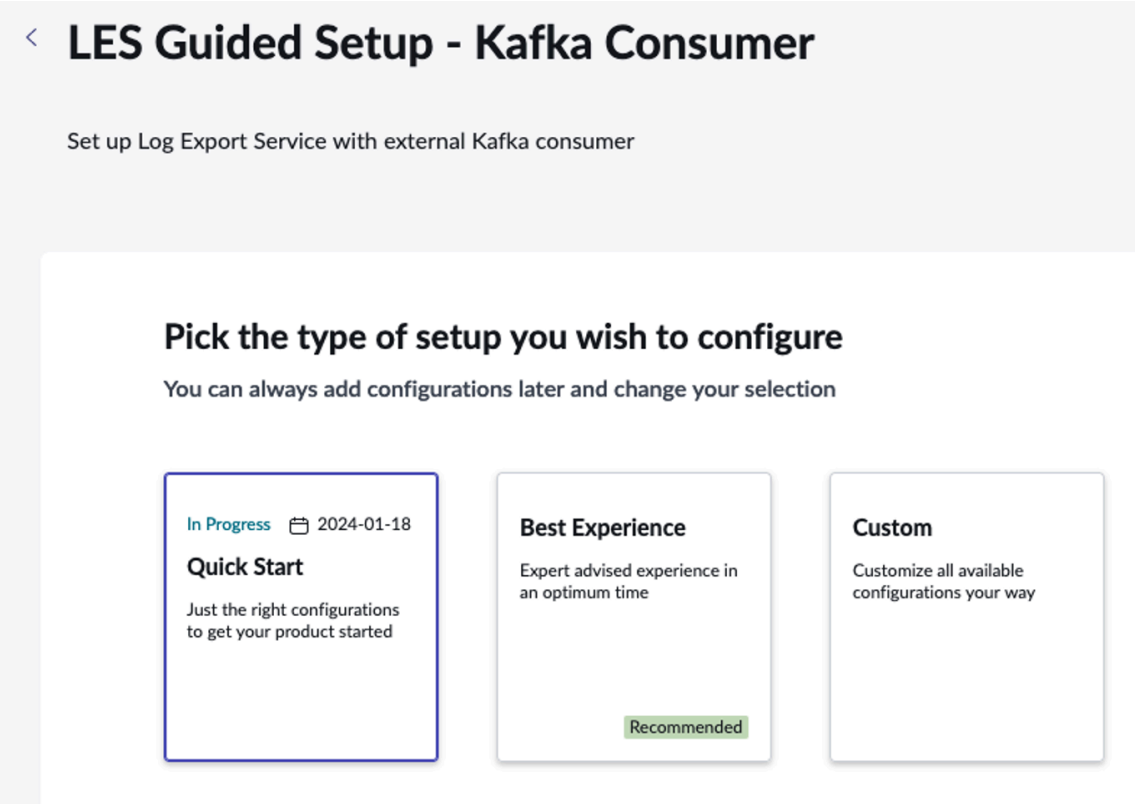
Verwenden Sie das geführte Setup, um die anfängliche Konfiguration von LES schrittweise zu durchlaufen. Das geführte Setup unterstützt Sie bei der Planung der Einführung des Produkts und der Durchführung der grundlegenden Konfiguration für den Go-Live.

Das geführte Setup unterteilt Konfigurationsaktivitäten in Kategorien. Jede Kategorie enthält Informationen wie Planungsleitfäden, Schritte vor dem Setup und Links zu nützlichen Hilfeinhalten. Kategorien bieten auch eine Reihe von Links zu den Seiten in Ihrer Instanz, auf denen Sie die Konfiguration durchführen. Im geführten Setup-Prozess wird verfolgt, was Sie abgeschlossen haben, sodass Sie anhalten und erneut beginnen können, wo Sie aufgehört haben.

Homepage des geführten Setups

Die Homepage für das geführte Setup enthält eine Übersicht der Konfigurationstypen für das geführte Setup. Sie können den Typ des geführten Setups auswählen und **Fortsetzen** wählen, um die Schritte des geführten Setups zu öffnen und mit der Konfiguration zu beginnen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

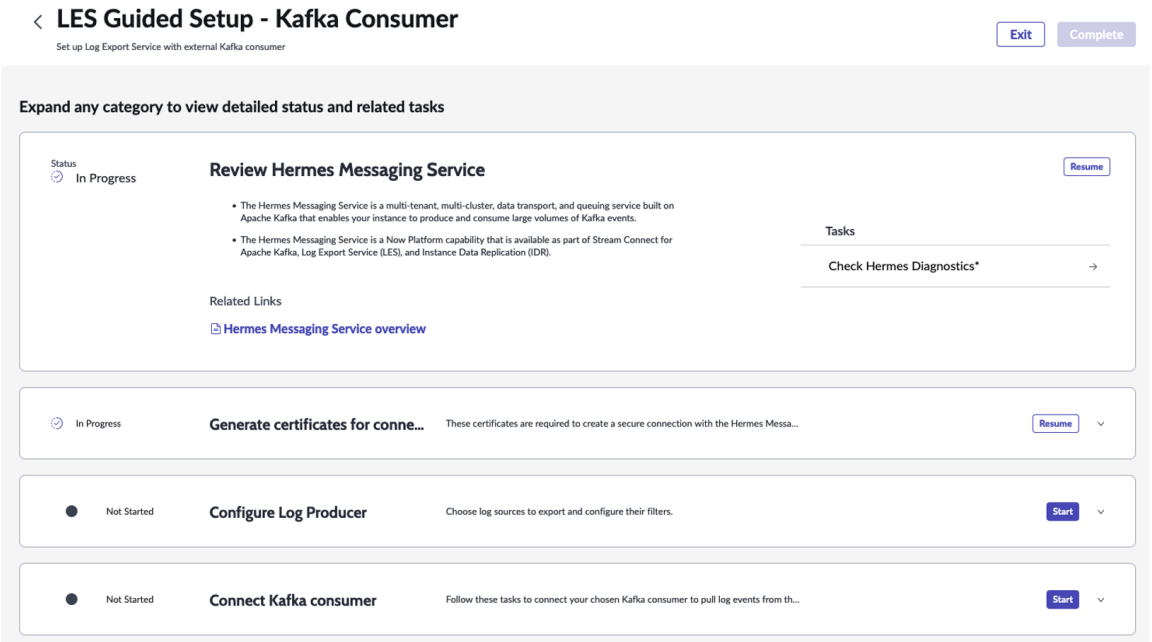


Alle drei Setups auf dieser Seite, Schnellstart/Beste Experience/Anwenderdefiniert, bieten dieselben Aufgaben und Funktionen. ist erforderlich, um die Integration zwischen der ServiceNow-Instanz und dem Zielprotokoll-Analysetool mit dem jeweiligen Administrator zu koordinieren. Der Log Analytics-Administrator muss sein Tool konfigurieren, um eine sichere Verbindung zur ServiceNow-Instanz herzustellen. Es wird empfohlen, das Dokument Richten Sie eine sichere Verbindung zum ein Hermes Messaging-Service vorab für den Log Analytics-Administrator freizugeben. Selbst wenn Sie eine Aufgabe als abgeschlossen markiert haben, können Sie zurückgehen und sie wieder auf „In Bearbeitung“ setzen. Klicken Sie dazu zuerst auf das Feld **Bearbeiten** in der oberen rechten Ecke der Kategorie. Klicken Sie dann auf das Kontrollkästchen „ **Bearbeiten** “ für die Aufgabe, die Sie deaktivieren möchten. Das **Kontrollkästchen „Als abgeschlossen** markieren“ wird nicht mehr markiert.

Kategorieseite des geführten Setups

Die Kategorieseite enthält eine Übersicht und Beschreibungen der Kategorien und der zugehörigen Aufgaben. Sie können entweder auf den Dropdown-Pfeil klicken, um Informationen zur Kategorie anzuzeigen, oder auf die Schaltfläche Start klicken, um die Schritte des geführten Setups zu öffnen und mit der Konfiguration zu beginnen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Schließen Sie die Aufgaben in den einzelnen Kategorien ab, indem Sie die Setup-Anweisungen befolgen.

Geführtes Setup für Kafka-Verbraucher

Implementieren Sie die folgenden Schritte für ein vollständiges geführtes Setup für Kafka-Verbraucher.

Vorbereitungen

Navigieren zu **Protokollexportservice (LES)** > **Kafka-Verbraucher** > **Geführtes Setup**an. Wählen Sie den Setup-Typ aus, den Sie konfigurieren möchten, und klicken Sie auf **Fortsetzen**.

Hinweis: Während der Installation der Anwendung [Log Export Service stellt ServiceNow die zugrunde liegende Infrastruktur Hermes Messaging-Service bereit. Beachten Sie, dass dieser Vorgang ab dem Zeitpunkt, zu dem Sie die Installation der Anwendung Log Export Service anfordern, einige Stunden in Anspruch nehmen kann.

Erforderliche Rolle: admin

Prozedur

1. Überprüfen Sie die Hermes Messaging-Service Diagnose.

   Es wird empfohlen, mit dem Diagnosetool Hermes, das während dieses Schritts auf dem Bildschirm angezeigt wird, zu überprüfen, ob Hermes Messaging-Service ausgeführt wird. Wenn auf dieser Seite der Fehler „Seite nicht gefunden“ angezeigt wird, ist Hermes nicht installiert, und Sie sollten sich an Ihren Systemadministrator wenden.

   - Setup-Informationen: Die folgenden Bootstrap-Informationen werden verwendet, um eine Verbindung mit Hermes Messaging-Serviceherzustellen . „Producer Bootstrap“ ist die Verbindung, die zum Senden von Nachrichten an Hermes verwendet wird, und „Consumer Bootstrap 1 und 2“ werden zum Abrufen von Nachrichten von Hermes verwendet.
     - Bootstrap des Herstellers
     - Verbraucher-Bootstrap 1
     - Verbraucher-Bootstrap 2

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Instanz-PKI: Die Komponente Instance Public Key Infrastructure (PKI) ermöglicht es einer ServiceNow-Instanz, als Aussteller in einer X.509-Vertrauenshierarchie zu fungieren.
- Bootstrap-Konnektivität: Klicken Sie auf „ **Test ausführen** “, um zu bestätigen, dass der externe Client eine Verbindung zu den definierten Instanzports (Ersteller und Verbraucher) herstellen kann.
- Instanzkonnektivität: Klicken Sie auf **Run Test** (Test ausführen), um zu bestätigen, dass die Instanz Nachrichten senden und empfangen kann.
- Themen anzeigen: Klicken Sie auf das aufgelistete Thema, um den Zeitstempel der letzten bekannten Nachricht abzurufen.

Hinweis: Sie können in Zukunft auf die Diagnose Hermes zugreifen, um potenzielle Konnektivitätsprobleme zu beheben, indem Sie zu diesem Schritt des geführten Setups zurückkehren oder zu navigieren **Alle** > *Hermes Messaging-Service* > **Diagnosen**an.

2. Generieren Sie Zertifikate für eine sichere Verbindung zu Hermes Messaging-Service, und rufen Sie Protokollereignisse ab.

Sie verwenden diese Zertifikate, wenn Sie Ihr externes System verbinden.

Richten Sie eine sichere Verbindung mit Hermes Messaging-Serviceein. Weitere Informationen finden Sie unter Richten Sie eine sichere Verbindung zum ein Hermes Messaging-Service . Sie benötigen diese Zertifikate für die Authentifizierung und Autorisierung im Client, der die Protokolle aus Hermes abruft.

Hinweis: Für diesen Schritt sind die Rollen „admin“ oder „Hermes_admin“ erforderlich.

3. Protokollersteller konfigurieren: Wählen Sie die zu exportierenden Protokollquellen aus, und konfigurieren Sie deren Filter.
Führen Sie die folgenden Aufgaben aus, um den Protokollersteller zu konfigurieren.

- Konfigurieren Sie Protokollquellen für den Export: Erstellen Sie einen Quelldatensatz für jede der Protokollquellen, die Sie exportieren möchten.

  Hinweis: Die Rollen admin oder sn_logstoanalytics.admin sind erforderlich, um diesen Schritt abzuschließen

  a. Klicken Sie oben rechts auf **Neu**

  b. Wählen Sie einen Quelltyp aus

  c. Wählen Sie die entsprechenden Filter für den ausgewählten Quelltyp aus

  Hinweis: Die Filter sind je nach ausgewähltem Quelltyp unterschiedlich

  d. Klicken Sie auf Aktualisieren.
  Bei erfolgreicher Erstellung wird der Name des Hermes-Themas angezeigt, in den diese Protokollquelle exportiert wird. Notieren Sie sich den Namen des Themas. Sie benötigen ihn später, wenn Sie Ihr Protokollverbrauchersystem konfigurieren. Das Feld Aktiv steuert, ob diese Protokollquelle exportiert wird oder nicht. Wenn Fehler angezeigt werden, kehren Sie zur Aufgabe „Hermes-Diagnose überprüfen“ zurück, und überprüfen Sie den Hermes-Status.

- Protokollersteller validieren: Sobald Sie eine Quelle erstellt haben, aus der Protokolle erstellt werden sollen, können Sie mithilfe von Live-Protokolldatensätze im Thema anzeigen **Hermes Messaging Service** > **Hermes-Themeninspektor**an.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie Externe Themen aus

b. Klicken Sie auf Listenthemen

c. Wählen Sie die Zeile mit Ihrem Thema aus dem vorherigen Schritt aus (aufgeführt in Quellen).

d. Passen Sie bei Bedarf das Startdatum der Nachricht an

e. **Klicken** Sie auf Anzeigen, um eine Protokollnachricht anzuzeigen, die in das Thema exportiert wurde

4. Kafka-Verbraucher verbinden: Führen Sie diese Aufgaben aus, um den ausgewählten Kafka-Verbraucher zu verbinden und Protokollereignisse aus Hermes abzurufen.

- Kafka-Verbraucher identifizieren: Je nach Ihrer Log Analytics-Architektur haben Sie zwei Möglichkeiten.
  - Wenn Sie über ein eigenes Kafka-System verfügen und dieses für die Protokollzusammenfassung auswählen, können Sie über das native Kafka-Protokoll eine direkte Verbindung zum Hermes-Messaging-Service herstellen.
  - Wenn Sie möchten, dass Ihr Log Analytics-Tool eine direkte Verbindung zum Hermes Messaging Service herstellt, müssen Sie einen Kafka-Connector bereitstellen, der von Ihrem Log Analytics-System unterstützt wird (z. B. Splunk Connect für Kafka).

  Hinweis: In beiden Fällen müssen Sie mit dem Administrator dieser Systeme zusammenarbeiten, um die Verbindung mit dem Hermes Messaging Service zu koordinieren.

- Hermes-Zertifikate in das Kafka-Verbrauchersystem importieren: Melden Sie sich bei Ihrem Kafka-Verbrauchersystem an, und vergewissern Sie sich, dass Sie über die entsprechenden Administratorberechtigungen verfügen, um es zu konfigurieren und mit einem externen System zu verbinden. Importieren Sie die in der Aufgabe „Sichere Verbindung mit dem Hermes-Messaging-Service einrichten“ generierten Zertifikate in Ihren Kafka-Connector oder Kafka-Server. Befolgen Sie die Anweisungen in der Dokumentation für den von Ihnen ausgewählten Kafka-Verbraucher.
- Kafka-Prozesse konfigurieren: Der Hermes Messaging Service ist auf Hochverfügbarkeit ausgelegt. Zwei Prozesse sind erforderlich, um Nachrichten von Hermes zu verarbeiten. Zwei Prozesse sind erforderlich, da Hermes ein Paar Kafka-Cluster für Failover-Zwecke verwendet. Wenn ein Cluster ausfällt, werden Daten für das andere Hermes Kafka-Cluster erzeugt.

  In Ihrem Kafka-Verbrauchersystem müssen Sie zwei separate Verbraucherprozesse erstellen, um eine Verbindung zu beiden Hermes-Kafka-Clustern herzustellen. Für beide Prozesse geben Sie dasselbe Hermes-Kafka-Thema an, Sie müssen jedoch zwei separate Bootstrap-Adressen konfigurieren:

  - <instance_name>.service-now.com:4100, .service-now.com:4101, .service-now.com:4102, .service-now.com:4103
  - <instance_name>.service-now.com:4200, .service-now.com:4201, .service-now.com:4202, .service-now.com:4203

  Wichtige Hinweise:

  - Wenn Sie von externen Systemen aus auf das Kafka-Thema zugreifen, müssen Sie „snc.“ voranstellen.<instance name> .“ zu dem Thema, an das die Protokolle weitergeleitet werden.
  - Konfigurieren Sie jeden Verbraucher mit derselben Kafka-Verbrauchergruppen-ID.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Installieren Sie Ihre Schlüsselspeicher- und Truststore-Dateien an einem Ort, an dem Ihre Verbraucher darauf zugreifen können.
- Wenn Ihre Verbraucher dies benötigen, geben Sie die Eigenschaften der Kafka-JSON-Konverter an, um Schemas zu deaktivieren: „key.converter.schemas.enable=false“, „value.converter.schemas.enable=false“

◦ Überprüft, ob der Kafka-Verbraucher Protokolle aus Hermes abruft: Verifiziert im ausgewählten Kakfa-Verbraucher, dass Protokollereignisse vom Hermes-Messaging-Service abgerufen werden können.

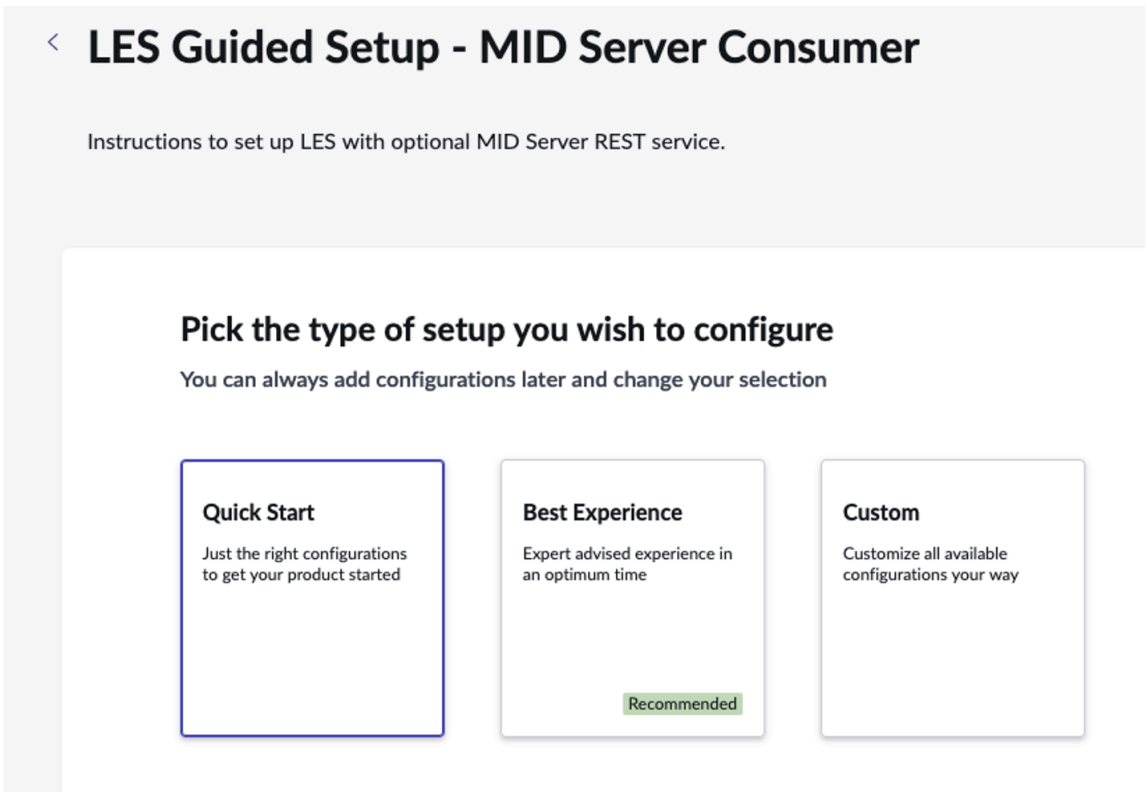
MID-Server-Verbraucher

Verwenden Sie das geführte Setup, um die anfängliche Konfiguration von LES schrittweise zu durchlaufen. Das geführte Setup unterstützt Sie bei der Planung der Einführung des Produkts und der Durchführung der grundlegenden Konfiguration für den Go-Live.

Das geführte Setup unterteilt Konfigurationsaktivitäten in Kategorien. Jede Kategorie enthält Informationen wie Planungsleitfäden, Schritte vor dem Setup und Links zu nützlichen Hilfeinhalten. Kategorien bieten auch eine Reihe von Links zu den Seiten in Ihrer Instanz, auf denen Sie die Konfiguration durchführen. Im geführten Setup-Prozess wird verfolgt, was Sie abgeschlossen haben, sodass Sie anhalten und erneut beginnen können, wo Sie aufgehört haben.

Homepage des geführten Setups

Die Homepage für das geführte Setup enthält eine Übersicht der Konfigurationstypen für das geführte Setup. Sie können den Typ des geführten Setups auswählen und **Fortfahren** wählen, um die Schritte des geführten Setups zu öffnen und mit der Konfiguration zu beginnen.



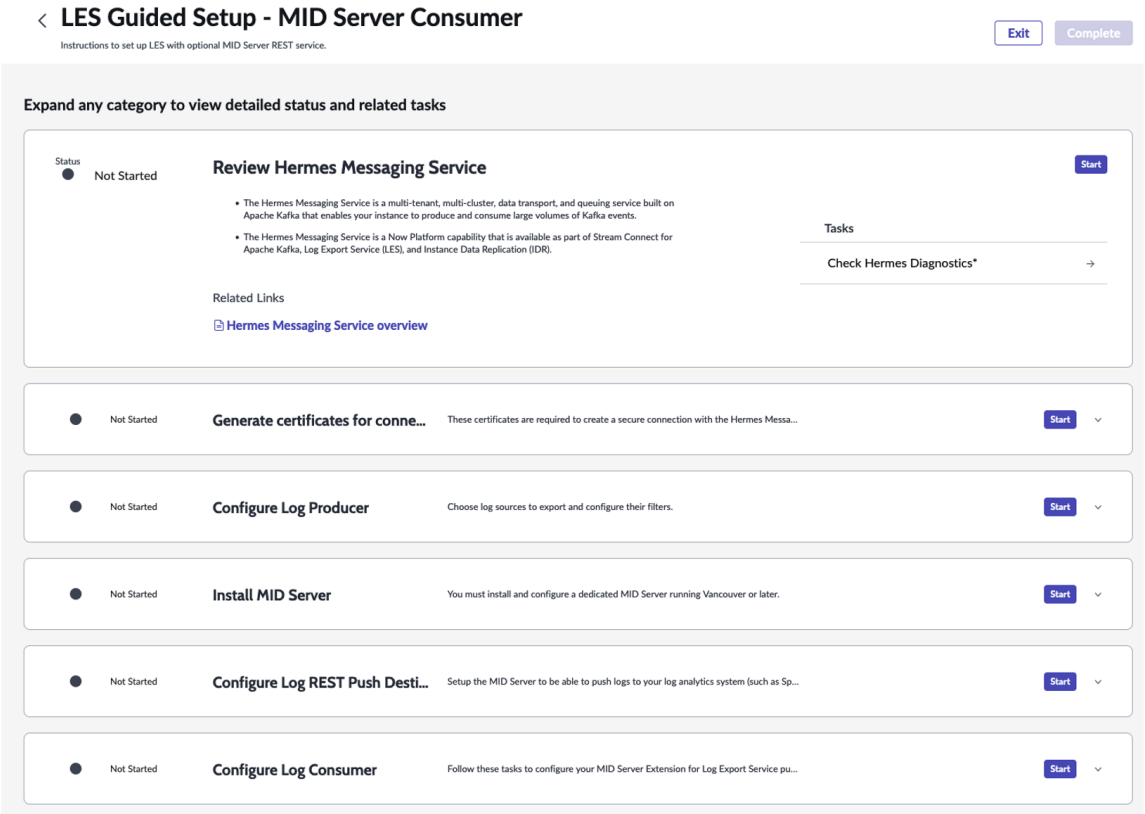
Alle drei Setups auf dieser Seite, Schnellstart/Beste Experience/Anwenderdefiniert, bieten dieselben Aufgaben und Funktionen. Damit Protokolle kontinuierlich von Ihrer -Instanz an Ihr Protokollanalysesystem gestreamt werden, ist ein dedizierter MID-Server erforderlich.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der MID Server benötigt ein einmaliges Setup, um eine sichere Verbindung zum Hermes Messaging Service herzustellen. Auch wenn Sie eine Aufgabe als abgeschlossen markiert haben, können Sie zurückgehen und sie wieder auf „In Bearbeitung“ setzen. Klicken Sie dazu zuerst auf das Feld **Bearbeiten** in der oberen rechten Ecke der Kategorie. Klicken Sie dann auf das Kontrollkästchen „ **Bearbeiten** “ für die Aufgabe, die Sie deaktivieren möchten. Das **Kontrollkästchen „Als abgeschlossen** markieren“ ist nicht mehr markiert.

Kategorieseite des geführten Setups

Die Kategorieseite enthält eine Übersicht und Beschreibungen der Kategorien und der zugehörigen Aufgaben. Sie können entweder auf den Dropdown-Pfeil klicken, um Informationen zur Kategorie anzuzeigen, oder auf **Start** klicken, um die Schritte des geführten Setups zu öffnen und mit der Konfiguration zu beginnen.



Schließen Sie die Aufgaben in den einzelnen Kategorien ab, indem Sie die Setup-Anweisungen befolgen.

Geführtes Setup für MID-Server-Verbraucher

Implementieren Sie die folgenden Schritte für ein vollständiges geführtes Setup für MID-Server-Verbraucher.

Vorbereitungen

Navigieren zu **Protokollexportservice (LES)** > **MID-Server-Verbraucher** > **Geführtes Setup**an. Wählen Sie den Setup-Typ aus, den Sie konfigurieren möchten, und klicken Sie auf **Fortsetzen**.

Hinweis: Während der Installation der Anwendung [Log Export Service stellt ServiceNow die zugrunde liegende Infrastruktur Hermes Messaging-Service bereit. Beachten Sie, dass dieser Vorgang ab dem Zeitpunkt, zu dem Sie die Installation der Anwendung Log Export Service anfordern, einige Stunden in Anspruch nehmen kann.

Erforderliche Rolle: admin

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Überprüfen Sie die Hermes Messaging-Service Diagnose.

   Es wird empfohlen, mit dem Diagnosetool Hermes, das während dieses Schritts auf dem Bildschirm angezeigt wird, zu überprüfen, ob Hermes Messaging-Service ausgeführt wird. Wenn auf dieser Seite der Fehler „Seite nicht gefunden“ angezeigt wird, ist Hermes nicht installiert, und Sie sollten sich an Ihren Systemadministrator wenden.

   - Setupinformationen: Die folgenden Bootstrapinformationen werden zum Herstellen einer Verbindung mit dem Hermes Messaging Service verwendet. „Producer Bootstrap“ ist die Verbindung, die zum Senden von Nachrichten an Hermes verwendet wird, und „Consumer Bootstrap 1 und 2“ werden zum Abrufen von Nachrichten von Hermes verwendet.
     - Bootstrap des Herstellers
     - Verbraucher-Bootstrap 1
     - Verbraucher-Bootstrap 2
   - Instanz-PKI: Die Komponente Instance Public Key Infrastructure (PKI) ermöglicht es einer ServiceNow-Instanz, als Aussteller in einer X.509-Vertrauenshierarchie zu fungieren.
   - Bootstrap-Konnektivität: Klicken Sie auf „ **Test ausführen** “, um zu bestätigen, dass der externe Client eine Verbindung zu den definierten Instanzports (Ersteller und Verbraucher) herstellen kann.
   - Instanzkonnektivität: Klicken Sie auf **Run Test** (Test ausführen), um zu bestätigen, dass die Instanz Nachrichten senden und empfangen kann.
   - Themen anzeigen: Klicken Sie auf das aufgelistete Thema, um den Zeitstempel der letzten bekannten Nachricht abzurufen.

   Hinweis: Sie können in Zukunft auf die Diagnose Hermes zugreifen, um potenzielle Konnektivitätsprobleme zu beheben, indem Sie zu diesem Schritt des geführten Setups zurückkehren oder zu navigieren **Alle** > *Hermes Messaging-Service* > **Diagnosen**an.

2. Generiert Zertifikate für eine sichere Verbindung mit dem Hermes-Messaging-Service, und ruft Protokollereignisse ab.

   Richten Sie eine sichere Verbindung mit dem Hermes-Messaging-Service ein. Weitere Informationen finden Sie unter Richten Sie eine sichere Verbindung zum ein Hermes Messaging-Service . Sie benötigen diese Zertifikate für die Authentifizierung und Autorisierung im Client, der die Protokolle aus Hermes abruft.

   Hinweis: Für diesen Schritt sind die Rollen „admin“ oder „Hermes_admin“ erforderlich.

3. Protokollersteller konfigurieren: Wählen Sie die zu exportierenden Protokollquellen aus, und konfigurieren Sie deren Filter.
   Führen Sie die folgenden Aufgaben aus, um den Protokollersteller zu konfigurieren.

   - Konfigurieren Sie Protokollquellen für den Export: Erstellen Sie einen Quelldatensatz für jede der Protokollquellen, die Sie exportieren möchten.

     Hinweis: Die Rollen admin oder sn_logstoanalytics.admin sind erforderlich, um diesen Schritt abzuschließen

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie oben rechts auf **Neu**

b. Wählen Sie einen Quelltyp aus

c. Wählen Sie die entsprechenden Filter für den ausgewählten Quelltyp aus

Hinweis: Die Filter sind je nach ausgewähltem Quelltyp unterschiedlich

d. Klicken Sie auf Aktualisieren
Bei erfolgreicher Erstellung wird der Name des Hermes-Themas angezeigt, in den diese Protokollquelle exportiert wird. Notieren Sie sich den Namen des Themas. Sie benötigen ihn später, wenn Sie Ihr Protokollverbrauchersystem konfigurieren. Das Feld Aktiv steuert, ob diese Protokollquelle exportiert wird oder nicht. Wenn Fehler angezeigt werden, kehren Sie zur Aufgabe „Hermes-Diagnose überprüfen“ zurück, und überprüfen Sie den Hermes-Status.

- Protokollersteller validieren: Sobald Sie eine Quelle erstellt haben, aus der Protokolle erstellt werden sollen, können Sie mithilfe von Live-Protokolldatensätze im Thema anzeigen **Hermes Messaging Service** > **Hermes-Themeninspektor**an.

a. Wählen Sie Externe Themen aus

b. Klicken Sie auf Listenthemen

c. Wählen Sie die Zeile mit Ihrem Thema aus dem vorherigen Schritt aus (aufgeführt in Quellen).

d. Passen Sie bei Bedarf das Startdatum der Nachricht an

e. Klicken Sie auf Anzeigen, um eine Protokollnachricht anzuzeigen, die in das Thema exportiert wurde

4. MID-Server installieren: Sie müssen einen dedizierten MID-Server installieren und konfigurieren, der Vancouver oder höher ausführt.
Führen Sie die folgenden Aufgaben aus, um den MID-Server zu installieren.

   - Dedizierten MID-Server installieren: Der vom Protokollexportservice verwendete MID-Server sollte nur für diesen Zweck vorgesehen sein und es sollte nicht erwartet werden, dass er andere Prozesse ausführt. Dies ist wichtig, um sicherzustellen, dass exportierte Protokollnachrichten rechtzeitig an Ihren REST-Endpunkt übermittelt werden. Sie können den neuen MID-Server entweder mit Geführtes Setup „MID-Server verwenden“ oder manuell installieren. Befolgen Sie für die manuelle Installation zuerst die Dokumentation MID Server-Netzwerkverbindung konfigurieren und dann die Dokumentation MID Server installieren .

   - MID-Server validieren: Sie müssen den MID-Server nach der Installation manuell validieren, damit er Automatisierungsaufgaben ausführen kann. Informationen zum Validieren des MID-Servers, den Sie für LES reservieren, finden Sie unter MID-Server validieren

5. REST-Push-Ziel für Protokoll konfigurieren: Richten Sie den MID-Server so ein, dass Protokolle an Ihr Log Analytics-System (z. B. Splunk) übertragen werden können.
Führen Sie die folgenden Aufgaben aus, um das REST-Push-Ziel des Protokolls zu konfigurieren.

   - MID-Eigenschaften hinzufügen: Sie müssen MID-Server-Eigenschaften hinzufügen, damit eine Verbindung zu Hermes hergestellt werden kann. Navigieren Sie zu **MID-Server** >**Eigenschaften**, und legen Sie die entsprechenden Werte für alle unten aufgeführten Eigenschaften fest.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Wert
mid.les.kafka.ssl.truststore.passwort	<password>
mid.les.kafka.ssl.schlüsselspeicher.passwort	<password>
mid.les.kafka.ssl.key.password	<password>
mid.les.kafka.ssl.truststore.location	<your_path>/<truststore> .p12
mid.les.kafka.ssl.keystore.location	<your_path>/<keystore> .p12
mid.les.kafka.ssl.truststore.type	PKCS12
mid.les.kafka.ssl.keystore.type	PKCS12
mid.les.kafka.client.id	<instance_name>
mid.les.kafka.group.id	snc<instance_name> .Gruppe1
mid.les.kafka.bootstrap.server	<instance_name>.servicenow.com:4100,<instance_name>
mid.les.kafka.set2.bootstrap.server	<instance_name>.servicenow.com:4200,<instance_name>

Befolgen Sie diese Hinweise, um einige der oben genannten Werte zu erhalten

- <password>ist das Passwort, das Sie für den Schlüsselspeicher und den Truststore festlegen
- <your_path>ist der Dateipfad zu dem Verzeichnis, in dem Sie die heruntergeladenen Schlüsselspeicher- und Truststore-Dateien speichern. Die Zertifikate müssen sich auf dem Server befinden, auf dem Sie MID ausführen
- <instance_name>ist der Name Ihrer ServiceNow-Instanz. Wenn Sie sich nicht sicher sind, finden Sie sie in der Tabelle „sys_properties“.
- Sie können die Werte für mid.les.kafka.bootstrap.servers und mid.les.kafka.set2.bootstrap.servers auf der Seite „Hermes-Diagnose“ abrufen. Navigieren zu **Hermes Messaging Service** > **Diagnosen** und kopieren Sie die Zeichenfolgen unter Consumer Bootstrap 1 bzw. Consumer Bootstrap 2.

◦ Ziel konfigurieren: Erstellen Sie einen neuen Zielkonfigurationsdatensatz, der den REST-Endpunkt definiert, an den diese Erweiterung Protokolle weiterleitet.

Hinweis: Die Rollen admin oder sn_logstoanalytics.admin sind erforderlich, um diesen Schritt abzuschließen.

a. Navigieren zu **Protokollexportservice (LES)** > **Zielkonfigurationen**

b. Erstellen Sie einen neuen Konfigurationsdatensatz

c. Geben Sie die URL für den gewünschten Endpunkt für die exportierten Protokollquellen an

d. Suchen Sie nach Anmeldeinformationen, oder erstellen Sie neue, um eine Verbindung mit Ihrem Endpunkt herzustellen. Beachten Sie beim Erstellen von Anmeldeinformationen für Ihren Endpunkt, dass nur die folgenden Anmeldeinformationstypen mit LES gültig sind: Standardauthentifizierung, OAuth, API-Schlüssel

e. Suchen Sie nach einem Transformationsskript, oder erstellen Sie ein neues. Im Lieferumfang enthalten ist das vorgefertigte Skript **SplunkTransform** for Splunk

6. LOG-Verbraucher konfigurieren: Führen Sie diese Aufgaben aus, um Ihre MID-Servererweiterung für Protokollexport-Service-Zwecke zu konfigurieren.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

◦ LES-Verbraucherkontext konfigurieren: In diesem Schritt aktualisieren Sie den LES-Verbraucherdatensatz für die Ausführung auf dem dedizierten MID-Server, den Sie gerade für den Protokollexportservice installiert haben. Navigieren zu **MID-Server** > **Erweiterungen** > **LES-Verbraucherkontext** und aktualisieren Sie den LES-Verbraucherdatensatz, indem Sie die folgenden Felder festlegen:

- Klicken Sie auf „LES-Verbraucher“, um den MID-Server-Kontextdatensatz zu öffnen
- Wählen Sie Spezifischer MID-Server für das Feld „Ausführen auf“ aus
- Geben Sie den Namen des MID ein, den Sie im vorherigen Schritt für das Feld „MID-Server“ validiert haben

Klicken Sie zum Speichern auf **Aktualisieren**.

Hinweis: Die Lieferung erfolgt mit einem vordefinierten Kontext. Erstellen Sie keine zweite. Dies kann unbeabsichtigte Folgen haben.

◦ Verbraucher konfigurieren: Erstellen Sie einen neuen Verbraucherdatensatz, der den Prozess darstellt, der Teil der MID-Servererweiterung des Protokollexportservice ist. Navigieren zu **Protokollexportservice (LES)** > **Verbraucher** und erstellen Sie einen neuen Konfigurationsdatensatz, in dem Sie das Hermes-Thema angeben, von dem Protokollnachrichten abgerufen werden sollen, und das Ziel, an das sie weitergeleitet werden sollen. Wenn Sie das Modul **Verbraucher** auswählen, werden Informationen zum Verbrauchernamen und zur Zielkonfiguration angezeigt.

a. Erstellen Sie einen neuen Verbraucherdatensatz

b. Wählen Sie ein Quellthema aus der Dropdown-Liste aus

c. Wählen Sie die Zielkonfiguration aus

d. Verbraucher starten

◦ MID-Server-Integration überprüfen: Navigieren Sie zu **Protokollexportservice (LES)** > **Verbraucherstatus** und zeigen Sie die Felder Status und Statusdetails des definierten Datensatzes an. Die Informationen in diesen Feldern geben den aktuellen Status des auf dem MID-Server ausgeführten Prozesses an, einschließlich Fehlern, die bei der Weiterleitung von Nachrichten an den REST-Endpunkt aufgetreten sind. Dies ist nur eine Statusansichtsseite. Navigieren zu **Protokollexportservice (LES)** > **Verbraucher** wenn Sie einen neuen Verbraucherdatensatz erstellen möchten. Wenn der Verbraucherstatus anzeigt, dass der Prozess gestartet wurde, sollten Sie in der Lage sein, Ihren Endpunkt zu überprüfen, um die an ihn weitergeleiteten Protokolle anzuzeigen. Darüber hinaus können Sie die Protokolle auf dem MID-Server anzeigen, um zusätzliche Details zu möglicherweise aufgetretenen Fehlern zu ermitteln. Sie können auch die Debug-Protokollierung auf dem MID-Server aktivieren, um bei Bedarf zusätzliche Informationen zu erhalten.

Hinweis: Wenn Sie in einem der Verbraucherdatensätze eine Änderung vornehmen, wird diese auf der Ansichtsseite „Verbraucherstatus“ angezeigt. Wenn Sie in der Liste Verbraucherstatus den Namen eines Verbraucherdatensatzes auswählen, wird das Verbraucherformular für den ausgewählten Datensatz geöffnet. Sie können dann den Namen und die Zielkonfiguration des ausgewählten Datensatzes aktualisieren.

Überprüfen Sie den Protokollbericht

Analysieren Sie die Größe jedes Datenprotokolls, indem Sie das Protokollberichts-Dashboard überprüfen.

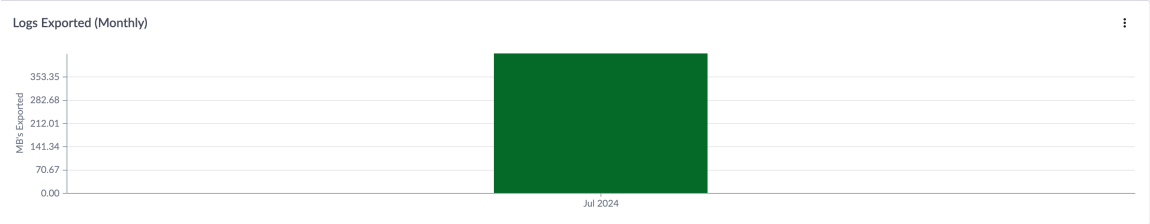
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: admin oder sn_logstoanalytics.admin

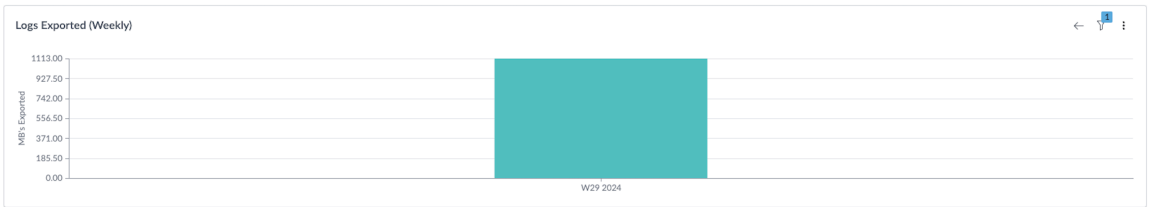
Prozedur

1. Navigieren zu **Alle** > **Protokollexportservice** > **Berichte**an.
2. Überprüfen Sie Protokolldaten in den folgenden Widgets.
   - Exportierte Protokolle (monatlich): Zeigt die Megabytes an, die pro Monat in der ersten Ansicht exportiert werden. Sie können im Diagramm einen Drilldown ausführen, um die Daten für jede Woche oder tägliche Daten anzuzeigen. Sie können Daten der letzten 395 Tage anzeigen.

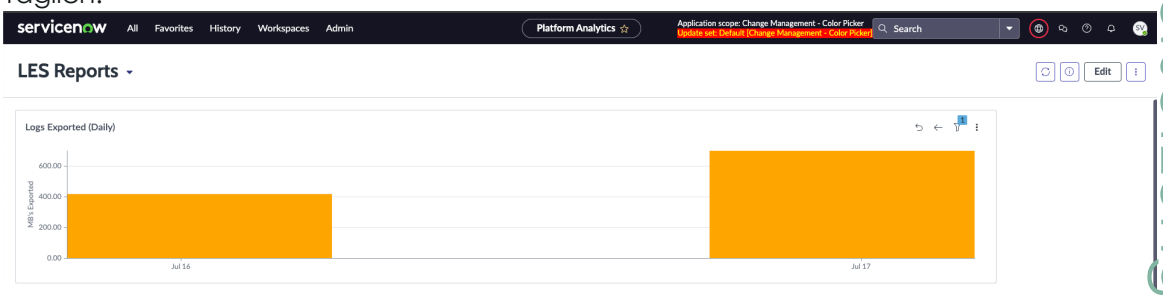


Hinweis: Klicken Sie auf die Pfeile oben rechts im Widget, um die Daten aufzuschlüsseln. Sie können auch zurück zu den übergeordneten Daten wechseln.

Wöchentlich:

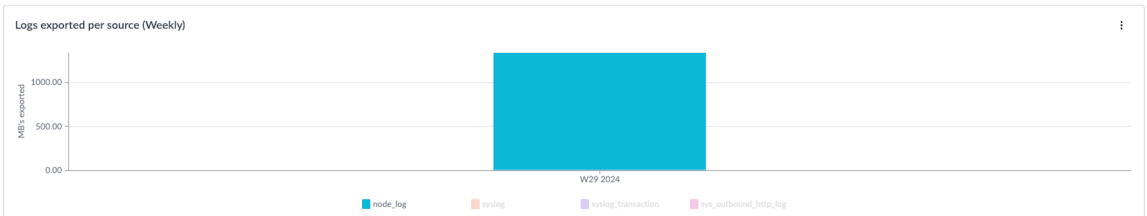


Täglich:



Die Daten in diesem Bericht spiegeln die Sammlung wider, die 4 Stunden zuvor durchgeführt wurde.

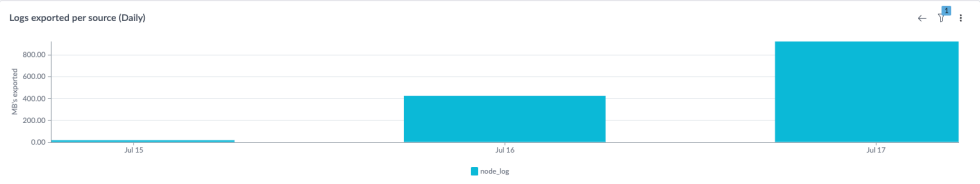
   - Pro Quelle exportierte Protokolle (wöchentlich): Dieses Widget zeigt die Art der Protokolle an, die wöchentlich exportiert wurden. Sie können auch einen Drilldown ausführen, um tägliche Protokolldaten anzuzeigen. Sie können Daten der letzten 32 Tage anzeigen.



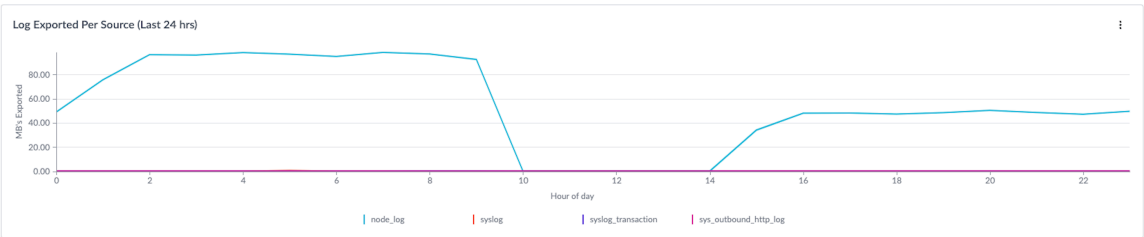
Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Sie können die Quelle, aus der Sie die Daten anzeigen möchten, auswählen oder abwählen. Die Quellen, aus denen Sie die Protokolle anzeigen können, sind node_log, syslog, syslog_transaction und sys_outbound_http_log.

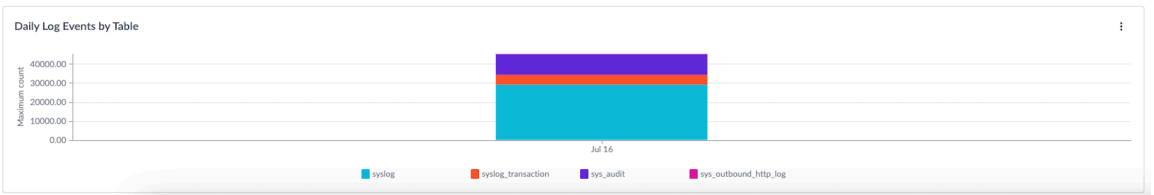


- Pro Quelle exportiertes Protokoll (letzte 24 Stunden): Zeigt die Daten der letzten 24 Stunden an. Das Diagramm verläuft chronologisch von links nach rechts auf einer 24-Stunden-Skala, wobei die ältesten Daten (24. Stunde) auf der rechten Seite und die neuesten Daten auf der linken Seite des Berichts positioniert sind. Sie können die Quelle, aus der Sie die Daten anzeigen möchten, auswählen oder abwählen. Die Quellen, aus denen Sie die Protokolle anzeigen können, sind node_log, syslog, syslog_transaction und sys_outbound_http_log.



Hinweis: Abhängig von der Tageszeit, zu der Sie diese Daten überprüfen, wird das Widget dynamisch aktualisiert, um genau die letzten 24 Stunden widerzuspiegeln.

- Tägliche Protokollereignisse nach Tabelle: Zeigt die Protokollereignisse an, die von den einzelnen Protokolltabellen pro Tag generiert werden. Sie können die Tabellen auswählen oder abwählen, aus denen Sie die Daten anzeigen möchten.



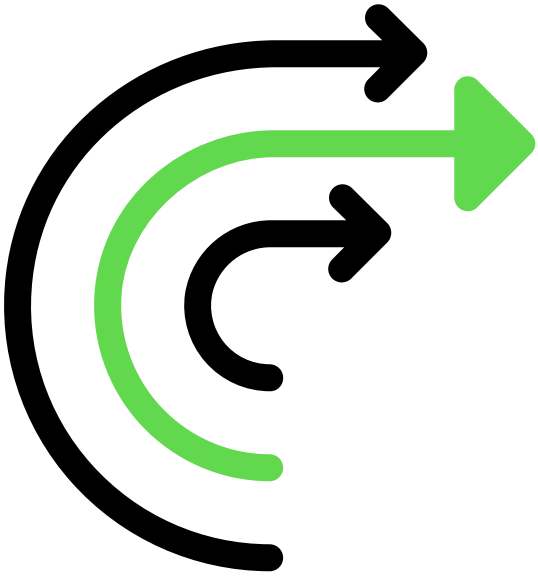
Hinweis: Die Tabellen, aus denen Sie die Protokollereignisse anzeigen können, sind: syslog, syslog_transaction, sys_audit und sys_outbound_http_log.

Protokolle

Das Modul „Protokolle“ bietet eine Vielzahl von Protokollen, mit denen Sie bei Transaktionen und Ereignissen, die innerhalb der Instanz stattfinden, Probleme beheben und Debuggen können.

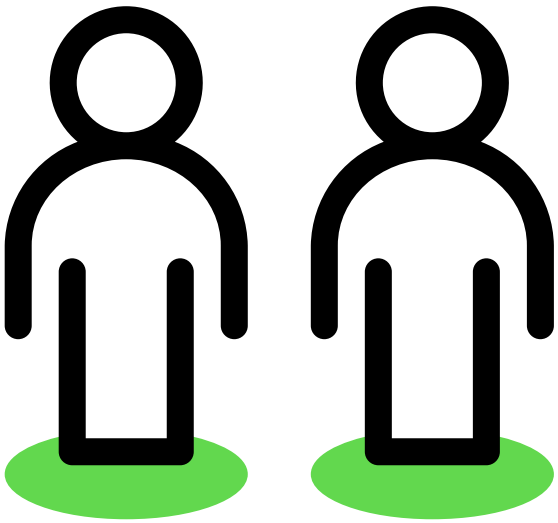
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Systemprotokolle



Das Modul „Systemprotokolle“ bietet eine Vielzahl von Protokollen, die Sie zum Beheben und Debuggen von Transaktionen und Ereignissen innerhalb der Instanz verwenden können.

Protokollierung, Audits und Fehler



Wenden Sie eine Protokollierungs- und Auditstrategie an, damit Sie verdächtige Aktivitäten rechtzeitig erkennen und entsprechende Maßnahmen ergreifen können.

Systemprotokolle

Das Modul „Systemprotokolle“ bietet eine Vielzahl von Protokollen, die Sie zum Beheben und Debuggen von Transaktionen und Ereignissen innerhalb der Instanz verwenden können.

Greifen Sie über das Modul „Systemprotokolle“ auf die folgenden Protokolle zu:

Protokoll	Beschreibung
Transaktionen	Alle Anwendungsaktivitäten für eine Instanz.
E-Mail und Push	Alle E-Mail-Benachrichtigungen und Push-Nachrichten, die von allen Instanzen im System gesendet werden.
Ereignisprotokolle	Alle Systemereignisse, die innerhalb des Systems auftreten.
Importieren	Datenimportaktivität innerhalb der Plattform.
Tabellenänderungen	Änderungen an allen Tabellen im System.
Protokollierung für ausgehende Webservices	Alle ausgehenden Webservices-Anforderungen wie REST- und SOAP-Anforderungen.
Signaturbilder	Elektronische Signaturen für das HR-Signaturpad.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Protokoll	Beschreibung
System	Warnungen und Fehler für Instanzprozesse, Datensätze und nicht kritische Ereignisse, z. B. Auslastung des Arbeitsspeichers auf dem Servercomputer.

Verwenden Sie den Protokolldateibrowser, um Protokolle zu suchen und herunterzuladen. Sie können auch archivierte Protokolle im Protokollverlaufdurchsuchen.

Andere Protokolle

Ihre Instanz von bietet zusätzlich zu den im Modul „Systemprotokolle“ enthaltenen Protokollen weitere Protokolle. Modul „Systemdiagnostik“. stellt beispielsweise den Upgradeverlauf und langsame Abfrageprotokolle bereit, mit denen Sie Einblicke in die Auswirkungen von Abfragen auf die Plattformleistung erhalten können. Tabelle „Kundenupdates“. zeichnet jede Änderung auf, die im System vorgenommen wird.

Systemprotokoll

Zeigen Sie Warnungen und Fehler für Instanzprozesse, Datensätze und nicht kritische Ereignisse an, z. B. die Auslastung des Arbeitsspeichers auf dem Servercomputer.

Die folgenden Informationen werden im Systemprotokoll nachverfolgt:

- Workflows
- Konfiguration
- Chats-Sitzungen
- Transaktionen für jede Ansicht jeder Seite im System, einschließlich Ladezeiten für Netzwerk, Server und Browser
- Eingehende und ausgehende E-Mails
- Ereignisse, die im System ausgelöst werden
- Importe und Integrationen
- Systemwarnungen, -fehler und -skriptprotokolle
- Upgrade-Informationen für Plugin-Aktivierungen, Update-Sätze oder System-Upgrades

Protokolleinträge werden nur für den aktuellen Tag angezeigt. Um andere Protokolldateien anzuzeigen, verwenden Sie den Protokolldateibrowser. Dieses Protokoll enthält die folgenden Informationen für alle Vorkommen:

Systemprotokoll

Feld	Beschreibung
Erstellt	Datum und Uhrzeit der Protokollierungsaktivität für das Gebietsschema des Computers, auf dem die Instanz ausgeführt wird.
Ebene	Typ der Nachricht Die Ebenen sind Debuggen, Fehler, Warnung und Information. • Eine Warnung ist ein Fehler, der behandelt und behoben wurde. • Ein Fehler ist etwas, das behoben werden muss.
Nachricht	Vom System generierte Nachricht bezüglich der Art des Vorkommens.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Systemprotokoll (Fortsetzung)

Feld	Beschreibung
Quelle	Name des Prozesses oder Bereichs, der vom Vorkommnis betroffen ist. Die Quelle des Vorkommens kann beispielsweise E-MAIL oder Arbeitsspeicher sein.
Quellpaket	Name des Anwendungspakets, das dem Vorkommen zugeordnet ist. Klicken Sie auf den Namen, um den Datensatz der Store-Anwendung [sys_store_app] für dieses Paket anzuzeigen.

Workflow-Protokollierung

- Jede ausgeführte Aktivität, einschließlich:
  - Datum und Uhrzeit des Starts
  - Datum und Uhrzeit des Endes
  - Status, z. B. Beendet, Abgebrochen, Zeitüberschreitung, Fehler
  - Ergebnis
  - Fehlerbeschreibung, wenn ein Fehler aufgetreten ist
- Übergangsverlauf, einschließlich:
  - Zeit des Übergangs
  - Aktivität übertragen von
  - Aktivität wurde in geändert
  - Welcher Übergang ausgelöst wurde
- Workflow-Protokoll, einschließlich aller Protokollanweisungen, die dem Workflow hinzugefügt wurden

Konfigurationsinformationen

- Ausgeführte Aktion, einschließlich Einfügen, Aktualisieren und Löschen
- Kategorie des Change
- Kommentare, die mit dem Change aufgezeichnet wurden
- Name des Change
- XML-Unterschied des Change
- Update-Satz, dem der Change zugeordnet ist
- Datum und Uhrzeit des Change
- Benutzer, der die Änderung vorgenommen hat
- Tabelle, in der die Änderung vorgenommen wurde
- Name des Objekts, das geändert wird
- Typ des Objekts, das geändert wird
- Zeigen Sie für Änderungen an Formularen oder Listen die vorgenommene Änderung in an

Transaktionsprotokolle

Das Transaktionsprotokoll zeichnet alle Browseraktivitäten für eine Instanz auf. Um das Debuggen von Systemproblemen zu erleichtern, können Sie Transaktionsprotokolle nach

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungsbereich filtern und so die angezeigten Transaktionen auf Transaktionen beschränken, die aus bestimmten Bereichen stammen.

Das Transaktionsprotokoll enthält die folgenden Informationen für alle Aktivitäten.

Feld	Beschreibung
Erstellt	Datum und Uhrzeit der Anwendungsaktion für das Gebietsschema des Computers, auf dem die Instanz ausgeführt wird.
Typ	Typ der aufgezeichneten Transaktion.
Erstellt von	Anwender, der diese Aktivität erstellt hat.
Ursprungsanwendung	Anwendungsbereich, aus dem die Transaktion stammt. Global wird angezeigt, wenn die Transaktion aus dem globalen Bereich stammt.
Antwortzeit	Roundtrip-Antwortzeit für die Anwendungsanforderung in Millisekunden.
Netzwerkzeit	Latenzzeit der Netzwerkantwort nach der Anwendungsanforderung in Millisekunden.
Ausgabelänge	Größe der Ausgabezeichenfolge, die von der Instanz an die Anwendung gesendet wird, in Byte.
SQL-Anzahl	Anzahl der für diese Aktivität ausgeführten SQL Server-Befehle.
Business-Regel-Anzahl	Anzahl der für diese Aktivität ausgeführten Business-Regeln.
Business-Regel-Zeit	Verstrichene Zeit für die Ausführung der Business-Regeln für diese Aktivität.
URL	Anwendung oder Modul, die/das durch die Client-Anwendung mit verbunden ist.
System-ID	Vom System generierter Bezeichner der Client-Instanz, von der die Anforderung gesendet wird. Diese ID wird für Clusterumgebungen verwendet, in denen mehrere Instanzen (Knoten) mit der Datenbank kommunizieren.
IP-Adresse	IP-Adresse des Clients, der die Anforderung sendet.
GZipped	Angabe, ob eine komprimierte Webseite von der Anwendung angefordert wurde.
Protokoll	Von der Anwendung für diese Instanz verwendetes HTTP-Protokoll.

Client-Transaktionszeiten

Das Plugin „Client Transaction Timings“ verbessert die Systemprotokolle durch zusätzliche Informationen über die Dauer von Transaktionen zwischen Client und Server.

Sie können Leistungsprobleme bis zu ihrer Quelle zurückverfolgen, indem Sie anzeigen, wofür die Zeit verbraucht wird und wie die Zeit während einer Transaktion aufgewendet wurde.

Dieses Plugin erfordert, dass der Antwortzeit-Indikator Antwortzeit-Indikator aktiviert ist, und sammelt Informationen aus den folgenden Browsern:

- Firefox
- Internet Explorer
- Chrome

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Client-Transaktionsinformationen

Durch die Installation des Plugins wird das Modul „ *Client-Transaktionen* “ zur Anwendung „*Systemprotokolle*“ *hinzugefügt*. Stellt eine Liste aller protokollierten Transaktionen zwischen Client und Server innerhalb des letzten Tags bereit:

Client-Transaktionsinformationen

Feld	Beschreibung
Erstellt	Zeitpunkt, zu dem die Transaktion aufgezeichnet wurde.
Antwortzeit	Anzahl der ms, die der Server für die Erfüllung der Transaktion aufgewendet hat.
Business-Regel-Zeit	Anzahl der ms, die Business-Regeln verbracht haben, die durch die Transaktion ausgelöst wurden.
SQL-Zeit	Anzahl der von der SQL-Datenbank verbrauchten ms.
Client-Antwortzeit	(Load_complete_time) – (start_time). Sie beinhaltet die Serverzeit.
Client-Netzwerkzeit	Anzahl der ms, die das Netzwerk verbracht hat, über das der Client eine Verbindung herstellt.
Browser-Zeit	Anzahl der ms, die der Browser während der Transaktion verbracht hat.
Clientskriptzeit	Die Anzahl der für die Ausführung von Client-Skripts aufgewendeten ms.
UI-Richtlinienzeit	Anzahl der für die Ausführung der UI-Richtlinie aufgewendeten ms.
Typ	Typ der Transaktion: • Formular • Liste • Sonstige
Tabelle	Name der angezeigten Tabelle. Beispiel: incident, change_request.
Ansicht	Für dieses Formular/diese Liste anzeigen

Detaillierte Client-Informationen

Eine detailliertere Aufgliederung der Client-Zeiten für das Rendern aller Formulare (aber nicht Listen-Renderings) wird ebenfalls nachverfolgt. Um Details anzuzeigen, führen Sie einen Drilldown in einen bestimmten Client-Transaktionsdatensatz durch, und beobachten Sie die zugehörige Liste am unteren Bildschirmrand.

Detaillierte Client-Informationen

Feld	Beschreibung
Bestellung	Reihenfolge während der Last, in der dieser Vorgang auftrat.
Typ	Typ des Vorgangs
Name	Beschreibender Name dieses bestimmten Vorgangs
Dauer	Anzahl der für diesen Vorgang benötigten ms.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Push-Protokolle

Konsultieren Sie das Push-Protokoll, um den Status von Push-Benachrichtigungen nachzuverfolgen, die sich in der Warteschlange zum Senden über Ihr System befinden.

Um das Push-Protokoll anzuzeigen, navigieren Sie zu **Systemprotokolle** > **Push-Benachrichtigungen**an. Benutzer müssen über die Rolle push_admin oder admin verfügen, um das Push-Protokoll anzuzeigen.

Push-Protokollfelder

Feld	Beschreibung
Anspruch	Identifikationsnummer, die von der geplanten Aufgabe generiert wird, die die Push-Benachrichtigung sendet. Diese Nummer wird auf das Feld **Anspruch** angewendet, um die Konsistenz über mehrere geplante Push-Aufgaben hinweg sicherzustellen.
Nutzlast	Inhalt der Push-Benachrichtigung.
Anzahl Warteschlange	Anzahl der Versuche des Systems, die Push-Benachrichtigung zu senden. Der Status einer Push-Benachrichtigung hängt von der Anzahl der Warteschlange ab. • Wenn die Anzahl der Warteschlange länger als erwartet 0 ist, gibt es keine geplanten Aufgaben, die versuchen, die Push-Benachrichtigung zu senden. • Wenn die Anzahl der Warteschlangen größer als 0 ist und der **Typerfolgreich**ist, können Sie daraus schließen, dass das System so oft versucht hat, die Push-Benachrichtigung zu senden, bevor es endgültig gesendet wurde. • Wenn die Anzahl der Warteschlangen 10 erreicht, versucht das System, die Push-Benachrichtigung nicht mehr zu senden. Der **Typ** ändert sich in **Fehler**.
Anforderungs-ID	Eindeutige Identifikationsnummer für die Push-Benachrichtigung. Ähnlich wie die Nachrichten-ID für eine E-Mail wird die Anforderungs-ID als Korrelationstoken für die Push-Benachrichtigung verwendet.
Typ	Status, der angibt, ob die Push-Benachrichtigung gesendet wurde. Die Spalte „Typ“ kann folgende Werte haben: • **Fehler**: Die Nachricht konnte nicht gesendet werden. • **Ausstehend**: Die Nachricht wird zur Verarbeitung in die Warteschlange versetzt. • **Erfolg**: Die Nachricht wurde erfolgreich gesendet, obwohl sie nicht unbedingt vom mobilen Gerät empfangen wurde.

Zugehörige Informationen

Geplante Aufgaben

System-E-Mail-Protokoll und -Postfächer

Im System-E-Mail-Protokoll werden alle E-Mails erfasst, die von der Instanz erstellt oder empfangen werden. Systempostfächer sind gefilterte Ansichten dieses Protokolls.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Alle Benachrichtigungs-E-Mails, die von der Instanz erstellt oder empfangen werden, werden in einem E-Mail-Datensatz [sys_email] aufgezeichnet. Zu einem Protokoll dieser Datensätze können Sie unter navigieren **Systemprotokolle** > **E-Mails**an.

Die Systempostfächer sind gefilterte Ansichten der E-Mail-Tabelle [sys_email]. Die Instanz weist abhängig von den Werten in den Feldern **Typ** und **Status** einem System-Postfach einen E-Mail-Datensatz zu. Weitere Informationen finden Sie unter System-Mailboxen .

Die folgenden Felder können in das Layout vom Systemprotokoll und von allen Systempostfächern aufgenommen werden:

E-Mail-Protokoll

Feld	Beschreibung
Mailbox	Das Systempostfach, das diesen E-Mail-Datensatz enthält. Die Instanz legt den Wert dieses Felds entsprechend den Werten in den Feldern **Typ** und **Status** fest.
Status	Der aktuelle Status der E-Mail (Fehler, Ignoriert, Verarbeitet oder Bereit).
Empfangstyp	Die Art der eingehenden E-Mail (Keine, Weiterleiten, Neu oder Antwort).
Typ	Der Status der E-Mail. Die Auswahlmöglichkeiten sind: • erhalten: Der Server hat diese E-Mail erhalten. • erhalten - ignoriert: Der Server hat diese E-Mail erhalten, sie wurde jedoch von der Instanz aufgrund von Aktionen bei eingehender E-Mail ignoriert. Normalerweise handelt es sich bei diesen E-Mails entweder um Spam oder um automatische Antworten. Weitere Informationen finden Sie im Feld „Fehlerzeichenfolge“. • senden - fehlgeschlagen: Der Server hat versucht, die E-Mail zu senden, und ist fehlgeschlagen. Weitere Informationen finden Sie im Feld „Fehlerzeichenfolge“. • senden - ignoriert: Der Server hat das Senden dieser E-Mail übersprungen. Normalerweise handelt es sich hierbei um eine E-Mail, die generiert wurde, jedoch keine Empfänger-E-Mail-Adresse hatte oder eine doppelte E-Mail ist. Weitere Informationen finden Sie im Feld „Fehlerzeichenfolge“. • senden - bereit: Die E-Mail kann gesendet werden, wurde jedoch vom Mail-Server nicht gesendet. Normalerweise bleibt eine E-Mail nur für kurze Zeit in diesem Status. • senden - Übersetzung - bereit: Die E-Mail wird während der E-Mail-Übersetzung generiert und gesendet. Normalerweise bleibt eine E-Mail nur für kurze Zeit in diesem Status. • gesendet: Die E-Mail wurde von der Instanz ohne Fehler oder Probleme gesendet.
Zielvorgabe	Eine Dokument-ID-Referenz auf den Datensatz, wenn die E-Mail durch Einfügen, Aktualisieren oder Löschen eines bestimmten Datensatzes generiert wird.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

E-Mail-Protokoll (Fortsetzung)

Feld	Beschreibung
Anwender	Der Name des Benutzers aus dem Benutzerdatensatz der Instanz, von der die E-Mail-Benachrichtigung gesendet wurde. **Hinweis:** Dies ist ein Zeichenfolgen-Feld.
Benachrichtigungstyp	Der Typ der Benachrichtigung. Die Auswahlmöglichkeiten lauten wie folgt: • Keiner • SMS • SMTP
UID	Die eindeutige ID der auf dem Server gespeicherten E-Mail.
Erstellt	Datum und Uhrzeit der E-Mail-Aktivität für das Gebietsschema des Computers, auf dem die Instanz ausgeführt wird.
Gelöscht	Gibt für eingehende E-Mails an, ob die E-Mail vom E-Mail-Server gelöscht wurde.
Gewichtung	Die Gewichtung der E-Mail, die die Sendepriorität relativ zu anderen Benachrichtigungen in derselben Tabelle bestimmt.
Wichtigkeit	Ein Hinweis darauf, dass die E-Mail mit einem geänderten Wichtigkeitsgrad gesendet wurde, z. B. Dringend.
Auslösendes Ereignis und Benachrichtigung	Für durch Benachrichtigungen generierte E-Mails: eine eingebettete Liste, in der das Ereignis und die Benachrichtigung gespeichert sind, durch die die E-Mail erstellt wurde.
Betreff	Der E-Mail-Betreff. Für Benachrichtigungen erstellen Sie den Betrefftext in **Systembenachrichtigung** > **E-Mail** > **Benachrichtigungen**an.
Fehlerzeichenfolge	Die vom E-Mail-Server erfasste Fehlerzeichenfolge, um festzustellen, warum die E-Mail nicht gesendet wurde. Dies wird nur protokolliert, wenn die E-Mail fehlgeschlagen ist.
Empfänger	Die E-Mail-Adressen der Empfänger
Textkörper	Der Textkörper der E-Mail, der in unformatiertem HTML-Markup angezeigt wird. Verwenden Sie den zugehörigen Link „HTML-Textvorschau“, um den Nachrichtentext als gerenderten HTML-Code anzuzeigen.
Content Typ	Der E-Mail-Content Typ
Kopfzeilen	Alle in die E-Mail eingebetteten Header.

Ereignisprotokolle

Das Ereignisprotokoll zeichnet alle Systemereignisse auf, die innerhalb von Now Platformauftreten.

Dieses Protokoll enthält die folgenden Informationen für alle auftretenden Ereignisse:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ereignisprotokoll

Feld	Beschreibung
Erstellt	Datum und Uhrzeit des Ereignisses für das Gebietsschema des Computers, auf dem die Instanz ausgeführt wird.
Name	Name des Ereignisses, wie in der Ereignisregistrierung aufgeführt.
URI	HTTP-Abfrage, die das Ereignis generiert hat.
Parm1	Ereignisspezifischer Wert, der vom Ereignis und vom Empfänger abhängt.
Parm2	Ereignisspezifischer Wert, der vom Ereignis und vom Empfänger abhängt.
Tabelle	Datenbanktabelle, auf die für dieses Ereignis reagiert wird.
Verarbeitet	Zeitpunkt (Datum und Uhrzeit), zu dem die Verarbeitung des Ereignisses begonnen hat. Diese Zeit entspricht dem Gebietsschema des Computers, auf dem die Instanz ausgeführt wird.
Verarbeitungsdauer	Für die Verarbeitung dieses Ereignisses benötigte Zeit in Millisekunden.
Warteschlange	Name der Prozessorwarteschlange.

Importprotokolle

Das Importprotokoll zeigt Informationen in einem ausführlichen Format zu Datenimportaktivitäten innerhalb der Plattform an.

Eine detailliertere Ansicht der Importsätze, die ein bestimmtes Protokoll erstellt haben, finden Sie unter **Importsätze** > **Verlauf umwandeln**an.

Dieses Protokoll enthält die folgenden Informationen für alle Importe:

Importprotokoll

Feld	Beschreibung
Erstellt	Datum und Uhrzeit des Imports für das Gebietsschema des Computers, auf dem die Instanz ausgeführt wird.
Ebene	Typ der angezeigten Nachricht Für importierte Dateien lautet die Ebene „Information“.
Nachricht	Vom System generierte Meldung zum Status des Imports
Quelle	Name der externen Quelle des Imports, z. B. eine Integration.

Modul „Systemdiagnostik“.

Die Anwendung „Systemdiagnose“ stellt Protokolle bereit, die sich auf die Plattform beziehen.

Diese Protokolle sind verfügbar:

Upgradeverlauf

Verfolgt jedes Upgrade auf eine Instanz.

Langsame Abfragen

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bietet Einblick, wie sich Abfragen auf die Leistung der Plattform auswirken. Weitere Informationen finden Sie unter Langsames Abfrageprotokoll verwenden .

Tabelle „Kundenupdates“.

Im System vorgenommene Änderungen werden chronologisch in der Tabelle „Kundenupdates“ [sys_update_xml] aufgezeichnet. Es gibt einige Ausnahmen, wie unten angegeben.

Um zu dieser Tabelle zu navigieren, geben Sie im Navigationsfilter `sys_update_xml.list` ein. Informationen zu Update-Sätzen finden Sie unter System-Update-Sätze .

Die folgenden Informationen werden zu jedem Update gespeichert:

Tabelle „Kundenupdates“.

Feld	Beschreibung
Name	Ein Name, der den aktualisierten Datensatz identifiziert
Erstellt	Datum und Uhrzeit der Erstellung des Kunden-Update-Datensatzes.
Erstellt von	Der Benutzer, der den Change durchgeführt hat.
Typ	Der Typ des Updates.
Aktualisiert	Datum und Uhrzeit der Aktualisierung des Kunden-Update-Datensatzes.
Aktualisiert von	Der Anwender, der das Update durchgeführt hat.
Updates	Angabe, wie oft der Datensatz aktualisiert wurde.
Zielname	Der Name des Elements, das geändert wurde.
Ansicht	Die Ansicht des Formulars, das geändert wurde, wenn es sich um eine Formularlayoutänderung handelte.
Nutzlast	Der XML-Inhalt des Datensatzes nach dem Change.
Remote-Update-Satz	Ein Verweis auf diesen Update-Satz, wenn die Änderung von einem Remote-Update-Satz durchgeführt wurde.
Lokales Update Set	Der Update-Satz, dem der Change zugeordnet ist.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Einige Anwendungsänderungen werden nicht durch Kunden-Update-Datensätze (sys_update_xml) Beispiele dargestellt:

- Metadatentypen, bei denen updateSynch = falsch ist
- Kaskadierende Änderungen an Tabellen und Feldern wie z. B. Anzeigenamen
- Unaufgelöste Metadatenreferenzen aus anderen Anwendungen (führt zu keinem „Anzeigewert“ für das Element)
- sys_id ändert sich für zusammengefügte Dateien
- Änderungen an Flow/Flow-Aktionen, die sys_documentation generieren können
- ua_table_license_config-Datensätze, die bei der Tabellenerstellung generiert werden
- Aufträge, die im Hintergrund ausgeführt werden, z. B. Natural Language Processing
- Fälle, in denen „sys_update_xml“ manuell geändert oder entfernt wird

Weitere Informationen finden Sie unter Changes festschreiben .

Protokollverlauf

Das System verwendet Tabellenrotation und Tabellenerweiterung, um ältere Protokolle zu archivieren.

Standardmäßig verwendet das System den folgenden Zeitplan für die Archivierung allgemeiner Protokolle:

Gemeinsamer Protokollarchiv-Zeitplan

Tabelle	Archivzeitplan	Rotationen	Typ
Ereignis [ecc_event]	Jeden Tag	7	Rotation
Warteschlange [ecc_queue]	Jeden Tag	7	Rotation
Ereignis [sysevent]	Jeden Tag	7	Rotation
Protokoll [syslog]	Jede Woche	8	Rotation
Transaktionsprotokoll [syslog_transaction]	Jede Woche	8	Rotation
E-Mail [sys_email]	Alle 30 Tage	8	Erweiterung

Verwenden Sie den Protokolldateibrowser

Die Instanz stellt die Dienstprogramme Protokolldateibrowser und Protokolldateidownload bereit.

Verwenden **Systemprotokolle** > **Dienstprogramme** > **Knoten-Protokolldateibrowser** um einen beliebigen Systemprotokolleintrag anzuzeigen. Sie können mit den folgenden Filtern nach Protokolldateien suchen:

Protokolldateibrowser

Feld	Beschreibung
Startzeit	Startdatum und -uhrzeit des zu durchsuchenden Bereichs für das Gebietsschema des Computers, auf dem die Instanz ausgeführt wird.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Protokolldateibrowser (Fortsetzung)

Feld	Beschreibung
Sitzungs-ID	Vom System generierte Hexadezimalzeichenfolge, die die Sitzung identifiziert, die den Protokolleintrag generiert hat.
Endzeit	Enddatum und -uhrzeit des zu durchsuchenden Bereichs für das Gebietsschema des Computers, auf dem die Instanz ausgeführt wird.
Nachricht	Vom System generierte Beschreibung des Vorkommens
Ebene	Typ der angezeigten Nachricht Die Ebenen sind Debuggen, Fehler, Warnung und Information. Eine Warnung ist ein Fehler, der behandelt und behoben wurde. Ein Fehler ist etwas, das behoben werden muss.
Thread-Name	Vom System generierter Bezeichner des Threads, der die Protokolldatei erstellt hat.
Maximale Zeilen	Maximale Anzahl der für einen bestimmten Filter zurückgegebenen Datensätze.

Die Instanz erstellt alle 2 Tage komprimierte Archive von Systemprotokollen und löscht die Protokollarchive nach 21 Tagen.

Wichtig: Wenn ein Knoten außer Kraft gesetzt wird, werden die Protokolldateien des Knotens sofort gelöscht. Das bedeutet, dass sie keine weiteren 21 Tage lang archiviert werden.

Sie können Protokolldateiarchive herunterladen und mit anzeigen **Systemprotokolle** > **Dienstprogramme** > **Knotenprotokolldatei-Download**an. Wählen Sie ein Protokollarchiv aus der Liste aus, und klicken Sie dann auf **Protokoll herunterladen** unter *Zugehörige Links*, um das Archiv zu öffnen oder zu speichern.

Hinweis: Protokolldateien sind nur für den Knoten verfügbar, bei dem Sie gerade angemeldet sind. Um den aktuell angemeldeten Knoten anzuzeigen, navigieren Sie zu **Systemdiagnostik** > **Statistiken**an.

Verwenden Sie die neue Schaltfläche **Syslog-Datensätze** anzeigen in den Formularen „Transaktion“ und „Aktive Transaktion“, um alle Systemprotokolleinträge anzuzeigen, die während der Ausführung der Transaktion generiert wurden. Eine Transaktion kann eine beliebige Anzahl von Syslog-Einträgen aufweisen. Die verschiedenen Syslog-Einträge für alle Transaktionen erschweren die Zuordnung einer Transaktion zu ihren jeweiligen Syslog-Einträgen. Die UI-Aktion **„Syslog-Datensätze** anzeigen“ hilft bei der Zuordnung der aktiven und abgeschlossenen Transaktionen zu ihren jeweiligen Syslog-Einträgen, indem eine URL zum Abfragen der Syslog-Tabelle erstellt wird. Das Identifizieren der richtigen Syslog-Einträge für eine bestimmte Transaktion hilft beim Debuggen und Behandeln von Sicherheitsbedenken.

Verbesserte Protokollierungssicherheit

Untersuchen Sie das Feld **Attribution** in den Knotenprotokollzeilen, um das Skript oder die Komponente zu identifizieren, das bzw. die die Protokollnachricht generiert hat. Transaktionsstartzeilen enthalten das neue Feld, um den Typ der gestellten Anforderung zu identifizieren.

Mit den neuen Erweiterungen wird Folgendes erreicht:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Verfolgen Sie den Quellurheber jeder der Protokollzeilen
- Falls die Absenderinformationen nicht verfügbar sind, geben Sie den Java-Klassennamen und eine Attribution aus
- Am Anfang jeder Transaktionszeile stehen die Transaktions-ID und der Transaktionstyp

Verwenden Sie die Transaktions-ID jeder Protokollzeile, um die Informationen zu verstehen, die in jeder Protokollzeile angegeben sind. Sobald Sie den Transaktionstyp identifiziert haben, erhalten Sie die Absenderinformationen für jede Protokollzeile. Transaktionstyp und Ursprung Informationen jeder Protokollzeile zusammen ergeben die erforderlichen Quellinformationen zu jeder Knotenprotokollzeile.

Hinweis: Die Skripttypen SYS_UI_MACRO und SERVICE_PORTAL_WIDGET in der Attribution werden nicht gemeldet.

Transaktionstypen

Es folgt die Liste der Transaktionstypen:

- Liste
- Formular
- XMLHttp
- Bericht
- SOAP
- Exportieren
- Zeitplaner
- TextSearch
- Sonstige
- REST
- JSON
- AMB
- Archiv
- Batch-REST
- Instanz-Scan

Systemeigenschaften

Die folgenden Systemeigenschaften sind für diese Funktion erforderlich:

- Glide.log.append.attribution: Diese Eigenschaft ist standardmäßig aktiviert. Aktiviert/deaktiviert die Attributionsinformationen jeder Knotenzeile
- Glide.db.log.append.classname.attribution: Diese Eigenschaft ist standardmäßig aktiviert. Aktiviert/deaktiviert die Protokollierung der Java-Klassennamenzuordnung

Vermeiden Sie Protokollmanipulationen

Konfigurieren Sie Schutzregeln für Systemprotokolltabellen, um den Umfang der Änderung und Löschung von Anwendungsprotokolldatensätzen einzuschränken. Mit den Regeln können Sie die Protokollierung von Änderungen oder Änderungsversuchen in diesen Tabellen bestimmen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie security_admin sind, aktivieren Sie das Plugin „Protected Tables“ (com.glide.protected_tables), mit dem die Plattform Aktualisierungs-, Einfüge- und Löschvorgänge für die folgenden Systemprotokolltabellen einschränken kann:

- syslog
- syslog_transaction
- sys_outbound_http_log
- sysevent
- sys_audit
- sys_push_notification
- syslog_app_scope
- opened_table_configuration (Konfiguration nicht veränderbar)

Hinweis: Das Plugin „com.glide.protected_tables“ bietet nur Schutz für die oben genannten Systemprotokolltabellen. Bei jedem Versuch, einen Datensatz zu aktualisieren, einzufügen oder zu löschen, wird eine Meldung in der Tabelle „protected_table_log“ protokolliert.

Weitere Informationen finden Sie unter Protokollschutz-Plugin installieren und konfigurieren.

Sie können für jede der Systemprotokolltabellen eine der folgenden Protokollschutzstufen angeben.

- Versuch blockieren und protokollieren: Blockiert jede Änderung und protokolliert den Versuch
- Nur Versuch blockieren: Blockiert jede Änderung und protokolliert den Versuch nicht
- Nur den Versuch protokollieren: Blockiert nicht die Änderung, aber protokolliert den Versuch
- Nicht blockieren und Versuch nicht protokollieren: Blockiert die Änderung nicht und protokolliert den Versuch nicht

Die Plattform verwendet die für jede der Systemprotokolltabellen angegebenen Protokollschutzebenen, um alle Versuche, einen Datensatz nach der ersten Erstellung zu ändern, zu blockieren und/oder zu protokollieren.

Hinweis: Wenn Sie ein security_admin sind, können Sie die standardmäßigen Protokollschutzstufen in allen Systemprotokolltabellen überschreiben, um sie an die Anpassungen in Ihrer Instanz anzupassen.

Alle Versuche, die Systemprotokolltabellen zu ändern, werden in der Tabelle „protected_table_log“ protokolliert.

Hinweis: Wenn für eine Tabelle keine Schutzstufe angegeben ist, werden Änderungsversuche nicht in der Tabelle „protected_table_log“ protokolliert.

Um die Plugin-Vorgänge für Tabellen im Administratorbereich zu deaktivieren, legen Sie die Eigenschaft com.glide.security.protected_table.enabled auf „falsch“ fest. Weitere Informationen finden Sie unter Protokollschutzeigenschaft erstellen.

Protokollschutz-Plugin konfigurieren

Konfigurieren Sie die Schutzregeln für jede Tabelle und jeden Vorgang, um die Konfiguration des Protokollschutz-Plugins abzuschließen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Alle** > **Geschützte Tabellen** > **Protokollschutz**an.
   Die Seite des Administratorbereichs wird angezeigt.

   Hinweis: Ab dem Release Utah ist das Plugin „Protected Tables“ standardmäßig installiert, aber deaktiviert.

2. Erhöhen Sie Ihre Rolle auf security_admin, um mit der Konfiguration des Plugins fortzufahren.

   a. Wählen Sie **Systemadministrator aus**.

   b. Wählen Sie **Rolle erweitern aus**.
   Das Modal „Rolle erweitern“ wird angezeigt.

   c. Wählen Sie die Option security_admin aus, um Ihre Rolle zu erhöhen, und wählen Sie **Aktualisieren**aus.

3. Konfigurieren Sie die Schutzregeln für jede Tabelle und jeden Vorgang. Die Schutzregeln gelten für das Aktualisieren, Einfügen und Löschen. Die Schutzstufen können für einige Tabellen nicht geändert werden. Die Tabellen „syslog“ und „syslog_app_scope“ enthalten feste Werte für den Aktualisierungs- und Löschschutz. Die Tabelle „protected_table_configuration“ hat feste Schutzwerte für alle drei Vorgänge.

   Hinweis: Für die Sysevent-Tabelle können Einfügeschutze nicht auf „Blockieren“ festgelegt werden.

   Wenn Sie Im vorherigen Release die Option Auf **untergeordnete Tabellen anwenden** für syslog aktiviert hatten, werden die untergeordneten Tabellen beim Upgrade auf das Release Utah dem Protokollschutz mit denselben Schutzregeln wie syslog hinzugefügt. Dies geschieht nur für syslog, nicht für andere Tabellen.

4. Aktivieren Sie die Funktion, indem Sie den **Umschalter Protokollschutz aktivieren** auswählen.

   Hinweis: Sie können dieses Plugin nur deaktivieren, indem Sie die Eigenschaft „com.glide.security.protected_table.enabled“ in der Tabelle „sys_properties“ ändern.

Erstellen Sie eine Protokollschutzeigenschaft

Erstellen Sie eine Protokollschutzeigenschaft, um das Risiko der Protokollmanipulation zu vermeiden.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Wenn die Eigenschaft *com.glide.security.protected_table.enabled*in der Liste „Systemeigenschaften“ nicht vorhanden ist, wählen Sie **Neu**aus.
   Das Formular für neue Systemeigenschaft wird angezeigt.
2. Füllen Sie die Details im Formular aus

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder	Beschreibung
Name	Name der Eigenschaft als com.glide.security.protected_table.enabled
Anwendung	Anwendung, die über die Eigenschaft verfügt.
Beschreibung	Beschreibung der Eigenschaft
Auswahlmöglichkeiten	
Typ	Werttyp: „true“ oder „false“.
Wert	Ist-Wert der Eigenschaft
Cache ignorieren	Option zum Ignorieren des Cache-Inhalts
Privat	Option, um die Eigenschaft als privat zu definieren ◦ Leserollen ◦ Schreibrollen

3. Wählen Sie **Absenden** aus, um die Eigenschaft zu erstellen.

Protokollierung, Auditing und Fehler (Härtung der Instanzsicherheit)

Wenden Sie eine Protokollierungs- und Auditstrategie an, damit Sie verdächtige Aktivitäten rechtzeitig erkennen und entsprechende Maßnahmen ergreifen können.

Weitere Informationen darüber, was in der Instanz protokolliert werden kann, finden Sie unter Systemprotokolle. Stellen Sie sicher, dass ein Zeitplan für die Überwachung von Systemereignissen wie Anmeldungen und fehlgeschlagenen Anmeldungen vorhanden ist, indem Sie verwenden **Systemprotokolle** > **Ereignisse**an.

Deaktivieren von SQL-Fehlermeldungen (Härtung der Instanzsicherheit)

Verwenden Sie die Eigenschaft *glide.db.loguser*, um die Darstellung von SQL-Fehlermeldungen in einem Browser zu deaktivieren.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.db.loguser
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurierbar im Instanz-Sicherheitszentrum	Nein
Zweck	Um die Anzeige von SQL-Fehlermeldungen im Browser zu deaktivieren.
Typ	Wahr | Falsch
Empfohlener Wert	falsch

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Funktionale Auswirkung	(Niedrig) Diese Korrektur deaktiviert das Rendern von SQL-Fehlermeldungen. Es gibt keine Auswirkungen auf Funktionen.
Sicherheitsrisiko	(Mittel) Es sollten keine vertraulichen SQL-Informationen, die einem Angreifer helfen könnten, als Teil der Fehlermeldung auf einer Webseite angezeigt werden.

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Geheimnisverwaltung

Verwenden Sie ServiceNow Geheimnisverwaltung für eine granulare Verwaltung des Zugriffs auf Ihre Passwörter entsprechend Ihren Geschäftsanforderungen.

Untersuchen



Lernen Sie die wichtigsten Funktionen und den Geschäftsnutzen von Geheimnisverwaltung kennen.

Analysieren



Erfahren Sie mehr über das Dashboard „Geheimnisverwaltung“.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren



Planen Sie Ihre Kernkonfigurationen.

Geheimnisverwaltung erkunden

Verwenden Sie ServiceNow Geheimnisverwaltung für eine granulare Verwaltung des Zugriffs auf Ihre Passwörter entsprechend Ihren Geschäftsanforderungen.

Wichtig: Administratoren müssen über die Rolle verfügen, um Module und Datensätze im Zusammenhang mit der Geheimnisverwaltung anzuzeigen. Informationen zur Geheimnisverwaltungsrolle finden Sie unter Geheimnisverwaltungsrollen.

Wählen Sie eine der Core- und Enterprise-Versionen von Geheimnisverwaltung aus

Wählen Sie je nach Geschäftsanforderungen zwischen „Geheimnisverwaltung Core“ und „Geheimnisverwaltung Enterprise“ aus.

Geheimnisverwaltungs-Core	Geheimnisverwaltungsunternehmen
Secrets Management Core kann in Ihrer Instanz ohne zusätzliche Kosten aktiviert werden. Das Plugin bietet die Möglichkeit, Geheimnisgruppen mit Kriterien in nicht anwenderdefinierten Tabellen zu verwenden, die auf der Plattform ServiceNow bereitgestellt werden und von den Anwendungsentwicklungsteams von ServiceNow erstellt wurden.	Geheimnisverwaltung Enterprise enthält zusätzliche Funktionen, mit denen Administratoren Geheimnisgruppen erstellen und verwalten können. Enterprise bietet zusätzlich zu den in Core aufgeführten Funktionen die folgenden Funktionen. • Verwenden Sie granulare Zugriffssteuerungen, um Geheimnisgruppen basierend auf einem dieser Kriterien zu erstellen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geheimnisverwaltungs-Core	Geheimnisverwaltungsunternehmen
	◦ Umfang ◦ Tabelle ◦ Spalte ◦ Datensatz • Erstellen Sie für den Client zugängliche Geheimnisse, die mit Ihrem eigenen Schlüssel verschlüsselt sind, auf den ServiceNow nicht zugreifen kann. • Verwenden Sie das Geheimnisverwaltungs-Dashboard, um die in Ihrer Instanz konfigurierten geheimen Gruppen zu überprüfen und mehr über potenzielle Sicherheitsprobleme zu erfahren. **Hinweis:** Secrets Management Enterprise ist ein kostenpflichtiges Plugin, das die Mitarbeiter von ServiceNow in Ihrer Produktionsinstanz aktivieren müssen.

Verwenden Sie geheime Gruppen, um Ihre Geheimnisse zu organisieren

Verwenden Sie die Geheimnisverwaltung, um Ihre Geheimnisse in Gruppen zu organisieren und dann Zugriffsrichtlinien auf Gruppenebene auf diese Geheimnisse anzuwenden.

Grundlegende geheime Gruppe

Diese Gruppen gelten für alle Geheimnisse in einem Bereich. Diese Geheimnisse werden durch ein gemeinsames kryptografisches Modul und Modulzugriffsrichtlinien entschlüsselt.

Geheime Gruppe mit Kriterien

Geheimnisgruppen mit Kriterien funktionieren genauso wie eine einfache Geheimnisgruppe, verfeinern jedoch die Inhalte mithilfe von Kriterien weiter. Diese Kriterien umfassen:

- Anwendungsbereich
- Paket
- Tabelle
- Geheime Spalte
- Filterdatensatz

Geheime Gruppen beider Typen können auf Instanzen oder Clients beschränkt werden.

Geheime Gruppen auf Instanzseite

Geheime Gruppen auf Instanzseite enthalten Geheimnisse, die von Ihrer Instanz entschlüsselt werden können.

Clientseitige geheime Gruppen

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Clientseitige Geheimnisgruppen verwenden ein öffentliches und privates Schlüsselpaar, um sicherzustellen, dass Geheimnisse nur vom Client entschlüsselt werden können. Wenn Sie eine für den Client zugängliche Geheimnisgruppe erstellen, laden Sie den öffentlichen Schlüssel in die Instanz hoch und behalten den privaten Schlüssel auf Ihrem MID-Server. Die Instanz von verwendet den öffentlichen Schlüssel, um Ihre Geheimnisse zu verschlüsseln, sie können jedoch nur mit dem privaten Schlüssel entschlüsselt werden.

Hinweis: Weitere Informationen zu diesen Gruppentypen finden Sie unter Client-Seite verstehen Geheimnisverwaltung.

Verwenden Sie Geheimnisgruppen für eine präzisere Steuerung

Während „password2“ auf der Plattform ServiceNow verfügbar ist, bietet die Geheimnisverwaltung die folgenden zusätzlichen Funktionen.

Granulare Zugriffssteuerungen	Passwort2 Mit password2 können Administratoren den Zugriff auf einen Anwendungsbereich steuern, aber den Zugriff auf Elemente innerhalb des Bereichs nicht einschränken. Geheimnisverwaltung Mit der Geheimnisverwaltung können Administratoren den Zugriff basierend auf von ihnen definierten Kriterien einschränken. Kriterientypen können auf Kriterien wie Paket, Tabelle oder Spalte basieren.
Sicherer Speicher	Für clientseitige geheime Gruppen verwendet die Geheimnisverwaltung ein neues Verschlüsselungsschema. In diesem Verschlüsselungsschema speichert ServiceNow den Verschlüsselungsschlüssel nicht. Aus diesem Grund hängt die Sicherheit Ihrer Daten nicht von der Sicherheit von ServiceNow ab.

Wenden Sie Modulzugriffsrichtlinien auf Ihre Gruppen an

Nachdem Sie Ihre Geheimnisse in einer Geheimnisgruppe gruppiert haben, können Sie Richtlinien anwenden, die bestimmen, wie Sie auf Gruppenebene auf diese Geheimnisse zugreifen können. Modulzugriffsrichtlinien sind die Zugriffskontrollmechanismen, die Sie auf kryptografische Module anwenden, um Steuerungen auf Instanzebene zu definieren, z. B. einen Gültigkeitszeitraum für den kryptografischen Schlüssel. Weitere Informationen zu Modulzugriffsrichtlinien finden Sie unter Übersicht über Modulzugriffsrichtlinien.

Mit Geheimnisverwaltung installierte Tabellen

Die Geheimnisverwaltung fügt diese Tabellen hinzu oder ändert sie.

Neue Tabellen	
sn_sm_secret_group	Speichert geheime Gruppen
[sn_sm_secret_group_criteria]	Speichert geheime Kriteriengruppen
sn_sm_secret	Speichert umschlossene Geheimnisse

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

sn_sm_identity_group	Definiert die Identitätsgruppe für die Zuordnung einer Gruppe von Identitäten zum öffentlichen Schlüssel
[sys_kmf_wrapped_module_key]	Speichert die umschlossenen symmetrischen kryptografischen Schlüssel
Geänderte Tabellen	
[sys_kmf_crypto_module]	Kryptografischer Modultyp hinzugefügt. (Kryptografisches Modul der Identität oder geheimen Gruppe)
[sys_kmf_module_key]	• Speichert den konzeptionellen geheimen Verschlüsselungsschlüssel (ohne Schlüsselmaterial) • Speichert den öffentlichen Identitätsschlüssel
[sys_kmf_crypto_caller_policy]	Neuen Modulzugriff-Richtlinientyp hinzugefügt

Anwendungsfallbeispiele für die Geheimnisverwaltung

Tragen Sie zur sicheren ITOM-Discovery bei

Diese Infografik zeigt eine vereinfachte Referenzarchitektur, wie ServiceNow IT Operations Management (ITOM) Discovery von Ihrer Organisation bereitgestellt werden kann. Wie in der Infografik gezeigt, stellen mehrere Windows- und Linux-Server eine Verbindung zum MID-Server her, und mehrere MID-Server-Agents ermöglichen es dem Discovery-Prozess, die CMDB zu aktualisieren. Jede MID-Server-Transaktion erfordert eine sichere Authentifizierung. Daher ist die Verwaltung der Anmeldeinformationen aus Sicherheitsgründen von entscheidender Bedeutung.

Workflow-Konnektivität mit Integration Hub auf sichere Weise beschleunigen

Verwenden Sie den Integration Hub von ServiceNow, um über automatisierte Anwendungsprogrammierschnittstellen (APIs) eine Verbindung zu anderen Systemen herzustellen. Jedes Mal, wenn Integration Hub über eine API eine Verbindung zu einem System herstellt, sind Anmeldeinformationen zur Authentifizierung erforderlich, um die Konnektivität herzustellen. Die Verwaltung einer Vielzahl von Anwendungen und Konnektivitäts-APIs erfordert eine Lösung zur Verwaltung von Geheimnissen.

Die Verwaltung von Geheimnissen ist ein wichtiger Bestandteil bei der Gewährleistung der Cybersicherheit Ihres Unternehmens. Sie deckt alle Prozesse und Tools im Zusammenhang mit der Erstellung, Speicherung, Übertragung und Verwaltung von digitalen Anmeldeinformationen wie Verschlüsselungsschlüssel, API-Token und Passwörter ab. Um Geheimnisse sicher und effektiv zu verwalten, können Sie eine Richtlinie für die Verwaltung zentraler Geheimnisse erstellen, die Standardregeln und -verfahren für alle Phasen des Lebenszyklus eines Geheimnisses festlegt.

Client-Seite verstehen Geheimnisverwaltung

Erfahren Sie, wie Sie mit Geheimnisverwaltung den Zugriff auf Geheimnisse und Gruppen verwalten.

Terminologie

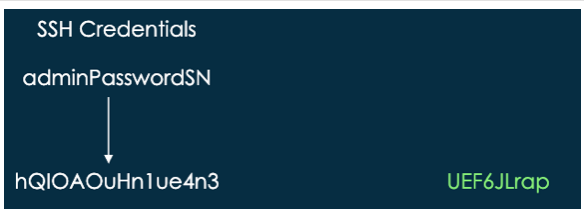
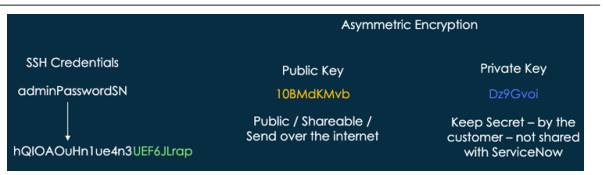
Die clientseitige Verwaltung von Geheimnissen bietet eine Methode zum Verwalten von Geheimnissen ohne Verwendung von Proxys und ohne ServiceNow Zugriff auf Ihre

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

entschlüsselten Daten. Um diesen Prozess zu verstehen, beginnen Sie mit den folgenden Verschlüsselungsbegriffen.

Benennung	Beschreibung
Symmetrische Verschlüsselung	Die symmetrische Verschlüsselung verwendet denselben Schlüssel zum Verschlüsseln und Entschlüsseln von Daten. Wenn Daten mit einem symmetrischen Schlüssel verschlüsselt werden, reicht dieser Schlüssel aus, um sie zu entschlüsseln.
Symmetrischer Schlüssel	Der symmetrische Schlüssel verschlüsselt ein Geheimnis und wandelt Ihr Klartextpasswort in unlesbaren Geheimtext um.
Asymmetrische Verschlüsselung	Die asymmetrische Verschlüsselung verwendet zwei Schlüssel, einen zum Verschlüsseln und einen zum Entschlüsseln.
Öffentlicher Schlüssel	Der öffentliche Schlüssel ist die eine Hälfte des asymmetrischen Schlüsselpaars. Dieser Schlüssel wird in Ihrer -Instanz gespeichert, die den Schlüssel zum Verschlüsseln eines symmetrischen Schlüssels verwendet. Dieser verschlüsselte symmetrische Schlüssel kann nur entschlüsselt werden, wenn er mit dem privaten Schlüssel gekoppelt ist.
Privater Schlüssel	Der private Schlüssel ist die eine Hälfte des asymmetrischen Schlüsselpaars. Dieser Schlüssel wird in einem Schlüsselspeicher auf Ihrem MID-Server gespeichert. ServiceNow hat keinen Zugriff auf diesen Schlüssel. In Kombination mit dem öffentlichen Schlüssel wird das asymmetrische Schlüsselpaar zur Entschlüsselung Ihrer Geheimnisse verwendet.

Client-seitiger Verschlüsselungsprozess

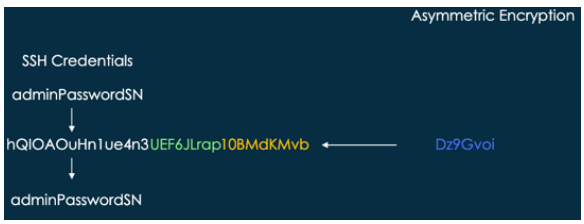
Ein symmetrischer Schlüssel verschlüsselt Anmeldeinformationen (in diesem Fall ein Administratorpasswort) und ändert sie von lesbarem Klartext in verschlüsselten Geheimtext.	
Der symmetrische Schlüssel (grün dargestellt) kann auf die Anmeldeinformationen angewendet werden, um sie zu verschlüsseln oder zu entschlüsseln.	
An diesem Punkt beginnt die asymmetrische Verschlüsselung mit der Verwendung von öffentlichen (gelb) und privaten Schlüsseln (blau).	

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der öffentliche Schlüssel verschlüsselt die Anmeldeinformationen zusammen mit dem symmetrischen Schlüssel. Der symmetrische Schlüssel ist jetzt geschützt und kann nicht zum Entschlüsseln der Anmeldeinformationen verwendet werden. Obwohl der öffentliche Schlüssel diese Verschlüsselung durchführen kann, kann er nicht allein zum Entschlüsseln verwendet werden.



Nach der Verschlüsselung mit dem öffentlichen Schlüssel wird der private Schlüssel benötigt, um die Anmeldeinformationen zu entschlüsseln. Da nur der Kunde über diesen Schlüssel verfügt, ist er der einzige, der auf die verschlüsselten Anmeldeinformationen zugreifen kann.



Für den Client zugängliche Geheimnisse konfigurieren

Erfahren Sie, wie Sie Ihre -Instanz für die Verwendung von vom Client zugänglichen Geheimnissen konfigurieren.

Verwenden Sie diese Beispielimplementierung, um Geheimnisverwaltung zu konfigurieren, ohne Proxys zu verwenden oder ServiceNow Zugriff auf Ihre entschlüsselten Daten zu gewähren.

Weitere Informationen zur Verwendung von clientseitigen Geheimnisverwaltung zum Verwalten des Zugriffs auf Passwörter und Gruppen finden Sie unter Client-Seite verstehen Geheimnisverwaltung.

Diese Anweisungen setzen voraus, dass in Ihrem lokalen Netzwerk ein MID-Server konfiguriert ist. Weitere Informationen zu diesem Prozess finden Sie unter MID-Server .

Prozessübersicht

1. Erstellen Sie Verschlüsselungsschlüssel und Zertifikat

   Erstellen Sie Verschlüsselungsschlüssel und ein Zertifikat mit Terminalbefehlen in Ihrer lokalen Umgebung.

2. Fügen Sie Ihr -Zertifikat dem ServiceNow Trusted Key Store hinzu

   Laden Sie Ihren Schlüssel und Ihr Zertifikat in den Trusted Key Store ServiceNow hoch.

3. Erstellen Sie eine geheime Gruppe mit Kriterien

   Erstellen Sie eine Gruppe für Ihre Geheimnisse. Geheimnisgruppen, um Ihre Geheimnisse in Gruppen zu organisieren. Wenn Sie diese Gruppen verwenden, können Sie Zugriffsrichtlinien auf Gruppenebene auf diese Geheimnisse anwenden. Ordnen Sie dann Ihre Geheimnisgruppe einer Identitätsgruppe zu, und fügen Sie Ihren MID-Server dieser Identitätsgruppe hinzu.

4. Laden Sie das öffentliche/private Schlüsselpaar auf den MID-Server hoch

   Laden Sie Ihr öffentliches/privates Schlüsselpaar auf Ihren MID-Server hoch. Mit diesem Schlüsselpaar kann der MID-Server Authentifizierungsanforderungen von Ihrer Instanz verarbeiten.

5. Erstellen Sie Anmeldeinformationen, und testen Sie die Verschlüsselung der Anmeldeinformationen

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie Anmeldeinformationen, um sich bei einem Drittanbietersystem zu authentifizieren, und testen Sie, dass ServiceNow nicht auf die Anmeldeinformationen zugreifen kann.

6. Konfigurieren Sie Flow Designer, um die Integration zu verwalten

   Verwenden Sie in Ihrer -Instanz Flow Designer, um eine Integration zwischen Ihrem lokalen Netzwerk und Ihrer -Instanz zu verwalten.

7. Testet die Client-seitige End-to-End-Integration für verschlüsselte Geheimnisse

   Testen Sie Ihre Integration und überprüfen Sie die Ausführungsdetails, um zu bestätigen, dass Ihre Konfiguration funktioniert.

Erstellen Sie Verschlüsselungsschlüssel und Zertifikat

Erstellen Sie Verschlüsselungsschlüssel und ein Zertifikat mit Terminalbefehlen in Ihrer lokalen Umgebung.

Vorbereitungen

Erforderliche Rolle: keine

Prozedur

1. Öffnen Sie in Ihrer lokalen Umgebung Terminal (unter Mac oder Linux) oder Befehlszeile (unter Windows).
2. Verwenden Sie das Terminal, um mit `cd` in den Ordner zu wechseln, in dem Sie Ihre Verschlüsselungsschlüssel speichern möchten.
3. Geben Sie im Terminal Folgendes ein:

```
openssl req -newkey rsa:4096 -nodes -keyout sm_private_key.pem -x509
 -days 365 -out sm_public_cert.pem
```

Hinweis: In diesem Beispiel wird OpenSSL zum Generieren von Schlüsseln und Zertifikaten verwendet. Sie können andere vergleichbare Tools basierend auf Ihren Anforderungen ersetzen.

Der Befehl generiert einen privaten Schlüssel und ein öffentliches Zertifikat (mit dem entsprechenden öffentlichen Schlüssel). Es folgt eine Reihe von Aufforderungen zur Eingabe erforderlicher Informationen, beginnend mit „Ländername“.

4. Füllen Sie die Eingabeaufforderungen mit den erforderlichen Informationen aus. Die folgenden Eingabeaufforderungen werden angezeigt.
   - Ländername
   - Name des Bundesstaats oder der Provinz
   - Name des Ortes (z. B. Stadt)
   - Organisationsname (z. B. Unternehmen)
   - Name der Organisationseinheit (z. B. Abschnitt)
   - Allgemeiner Name (z. B. vollqualifizierter Hostname)
   - E-Mail-Adresse

   Arbeiten Sie mit Ihrem Sicherheitsteam zusammen, um sicherzustellen, dass Sie die richtigen Zertifikatinformationen eingeben.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
Country Name (2 letter code) []:US
State or Province Name (full name) []:CO
Locality Name (eg, city) []:Boulder
Organization Name (eg, company) []:ServiceNow
Organizational Unit Name (eg, section) []:Product Management
Common Name (eg, fully qualified host name) []:fake@servicenow.com
Email Address []:fake@servicenow.com
```

5. Überprüfen Sie den Ordner, den Sie in Schritt 2 ausgewählt haben, um sicherzustellen, dass der private Schlüssel und das öffentliche Zertifikat erstellt wurden.
   Wenn Sie dieselben Dateinamen wie im Beispiel in Schritt 3 verwendet haben, sollten die folgenden Dateien angezeigt werden:
   - sm_private_key.pem
   - sm_public_cert.pem
6. Verwenden Sie im selben Ordner den folgenden Befehl:

   Wichtig: Welcher Befehl genau zu verwenden ist, hängt von Ihrem Betriebssystem ab.

Für Linux:	`cat sm_private_key.pem sm_public_cert.pem > sm_keypair_bundle.pem`
Für Windows:	`sm_private_key.pem sm_public_cert.pem > sm_keypair_bundle.pem`

   Dieser Befehl bündelt den privaten Schlüssel und das öffentliche Zertifikat in einer einzelnen Datei, die in den folgenden Schritten in Ihren MID-Server geladen wird.
7. Überprüfen Sie den Ordner erneut, um sicherzustellen, dass die neue Datei mit Ihrem privaten Schlüssel (sm_keypair_bundle.pem) und Ihrem öffentlichen Zertifikat erstellt wurde.

Fügen Sie Ihr -Zertifikat dem ServiceNow Trusted Key Store hinzu

Laden Sie Ihren Schlüssel und Ihr Zertifikat in den Trusted Key Store ServiceNow hoch.

Vorbereitungen

Erforderliche Rolle: keine

Das öffentliche Zertifikat, das Sie in diesem Beispiel erstellt haben, wird als „selbstsigniertes“ Zertifikat betrachtet (d. h. es stammt nicht von einer vertrauenswürdigen Stammzertifizierungsstelle). Sie müssen das Zertifikat dem vertrauenswürdigen Schlüsselspeicher ServiceNow hinzufügen, damit es verwendet werden kann. Wenn Sie ein Zertifikat verwenden, das von einer Zertifizierungsstelle stammt, müssen Sie diesen Schritt nicht ausführen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

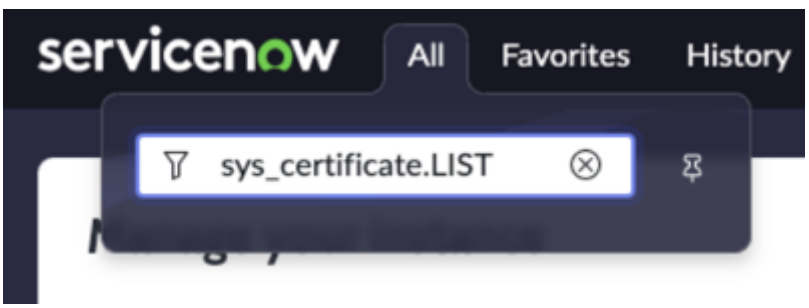
1. Öffnen Sie in Ihrer lokalen Umgebung Terminal (unter Mac oder Linux) oder Befehlszeile (unter Windows).
2. Verwenden Sie das Terminal, um mit `cd` in den Ordner zu wechseln, in dem Sie Ihre Verschlüsselungsschlüssel erstellt haben.
3. Geben Sie im Terminal den folgenden Befehl ein:

   ```
   cat sm_public_cert.pem
   ```

   Sie müssen den Inhalt Ihres öffentlichen Zertifikats anzeigen, um es in den vertrauenswürdigen Schlüsselspeicher zu kopieren. Dieser `„cat"` -Befehl zeigt das Zertifikat an.

4. Kopieren Sie die Zertifikatinformationen in die Zwischenablage.
   Beginnen Sie mit, und schließen Sie die Zeile `-----BEGIN CERTIFICATE-----` ein, enden Sie mit und schließen Sie die Zeile `-----END CERTIFICATE-----` ein.
5. Navigieren Sie in Ihrer Instanz ServiceNow zur Liste der **X.509-Zertifikate**, indem Sie im Navigationsfilter `sys_certificate.LIST eingeben`.

6. Wählen Sie **Neu** aus, um einen **X.509-Zertifikatdatensatz** zu erstellen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Füllen Sie im Formular die folgenden Felder aus.

X.509-Zertifikatfelder

Feld	Wert
Name	Name des Zertifikats. Dieser Name kann ein beliebiger Name sein.
Format	Wählen Sie **PEM aus** **Hinweis:** Privacy Enhanced Mail(PEM)-Dateien sind eine Art von Public Key Infrastructure(PKI)-Datei, die für Schlüssel und Zertifikate verwendet wird. Die Datensätze, die Sie in den vorherigen Schritten erstellt haben, sind von diesem Dateityp.
Typ	Wählen Sie **Trusted Store-Zert**
Kurzbeschreibung	Beschreibung des Zertifikats. Geben Sie einen Wert ein, der Aufschluss darüber gibt, wofür dieses Zertifikat verwendet wird.
PEM-Zertifikat	Fügen Sie die in Schritt 4 kopierten Zertifikatinformationen ein.

8. Wählen Sie **Absenden** aus, um den Datensatz zu speichern.

Erstellen Sie eine geheime Gruppe mit Kriterien

Erstellen Sie eine Gruppe für Ihre Geheimnisse. Geheimnisgruppen, um Ihre Geheimnisse in Gruppen zu organisieren und Zugriffsrichtlinien auf Gruppenebene auf diese Geheimnisse anzuwenden. Ordnen Sie dann Ihre Geheimnisgruppe einer Identitätsgruppe zu, und fügen Sie Ihren MID-Server dieser Identitätsgruppe hinzu.

Vorbereitungen

Erforderliche Rolle: admin, KMF_admin, sn_secrets.secret_manager und sn_kmf.cryptographic_manager

Prozedur

1. Navigieren zu **Alle** > **Geheimnisverwaltung** > **Geheimnisgruppen mit Kriterien**an.
2. Wählen Sie **Neu** aus, um eine **Geheimnisgruppe mit Kriteriendatensatz** zu erstellen.
3. Füllen Sie im Formular die folgenden Felder aus.

Geheimnisgruppe mit Kriterienfeldern

Feld	Wert
Gruppenname	Name der geheimen Gruppe. Dieser Name kann ein beliebiger Name sein.
Geheimnistyp	Wählen Sie **Vom Client zugänglich aus**
Autogen-Modul	Aktivieren Sie das Kontrollkästchen

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
Kurzbeschreibung	Beschreibung der geheimen Gruppe. Geben Sie einen Wert ein, der angibt, wofür diese Gruppe verwendet wird.
Kriteriumstyp	Wählen Sie **Zieltabelle aus**
Zieltabelle	Wählen Sie **die SSH-Anmeldeinformationen [ssh_credentials] aus.**

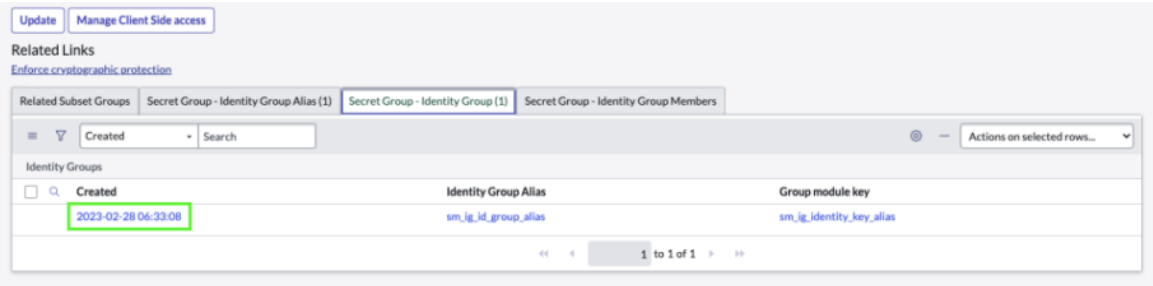
4. Wählen und halten Sie den Formularheader (oder klicken Sie mit der rechten Maustaste darauf), und wählen Sie im Kontextmenü **Speichern** aus, um den Datensatz zu speichern.
5. Stellen Sie sicher, dass das Kontrollkästchen **Aktiv** nicht aktiviert ist.
6. Wählen Sie die Schaltfläche **Clientseitigen Zugriff verwalten** aus, um eine Identitätsgruppe zu erstellen.
   Ein Fenster **„Identitätsgruppenalias“** wird angezeigt.
7. Wählen Sie die Schaltfläche **Neu** aus.
8. Wählen Sie das Referenzsymbol ( ) neben dem Feld **Identitätsgruppenalias** aus.
9. **Geben Sie im Feld Gruppenaliasname** einen Wert ein.
   Dieser Name kann ein beliebiger Wert sein.
10. Wenn Sie in Schritt 9 einen eindeutigen Namen gewählt haben, wählen Sie **Absenden**aus.
11. Wählen Sie die Schaltfläche **Identitätsschlüssel** hochladen aus.
    Das Fenster zum **Importieren des öffentlichen Identitätsschlüsselzertifikats** wird angezeigt.
12. Geben Sie im Feld **Identitätsschlüssel-Alias** einen Wert ein.

> **Wichtig:** Dieser Wert kann beliebig sein, er muss jedoch genau mit dem übereinstimmen, was Sie in den nachfolgenden Schritten in den MID-Server einfügen.

13. Wählen Sie **Importieren aus**
    Das Fenster **Anhang** wird angezeigt.
14. Wählen **Sie Datei wählen aus**.
15. Wählen Sie das öffentliche Zertifikat aus, das Sie in den vorherigen Schritten erstellt haben. Dieses Zertifikat muss die Datei „ `sm_public_cert.pem` “ sein.
16. Wählen Sie das X-Symbol aus, um das Fenster zu schließen.
17. Wählen Sie **OK** aus, um das Fenster **„Identität des öffentlichen Schlüsselzertifikats** importieren“ zu schließen.
    Ein blaues Banner **mit Schlüsseln und Zertifikaten wurde erfolgreich in die Instanz importiert und** bestätigt einen erfolgreichen Import.
18. Wählen Sie **Absenden**.
    Die Liste **Identitätsgruppen wird** angezeigt.
19. Aktivieren Sie das Kontrollkästchen links neben Ihrem Identitätsgruppendatensatz in der Liste.
20. Wählen Sie die Schaltfläche **Geheime Gruppe** zuordnen aus.
    Sie kehren zu Ihrer **geheimen Gruppe mit Kriteriendatensatz** zurück. Die zugehörigen Listen **Geheime Gruppe – Identitätsgruppen-Alias**„“ und **Geheime Gruppe – Identitätsgruppe** sind sichtbar. Diese zugehörigen Listen zeigen die Datensätze an, die Sie in den vorherigen Schritten erstellt haben.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

21. Wählen Sie in der zugehörigen Liste **„Geheimnisgruppe – Identitätsgruppe“** für den Datensatz in dieser Liste das Feld **Erstellt** aus.



Ein **Identitätsgruppen-** Datensatz wird angezeigt.

22. Wählen Sie in der zugehörigen Liste **„Identitätsgruppenmitglieder“** die Schaltfläche **Neu** aus.
Ein Datensatz des **Identitätsgruppenmitglieds wird** angezeigt.
23. Wählen Sie im Feld **MitgliedstabelleMID-Server [ecc_agent] aus**.
24. Wählen Sie das Referenzsymbol ( ) neben dem Feld **„Identitätsgruppenmitgliedsdatensatz“** und anschließend Ihren MID-Server aus.

> **Hinweis:** Wenn Sie das Kontrollkästchen **Alle Datensätze einbeziehen** aktivieren, werden alle mit Ihrer Instanz verbundenen MID-Server der Identitätsgruppe hinzugefügt.

25. Wählen Sie **OK**, um das Fenster **„Dokument** auswählen“ zu schließen.
26. Wählen Sie **Absenden**.
27. Navigieren Sie zurück zu **Alle** > **Geheimnisverwaltung** > **Geheimnisgruppen mit Kriterien**, und öffnen Sie den in Schritt 2 erstellten Datensatz.
28. Aktivieren Sie das Feld **Aktiv**.
29. Wählen Sie **Aktualisieren** aus, um den Datensatz zu speichern.

Laden Sie das öffentliche/private Schlüsselpaar auf den MID-Server hoch

Laden Sie Ihr öffentliches/privates Schlüsselpaar auf Ihren MID-Server hoch. Mit diesem Schlüsselpaar kann der MID-Server Authentifizierungsanforderungen von Ihrer Instanz verarbeiten.

Vorbereitungen

Erforderliche Rolle: keine

Da ServiceNow keinen Zugriff auf den privaten Schlüssel hat, kann er nicht mit dem öffentlichen Schlüssel gekoppelt werden, um den symmetrischen Schlüssel zu entschlüsseln und dann die Anmeldeinformationen zu entschlüsseln. Wenn der MID-Server versucht, diese verschlüsselten Anmeldeinformationen zu verwenden, kann er sie ohne Zugriff auf den privaten Schlüssel nicht für die Authentifizierung entschlüsseln.

In diesen Schritten laden Sie den privaten Schlüssel auf den MID-Server hoch, um den öffentlichen/privaten Schlüsselbund fertig zu stellen. Dieser Upload gewährt den Zugriff auf den MID-Server, ohne ServiceNow Zugriff zu gewähren.

Um dem MID-Server Zugriff auf den privaten Schlüssel zu gewähren, müssen Sie einen Befehl erstellen, der als Administrator in PowerShell ausgeführt werden soll. In diesem Beispiel gilt der Befehl für die virtuelle Azure Windows-Maschine.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:

Stellen Sie sicher, dass das System, auf dem Sie diese Schritte ausführen, Zugriff auf den MID-Server und die Schlüsselpaardatei hat.

Prozedur

1. Suchen Sie in Ihrer lokalen Umgebung den Ordner, in dem Sie Ihr Schlüsselpaar in den Schritten Erstellen Sie Verschlüsselungsschlüssel und Zertifikat erstellt haben.
2. Suchen und kopieren Sie den vollständigen Pfad in die Datei „`manage-certificates.bat`“.

   Hinweis: Diese Datei befindet sich im Ordner Ihres MID Servers. Je nachdem, wo Sie Ihren MID-Server-Ordner gespeichert haben, kann Ihr Pfad wie im folgenden Beispiel aussehen:

   ```
   C:
   \Users\<your_user_account>\Documents\SM_Implementation\mid.utah-07-08-2022__patch4b01-31-2023_02-07-2023_1702.windows.x86-64\sm_ig_MIDS\bin\scripts\manage-certificates.bat
   ```

3. Erstellen Sie eine Textdatei, und fügen Sie den Pfad in die Datei ein.
4. Fügen Sie in der Textdatei nach dem Pfad Folgendes hinzu:
   `-a your_identity_key_alias`

   Ersetzen Sie `your_identity_key_alias` durch den Namen des Identitätsschlüssel-Alias, den Sie beim Hochladen Ihres öffentlichen Zertifikats erstellt haben.
5. Suchen Sie den vollständigen Pfad zu Ihrer Schlüsselpaardatei, und kopieren Sie ihn.

   Hinweis: Wenn Sie die Namen in diesen Schritten verwendet haben, heißt diese Datei `sm_keypair_bundle.pem`.

6. Fügen Sie in Ihrer Textdatei diesen Pfad am Ende der Zeile hinzu, und fügen Sie dabei ein Leerzeichen zwischen diesem Pfad und den vorherigen Informationen hinzu.
   Der Text in Ihrer Textdatei sollte wie im folgenden Beispiel aussehen:

   ```
   C:
   \Users\<your_user_account>\Documents\SM_Implementation\mid.utah-07-08-2022__patch4b01-31-2023_02-07-2023_1702.windows.x86-64\sm_ig_MIDS\bin\scripts\manage-certificates.bat -a your_identity_key_alias
    C:\Users\<your_user_account>\Desktop\sm_keypair_bundle.pem
   ```

   Hinweis: In diesem Beispiel befindet sich die Datei `sm_keypair_bundle.pem` auf dem Desktop, um den Pfad kürzer zu machen.

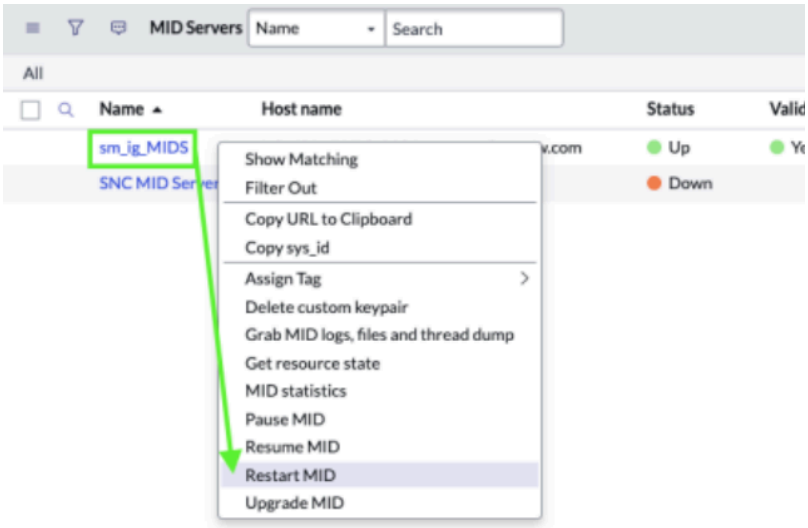
7. Kopieren Sie den gesamten Text Ihrer Textdatei in die Zwischenablage.
8. Suchen Sie auf Ihrem System nach PowerShell, und wählen Sie die Option **Als Administrator** ausführen aus.
9. Fügen Sie den Text aus Ihrer Textdatei in PowerShell ein, und drücken Sie die Eingabetaste.
   Bei Erfolg wird die folgende Meldung angezeigt:

   ```
   Installed certificate with alias: <your_identity_key_alias> into the
    MID keystore.
   ```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tipp: Wenn diese Nachricht nicht angezeigt wird, stellen Sie sicher, dass Ihr Befehl keine Fehler, Leerzeichen oder unnötigen Anführungszeichen enthält. Stellen Sie sicher, dass der vollständige Pfad richtig eingegeben wurde.

10. Starten Sie Ihren MID-Server neu, indem Sie zu Ihrem MID-Server-Datensatz navigieren, mit der rechten Maustaste auf den Datensatz klicken und **MID neu starten**auswählen.



Durch einen Neustart des MID-Servers wird das hochgeladene Schlüsselpaar im MID-Schlüsselspeicher zur Verwendung mit Vorgängen synchronisiert. Warten Sie, **bis** der MID-Server mit dem Status In Betrieb und dem validierten Wert **Ja** neu gestartet wird, bevor Sie fortfahren.

Erstellen Sie Anmeldeinformationen, und testen Sie die Verschlüsselung der Anmeldeinformationen

Erstellen Sie Anmeldeinformationen für die Authentifizierung bei einem Drittparteisystem.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren Sie zur Liste der **SSH-Anmeldeinformationen**, indem Sie im Navigationsfilter `ssh_credentials.list eingeben`.
2. Wählen Sie **Neu** aus, um einen **SSH-Anmeldeinformationsdatensatz** zu erstellen.
3. Füllen Sie im Formular die folgenden Felder aus.

SSH-Anmeldeinformationsformular

Feld	Wert
Name	Geben Sie einen Namen für Ihren Anmeldeinformationsdatensatz ein. Dieser Name kann ein beliebiger Wert sein.
Betrifft	Wählen Sie **Bestimmte MID-Server aus**

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

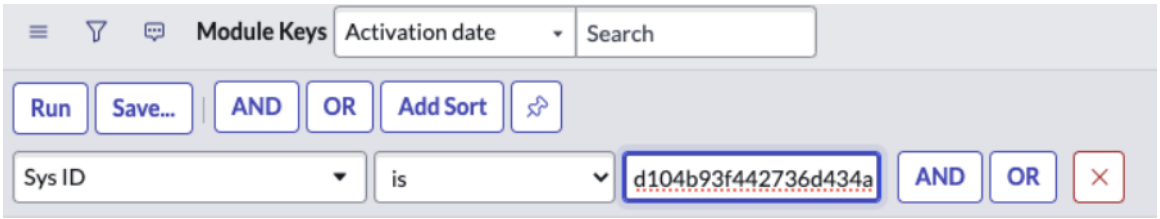
Feld	Wert
MID-Server	Wählen Sie Ihren MID-Server aus.
Anwendername	Geben Sie den Benutzernamen ein.
Passwort	Geben Sie das entsprechende Anwenderpasswort im Feld **Anwendername** ein.

4. Wählen Sie das Sperrsymbol ( ) neben dem Feld **Alias für Anmeldeinformationen**.
5. Wählen Sie das Referenzsymbol ( ), um die Liste der **Aliasse für Verbindungen und Anmeldeinformationen** zu öffnen.
6. Wählen Sie **Neu** aus, um einen **Aliasdatensatz für Verbindungen und Anmeldeinformationen** zu erstellen.
7. Geben Sie einen Namen in das Feld **Name** ein.
8. Wählen Sie **Anmeldeinformationen** im Feld **Typ** aus.
9. Wählen Sie **Absenden**.
   Sie kehren zum Datensatz mit den **SSH-Anmeldeinformationen** zurück. In den nächsten Schritten testen Sie, ob die Anmeldeinformationen verschlüsselt sind.
10. Wählen und halten Sie den Formularheader (oder klicken Sie mit der rechten Maustaste darauf), und wählen Sie **XML anzeigen aus**.
11. Suchen Sie nach<password> XML-Tag in der XML.
12. Kopieren Sie die sys_id in diese<password> Tag in die Zwischenablage.
    Die sys_id ist ein 32-Zeichen-Code, der den symmetrischen Schlüssel darstellt, der zum Verschlüsseln dieser Anmeldeinformationen verwendet wird. Das verschlüsselte Passwort, das Sie in die Tabelle der SSH-Anmeldeinformationen eingegeben haben, befindet sich rechts neben den beiden Kästchen in derselben Zeile.



13. Navigieren Sie zur Liste der `Modulschlüssel, indem Sie im Navigationsfilter sys_kmf_module_key.list eingeben`.
14. Filtern Sie die Liste nach Datensätzen, bei denen das Feld **Sys-ID** mit der sys_id übereinstimmt, die Sie in Schritt 12 kopiert haben, und wählen Sie **Ausführen**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Ihre Suche sollte einen einzelnen **Modulschlüssel** -Datensatz zurückgeben. Dieser Datensatz zeigt, dass Sie erfolgreich einen symmetrischen Schlüssel erstellt haben und verwenden.

15. Navigieren Sie zur Liste Umschlossene **Modulschlüssel,** indem Sie im Navigationsfilter `sys_kmf_wrapped_module_key.list eingeben`.
16. Filtern Sie die Liste nach Datensätzen, bei denen das Feld **Krypto-Modul** mit dem kryptografischen Modul übereinstimmt, das Sie in den vorherigen Schritten erstellt haben, und wählen Sie **Ausführen**.
    Ihre Suche sollte einen einzelnen **umschlossenen Modulschlüssel** -Datensatz zurückgeben. Mit dieser Liste können Sie Folgendes überprüfen:
    - Die Spalte **Wrapped key material** (Umwickeltes Schlüsselmaterial) zeigt, dass der symmetrische Schlüssel im Krypto-Modul (das zum Verschlüsseln der SSH-Anmeldeinformationen verwendet wird) mit dem öffentlichen Schlüssel verschlüsselt wird, den Sie in die Identitätsgruppe hochgeladen haben.
    - Das Feld **Sys-ID** des Wrapping-Schlüssels zeigt an, dass es sich um den Schlüssel (den symmetrischen Krypto-Modulschlüssel) handelt, der von der **Sys-ID des Wrapping-Schlüssels** (dem in die Identitätsgruppe hochgeladenen öffentlichen Schlüssel) verschlüsselt wird.

    Wenn sich die vorhergehenden Felder nicht standardmäßig in Ihrer Liste befinden, können Sie sie der Liste hinzufügen, indem Sie das Symbol Liste **personalisieren** (Liste personalisieren) wählen.

> **Hinweis:** Ihre Instanz von führt alle 10 Minuten eine Bereinigungsaufgabe aus, die verwaiste Schlüssel entfernt und die Weitergabe nicht zugeordneter Schlüssel verhindert, nachdem Sie Ihre Anmeldeinformationen aktualisiert haben.

Konfigurieren Sie Flow Designer, um die Integration zu verwalten

Verwenden Sie in Ihrer -Instanz Flow Designer, um eine Integration zwischen Ihrem lokalen Netzwerk und Ihrer -Instanz zu verwalten.

Vorbereitungen

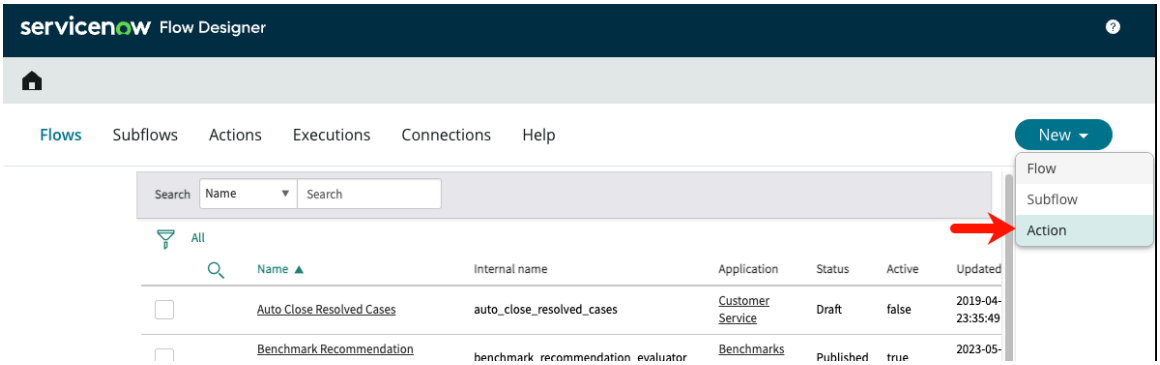
Erforderliche Rolle: admin

In diesen Schritten erstellen Sie einen Workflow Flow Designer, um eine Textdatei auf Ihrem lokalen System zu erstellen.

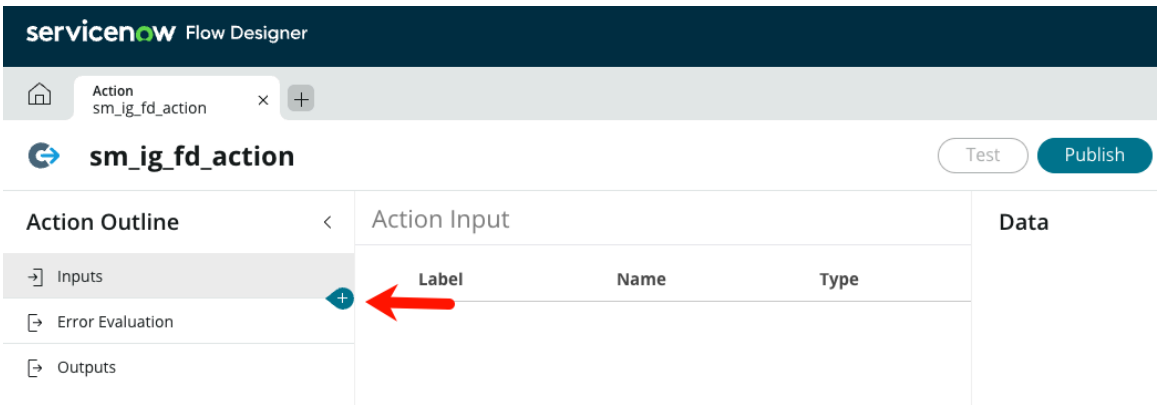
Prozedur

1. Navigieren Sie in Ihrer -Instanz zu **Alle** > **Prozessautomatisierung** > **Flow Designer**an.
2. Erstellen Sie eine Aktion in ServiceNow, indem Sie **Neu** und dann **Aktion**wählen.

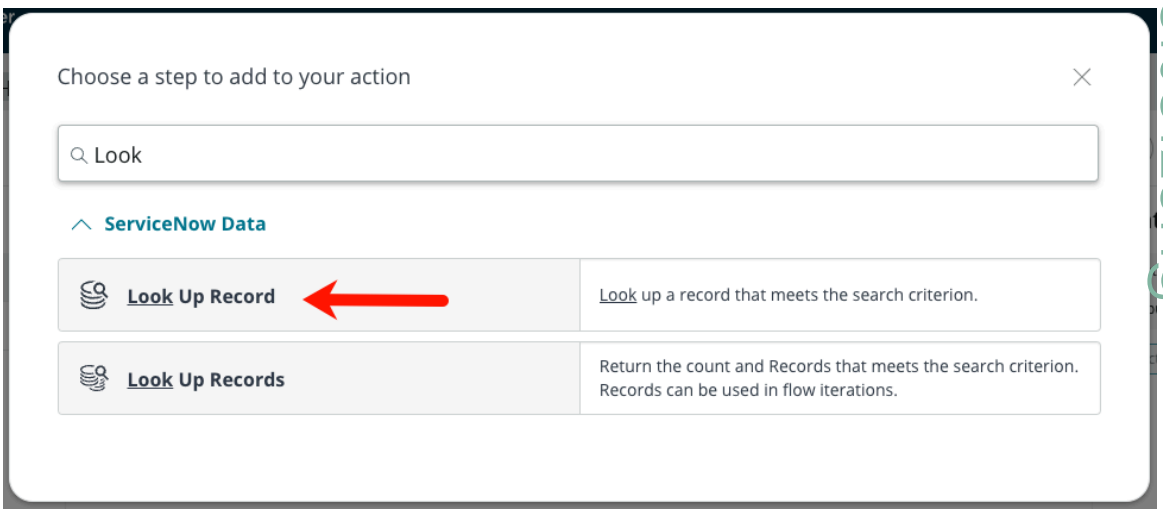
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Geben Sie im Feld **Aktionsname einen Namen** ein, und wählen Sie **Absenden**aus.
4. Erstellen Sie einen Schritt, indem Sie in der **Aktionsgliederung** das Pluszeichen zwischen **Eingaben** und **Fehlerauswertung**wählen.



5. **Wählen Sie im Fenster Schritt zum Hinzufügen zu Ihrer Aktion** auswählen die **Option Datensatz suchen aus**.



6. Wählen Sie im Abschnitt „Datensatz suchen“ im Feld **Tabelle** die **Option MID-Server [ecc_agent]aus**.
7. Erstellen Sie einen weiteren Schritt, indem Sie das Pluszeichen unter dem **Schritt „Datensatz suchen“**auswählen.
8. **Wählen Sie im Fenster Einen Schritt auswählen, der Ihrer Aktion hinzugefügt werden** soll **SSH**aus.

Automatische Übersetzung

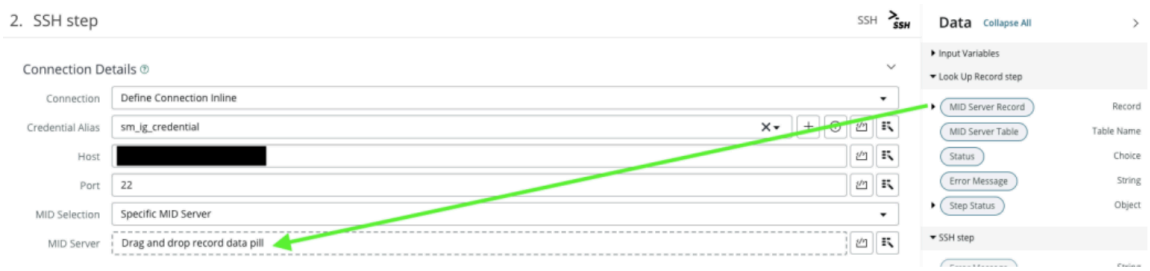
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn die Option „ **SSH** “ nicht angezeigt wird, müssen Sie das erforderliche Plugin aktivieren.

9. Geben Sie im Abschnitt „ **SSH-Schritt** “ die folgenden Informationen ein:

Feld	Wert
Verbindung	Wählen **Sie Verbindung inline definieren aus**
Anmeldeinformationsalias	Wählen Sie den Anmeldeinformationsalias für die SSH-Anmeldeinformationen aus, der in den vorherigen Schritten erstellt wurde.
Host	Geben Sie die IP-Adresse für den Host ein, zu dem Sie über SSH eine Verbindung herstellen.
Port	Geben Sie `22 ein.`
MID-Auswahl	Wählen Sie **Spezifischer MID-Server aus**.

10. Um das Feld „ **MID-Server** “ auszufüllen, ziehen Sie die Pille „ **MID-Server-Datensatz** “ aus dem Abschnitt „ **Daten** “ in das Feld.



Warnung: Wählen Sie beim Ziehen der Pille in das Feld die Pille und nicht den schwarzen Pfeil neben der Pille aus.

11. Geben Sie im Abschnitt **SSH-Konfiguration** im Feld **Befehl** den folgenden Wert ein.

```
/bin/date > sm_ig_text_file.txt
```

Dieser Befehl erstellt eine Textdatei in Ihrem lokalen System unter Verwendung der entschlüsselten Geheimnisse des MID-Servers. Der MID Server gewährt Zugriff auf die Instanz ServiceNow (über Flow Designer), ohne der Instanz ServiceNow Zugriff auf das entschlüsselte Geheimnis zu gewähren.

Tipp: Mit dem Befehl „ `/bin/date` “ werden das aktuelle Datum/die aktuelle Uhrzeit in die erstellte Textdatei eingefügt. Dieser Befehl demonstriert, dass die Integration in Echtzeit basierend auf dem aktuellen Datum/der aktuellen Uhrzeit im Vergleich zum Zeitpunkt der Erstellung der Textdatei erfolgt.

12. Wählen Sie die Schaltfläche **Speichern**, um den Workflow zu speichern.

Testet die Client-seitige End-to-End-Integration für verschlüsselte Geheimnisse

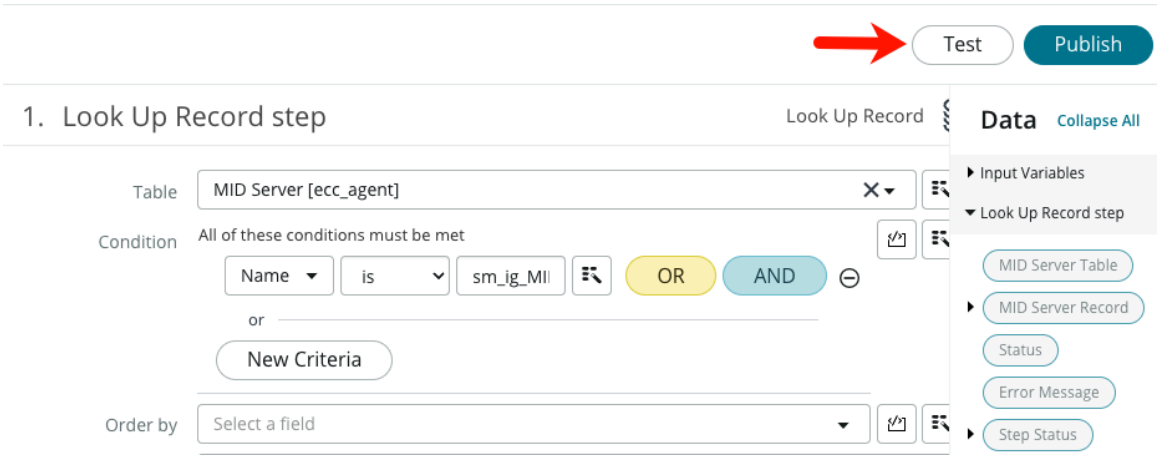
Testen Sie Ihre Integration und überprüfen Sie die Ausführungsdetails, um zu bestätigen, dass Ihre Konfiguration funktioniert.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Wählen Sie in Flow Designer die Schaltfläche **Test** in der oberen rechten Ecke des Bildschirms.



2. **Wählen** Sie im Fenster Testaktion die **Option Test ausführen**aus.
3. Wählen Sie **aus. Die Ausführung des Tests wurde abgeschlossen. Zeigen Sie die Details der Aktionsausführung an.**
4. Aktualisieren Sie Ihren Bildschirm, bis Sie **Testlauf – Abgeschlossen** oben rechts im Bildschirm sehen.
5. Wählen Sie den Pfeil **Schritte** unten links im Bildschirm.
6. Scrollen Sie nach unten, bis Sie die Überschrift **Schrittausgabedaten** mit der folgenden Erfolgsmeldung sehen:

```
{"Step Status";{"code";0,"message";"Success"}}
```

7. Nachdem Sie diese Nachricht in Flow Designerangezeigt haben, vergewissern Sie sich, dass die Textdatei im lokalen System erstellt wurde.

Testen Sie mit der Geheimnisverwaltung verschlüsselte Anmeldeinformationen für die Windows-Verwaltungsinstrumentation

Stellen Sie sicher, dass Ihre Anmeldeinformationen für Windows Management Instrumentation (WMI) mit der Geheimnisverwaltung verschlüsselt sind, und verwenden Sie einen Integration Hub-Workflow, um End-to-End-Tests durchzuführen.

Vorbereitungen
Erforderliche Rolle: admin

- Integration Hub Enterprise muss in Ihrer Instanz aktiv sein. Details finden Sie unter Fordern Sie ein IntegrationHub -Plugin an .
- Sie müssen über eine konfigurierte Geheimnisgruppe in Ihrer -Instanz verfügen. Siehe Schritte 1 bis 3 in Für den Client zugängliche Geheimnisse konfigurieren.
- Sie müssen über konfigurierte Anmeldeinformationen verfügen, die mit der Geheimnisverwaltung verschlüsselt sind. Siehe Schritte 1 bis 9 in Erstellen Sie Anmeldeinformationen, und testen Sie die Verschlüsselung der Anmeldeinformationen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

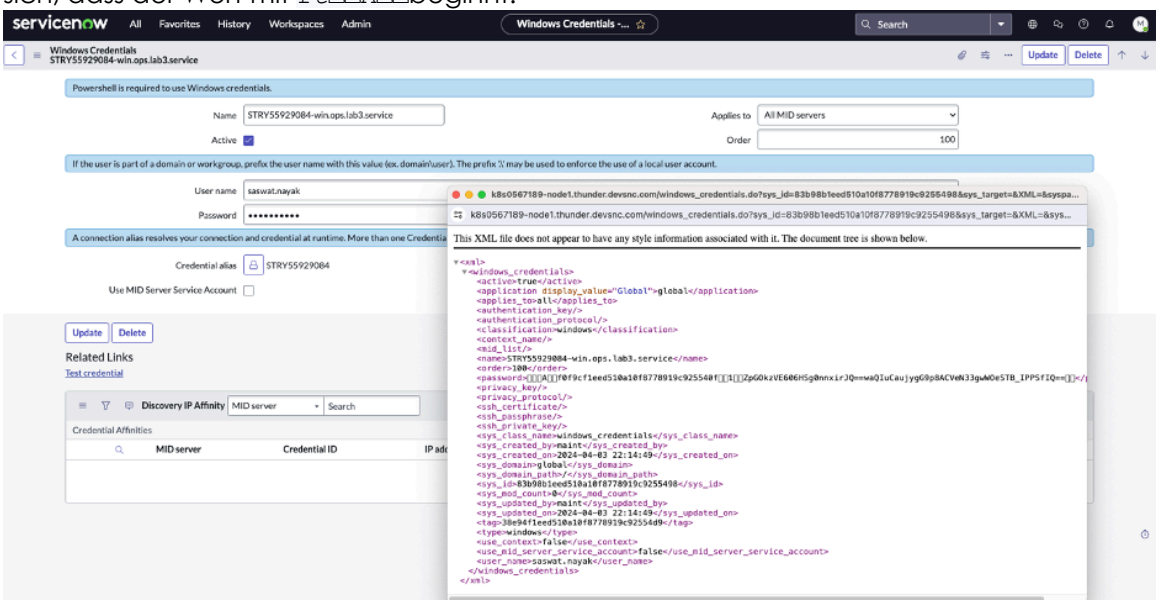
1. Bestätigen Sie, dass der gewünschte MID-Server der geheimen Gruppe zugeordnet ist. Öffnen Sie den Datensatz „Geheime Gruppe mit Kriterien“ [sn_sm_criteria_secret_group], und suchen Sie in der Liste **„Geheime Gruppe – Identitätsgruppenmitglieder“** nach Ihrem MID-Server. Wenn Ihr MID-Server keiner Gruppe zugeordnet ist, lesen Sie Erstellen Sie eine geheime Gruppe mit Kriterien.
2. Vergewissern Sie sich, dass die Anmeldeinformationen mit der Geheimnisverwaltung verschlüsselt sind.

   a. Navigieren zu **Alle** > **IntegrationHub** > **Verbindungen und Anmeldeinformationen** > **Anmeldeinformationen**an.

   b. Öffnen Sie Ihren Anmeldeinformationsdatensatz.
   Vergewissern Sie sich, dass im Feld „ **Alias** für Anmeldeinformationen“ ein Anmeldeinformationsalias aufgeführt ist. Wenn Sie noch keinen erstellt haben, lesen Sie Verbindungs- und Anmeldealias erstellen.

   c. Wählen und halten Sie den Header Ihres Anmeldeinformationsdatensatzes (oder klicken Sie mit der rechten Maustaste darauf), und wählen Sie **XML anzeigen** aus der Liste aus.

   d. Suchen Sie in der XML-Ansicht des Datensatzes nach dem Passwort, und vergewissern Sie sich, dass der Wert mit `rt□□A□□`beginnt.



3. Erstellt einen Test-Workflow in Workflow-Studio.

   a. Navigieren zu **Alle** > **Prozessautomatisierung** > **Workflow-Studio**an.

   b. Wählen Sie **Neu**und anschließend **Aktion** aus der Liste aus.

   c. Geben Sie einen Namen in das Feld **Aktionsname** ein.
   Belassen Sie das Feld **Anwendung** auf Global.

   d. Wählen Sie die Schaltfläche **Build-Aktion** aus.

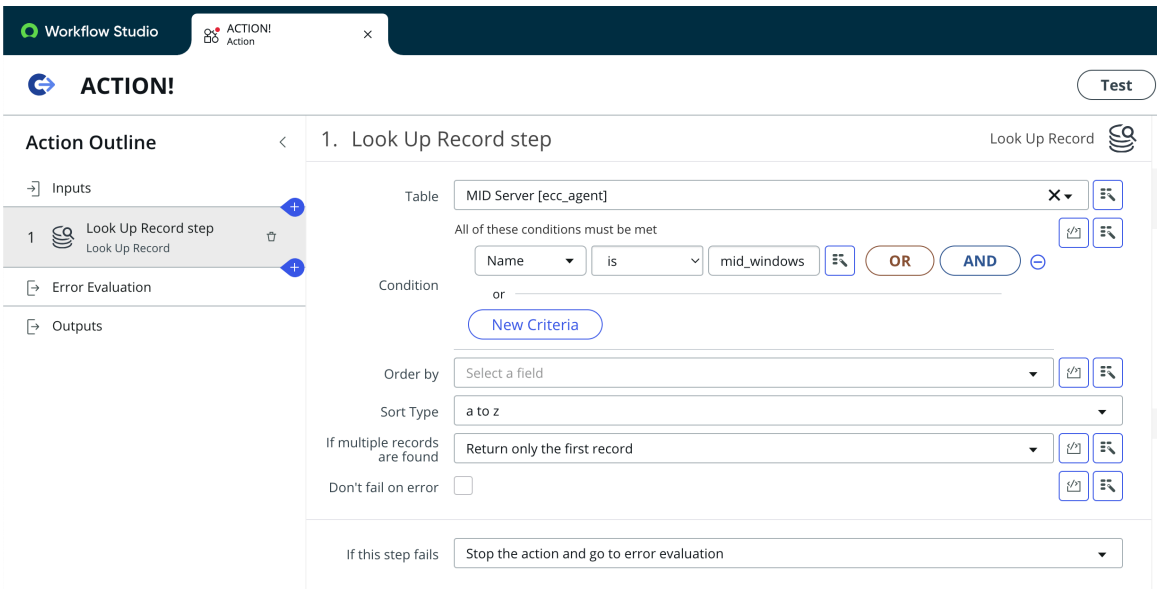
4. Konfigurieren Sie einen Datensatzsuchschritt in Workflow-Studio.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie in der **Aktionsgliederung**die Plus-Schaltfläche aus, um einen neuen Schritt hinzuzufügen.
Suchen und wählen Sie den Schritttyp **„Datensatz** nachschlagen“ aus.

b. Wählen Sie im Feld **Tabelle** die **Option MID-Server [ecc_agent] aus**.

c. Wählen Sie als Bedingung **Name ist**, gefolgt vom Namen Ihres MID-Servers.



Wichtig: Stellen Sie sicher, dass der ausgewählte MID-Server mit dem der geheimen Gruppe zugeordneten übereinstimmt.

5. Konfigurieren Sie einen Datensatzsuchschritt in Workflow-Studio.

a. Wählen Sie in der **Aktionsgliederung**die Plus-Schaltfläche aus, um einen neuen Schritt unter dem Schritt „Datensatz suchen“ hinzuzufügen.
Suchen Sie den Schritttyp **PowerShell**, und wählen Sie ihn aus.

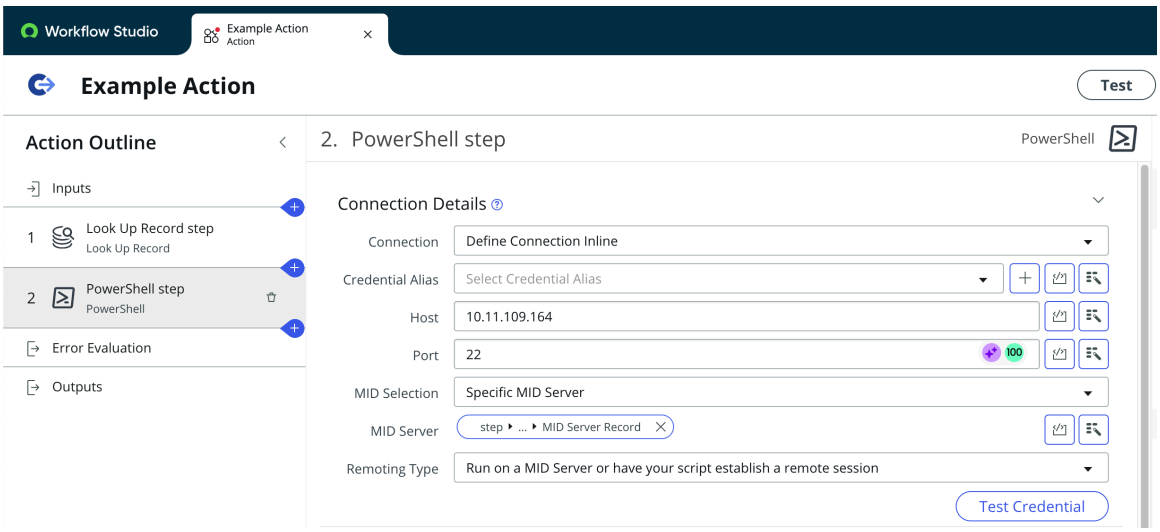
b. Füllen Sie im Formular **„PowerShell-Schritt** “ die Felder nach Bedarf aus.

PowerShell-Schrittfelder

Feld	Wert
Verbindung	Wählen **Sie Verbindung inline definieren aus**
Anmeldeinformationsalias	Wählen Sie Ihren Anmeldeinformationsalias aus
Host	Geben Sie die IP-Adresse des Windows-Zielservers ein
Port	Geben Sie `22` ein, wenn dies nicht bereits der Standard ist.
MID-Auswahl	Wählen Sie **Spezifischer MID Server** aus.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
MID-Server	Ziehen Sie die Pille **MID-Server-Datensatz** aus dem **Datenbereich** Diese Datenpille wird im **Datenbereich** am rechten Rand des Bildschirms unter dem **Schritt „Datensatz suchen“**angezeigt.
Remotingtyp	Wählen **Sie Auf MID-Server ausführen aus, oder lassen Sie Ihr Skript eine Remotesitzung einrichten**



6. Erstellen Sie ein Skript für Ihre Testaktion.

   a. **Wählen** Sie im Feld Skripttyp die **Option Inline-Skript**aus.

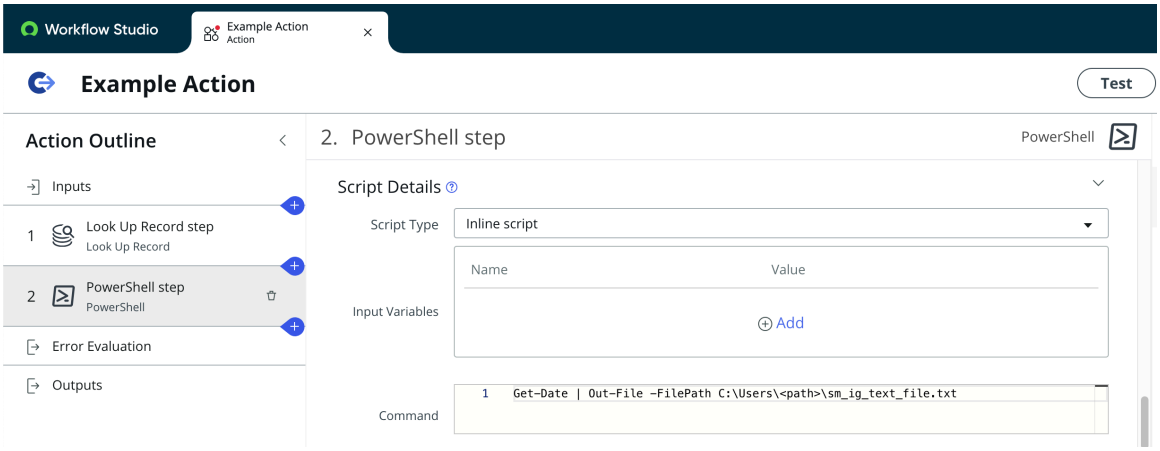
   b. Verwenden Sie das folgende Skript, und ersetzen Sie dabei den Beispielpfad durch den Pfad Ihres Testhosts.

```
Get-Date | Out-File -FilePath C:\Users\<path>\sm_ig_text_file.txt
```

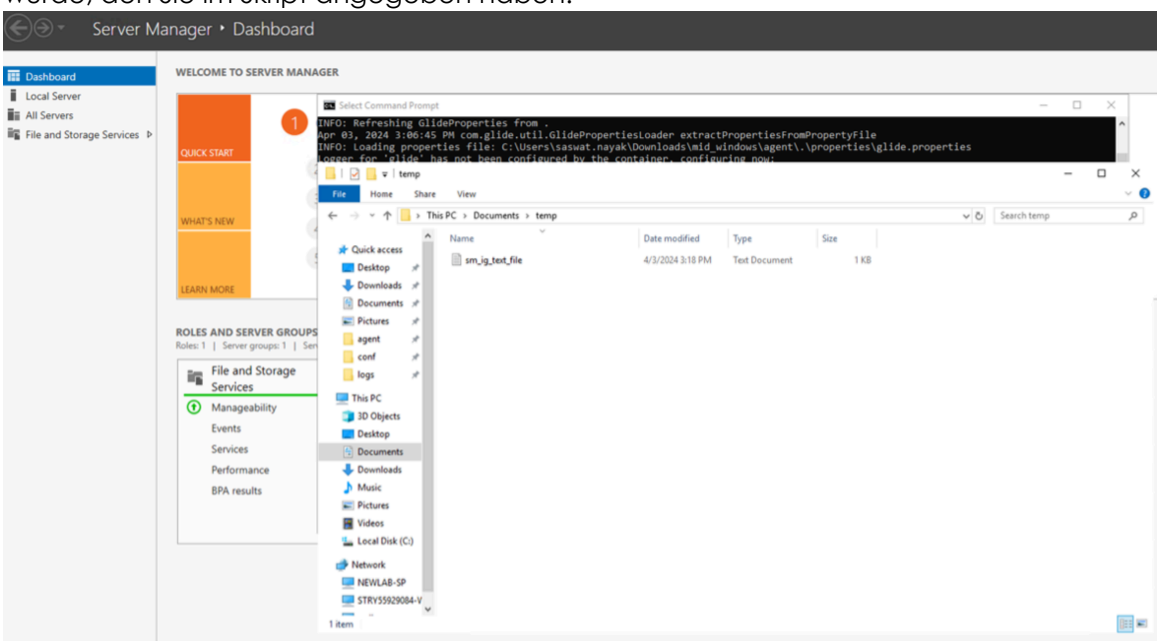
   Hinweis: Sie können auch ein eigenes Skript ausführen, das für Ihre Remote-Hostkonfiguration geeignet ist. Es ist wichtig zu bestätigen, dass eine Verbindung mit dem SM-verschlüsselten Wert hergestellt wurde.

   c. Wählen Sie die Schaltfläche **Speichern**, um Ihre Aktion zu speichern.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Wählen Sie die Schaltfläche **Test** aus, um Ihre Aktion zu testen.
8. Überprüfen Sie die Ausgabeprotokolle auf Fehlermeldungen.
9. Vergewissern Sie sich, dass auf dem Hostserver eine Testdatei in dem Dateipfad erstellt wurde, den Sie im Skript angegeben haben.



Klonen und Geheimnisverwaltung

Erfahren Sie, wie Sie Geheimnisgruppen und Client-Geheimnisgruppen nach einem Klon neu konfigurieren.

Nachdem Sie eine Instanz geklont haben, müssen Ihre Geheimnisgruppen und Clientgeheimnisgruppen möglicherweise neu konfiguriert werden, damit sie wie erwartet funktionieren.

Ursprung der Geheimnisgruppe	Verhalten nach einem Klon
Ursprüngliche Instanz: Geheimnisgruppen aus der Zielinstanz	Funktioniert wie erwartet nach dem manuellen Import des fehlenden kryptografischen Moduls. Weitere Informationen finden Sie unter Exportieren und Importieren von Daten über XML .

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ursprung der Geheimnisgruppe	Verhalten nach einem Klon
Ursprüngliche geheime Clientgruppen aus der Zielinstanz	Funktioniert wie erwartet nach dem manuellen Import des fehlenden kryptografischen Moduls. Weitere Informationen finden Sie unter Exportieren und Importieren von Daten über XML .
Geklonte Instanz schlüsselt Gruppen aus der Quellinstanz auf	Funktioniert nur bei manueller Einrichtung
Geklonte geheime Clientschlüsselgruppen aus der Quellinstanz	Arbeiten Sie, wenn Sie „sg/identity group/ alias/mid“ manuell konfigurieren

Dashboard für die Geheimnisverwaltung

Verwenden Sie das Geheimnisverwaltungs-Dashboard, um die in Ihrer Instanz konfigurierten geheimen Gruppen zu überprüfen und sich über Sicherheitsprobleme zu informieren.

Geheime Gruppenübersicht



Auf der Registerkarte **„Geheimnisgruppenübersicht“** werden Informationen zu Ihren konfigurierten Geheimnisgruppen angezeigt. Verwenden Sie diese Registerkarte, um Informationen zu den in Ihrer Instanz konfigurierten Geheimnisgruppen anzuzeigen.

Geheime Gruppe nach Typ

Zeigt ein Kreisdiagramm mit den auf Ihrer Instanz installierten geheimen Gruppen an, gruppiert nach Geheimnistyp (Instanzseite oder Clientseite).

Geheime Gruppe nach Kriteriumstyp

Zeigt ein Kreisdiagramm mit geheimen Gruppen mit Kriterien an, die in Ihrer Instanz nach dem Typ der verwendeten Kriterien konfiguriert sind.

Anzahl der inaktiven Geheimnisgruppen

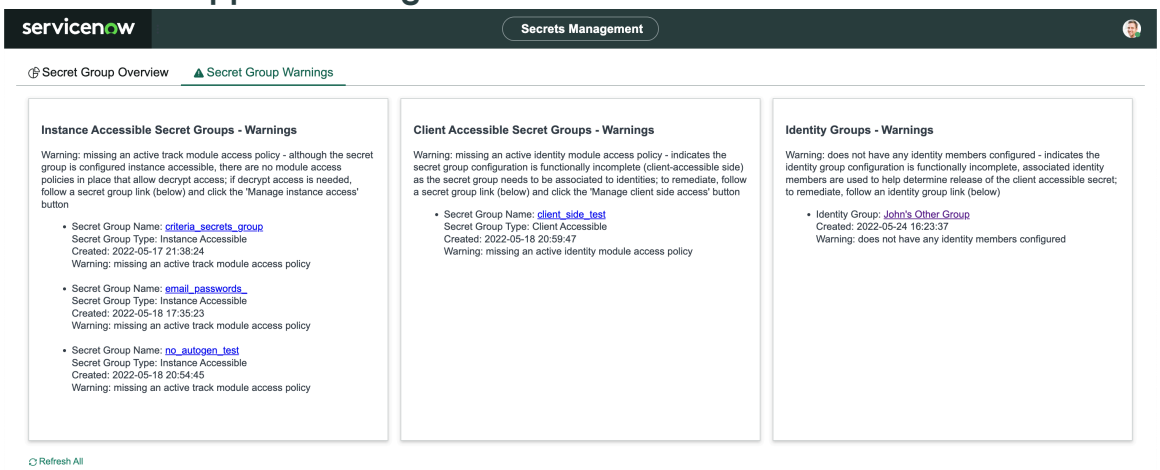
Zeigt die Anzahl der inaktiven geheimen Gruppen an, die in Ihrer -Instanz konfiguriert sind.

Anzahl der dedizierten Geheimnisse.

Zeigt eine Anzahl von Geheimnissen innerhalb von Basisgeheimnisgruppen an.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geheime Gruppenwarnungen



Auf der Registerkarte Warnungen zu geheimen **Gruppen** werden Warnungen im Zusammenhang mit Ihren geheimen Gruppen und Identitätsgruppen angezeigt.

Geheime Gruppen mit Instanzzugriff – Warnungen

Diese Karte zeigt Warnungen an, wenn geheime Gruppen ohne aktive Zugriffsrichtlinien vorhanden sind. Wählen Sie den Namen einer geheimen Gruppe aus, um diesen Datensatz anzuzeigen.

Für Client zugängliche geheime Gruppen – Warnungen

Diese Karte zeigt Warnungen an, wenn geheime Gruppen, auf die der Client zugreifen kann, keine aktive Identitätsmodul-Zugriffsrichtlinie (Identity Module Access Policy, MAP) haben. Wählen Sie den Namen einer geheimen Gruppe aus, um diesen Datensatz anzuzeigen.

Identitätsgruppen – Warnungen

Diese Karte zeigt Warnungen an, wenn Identitätsgruppen vorhanden sind, für die keine Gruppenmitglieder konfiguriert sind. Wählen Sie den Namen der Identitätsgruppe aus, um den Datensatz anzuzeigen.

Hinweis: Das Geheimnisverwaltungs-Dashboard ist ein Teil von Geheimnisverwaltung Enterprise. Secrets Management Enterprise ist ein kostenpflichtiges Plugin, das die Mitarbeiter von ServiceNow in Ihrer Produktionsinstanz aktivieren müssen.

Geheimnisverwaltungsrollen

Die Geheimnisverwaltung fügt diese Rollen hinzu.

Geheimnisadministrator [sn_secrets.admin]

Weisen Sie anderen Anwendern die Rolle eines Nicht-Administratorgeheimnisses zu. Geheimnisadministratoren verfügen über dieselben Berechtigungen wie Geheimnismanager und -betrachter.

Enthält die Rollen

Liste der Rollen, die in der Rolle enthalten sind.

Keine.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Keine.

Besondere Überlegungen

Wichtig: Vermeiden Sie das Gewähren einer Administratorrolle, wenn spezialisiertere Rollen verfügbar sind.

- Ein Benutzer muss über die Rollen admin und security_admin verfügen, um die Rolle sn_secret.admin zuzuweisen.
- Vermeiden Sie das Gewähren einer Administratorrolle, wenn gezieltere Rollen verfügbar sind.

Geheimnismanager [sn_secrets.manager]

Gewähren Sie diese Rolle Anwendern, die eine der folgenden Funktionen ausführen müssen.

- Zeigen Sie die Datensätze für Geheimnisse und geheime Gruppen an
- Zeigen Sie den Zugriffsverlauf und andere Informationen zu Nutzungsaktivitäten an
- Erstellen Sie geheime Gruppen und Filter
- Erstellen Sie einen Geheimnisanbieter
- Verschieben Sie Geheimnisse zwischen Geheimnisgruppen
- Ändern Sie die Einstellungen für die geheime Gruppe und den geheimen Provider

Enthält die Rollen

Liste der Rollen, die in der Rolle enthalten sind.

Keine.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Besondere Überlegungen

Wichtig: Geheimnismanager können Geheimnisse nicht im Nur-Text-Format anzeigen.

Geheimnisbetrachter [sn_secrets.viewer]

Gewähren Sie diese Rolle Anwendern, die in der Lage sein müssen, geheime und geheime Gruppendatensätze anzuzeigen.

Enthält die Rollen

Liste der Rollen, die in der Rolle enthalten sind.

Keine.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Besondere Überlegungen

Keine.

Erstellen Sie ein kryptografisches Modul für eine geheime Gruppe

Erstellen Sie ein kryptografisches Modul für eine geheime Gruppe, um die Verschlüsselung und Entschlüsselung durchzuführen.

Vorbereitungen

Erforderliche Rolle:

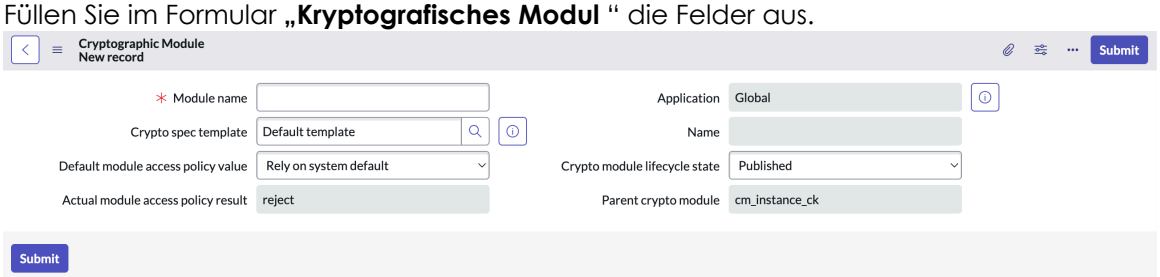
- Administrator
- sn_secrets.admin
- sn_secrets.secret_manager
- sn_kmf.cryptographic_manager
- sn_kmf.admin

Prozedur

1. Navigieren zu **Alle** > **Geheimnisverwaltung** > **Krypto-Modul für geheime Gruppe erstellen**an.
2. Wählen Sie den Typ des Gruppen-Krypto-Moduls aus, das Sie erstellen möchten.

Kryptografischer Modultyp	Beschreibung
Ein über die Instanz zugängliches Geheimnis-Krypto-Modul erstellen	Erstellen Sie über die Instanz zugängliche Geheimnisse, die von Ihrer Instanz entschlüsselt werden können.
Ein für den Client zugängliches Geheimnis-Krypto-Modul erstellt	Erstellen Sie für den Client zugängliche Geheimnisse, die mit Ihrem eigenen Schlüssel verschlüsselt sind und auf die ServiceNow nicht zugreifen kann.

3. Füllen Sie im Formular **„Kryptografisches Modul** “ die Felder aus.



Feld	Beschreibung
Modulname	Beschreibender Name für Ihr Modul
Anwendung	Der Anwendungsbereich, der das Modul enthält. Dieses Feld wird automatisch mit dem aktuellen Modul gefüllt.
Krypto-Spezifikationsvorlage	**Standardvorlage** ist standardmäßig ausgewählt.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Name des Moduls Dieser Name wird von basierend auf der Anwendung und dem Modulnamen automatisch generiert.
Standardwert der Modulzugriffsrichtlinie	◦ Systemvorgabe verwenden ◦ Ablehnen ◦ Titel
Lebenszyklusstatus kryptografisches Modul	Gibt an, ob sich das Modul im Status **Entwurf** oder **Veröffentlicht** befindet.
Tatsächliches Ergebnis der Modulzugriffsrichtlinie	Dieses Feld dient zur Information und ist schreibgeschützt.
Übergeordnetes kryptografisches Modul	Das übergeordnete kryptografische Modul, das durch den Typ des kryptografischen Moduls bestimmt wird, den Sie im vorherigen Schritt ausgewählt haben. Dieses Feld ist schreibgeschützt.

4. Wählen Sie **Absenden**.

Erstellen Sie eine einfache geheime Gruppe

Erstellen Sie eine geheime Standardgruppe, um beliebige Geheimnisse unabhängig von ihren Kriterien zu gruppieren.

Vorbereitungen

Erforderliche Rolle: admin

Grundlegende Geheimnisgruppen können jedes Geheimnis enthalten, das Sie ihnen hinzufügen, unabhängig von Tabelle, Umfang oder Anwendung. Nach dem Erstellen fügen Sie der Gruppe manuell Geheimnisse hinzu. Um eine Gruppe speziell für alle Geheimnisse zu erstellen, die ein gemeinsames Attribut gemeinsam haben, erstellen Sie eine Geheimnisgruppe mit Kriterien anhand der Anweisungen in Erstellen Sie eine geheime Gruppe mit Kriterien.

Prozedur

1. Navigieren zu **Alle** > **Geheimnisverwaltung** > **Geheimnisgruppen**an.
2. Wählen Sie **Neu**.
3. Im **Feld Welche Art von geheimer Gruppe möchten Sie erstellen?** wählen Sie **Grundlegende geheime Gruppe**aus.
4. Füllen Sie die Felder im Formular **„Geheimnisgruppe“** aus.

Geheime Gruppenfelder

Feld	Beschreibung
Gruppenname	Name für die Gruppe

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Namen von Geheimnisgruppen dürfen nur Kleinbuchstaben, Zahlen und Unterstriche (_) enthalten.
Geheimnistyp	Gibt an, ob die Gruppe über die **Instanz** oder den **Client zugänglich**ist.
Autogen-Modul	Generiert ein neues kryptografisches Modul für diese geheime Gruppe. Dieses Modul verschlüsselt und entschlüsselt Ihre Daten. Dieses Feld ist standardmäßig aktiviert.
Anwendung	Die bereichsbezogene Anwendung für diesen Datensatz. Dieses schreibgeschützte Feld wird automatisch mit dem aktuellen Umfang ausgefüllt.
Kurzbeschreibung	Beschreibung der Gruppe
Krypto-Modul	Wählen Sie das kryptografische Modul aus, das mit dieser Gruppe verwendet werden soll. Dieses Modul verschlüsselt und entschlüsselt Ihre Daten. Dieses Feld ist nur sichtbar, wenn **Autogen-Modul** nicht ausgewählt ist. Weitere Informationen zu Modulzugriffsrichtlinien finden Sie unter Übersicht über Modulzugriffsrichtlinien **Hinweis:** Sie können die Modulzugriffsrichtlinien für Ihre geheime Gruppe über die Schaltfläche **Instanzzugriff verwalten** überprüfen.

5. Klicken Sie auf **Absenden**.

Hinweis: Geheime Gruppen sind standardmäßig deaktiviert, wenn sie erstellt werden. Kehren Sie zum Gruppendatensatz zurück, und wählen Sie **Aktiv**, um die Gruppe zu aktivieren.

Erstellen Sie eine geheime Gruppe mit Kriterien

Erstellen Sie eine Geheimnisgruppe mit Kriterien, um in Password2-Felder eingegebene Geheimnisse automatisch zu organisieren, wenn sie ein gemeinsames Kriterium gemeinsam nutzen, z. B. Tabelle, Umfang oder Anwendung.

Vorbereitungen

Erforderliche Rolle: admin

Geheimnisse innerhalb dieses Typs von Geheimnisgruppen müssen gemeinsame Kriterien aufweisen. Für Gruppen ohne diese Einschränkung empfiehlt es sich, eine einfache geheime Gruppe zu erstellen. Erfahren Sie, wie Sie eine geheime Standardgruppe in Erstellen Sie eine einfache geheime Gruppeerstellen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Geheimnisverwaltung** > **Geheimnisgruppen**an.
2. Wählen Sie **Neu**.
3. Im **Feld Welche Art von geheimer Gruppe möchten Sie erstellen?** prompr, wählen Sie **Geheime Gruppe mit Kriterien**aus.
4. Füllen Sie die Felder im Formular **„Geheimnisgruppe“** aus.

Geheime Gruppenfelder

Feld	Beschreibung
Gruppenname	Name für die Gruppe **Hinweis:** Namen von Geheimnisgruppen dürfen nur Kleinbuchstaben, Zahlen und Unterstriche (_) enthalten.
Geheimnistyp	Gibt an, ob die Gruppe über die **Instanz** oder den **Client zugänglich ist.**
Autogen-Modul	Generiert ein neues kryptografisches Modul für diese geheime Gruppe. Dieses Modul verschlüsselt und entschlüsselt Ihre Daten. Dieses Feld ist standardmäßig aktiviert.
Anwendung	Die bereichsbezogene Anwendung für diesen Datensatz. Dieses schreibgeschützte Feld wird automatisch mit dem aktuellen Umfang ausgefüllt.
Kurzbeschreibung	Beschreibung der Gruppe
Kriteriumstyp	Die Kriterien, die die Geheimnisse in dieser Gruppe gemeinsam nutzen. ◦ Umfang ◦ Paket ◦ Zieltabelle ◦ Geheime Spalte ◦ Filterdatensatz
Krypto-Modul	Wählen Sie das kryptografische Modul aus, das mit dieser Gruppe verwendet werden soll. Dieses Modul verschlüsselt und entschlüsselt Ihre Daten. Dieses Feld ist nur sichtbar, wenn **Autogen-Modul** nicht ausgewählt ist. Weitere Informationen zu Modulzugriffsrichtlinien finden Sie unter Übersicht über Modulzugriffsrichtlinien

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Sie können die Modulzugriffsrichtlinien für Ihre geheime Gruppe über die Schaltfläche **Instanzzugriff verwalten** überprüfen.

Hinweis: Je nach Konfiguration verwendet das **Krypto-Modul** möglicherweise einen automatisch ausgewählten Wert.

Wenn das Feld **Kriteriumstyp** auf `Paket`festgelegt und das Feld **Autogen-Modul** ausgewählt ist:	Das Feld **„Krypto-Modul** " ist leer und schreibgeschützt. Ein vorhandenes Password2-Submodul wird verwendet. Wenn kein Password2-Submodul gefunden wird, wird das Glide Encrypter-Modul auf Instanzebene verwendet.
Wenn das Feld **Kriteriumstyp** auf `Paket`festgelegt und das Feld **Autogen-Modul deaktiviert** ist: (Das Feld **Autogen-Modul** kann nur von Enterprise-Benutzern deaktiviert werden.)	Das Feld **Krypto-Modul** kann bearbeitet werden, und Administratoren können ein zu verwendendes Krypto-Modul auswählen.

5. Drücken und halten Sie den Formularheader (oder klicken Sie mit der rechten Maustaste darauf), und wählen Sie **Speichern**.

   Hinweis: Geheime Gruppen sind standardmäßig deaktiviert, wenn sie erstellt werden.

6. Nach dem Speichern des Datensatzes werden je nachdem, wie Sie Ihre Gruppe konfiguriert haben, möglicherweise zusätzliche Felder angezeigt.

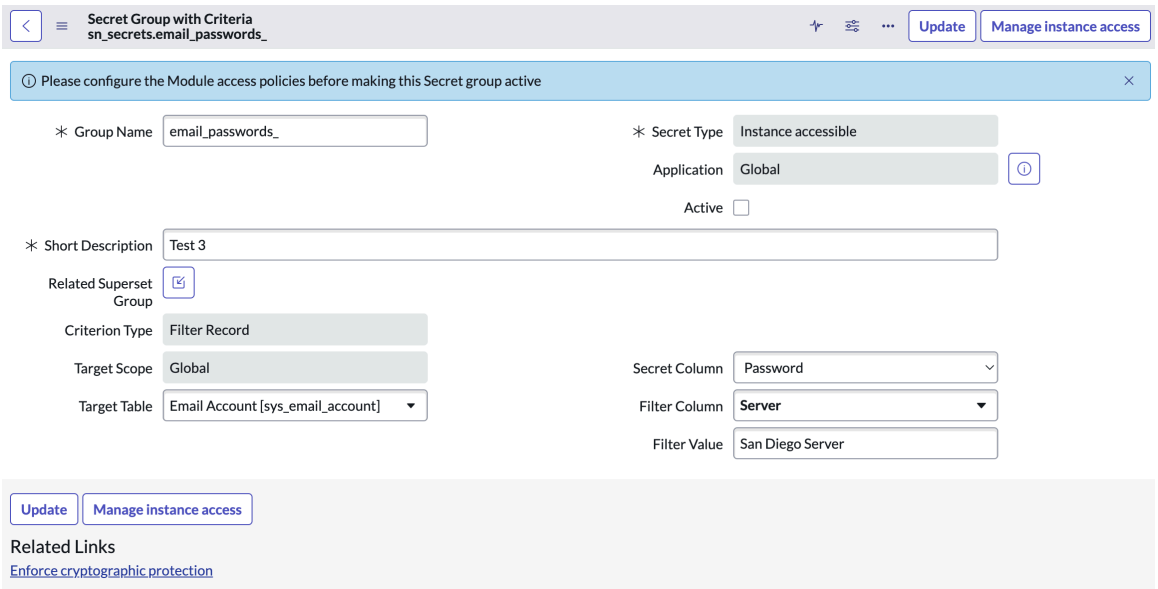
Zusätzliche geheime Gruppenfelder

Feld	Beschreibung
Zielbereich	Von den Geheimnissen gemeinsam genutzter Bereich, die dieser Gruppe zugewiesen werden sollen. Dieses Feld ist nur verfügbar, wenn Sie im Feld **Kriterientyp** die Option `Umfang` auswählen.
Zielpaket	Paket, das von den Geheimnissen geteilt wird, die dieser Gruppe zugewiesen werden sollen. Dieses Feld ist nur verfügbar, wenn Sie `Paket` im Feld **Kriterientyp** auswählen.
Zieltabelle	Tabelle, die von den Geheimnissen gemeinsam verwendet wird, die dieser Gruppe zugewiesen werden sollen. Dieses Feld ist nur verfügbar, wenn Sie im Feld **Kriterientyp** die Option `Tabelle` oder `Geheime Spalte` auswählen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zielbereich	Anwendungsbereich der im Feld Zieltabelle ausgewählten **Tabelle**. Dieses Feld ist nur sichtbar, wenn Sie im Feld **Kriterientyp** `Tabelle`, `Filterspalte` oder `Geheime Spalte` auswählen.
Geheime Spalte	Tabellenspalte, die die pasword2-Geheimnisse enthält, die Sie in diese Gruppe aufnehmen. Die in dieser Liste verfügbaren Felder hängen von der im Feld Zieltabelle ausgewählten **Tabelle** ab. **Hinweis:** Wenn in der Auswahltabelle keine Spalten vorhanden sind, die Geheimnisse enthalten, zeigt dieses Feld nur `– Keine –` als Auswahl an.
Spalte filtern	Die Spalte in der unter Zieltabelle ausgewählten **Tabelle**, die Sie als Filter verwenden möchten. Dieses Feld darf kein Password2-Feld sein.
Filterwert	Der Wert, den Sie als Filter verwenden möchten. Dieser **Filter** gilt für das Feld, das im Feld „Filterspalte“ ausgewählt ist.

Example: Eine für die Instanz zugängliche Gruppe, die alle E-Mail-Account-Passwörter für einen E-Mail-Server enthält



Nächste Maßnahme

Nach dem Erstellen Ihrer Gruppe werden alle neuen Datensätze, die den Kriterien entsprechen, verschlüsselt. Um vorhandene Datensätze mit dem kryptografischen Modul dieser Gruppe zu verschlüsseln, müssen Sie einen Sicherheitsauftrag ausführen. Details finden Sie unter Führen Sie Sicherheitsaufträge für die Geheimnisverwaltung aus.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für den Client zugängliche Gruppen benötigen einen vom Kunden bereitgestellten öffentlichen Schlüssel, um Ihre Geheimnisse zu verschlüsseln. Schritte zum Hochladen dieses Schlüssels finden Sie unter Laden Sie einen öffentlichen Schlüssel für die Geheimnisverwaltung hoch.

Laden Sie einen öffentlichen Schlüssel für die Geheimnisverwaltung hoch

Laden Sie einen öffentlichen Schlüssel für hoch, um Ihre Geheimnisse zu verschlüsseln.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Geheimnisverwaltung** > **Geheimnisgruppen**, und öffnen Sie den Datensatz der geheimen Gruppe.
2. Wählen Sie im **-Datensatz die Schaltfläche Clientseitigen Zugriff verwalten**.
   Ein neuer Identitätsgruppen-Datensatz wird geöffnet.
3. Wählen Sie die Schaltfläche **Identitätsschlüssel** hochladen aus.
   Ein Fenster zum **Importieren des öffentlichen Identitätsschlüsselzertifikats** wird angezeigt.
4. Geben Sie im Feld **Identitätsschlüssel** -Alias einen Alias für Ihren Schlüssel ein.
5. Wählen Sie die Schaltfläche **Importieren**, um den Schlüssel aus Ihrer lokalen Umgebung hochzuladen.
6. Wählen Sie die Schaltfläche **OK**.
   Das Feld **Modulschlüssel Gruppe** verwendet den Identitätsschlüssel-Aliasnamen.
7. Wählen Sie **Absenden** aus, um den Identitätsgruppen-Datensatz zu speichern.

Führen Sie Sicherheitsaufträge für die Geheimnisverwaltung aus

Planen Sie einen Geheimnisverwaltungsauftrag, um Verschlüsselungsaufgaben für Geheimnisfelder in Ihrer Instanz auszuführen.

Vorbereitungen

Erforderliche Rolle: sn_kmf.admin, security_admin und sn_secrets.admin

Um diese Schritte auszuführen, müssen Sie auf die Rolle security_admin hochstufen. Weitere Informationen zu diesem Prozess finden Sie unter Auf eine privilegierte Rolle hochstufen

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Security-Aufträge** > **Neu erstellen:**an.
2. Im **Feld Welche Art von Sicherheitsauftrag möchten Sie erstellen?**, wählen Sie **Geheimnisverwaltungsauftrag**aus.
3. Füllen Sie die Felder des Formulars aus.

Auftragsformular für die Geheimnisverwaltung

Feld	Beschreibung
Name	Name des Sicherheitsauftrags
Status	Der anfängliche Job-Status ist Neu. Nachdem die Aufgabe wie geplant ausgeführt wurde, wird der Status entsprechend aktualisiert

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zeitfensterstart	Startzeit für den Auftrag im 24-Stunden-Format. Die Ausführung des Auftrags beginnt zum gewählten Zeitpunkt.
Zeitfensterende	Endzeit für den Auftrag im 24-Stunden-Format. Wenn der Auftrag zu diesem Zeitpunkt nicht abgeschlossen ist, wird er während des nächsten angegebenen Verarbeitungsfensters fortgesetzt, bis der Auftrag abgeschlossen wird.
Durchsetzungsebene	Gibt an, ob sich der Auftrag auf alle Tabellen oder eine Auswahl bestimmter Tabellen oder Felder auswirkt. Wählen Sie aus folgenden Möglichkeiten aus: ◦ Alle Tabellen ◦ Bestimmte Tabellen ◦ Bestimmte Felder ◦ Bestimmte Pakete ⚠ **Warnung:** Die Auswahl der Option „ **Alle Tabellen** “ kann die Leistung der Instanz beeinträchtigen. Planen Sie außerhalb der Spitzenzeiten.
Pakete	Die Pakete, die in diesen Auftrag aufgenommen werden sollen. Die Verschlüsselung wird auf ausgewählte Pakete angewendet. Diese Option wird nur angezeigt, wenn das Feld **Durchsetzungsebene** auf **Bestimmte Pakete**festgelegt ist
Tabellen	Die in diesen Auftrag aufzunehmenden Tabellen. Die Verschlüsselung wird auf alle zutreffenden Felder in den ausgewählten Tabellen angewendet. Diese Option wird nur angezeigt, wenn die **Durchsetzungsebene** auf **Bestimmte Tabellen**festgelegt ist
Felder	Die in diesen Auftrag aufzunehmenden Tabellen. Verschlüsselung wird auf alle ausgewählten Felder angewendet. Diese Option wird nur angezeigt, wenn die **Durchsetzungsebene** auf **Bestimmte Felder**festgelegt ist
Auftragsmodus	Wählen Sie aus folgenden Möglichkeiten aus: Password2 an Geheimnisverwaltung Verschlüsseln Sie alle Passwort2-Felder in Ihren Geheimnisgruppen mit den

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	kryptografischen Modulen, die in der Modulzugriffsrichtlinie jeder Gruppe definiert sind. Geheimnisverwaltung an Password2 Verschlüsseln Sie Daten in Ihren Geheimnisgruppen mithilfe der Passwort2-Verschlüsselung erneut. Einzelheiten zu diesem Verschlüsselungstyp finden Sie unter Passwort2-Verschlüsselung mit KMF. Durchsetzung geheimer Gruppen Fragt alle Daten ab, die der im Feld **„Geheimnisgruppe“ ausgewählten Gruppe** entsprechen sollen. Wenn sich alle von der Abfrage gefundenen Daten bereits in der Gruppe befinden, nimmt die Aufgabe keine Änderungen vor. Wenn die Abfrage Daten findet, die sich noch nicht in der Gruppe befinden, verschlüsselt der Auftrag diese Daten innerhalb der geheimen Gruppe erneut. **Hinweis:** Wenn die in dieser Abfrage gefundenen Daten bereits verschlüsselt sind und Ihre Instanzen diese Daten nicht entschlüsseln können, werden sie nicht verschlüsselt und der Geheimnisgruppe hinzugefügt.
Geheimnisgruppe	Geheimnisgruppe, die die zu verschlüsselnden Geheimnisse enthält. Dieses Feld ist nur verfügbar, wenn im Feld **Auftragsmodus** eine **geheime Gruppe** ausgewählt ist.
Neueingabe von Daten erzwingen	
Zusammenfassung	Zeigt Informationen zum Auftragsfortschritt an. Die Zusammenfassung zeigt auch Datensätze an, die von der Aufgabe nicht verschlüsselt werden konnten.

4. Wählen Sie **Absenden**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme
Die Aufgabe fragt alle Daten ab, die mit der ausgewählten geheimen Gruppe übereinstimmen müssen. Wenn sich alle von der Abfrage gefundenen Daten bereits in der Gruppe befinden, nimmt die Aufgabe keine Änderungen vor. Wenn die Abfrage Daten findet, die sich noch nicht in der Gruppe befinden, verschlüsselt der Auftrag diese Daten innerhalb der geheimen Gruppe erneut. (Wenn die Instanz es entschlüsseln kann, was bei clientseitig verschlüsselten Geheimnissen möglicherweise nicht der Fall ist).

Codesignatur

Die Codesignatur erstellt digitale Signaturen für die Daten, die später überprüft werden, um die Authentizität und Integrität der Daten zu bestätigen. „Codesignatur" ist ein Modul, das als Komponente von ServiceNow Vaultlizenziert wird.

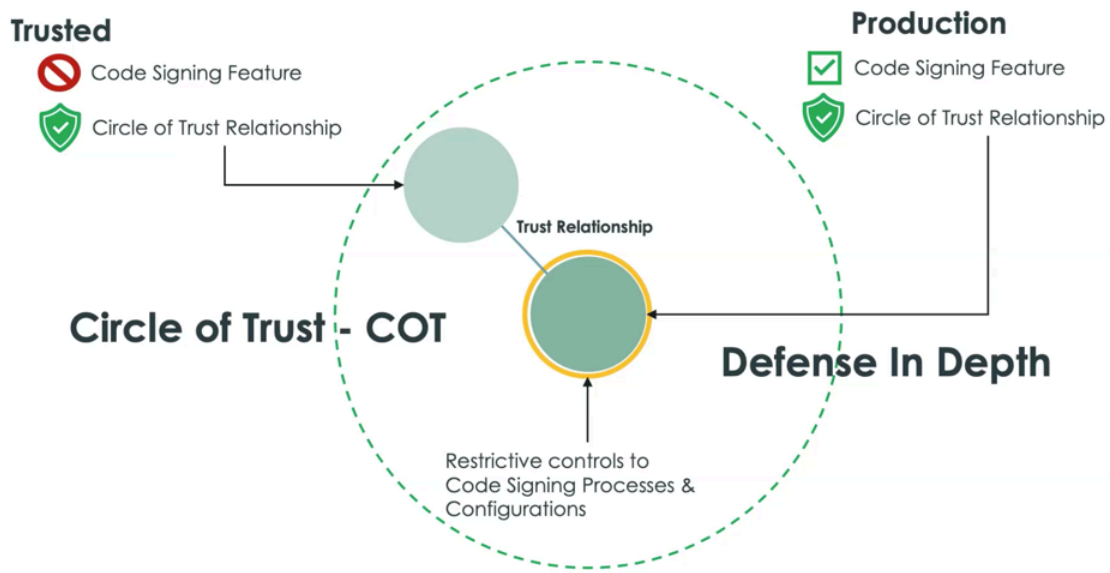
Codesignatur und Circle of Trust

Circle of Trust (COT) ist eine Voraussetzung für die Codesignatur, die eine sichere Kommunikation zwischen Ihren vertrauenswürdigen und Produktionsinstanzen herstellt, um sicherzustellen, dass nur autorisierte Benutzer auf die Codesignaturfunktion zugreifen können.

Mehrere Sicherheitsmaßnahmen tragen dazu bei, zu verhindern, dass böswillige Akteure die Codesignatur deaktivieren oder missbrauchen, falls eine Produktionsinstanz gefährdet wird. Im Rahmen der Strategie für eingehende Verteidigung verwendet der COT die folgenden Komponenten:

- In der Produktionsinstanz werden Steuerungen eingerichtet, die selbst die leistungsfähigsten Administratorkonten einschränken, um Codesignaturprozesse und -konfiguration zu schützen.
- Vertrauenswürdige Instanzen müssen mit Produktionsinstanzen zusammenarbeiten, um die Beziehung Circle of Trust herzustellen. Mindestens eine vertrauenswürdige Instanz ist erforderlich, es können jedoch mehrere vertrauenswürdige Instanzen für die Zusammenarbeit mit der Produktionsinstanz konfiguriert werden.

Übersicht über den Kreis des Vertrauens

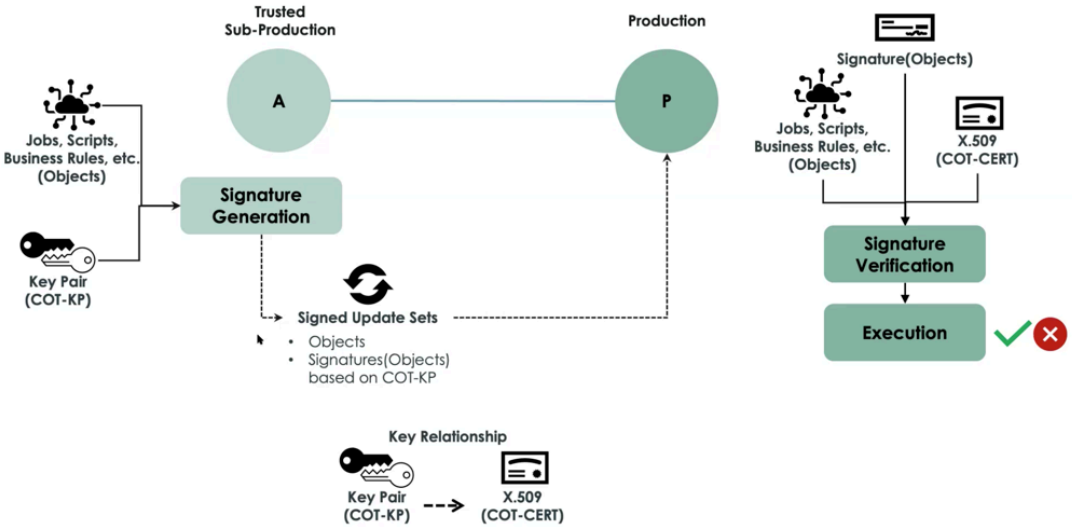


Circle of Trust verwendet Aufträge, Skripts und Geschäftsregeln zusammen mit einem Schlüsselpaar, um Signaturen zum Signieren von Update-Sätzen für die Produktionsinstanz zu generieren. Wenn der Auftrag aufgerufen wird, wird die Signatur zusammen mit

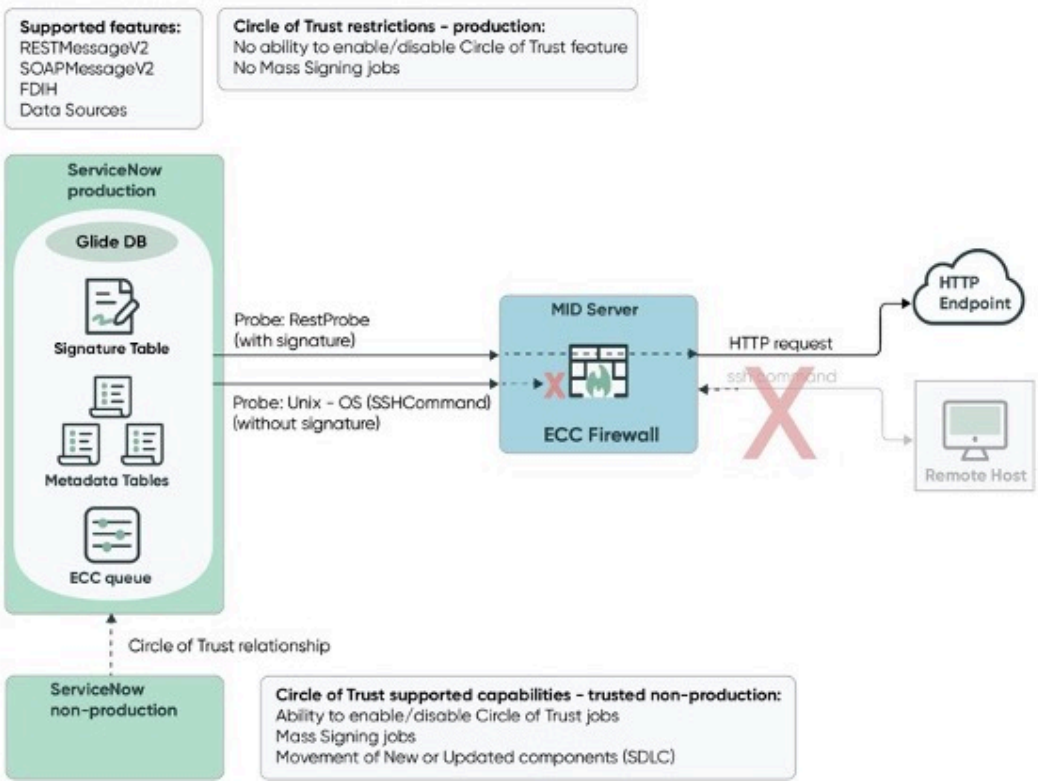
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

dem vertrauenswürdigen Zertifikat verifiziert, um Aktualisierungen der Produktionsinstanz auszuführen.

Prozess für vertrauenswürdige Update-Sätze



Flow zur Codesignatur

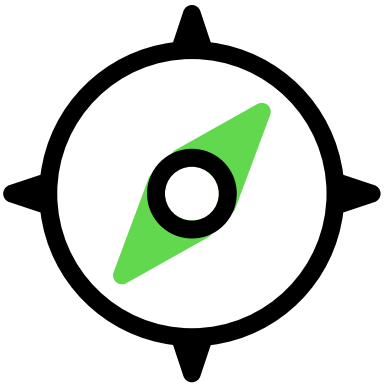


Circle of Trust erfordert eine anfängliche Vertrauensstellung zwischen vertrauenswürdigen Instanzen und Produktionsinstanzen, die verhindert, dass nicht autorisierte Benutzer mit einer beliebigen Autorisierungsebene auf nicht genehmigte Aktivitäten zugreifen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

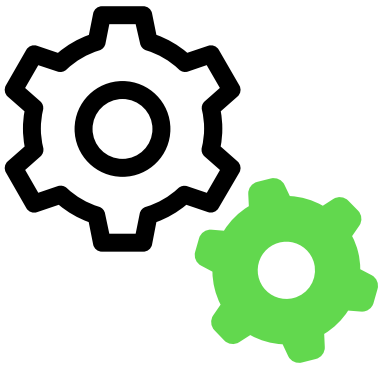
Erste Schritte

Untersuchen



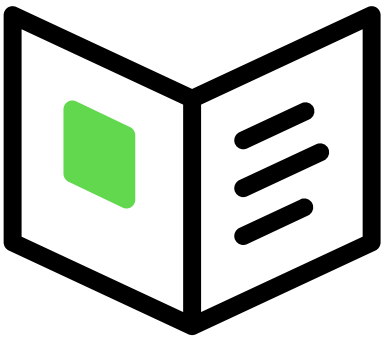
Lernen Sie die wichtigsten Funktionen und den Geschäftsnutzen von Codesignatur kennen.

Konfigurieren



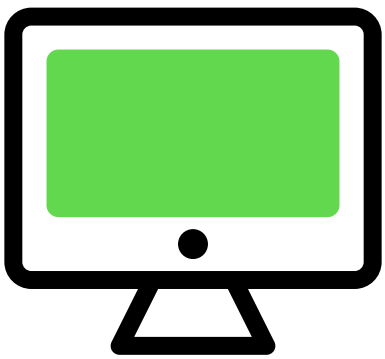
Codesignatur aktivieren und konfigurieren.

Referenz



Rufen Sie Details zu Eigenschaften und Problembehandlung ab

Verwenden



Erfahren Sie, wie Sie mithilfe von Codesignatur die Authentizität und Integrität Ihrer Daten überprüfen können.

Problembehandlung und Hilfe

- https://www.servicenow.com/community/secops/ct-p/security-operations
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Codesignatur erkunden

Codesignatur kann die Sicherheit verbessern, indem vertrauliche Anwendungskonfigurationsdaten und Skripts vor ihrer Verwendung validiert werden.

Die Codesignatur erstellt digitale Signaturen für die Daten, die später überprüft werden, um die Authentizität und Integrität der Daten zu bestätigen. „Codesignatur“ ist ein Modul, das als Komponente von ServiceNow Vaultlizenziert wird.

Hinweis: Das Team Kundenservice und Support muss Zugriff auf die Codesignatur gewähren.

Codesignatur deklariert die Absicht hinter dem durchgeführten Vorgang und validiert, ob die Ressource oder der Datensatz für den beabsichtigten Zweck verwendet werden kann. Um das Signieren von Codesignatur zu erleichtern, verwendet die Key Management Framework (KMF) digitale Zertifikate und asymmetrische Verschlüsselung nach Industriestandard für digitale Signaturen.

Verwenden Sie Codesignatur intern auf Plattform- und Infrastrukturseite. Codesignatur bietet eine Möglichkeit, den Inhalt bestimmter Tabellen oder einer Teilmenge von Datensätzen in einer bestimmten Metadatentabelle zu signieren.



Die Codesignatur verwendet ein sicheres Circle of Trust (COT) zwischen Ihren vertrauenswürdigen und Produktionsinstanzen, um sicherzustellen, dass nur autorisierte, sichere und vertrauenswürdige Instanzen auf die Codesignatur zugreifen können.

Anwendungsfälle

Codesignatur kann für Vorgänge mit MID-Server und IntegrationHubverwendet werden. Notarisierung ist die Verwendung von Codesignatur zum Erstellen digitaler Signaturen für ECC-Warteschlangendatensätze, die in MID-Server-Vorgängen und Integrations-Hub-Vorgängen verwendet werden.

Beispielsweise wird eine von ServiceNow geschriebene Skripteinbindung zum Erstellen von ECC-Warteschlangendatensätzen zur Laufzeit als „Basissysteminhalt“ signiert. Es ist als „ordnungsgemäß von der Instanz ServiceNow ausgestellt“ signiert, im Gegensatz zu einer Einfügung in die ECC-Warteschlange von einem Hintergrundskript oder einem anderen Ursprung, der nicht validiert und signiert ist.

IntegrationHub können Codesignatur verwenden, um auf der Plattform generierte dynamische Inhalte zu signieren und kritische Teile der Anwendungsdaten zu validieren.

Tipp:

Zeitstempel stellen sicher, dass signierte Datensätze nicht ablaufen, wenn das Zertifikat abläuft, sofern der Datensatz vor dem Ablauf des Zertifikats signiert wurde. Es gibt einen 4-Stunden-Kulanzzeitraum um das Zertifikatgültigkeitsfenster, um sicherzustellen, dass Zeitunterschiede zwischen Servern Zertifikate nicht absichtlich ungültig machen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Validierung und Aufträge der Codesignatur

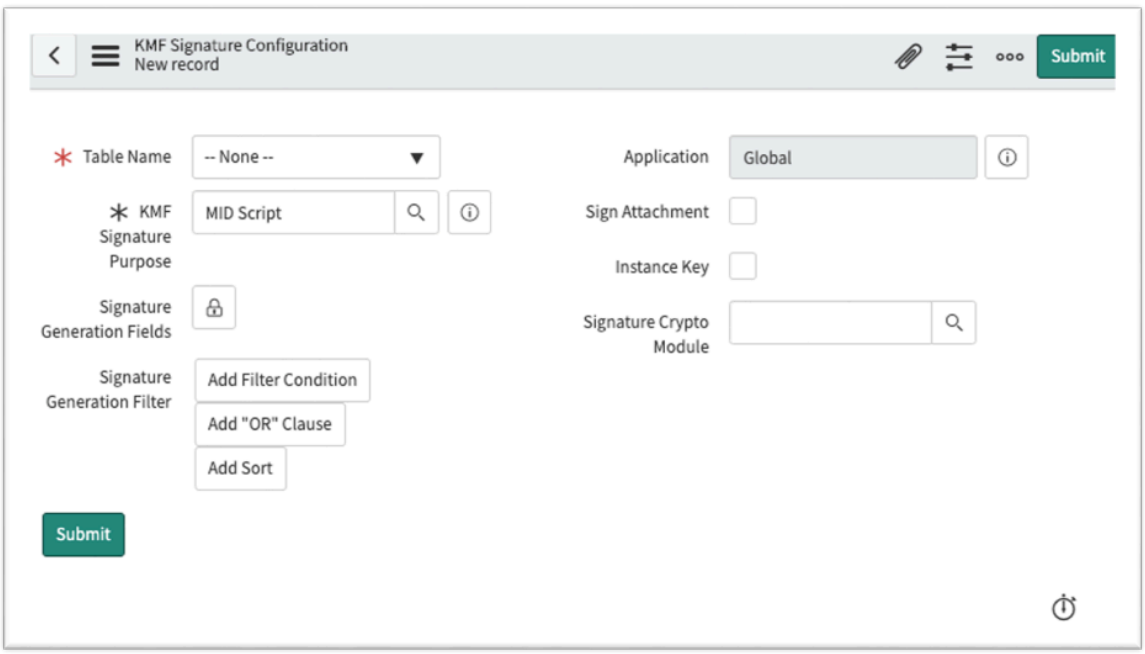
Alle Metadatentabellen mit gültigen Konfigurationen werden zur Erstellungszeit mit dem Metadaten-Plugin „Codesignatur“ (*com.glide.code_signing*) signiert. Wenn Sie Tabellen signieren möchten, haben Administratoren mit der Rolle „Sicherheitsadministrator“ Zugriff auf Verschlüsselungsaufträge für Codesignatur:

- Signieren Sie Update-Sätze.
- Massensignieren Sie Datensätze.
- Massensignieren Sie Anhänge.

Update-Satz signieren

Dieser Auftrag signiert Datensätze, die einer Signaturkonfiguration im Update Set entsprechen. Die Aufgabe fügt dem Update Set auch alle neuen Signaturdatensätze und Verifizierungszertifikate hinzu.

KMF-Signaturdatensatz für Update-Satz



Massensignieren Sie Datensätze

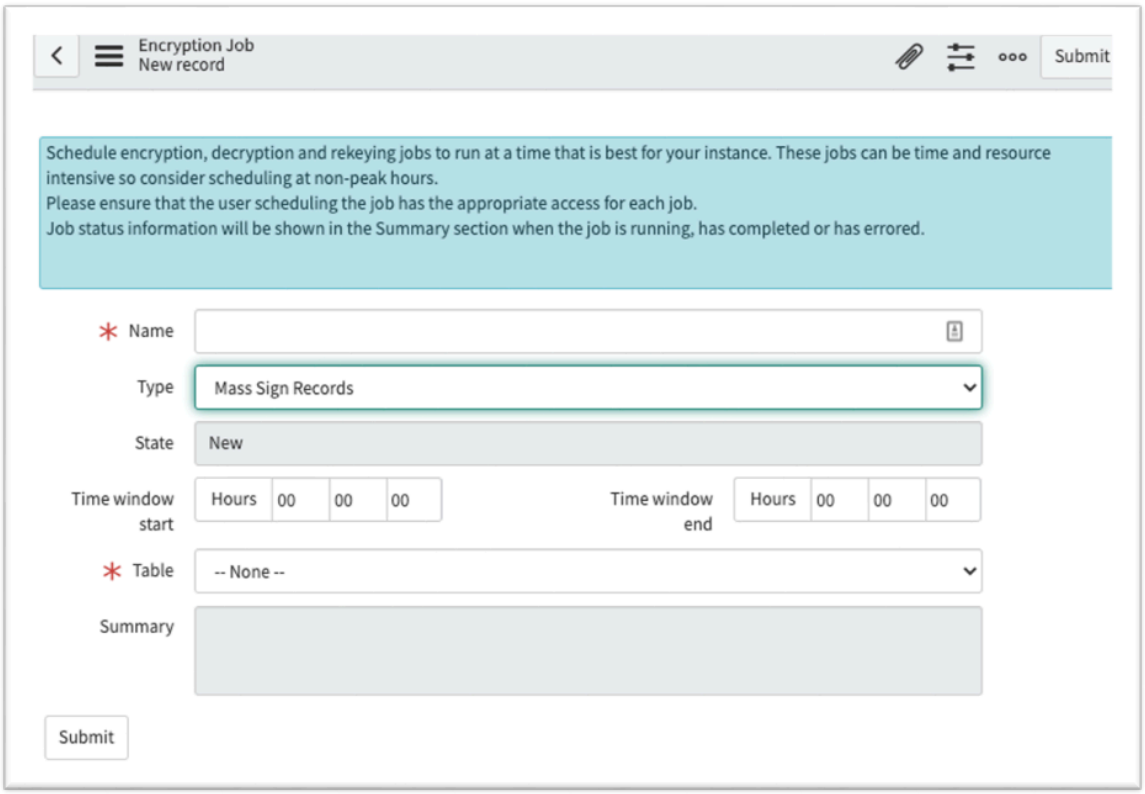
Dieser Auftrag signiert alle Datensätze, die der Signaturkonfiguration entsprechen, die auf eine bestimmte Metadatentabelle angewendet wurde.

Massensignieren Sie Anhänge

Dieser Auftrag signiert alle Anhangsdatensätze, die an eine Tabelle angehängt sind, die einer angegebenen Signaturkonfiguration entspricht.

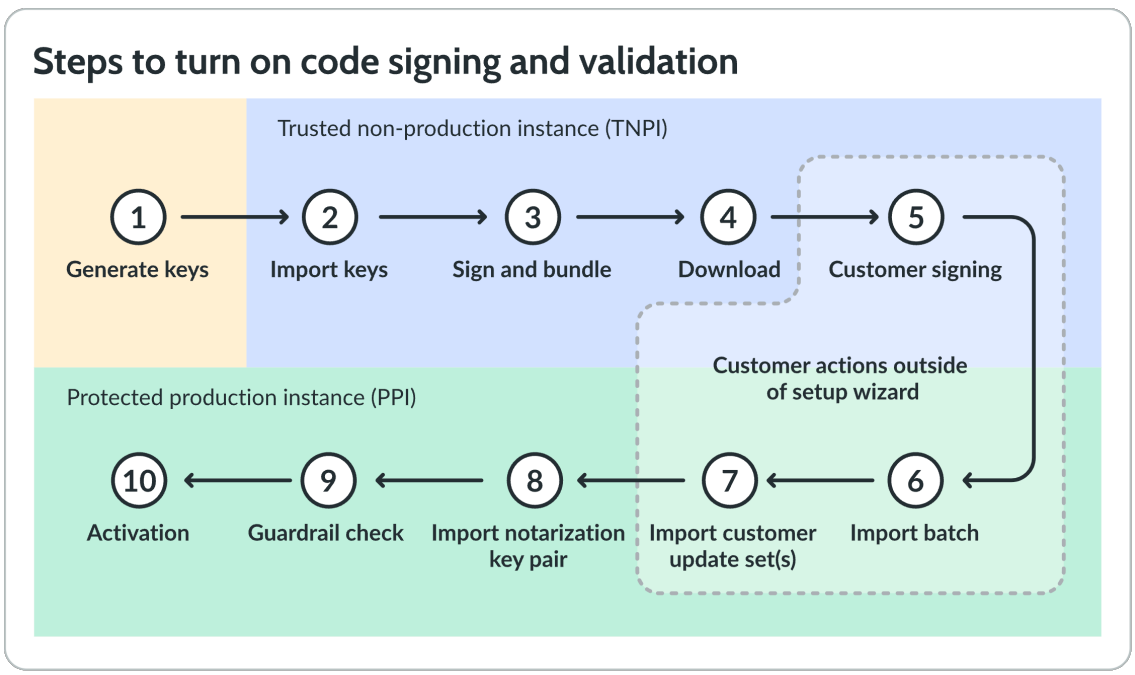
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verschlüsselungsauftrag zum Massensignieren von Datensätzen



Codesignatur konfigurieren

Aktivieren und konfigurieren Sie Codesignatur, um die Authentizität und Integrität Ihrer Daten zu überprüfen.



Codesignatur für Unternehmen erfordert eine anfängliche Vertrauensstellung zwischen vertrauenswürdigen Instanzen und Produktionsinstanzen, die verhindern, dass nicht autorisierte Benutzer mit einer beliebigen Autorisierungsebene auf nicht genehmigte Aktivitäten zugreifen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Lesen Sie die einzelnen Themen, um die Konfigurationsschritte zum Einrichten von Circle of Trust mit Co Signing Enterprise abzuschließen:

Weisen Sie die Codesignaturadministratorrolle zu

Weisen Sie einem Anwender die Rolle „Codesignaturadministrator“ zu, um auf die Konfigurations-Experience der Codesignatur zuzugreifen.

Konfigurieren Sie Codesignaturunternehmen in Ihrer vertrauenswürdigen Instanz außerhalb der Produktion

Aktivieren Sie die Codesignatur in Ihrer vertrauenswürdigen Instanz außerhalb der Produktion.

Laden Sie Ihre Konfigurationsdatei für die Codesignatur in Ihre geschützte Produktionsinstanz hoch

Laden Sie die Konfigurationsdatei hoch, die in Ihrer vertrauenswürdigen Instanz außerhalb der Produktion generiert wurde.

Konfigurieren Sie Co Signing Enterprise in Ihrer geschützten Produktionsinstanz

Aktivieren und konfigurieren Sie die Codesignatur in Ihrer geschützten Produktionsinstanz.

Aktivieren Sie die Zertifikatvalidierung

Aktivieren Sie die Zertifikatvalidierung für Ihre -Instanz.

Codesignatur deaktivieren

Deaktivieren Sie die Codesignatur in Ihrer geschützten Produktionsinstanz.

Hinweis: Dieser optionale Schritt ist nicht Teil der Erstkonfiguration für die Codesignatur

Weisen Sie die Codesignaturadministratorrolle zu

Weisen Sie einem Anwender die Rolle „Codesignaturadministrator“ zu, um auf die Konfigurations-Experience der Codesignatur zuzugreifen.

Vorbereitungen

Erforderliche Rollen:

- Administrator
- security_admin

Wichtig: Der Anwender, dem die Rolle „Codesignaturadministrator“ zugewiesen ist, muss sich im Bereich „Global“ befinden.

Prozedur

1. Wählen Sie eine Instanz außerhalb der Produktion aus, die als vertrauenswürdige Instanz außerhalb der Produktion verwendet werden soll.
   Das TNPI wird verwendet, um Aufträge zu erstellen, Datensätze zu signieren und andere erforderliche Aufgaben auszuführen, bevor die Signaturvalidierung in Ihrer geschützten Produktionsinstanz aktiviert wird.
2. Navigieren zu **Alle** > **Codesignatur** > **Verwaltung der Codesignaturrolle**an.
3. Gewähren Sie einem Anwender die Rolle „Codesignaturadministrator“, indem Sie einen Anwender aus der Liste **Verfügbare Anwender** in die Liste **Ausgewählte Anwender** verschieben.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie **Speichern**.

> **Wichtig:** Der der Rolle zugewiesene Benutzer muss sich abmelden und wieder anmelden, um Codesignaturaufgaben auszuführen.

Ergebnisse
Der ausgewählte Anwender hat die Rolle „Codesignaturadministrator“. Ein Anwender mit dieser Rolle kann auf die Konfigurations-Experience der Codesignatur zugreifen und Anwendern andere Codesignaturrollen zuweisen.

Weitere Informationen zu Codesignaturrollen finden Sie unter Mit Codesignatur installierte Rollen.

Konfigurieren Sie Codesignaturunternehmen in Ihrer vertrauenswürdigen Instanz außerhalb der Produktion

Aktivieren und konfigurieren Sie die Codesignatur in Ihrer vertrauenswürdigen Instanz außerhalb der Produktion.

Vorbereitungen
Erforderliche Rollen:

- Administrator
- security_admin
- „codesigning_admin“

> **Hinweis:** Die Rolle „codesigning_admin“ kann mit dem in Weisen Sie die Codesignaturadministratorrolle zubeschriebenen Prozess zugewiesen werden.

- sn_kmf.cryptographic_manager

Sie benötigen mindestens ein kryptografisches Schlüsselpaar und ein Zertifikat (p12-Dateierweiterung) für die Kundensignatur und die Circle of Trust-Administration (COT). Um die Sicherheit zu erhöhen, sollten Sie separate kryptografische Schlüsselpaare für die Kundensignatur und die COT-Verwaltung verwenden.

> **Warnung:** Nach Abschluss dieses Prozesses haben Sie eine Konfigurationsdatei heruntergeladen, die innerhalb von einer Stunde auf Ihrem PPI installiert werden muss. Stellen Sie sicher, dass Sie nach diesem Prozess Zeit haben, um die Konfigurationsdatei in Ihre Produktionsinstanz hochzuladen. Details zu diesem Prozess finden Sie unter Laden Sie Ihre Konfigurationsdatei für die Codesignatur in Ihre geschützte Produktionsinstanz hoch.

Prozedur

1. Navigieren Sie auf Ihrem TNPI zu **Alle** > **Codesignatur** > **Codesignaturkonfiguration** , um die Konfigurationsseite für die Codesignatur zu öffnen.
2. **Wählen** Sie im Feld Instanztyp die **Option Vertrauenswürdige Instanz außerhalb der Produktion aus**.
3. Wählen Sie die Schaltfläche **Weiter** aus.
4. **Wählen Sie** im Feld **Aktion**unter Gewünschte Aktion auswählen die **Option Codesignatur aktivieren aus**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie neben **Anhängen** im Abschnitt „ **Signaturschlüsselpaar und Zertifikat des Kunden** “ die Option **+Datei hinzufügen** aus, um ein kryptografisches Schlüsselpaar (p12-Dateierweiterung) für die Kundensignatur hochzuladen.

   Tipp: Wenn die Option **+Datei** hinzufügen nicht verfügbar ist, vergewissern Sie sich, dass Sie sich im Bereich „Global“ befinden und über die Rolle sn_kmf.cryptographic_manager verfügen.

6. **Geben Sie** im Feld Passwort das Passwort für das hochgeladene Schlüsselpaar ein.
7. Wählen Sie **Importieren**.
8. Wählen **Sie Fortsetzen**, um zum nächsten Abschnitt zu wechseln.
9. Wählen Sie neben **Anhängen** im Abschnitt „ **COT-Administrationsschlüsselpaar und -zertifikat** “ **+Datei hinzufügen** aus, um ein kryptografisches Schlüsselpaar (p12-Dateierweiterung) für die Kundensignatur hochzuladen.
10. **Geben Sie** im Feld Passwort das Passwort für das hochgeladene Schlüsselpaar ein.
11. Wählen Sie **Importieren**.
12. Wählen **Sie Fortsetzen**, um zum nächsten Abschnitt zu wechseln.
13. Warten Sie im Abschnitt „ **Vertrauenswürdige Aufgaben außerhalb der Produktion durchführen** “, bis alle Aufgaben abgeschlossen sind.

    Ihre -Instanz generiert und führt diese Aufgaben automatisch aus. Wenn Sie Codesignatur vor dem Release Vancouver verwendet haben, werden Aufgaben erstellt und ausgeführt, um Ihre Signaturen zu aktualisieren.

    In einigen Fällen sind keine Aufgaben erforderlich. Auf dieser Seite wird „**Keine Aufgaben erforderlich** “ angezeigt.

14. Wählen **Sie Fortsetzen**, um zum nächsten Abschnitt zu wechseln.
15. Wählen Sie auf der Seite „ **Konfigurationsdatei** exportieren“ **Exportieren** aus, um eine Konfigurationsdatei zu erstellen und herunterzuladen, die zum Aktivieren von Codesignatur in Ihrer geschützten Produktionsinstanz verwendet wird.
    Beim Exportvorgang wird eine XML-Datei auf Ihren lokalen Computer heruntergeladen, um sie in den Schrittdetails in Konfigurieren Sie Co Signing Enterprise in Ihrer geschützten Produktionsinstanzzu verwenden.

Laden Sie Ihre Konfigurationsdatei für die Codesignatur in Ihre geschützte Produktionsinstanz hoch

Laden Sie die Konfigurationsdatei hoch, die in Ihrer vertrauenswürdigen Instanz außerhalb der Produktion generiert wurde.

Vorbereitungen

Erforderliche Rollen:

- Administrator
- security_admin
- „codesigning_admin“

  Hinweis: Die Rolle „codesigning_admin“ kann mit dem in Weisen Sie die Codesignaturadministratorrolle zubeschriebenen Prozess zugewiesen werden.

- sn_kmf.cryptographic_manager

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie benötigen auch die Konfigurationsdatei, die in den in Konfigurieren Sie Codesignaturunternehmen in Ihrer vertrauenswürdigen Instanz außerhalb der Produktionbeschriebenen Schritten generiert wurde.

Prozedur

1. Navigieren zu **Alle** > **Systemupdate-Sätze** > **Abgerufene Update-Sätze**an.
2. Wählen Sie unten in der Liste der abgerufenen **Update Sets** die **Option Update Set aus XML** importieren aus.
3. Wählen **Sie Datei**wählen und wählen Sie Ihre Konfigurationsdatei (XML-Dateierweiterung).
4. Wählen Sie **Hochladen** aus.
   Der Update Set für die **Codesignatur-Konfiguration** sollte in der Liste der **abgerufenen Update-Sätze** angezeigt werden.
5. Wählen und öffnen Sie das Update Set für die **Codesignatur-Konfiguration**.
6. Wählen Sie **Vorschau auf Update-Satz-Batch anzeigen**.
   Wenn während der Vorschau Konflikte auftreten, lösen Sie sie, indem Sie **Remote-Update akzeptieren** oder **Bekannte CS-Konflikte**lösen wählen.
7. Wählen Sie nach der Lösung von Konflikten **Commit Update Set Batch**(Update-Satz-Batch festlegen) aus.

Konfigurieren Sie Co Signing Enterprise in Ihrer geschützten Produktionsinstanz

Aktivieren und konfigurieren Sie die Codesignatur in Ihrer geschützten Produktionsinstanz.

Vorbereitungen

Erforderliche Rollen:

- Administrator
- security_admin
- „codesigning_admin“

  Hinweis: Die Rolle „codesigning_admin“ kann mit dem in Weisen Sie die Codesignaturadministratorrolle zubeschriebenen Prozess zugewiesen werden.

- sn_kmf.cryptographic_manager

Prozedur

1. Navigieren Sie auf Ihrem PPI zu **Alle** > **Codesignatur** > **Codesignaturkonfiguration** , um die Konfigurationsseite für die Codesignatur zu öffnen.
2. **Wählen** Sie im Feld Instanztyp die Option **Geschützte Produktionsinstanz aus**.
3. Wählen Sie die Schaltfläche **Weiter** aus.
4. Aktivieren Sie das Kontrollkästchen **Bestätigen Sie, dass der Update-Satz für die Codesignaturkonfiguration importiert und bestätigt wurde**.
5. Wählen Sie die Schaltfläche **Weiter** aus.
6. Warten Sie, bis die Zertifikatinstallation abgeschlossen ist.
   Es wird eine blaue Warnmeldung angezeigt, die darauf hinweist, dass Elemente aus der Konfigurationsdatei installiert werden. Die Warnung wird in wenigen Sekunden ausgeblendet, wenn die Installation abgeschlossen ist.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Wählen Sie neben **Anhängen** im Abschnitt „ **Laufzeit-/Notarisierungsschlüsselpaar und Zertifikat** “ die Option **+Datei hinzufügen** aus, um ein kryptografisches Schlüsselpaar (p12-Dateierweiterung) zur Verwendung für Laufzeit-/Notarisierungszwecke hochzuladen. Sie können ein Schlüsselpaar aus der vertrauenswürdigen Instanz außerhalb der Produktion (TNPI) wiederverwenden oder ein neues speziell für diese Verwendung hochladen.

   Tipp: Wenn die Option **+Datei** hinzufügen nicht verfügbar ist, vergewissern Sie sich, dass Sie sich im Bereich „Global“ befinden und über die Rolle sn_kmf.cryptographic_manager verfügen.

8. **Geben Sie** im Feld Passwort das Passwort für das hochgeladene Schlüsselpaar ein.
9. Wählen Sie **Importieren**.
10. Wählen **Sie Fortsetzen**, um zum nächsten Abschnitt zu wechseln.
11. Warten Sie, während Ihre Instanz eine Schutzmaßnahmenprüfung durchführt. Diese Prüfung durchsucht Ihre Instanz nach ungültigen Signaturen. Der Vorgang kann einige Zeit in Anspruch nehmen. Beenden oder aktualisieren Sie die Seite erst, wenn der Scanvorgang abgeschlossen ist.
12. Wenn bei der Prüfung ungültige Signaturen gefunden werden, wählen Sie **Bericht herunterladen**.

    Wenn Sie **Bericht** herunterladen auswählen, wird ein Bericht (`scan_report.txt`) heruntergeladen, mit dem Sie die ungültigen Signaturen untersuchen und korrigieren können.

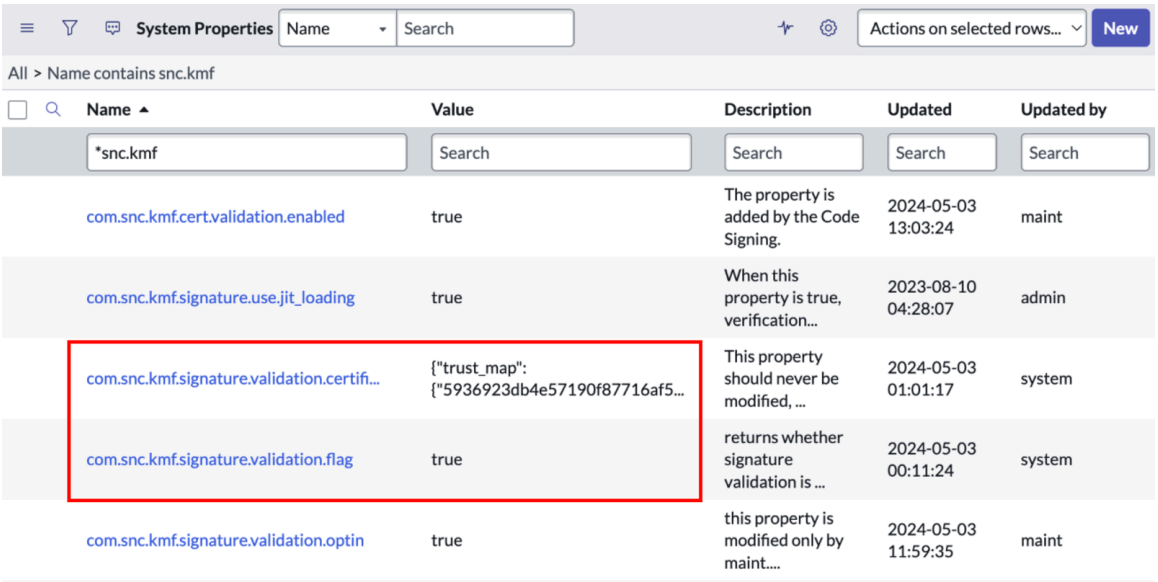
    Aktualisieren Sie nach der Behebung der Fehler die Seite, um die Prüfung erneut auszuführen.

13. Wenn keine Fehler auftreten, wählen Sie **Setup abschließen**aus.
14. Warten Sie, bis die Konfigurationsaufträge abgeschlossen sind. Ihre Instanz von führt einen oder mehrere Aufträge aus, um den Konfigurationsprozess abzuschließen. Schließen oder aktualisieren Sie die Seite erst, wenn die Aufträge abgeschlossen sind. Wenn Sie fertig sind, sollte die Meldung „ **Codesignaturkonfiguration erfolgreich abgeschlossen** “ angezeigt werden.

Ergebnisse

Die Signaturvalidierung wird jetzt für Ihre Produktionsinstanz erzwungen. Sie können den erfolgreichen Abschluss anhand Ihrer Systemeigenschaften überprüfen. Suchen Sie in der **Tabelle** „Systemeigenschaften“ [sys_property] nach der Eigenschaft com.snc.kmf.signature.validation.flag, und vergewissern Sie sich, dass der Wert **true**ist. Stellen Sie sicher, dass die Eigenschaft **com.snc.kmf.signature.validation.certificate_trust** keinen leeren Wert enthält.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Aktivieren Sie die Zertifikatvalidierung

Schützen Sie Ihre -Instanz mit der zertifikatbasierten Validierung.

Vorbereitungen

Erforderliche Rolle:

- „codesigning_admin“
- security_admin
- sn_kmf.cryptographic_manager

Prozedur

1. Navigieren Sie auf Ihrer vertrauenswürdigen Instanz außerhalb der Produktion zu **Alle** > **Codesignatur** > **Codesignaturkonfiguration** , um die Konfigurationsseite für die Codesignatur zu öffnen.
2. **Wählen** Sie im Feld Instanztyp die **Option Vertrauenswürdige Instanz außerhalb der Produktion aus**.
3. Wählen Sie die Schaltfläche **Weiter** aus.
4. Wählen Sie im Feld **Aktion** unter **Gewünschte Aktion**auswählen die **Option Zertifikatvalidierung aktivieren aus**.
5. Wählen Sie die Schaltfläche **Weiter** aus.
6. Wählen Sie neben **Anhängen** im Abschnitt „ **Signaturschlüsselpaar und Zertifikat des Kunden** “ die Option **+Datei hinzufügen** aus, um ein kryptografisches Schlüsselpaar (p12-Dateierweiterung) für die Kundensignatur hochzuladen.

   Tipp: Wenn die Option **+Datei** hinzufügen nicht verfügbar ist, vergewissern Sie sich, dass Sie sich im Bereich „Global“ befinden und über die Rolle sn_kmf.cryptographic_manager verfügen.

7. **Geben Sie** im Feld Passwort das Passwort für das hochgeladene Schlüsselpaar ein.
8. Wählen Sie **Importieren**.
9. Wählen **Sie Fortsetzen**, um zum nächsten Abschnitt zu wechseln.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. Wählen Sie neben **Anhängen** im Abschnitt „ **COT-Administrationsschlüsselpaar und -zertifikat** “ **+Datei hinzufügen** aus, um ein kryptografisches Schlüsselpaar (p12-Dateierweiterung) für die Kundensignatur hochzuladen.
11. **Geben Sie** im Feld Passwort das Passwort für das hochgeladene Schlüsselpaar ein.
12. Wählen Sie **Importieren**.
13. Wählen **Sie Fortsetzen**, um zum nächsten Abschnitt zu wechseln.
14. Warten Sie im Abschnitt „ **Vertrauenswürdige Aufgaben außerhalb der Produktion durchführen** “, bis alle Aufgaben abgeschlossen sind.

    Ihre -Instanz generiert und führt diese Aufgaben automatisch aus. Wenn Sie Codesignatur vor dem Release Vancouver verwendet haben, werden Aufgaben erstellt und ausgeführt, um Ihre Signaturen zu aktualisieren.

    In einigen Fällen sind keine Aufgaben erforderlich. Auf dieser Seite wird „**Keine Aufgaben erforderlich** “ angezeigt.
15. Wählen **Sie Fortsetzen**, um zum nächsten Abschnitt zu wechseln.
16. Wählen Sie auf der Seite „ **Konfigurationsdatei** exportieren“ **Exportieren** aus, um eine Konfigurationsdatei zu erstellen und herunterzuladen, die zum Aktivieren von Codesignatur in Ihrer geschützten Produktionsinstanz verwendet wird.
    Beim Exportvorgang wird eine XML-Datei auf Ihren lokalen Computer heruntergeladen, um sie in den in Konfigurieren Sie Co Signing Enterprise in Ihrer geschützten Produktionsinstanzbeschriebenen Schritten zu verwenden.
17. Navigieren Sie in Ihrer geschützten Produktionsinstanz (Protected Production Instance, PPI) zu **Alle** > **Systemupdate-Sätze** > **Abgerufene Update-Sätze**an.
18. Wählen Sie unten in der Liste der abgerufenen **Update Sets** die **Option Update Set aus XML** importieren aus.
19. Wählen **Sie Datei**wählen und wählen Sie Ihre Konfigurationsdatei (XML-Dateierweiterung).
20. Wählen Sie **Hochladen** aus.
21. Kehren Sie zur Konfigurationsseite für Codesignaturen unter zurück **Alle** > **Codesignatur** > **Codesignaturkonfiguration**an.
22. Verwenden Sie den Assistenten, um Ihre Konfiguration abzuschließen, indem Sie die Optionen zum Abschließen der Aktivierung der Zertifikatvalidierung auswählen.

Codesignatur deaktivieren

Deaktivieren Sie die Codesignatur in Ihrer geschützten Produktionsinstanz.

Vorbereitungen

Erforderliche Rolle: admin, codedesigning_admin

Prozedur

1. Navigieren Sie auf Ihrer vertrauenswürdigen Instanz außerhalb der Produktion zu **Alle** > **Codesignatur** > **Codesignaturkonfiguration** , um die Konfigurationsseite für die Codesignatur zu öffnen.
2. **Wählen** Sie im Feld Instanztyp die **Option Vertrauenswürdige Instanz außerhalb der Produktion aus**.
3. Wählen Sie die Schaltfläche **Weiter** aus.
4. **Wählen Sie** im Feld **Aktion**unter Gewünschte Aktion auswählen **die Option Codesignatur deaktivieren aus**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie im **Bereich „Konfigurationsdatei** exportieren“ **Exportieren**, um das Update Set herunterzuladen.
   Beim Exportvorgang wird eine XML-Datei auf Ihren lokalen Computer heruntergeladen, um sie in den nächsten Schritten zu verwenden.
6. Wählen Sie **Fertig**.
7. Melden Sie sich bei Ihrer geschützten Produktionsinstanz an.
8. Laden Sie Ihre Konfigurationsdateien anhand der Schritte in Laden Sie Ihre Konfigurationsdatei für die Codesignatur in Ihre geschützte Produktionsinstanz hochhoch.
9. Navigieren zu **Alle** > **Codesignatur** > **Codesignaturkonfiguration** , um die Konfigurationsseite für die Codesignatur zu öffnen.
10. **Wählen** Sie im Feld Instanztyp die Option **Geschützte Produktionsinstanz aus**.
11. Wählen Sie die Schaltfläche **Weiter** aus.
12. Aktivieren Sie das Kontrollkästchen **Bestätigen Sie, dass der Update-Satz für die Codesignaturkonfiguration importiert und bestätigt wurde**.
13. Wählen Sie die Schaltfläche **Weiter** aus.
14. Warten Sie, bis die Zertifikatinstallation abgeschlossen ist.
    Nach Abschluss wird die Meldung Codesignaturkonfiguration **erfolgreich abgeschlossen** angezeigt.

Ergebnisse

Sie können den erfolgreichen Abschluss anhand Ihrer Systemeigenschaften überprüfen. Suchen Sie in der **Tabelle** „Systemeigenschaften“ [sys_property] nach der Eigenschaft com.snc.kmf.signature.validation.flag, und vergewissern Sie sich, dass der Wert **false**ist.

Laden Sie die erforderlichen Schlüsselpaare und Zertifikate für die Codesignatur

Stellen Sie die Beziehung mithilfe von Codesignatur in einer festgelegten Instanz außerhalb der Produktion her. Dieser erste Schritt lädt zwei kryptografische Schlüssel in die Umgebung außerhalb der Produktion, um eine vertrauenswürdige Quelle für Updates für die Produktionsinstanz einzurichten.

Vorbereitungen

Erforderliche Rolle: security_admin und sn_kmf.cryptographic_manager

Warum und wann dieser Vorgang ausgeführt wird

Der erste Schritt zum Herstellen einer Beziehung besteht darin, in einer festgelegten Instanz außerhalb der Produktion mithilfe von Codesignatur die Vertrauensbasis herzustellen. Um diese Aufgabe auszuführen, benötigen Sie Folgendes.

- Sie benötigen zwei 4096-Bit-RSA-Paare aus öffentlichen/privaten Schlüsseln, um sie in kryptografische Codesignaturmodule zu laden:
  - Ein Paar für das kryptografische Modul „cm_code_signing“.
  - Ein Paar für das kryptografische Modul „cm_code_attest“.

  Weitere Informationen zu diesen Schlüsseln finden Sie unter Erstellen Sie Codesignaturschlüsselpaare und -zertifikate.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig: Diese Schlüsselpaare müssen von einer öffentlichen Zertifizierungsstelle oder von der internen Zertifizierungsstelle Ihrer Organisation signiert sein. Das Zertifikat kann nicht selbstsigniert werden.

- Eine Public Key Cryptography Standard #12-Datei (.p12), die Ihre End- und Zwischenzertifikate enthält.

Prozedur

1. Importieren Sie Ihre Schlüssel aus dem Schlüsselspeicher.
   a. Navigieren zu **Alle** > **Schlüsselverwaltung** > **Kryptografische Module** > **Alle**an.
   b. Suchen und öffnen Sie das kryptografische Modul `cm_code_signing`.
   c. **Wählen Sie in der Liste Krypto-Spezifikationen** den Namen der Krypto-Spezifikation aus, um sie zu öffnen.
   d. Wählen Sie im Bildschirm **Schlüssel aus Schlüsselspeicher importieren** die Option **Importschlüssel**aus.
2. Wiederholen Sie den ersten Schritt, um das kryptografische Modul `cm_code_attest`zu importieren.
3. **Geben Sie im Feld Schlüsselspeicher-Passwort** eingeben das Abfragepasswort ein, das Sie beim Generieren des RSA-Zertifikats erstellt haben.

   Hinweis: Das von Ihnen erstellte Abfragepasswort wird hier als **Schlüsselspeicher-Passwort**bezeichnet. In anderen Teilen des Prozesses kann dies entweder als **Importpasswort** oder als **Exportpasswort**bezeichnet werden. In allen Fällen ist dieses Passwort dasselbe Abfragepasswort, das Sie in den vorherigen Schritten erstellt haben.

4. Wählen Sie die Schaltfläche **Durchsuchen** neben **Schlüsselspeicher/Zertifikat importieren aus**.
5. Wählen Sie eine Public Key Cryptography Standard #12-Datei (.p12) aus, die Ihr Verteilungszertifikat enthält (im Abschnitt „Bevor Sie beginnen“ oben in diesem Dokument erwähnt).
6. Wählen Sie **OK**.

Wichtig: Wenn Sie Ihre eigene interne Zertifizierungsstelle verwenden, müssen Sie die Zwischenzertifikate der internen Zertifizierungsstelle entsprechend dem Prozess in den Schritten 5 bis 6 hochladen.

Bei einem erfolgreichen Import Ihres Schlüssels und Ihrer Zertifikate wird eine Bestätigungsmeldung angezeigt.

Sie können in der Tabelle „X.509-Zertifikate“ [sys_certificate] überprüfen, ob der Schlüssel und die Zertifikate in Ihrer Instanz vorhanden sind. Diese Datensätze haben den Typ **Truststore**-Zertifikat.

Sie können Ihren Schlüssel in der Tabelle „Kryptografische Module“ [sys_kmf_crypto_module] validieren.

Nächste Maßnahme

Exportieren Sie das Zertifikat in die Produktion. Details siehe Circle of Trust-Zertifikate vorbereiten.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Circle of Trust-Zertifikate vorbereiten

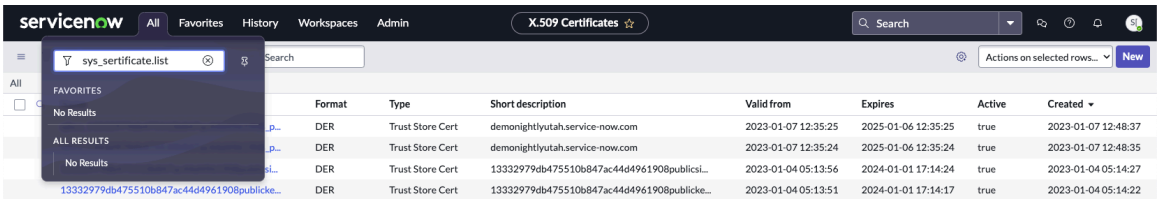
Erstellen Sie in der vertrauenswürdigen Umgebung ein Update Set, um das vertrauenswürdige Zertifikat in die Produktionsumgebung zu exportieren.

Vorbereitungen

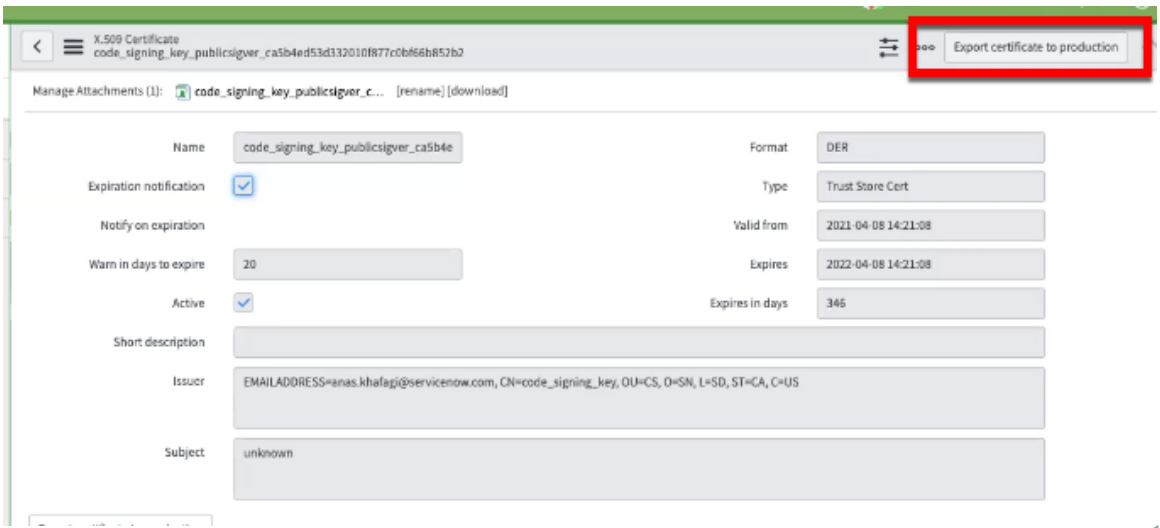
Erforderliche Rolle: admin, security_admin

Prozedur

1. Navigieren Sie in der vertrauenswürdigen Umgebung zu **sys_certificate.list**an.



2. Öffnen Sie das zuletzt erstellte X.509-Zertifikat, das mit dem Typ **Trust Store**-Zertifikat generiert wurde.
   Unter Umständen müssen Sie der Liste das Feld **Erstellt** hinzufügen, um den neuesten Datensatz zu finden. Siehe Persönliche Listen .
3. Wählen Sie **Zertifikat in Produktion exportieren aus**.



   Zusammen mit dem Zertifikat wird eine Signatur erstellt.
4. Navigieren zu **Systemupdate-Sätze** > **Lokale Update-Sätze**an.
5. Suchen und öffnen Sie das Codesignaturupdate.

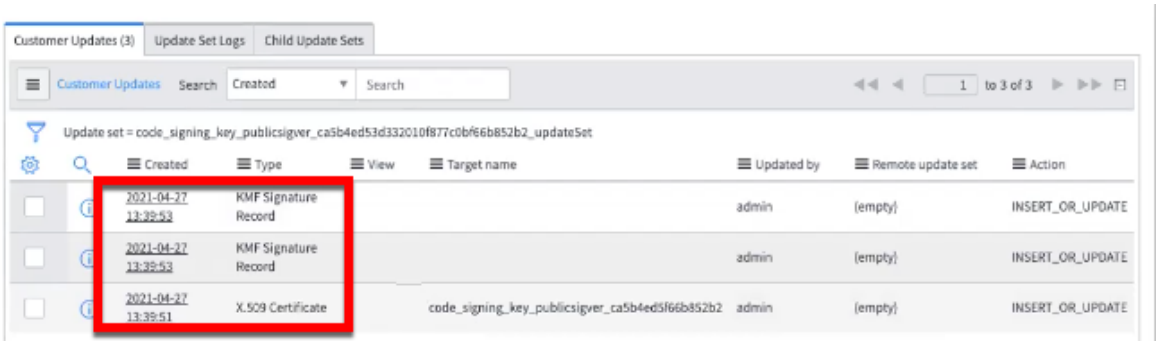
   Dieses Update beginnt mit dem Text `code_signing_key_publicsigver`.

   In den vorherigen Schritten wurde ein neuer Datensatz für einen Update-Satz für die Codesignatur erstellt. Um diesen Datensatz zu finden, sortieren Sie die Liste anhand des Felds **Erstellt von**, und suchen Sie nach Datensätzen mit im Feld **Name**.
6. Zeigen Sie die relevanten Signaturdatensätze und das X.509-Zertifikat an.

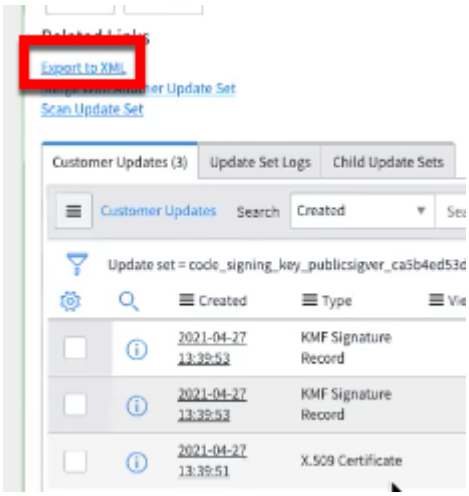
   Das Update Set enthält den Anhang für den Signaturdatensatz zusammen mit dem Eintrag der Signatur in der Tabelle und dem Zertifikat.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Wählen Sie den zugehörigen Link **In XML** exportieren aus.



8. Rufen Sie den Update-Satz in der Produktion ab.
Details siehe Update Set abrufen .

> **Wichtig:** Wiederholen Sie diese Schritte für Ihr zweites Schlüsselpaar. Denken Sie daran, dass es einen Schlüssel für die kryptografischen Module cm_code_attest und cm_code_signing gibt.

Importieren und installieren Sie Zertifikate für Circle of Trust

Rufen Sie das Update Set in der Produktion ab, um die Vertrauensstellung zwischen den beiden Instanzen herzustellen. Die Zertifikate, die erstellt wurden, um das Vertrauen in die vertrauenswürdige Instanz darzustellen, müssen in die Produktionsinstanz aufgenommen werden.

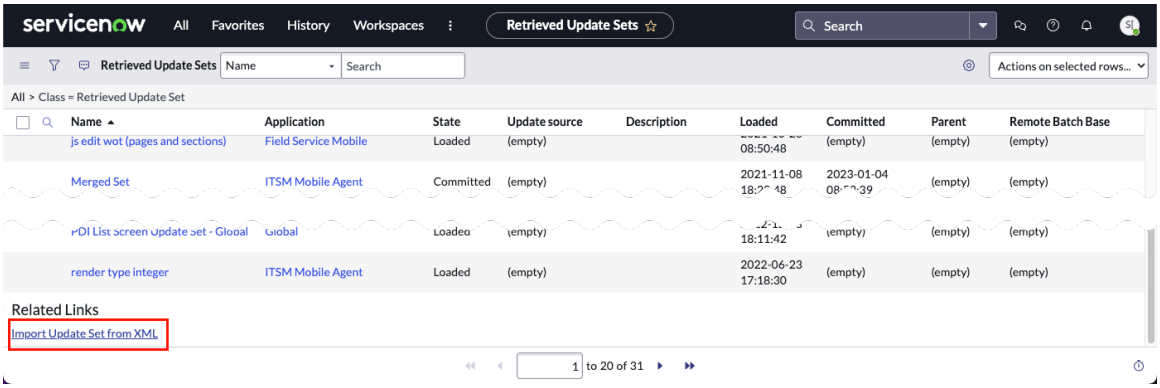
Vorbereitungen

Erforderliche Rolle: admin, security_admin

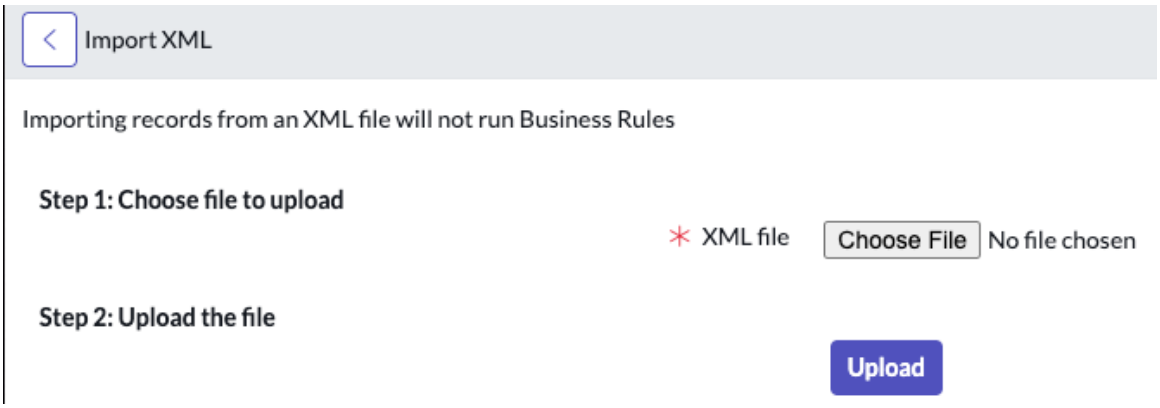
Prozedur

1. Navigieren Sie in der Produktionsinstanz zu **Systemupdate-Sätze** > **Abgerufene Update-Sätze**an.
2. Wählen Sie die Schaltfläche **Update Set aus XML** importieren unten links im Bildschirm aus.

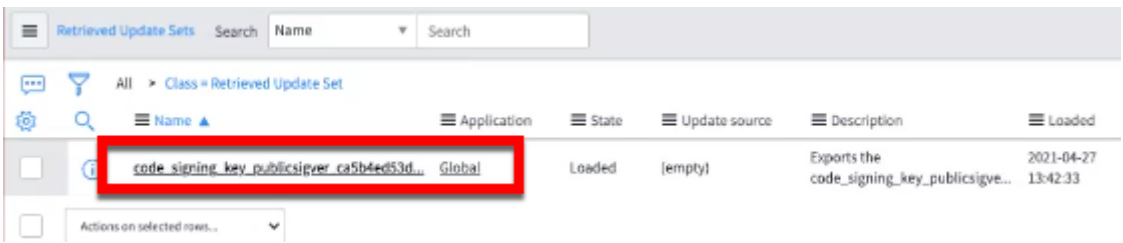
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Wählen **Sie Datei wählen** aus, und navigieren Sie zu der XML-Datei, die Sie in Circle of Trust-Zertifikate vorbereitenexportiert haben.



4. Wählen Sie **Hochladen** aus.
   Der Update-Satz für die Codesignatur wird der Tabelle der abgerufenen Update-Sätze hinzugefügt.

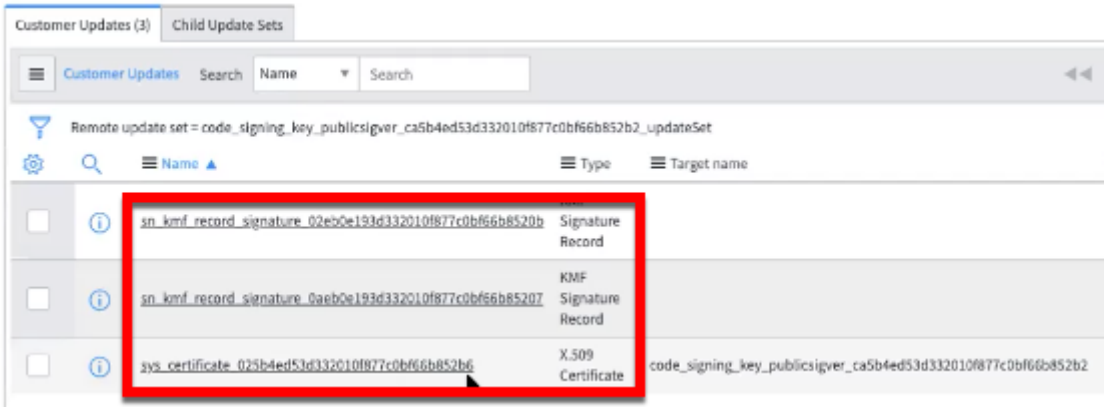


Hinweis: Wenn Ihr Update Set nicht angezeigt wird, filtern Sie Ihre Liste nach Datensätzen im Status Geladen, und sortieren Sie die Liste nach dem Feld **Geladen**.

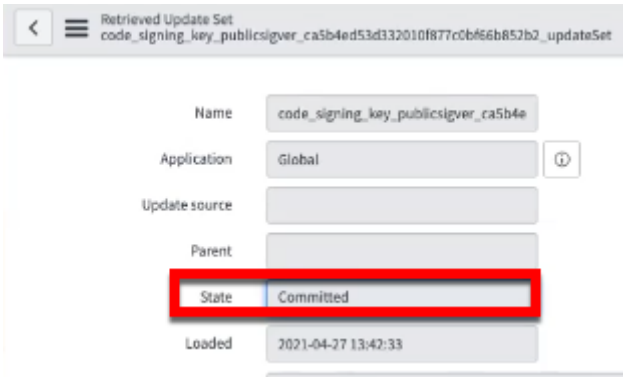
5. Öffnen Sie den Update-Satz-Datensatz, um sicherzustellen, dass die Tabelle „Kunden-Updates“ die folgenden drei Datensätze enthält:
   - Zwei KMF Signaturdatensätze
   - X.509-Zertifikat

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



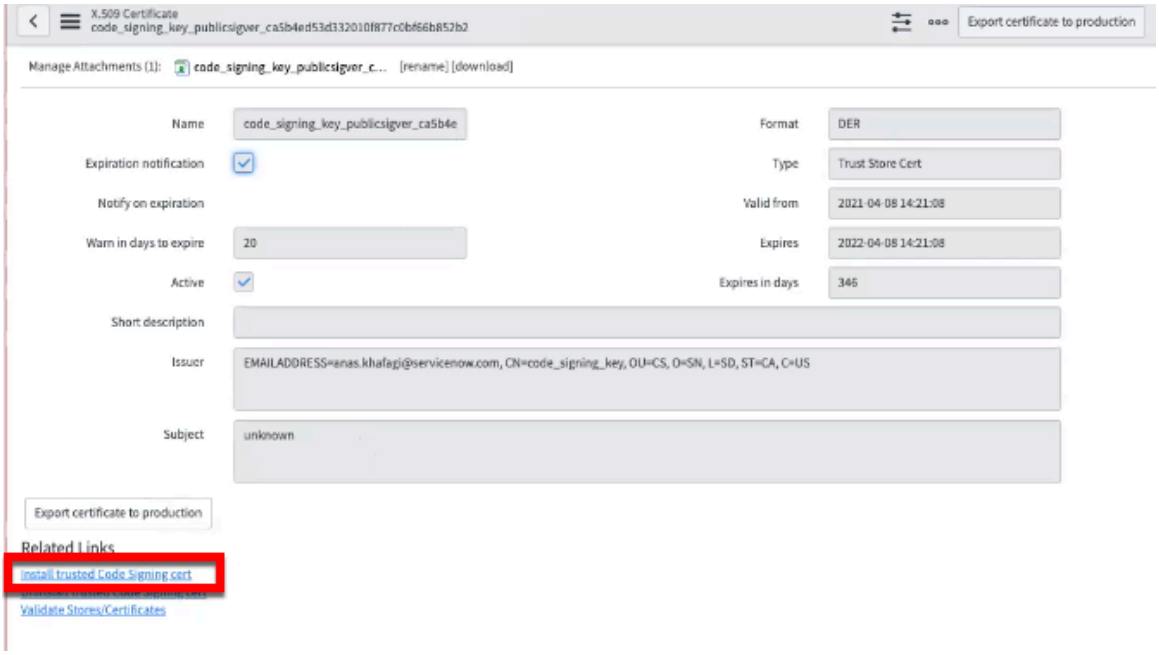
6. Wählen Sie **Update Set-Vorschau anzeigen aus**.
7. Wählen Sie **Update Set festlegen aus**.



Der Status des abgerufenen Update-Satzes wird auf **Bestätigt** aktualisiert.

8. Geben Sie im Navigator `sn_kmf_record_signature.list` ein, um die Liste der **KMF-Signaturdatensätze** zu öffnen.
9. Suchen Sie die beiden Signaturdatensätze KMF.
   Diese Datensätze sind die zuletzt erstellten Datensätze, bei denen das Feld **KMF-Signaturzweck** den Wert „ `Circle of Trust`"aufweist. Möglicherweise müssen Sie das Feld „ **Erstellt** " Ihrer Liste hinzufügen oder nach Datensätzen filtern, die am aktuellen Datum erstellt wurden.
10. Geben Sie im Navigator `sys_certificate.list` ein, und öffnen Sie den Datensatz mit dem Wert **Kurzbeschreibung** *`code_signing_key`* und dem Wert **Typ** `Truststore`-Zertifikat.
11. Wählen **Sie Zertifikat für vertrauenswürdige Codesignatur installieren**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Der Zertifikattyp wird auf *Vertrauenswürdiges Codesignaturzertifikat*aktualisiert.

Wichtig: Wiederholen Sie diese Schritte für Ihr zweites Zertifikat. Denken Sie daran, dass es ein Zertifikat für die kryptografischen Module cm_code_attest und cm_code_signing gibt.

Ergebnisse

Die Vertrauensstellung wird zwischen vertrauenswürdigen Instanzen und Produktionsinstanzen hergestellt. Sie können die Codesignatur aktivieren. Informationen zum Durchführen der Schritte finden Sie unter Codesignatur aktivieren.

Codesignatur aktivieren

Aktivieren Sie die Codesignatur in Ihrer vertrauenswürdigen Instanz außerhalb der Produktion, um die vertrauenswürdigen Instanzen zu identifizieren, die eine Verknüpfung zu Ihrer Produktionsinstanz herstellen.

Vorbereitungen

Erforderliche Rolle: security_admin und entweder sn_kmf.crypto_manager oder sn_kmf.admin

Bevor Sie die Codesignatur aktivieren, müssen Sie sich an das Team Kundenservice und Support wenden, um das Plugin „Codesignatur-Framework“ [com.glide.code_signing] zu aktivieren.

Warum und wann dieser Vorgang ausgeführt wird

Codesignaturaufträge mit signierten Update Sets werden verwendet, um die Codesignaturfunktion zu aktivieren oder zu deaktivieren. Es gibt keine andere Methode für diese Funktionalität. Dieser Prozess umfasst Folgendes:

- Erstellen Sie zwei Codesignaturaufträge in der vertrauenswürdigen Instanz: einen zum Aktivieren der Codesignatur und einen zum Deaktivieren der Codesignatur.
  - **Mit** der geplanten Aufgabe „Aktivieren“ wird der Prozess der MID-Server-Validierung von signiertem Code gestartet.
  - Mit der geplanten Aufgabe „ **Deaktivieren“** wird die Validierung von signiertem Code durch den MID-Server angehalten.

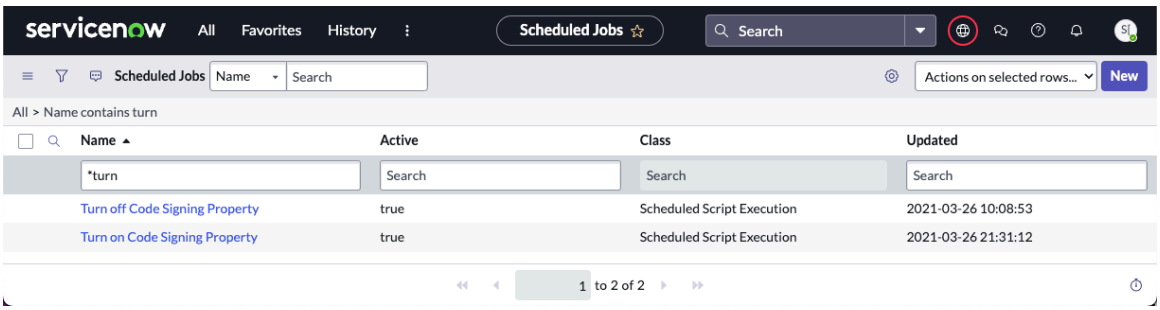
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Beim Deaktivieren der Codesignatur wird die Systemeigenschaft auf „ **false**“ gesetzt, die Liste der vertrauenswürdigen Freunde für die Codesignatur ist jedoch weiterhin verfügbar.

- Den Auftrag „ **Codesignatureigenschaft aktivieren** “ in ein Update Set einfügen.
- Den Auftrag in Produktion bringen.
- Verwenden Sie den Auftrag **Codesignatureigenschaft aktivieren** in der Produktion, wenn verifiziert wird, dass die Signatur von einer vertrauenswürdigen Instanz stammt.

Prozedur

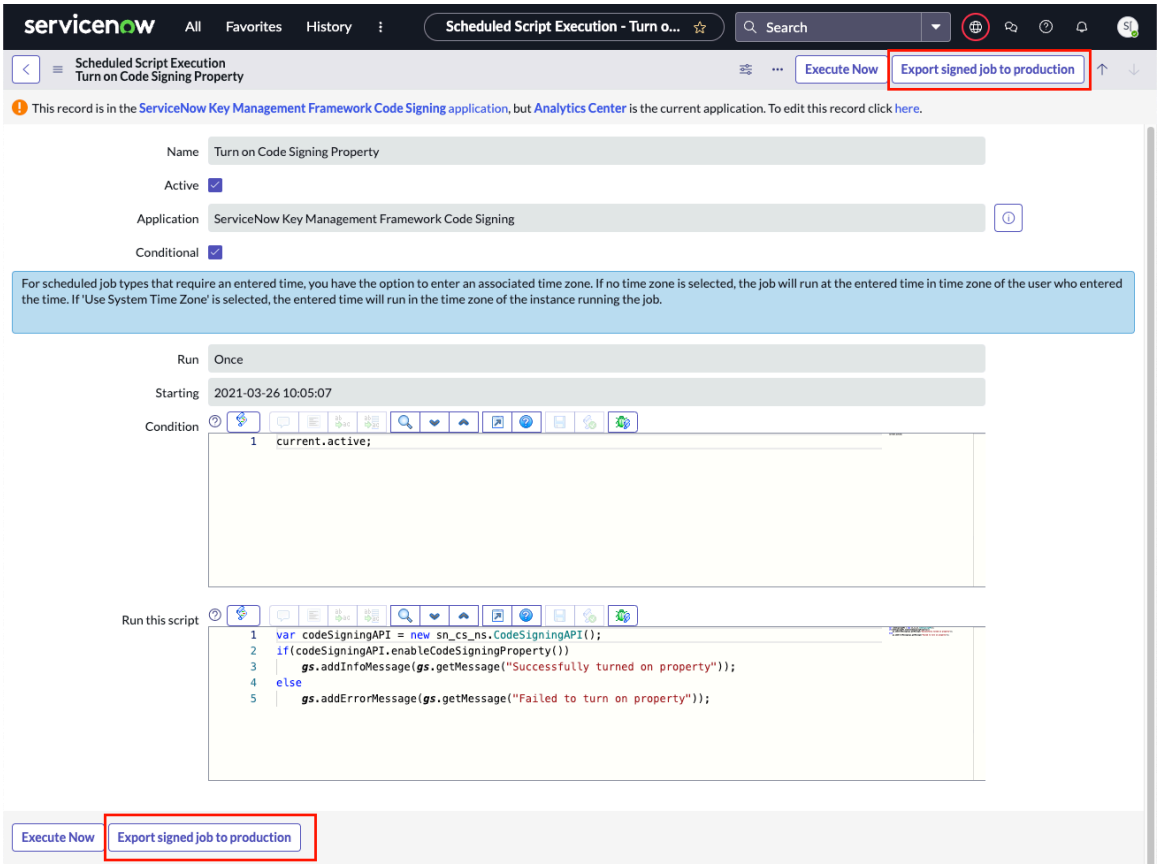
1. Navigieren Sie in Ihrer vertrauenswürdigen Instanz zu **Alle** > **Systemdefinition** > **Geplante Aufgaben**an.
2. Suchen Sie im Namensfeld nach „*Tour“.
3. Wählen **Sie Codesignatureigenschaft aktivieren aus**.



Die Formularlast der **geplanten Skriptausführung**. Dieses Formular enthält Informationen zum Aktivieren der Codesignatureigenschaft. Die Aufträge erstellen Update-Sätze, die die Aufträge und validierten Signaturen durch den Codesignaturprozess enthalten.

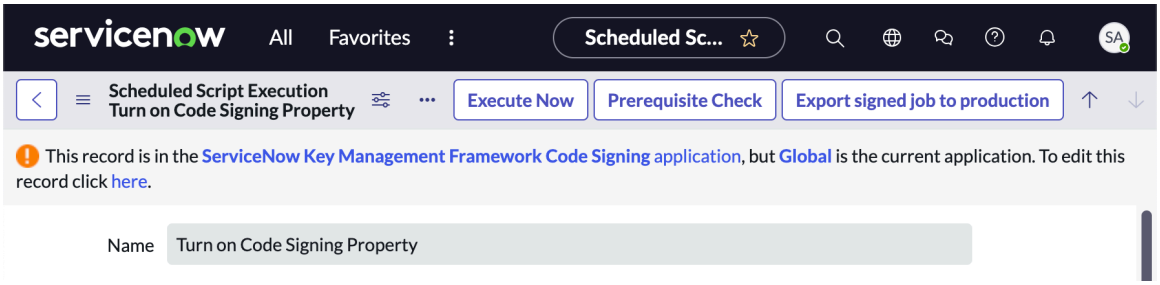
Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

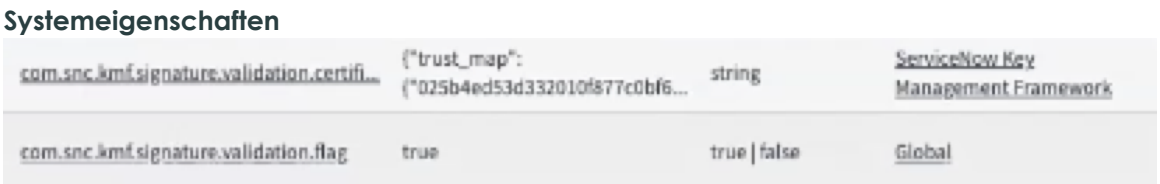


4. Um das Skript sofort auszuführen, signieren Sie das Zertifikat, erstellen Sie das Update Set, und wählen Sie **Export Signed Job to Production**(Signierten Auftrag in Produktion exportieren) aus.
   Sie können das Skript auch so konfigurieren, dass es nach einem festgelegten Zeitplan ausgeführt wird.
5. Navigieren zu **Systemupdate-Sätze** > **Lokale Update-Sätze**an.
6. Öffnen Sie alle Update-Sätze für die Codesignatureigenschaft, und wählen Sie **In XML exportieren aus**.
7. Melden Sie sich bei der Produktionsinstanz an.
8. Navigieren zu **Systemupdate-Sätze** > **Abgerufene Update-Sätze**an.
9. Wählen Sie die Schaltfläche **Update Set aus XML** importieren und anschließend das Update Set für die Codesignatureigenschaft aus.
10. Wählen **Sie Datei wählen** aus, laden Sie die Update-Sätze hoch und legen Sie sie fest.
11. Kehren Sie zur Liste der geplanten Aufgaben zurück, indem Sie zu navigieren **Alle** > **Systemdefinition** > **Geplante Aufgaben**an.
12. Öffnen Sie den Auftragsdatensatz **Codesignatureigenschaft aktivieren**.
13. Wählen Sie die Schaltfläche **Voraussetzungsprüfung** oben im Formular aus.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



14. Wählen Sie die Schaltfläche **Jetzt** ausführen aus, nachdem die Voraussetzungsprüfung abgeschlossen ist.
    Mit der geplanten Aufgabe **„Codesignatureigenschaft aktivieren** " wird der Prozess der MID-Server-Validierung von signiertem Code gestartet.
15. Geben Sie im Navigator `sn_kmf_record_signature.list` ein, um die Liste der **KMF-Signaturdatensätze** zu öffnen und nach Datensätzen zu filtern, bei denen der **KMF-Signaturzweck** „`Circle of Trust`" ist.
    Die Vertrauensstellung hat die Aufgaben verschoben, und wenn die Aufgaben verwendet werden, wird der Signaturverifizierungsprozess ausgeführt. Wenn die Aufträge, Signaturen und Zertifikate alle Teil von Circle of Trustsind, kann die Codesignatur mit Circle of Trust aktiviert werden.
16. Geben Sie im Navigator `sys_properties.list` ein, um die Liste der Systemeigenschaften zu öffnen.
17. Suchen Sie nach *`com_snc_kmf_signature.validation.flag`*, und stellen Sie sicher, dass der Wert auf **true**festgelegt ist.
18. Vergewissern Sie sich, dass die neue Eigenschaft *`com_snc_kmf_signature.validation.certificate`* in der Tabelle aufgeführt ist.



Verwenden Sie den Auftrag Circle of Trust in der Produktion, um die Vertrauensstellung zu überprüfen. In der Produktion kann kein direkter Auftrag ausgeführt werden, der versucht, Code zu signieren. Weitere Informationen zu Konfigurationsoptionen finden Sie unter Codesignatur konfigurieren.

Erstellen Sie Codesignaturschlüsselpaare und -zertifikate

Erstellen Sie zwei Schlüsselpaare für signierte Zertifikate, um eine Vertrauensstellung zwischen Ihren Instanzen in der Produktion und vertrauenswürdigen Instanzen herzustellen.

Um eine Vertrauensstellung zwischen Ihren Instanzen herzustellen, müssen Sie ein Schlüsselpaar und ein Zertifikat für jedes der kryptografischen Module `cm_code_attest` und `cm_code_signing erstellen`.

Das Erstellen von Schlüsselpaaren und Zertifikaten erfolgt mit einem kryptografischen Tool, das auf Ihrem lokalen Gerät installiert ist, z. B. OpenSSL. Weitere Informationen zu diesem Tool finden Sie unter https://www.openssl.org . Wenn Ihre Organisation andere kryptografische Tools wie LibreSSL oder GnuTLS verwendet, finden Sie ähnliche Schritte in der Dokumentation zu diesen Produkten.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spezifikationen des Schlüsselpaars

Die von Ihnen erstellten Schlüsselpaare müssen diese Anforderungen erfüllen.

Typ	RSA
Schlüssellänge	4096
Signaturalgorithmus	RSASSA_PKCS1_V1_5_SHA_512

Zertifikatspezifikationen

Zertifikate müssen von einer öffentlichen Zertifizierungsstelle signiert sein.

Geben Sie anwenderdefinierte Regeln in der ECC-Firewall an

Konfigurieren Sie die ECC-Firewall (External Communication Channel) in Ihrem MID-Server, indem Sie die anwenderdefinierten Regeln angeben, um die eingehende Nachricht selektiv zuzulassen oder abzulehnen und die Codesignaturkonfiguration zu überschreiben.

Sicherheitsadministratoren können die ECC-Firewall-Tags verwenden, um die Codesignaturkonfiguration zu überschreiben und bestimmte Vorgänge für MID-Serverzuzulassen oder abzulehnen. Diese anwenderdefinierten Regeln müssen in der YAML-Datei von unter `agent/boot-config.yaml angegeben werden`.

Diese Tags sind spezifisch für ein Protokoll. Die für das übergeordnete Tag angegebene Konfiguration gilt für das untergeordnete Tag. Wenn beispielsweise das HTTP-Protokoll zulässig ist, sind auch `REST-` und `SOAP-` Protokolle zulässig. Diese Tabelle beschreibt die verfügbaren übergeordneten und untergeordneten Tags.

Übergeordnetes Tag	Untergeordnetes Tag
DNS	
HTTP	• REST • SOAP
DIRECTORY_SERVICES	LDAP
SNMP	
SSH	• SCP • SFTP
SYSLOG	
FENSTER	• CIM • POWERSHELL • WMI • WINRM
JAVASCRIPT	

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übergeordnetes Tag	Untergeordnetes Tag
GROOVY	
VCS	GIT
DATENBANKEN	JDBC
DATA_SOURCES	
INTEGRATION_HUB	
ITOM	• CLOUD_PROVISIONING_GOVERNANCE • DISCOVERY • EVENT_MANAGEMENT • INTEGRITÄT_LOG_ANALYTICS • SERVICE_MAPPING
ORCHESTIERUNG	

So konfigurieren Sie die anwenderdefinierten Regeln:

1. Identifizieren Sie in MID-Serverdie Datei „`boot-config-sample.yaml`".
2. Benennen Sie die YAML-Datei in „`boot-config.yaml`" um, und verschieben Sie die Datei an den folgenden Speicherort: `agent/boot-config.yaml`.
3. Geben Sie in der YAML-Datei die anwenderdefinierten Regeln an, und speichern Sie die Änderungen. Beispiel für die YAML-Datei:

```
security:
  eccFirewall:
    mode: enforcing
    rules:
      - tags: [rest]
        action: accept
      - tags: [soap]
        action: accept
      - tags: [jdbc]
        action: reject
```

4. Starten Sie MID-Serverneu.

Ändern Sie Ihre Root of Trust-Konfiguration

Vertrauen und verwenden Sie Ihre eigenen Zertifikate, anstatt sich auf die Build-Zertifikate von ServiceNow zu verlassen (Standard), indem Sie zu Ihrem Root of Trust (ROT) wechseln. ServiceNow -Komponenten wie Skripteinbindungen, Business-Regeln usw. werden zur Build-Zeit mit einem ServiceNow -Build-Zeitschlüssel signiert (Verifizierungszertifikat ist das Build-Zertifikat ServiceNow).

Root of Trust ändern

Um den Root of Trust für diese Datensatzsignaturen zu ändern, müssen Sie dem Prozess zum Ändern des Root of Trust folgen.

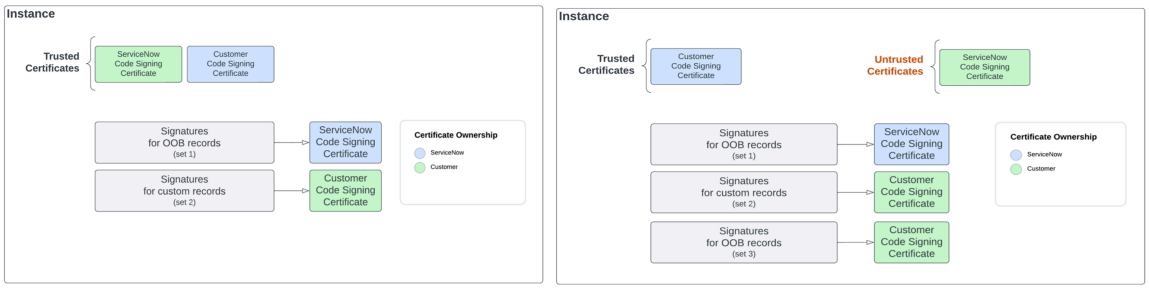
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Generieren und migrieren Sie mit dem bereitgestellten Zertifikat einen neuen Satz von Signaturen für alle bereitgestellten Komponenten.
- Deaktivieren Sie die Eigenschaft „Root of Trust“ mithilfe einer geplanten Aufgabe.

Weitere Informationen zu diesen Schritten finden Sie unter Migrieren Sie Signaturen, um ein Kundenzertifikat zu verwenden und Root of Trust für ServiceNow deaktivieren.

Auswirkungen auf den Signaturgenerierungs- und -verifizierungsprozess

Standardmäßig werden Build-Zertifikate für Codesignatur während des Signaturverifizierungsprozesses als vertrauenswürdig eingestuft. Nachdem Sie diese Änderung vorgenommen haben, akzeptiert Ihre Instanz Signaturen nur noch von Ihrem eigenen Codesignaturzertifikat.



ROT-Eigenschaft auf „falsch“ festgelegt (Standard)	ROT-Eigenschaft auf „wahr“ festgelegt
• Bei der Überprüfung werden Signaturen mit Build-Zertifikaten als vertrauenswürdig eingestuft. • Wenn Sie beim Signieren keine Schlüssel angeben, wird der Instanzsignaturschlüssel als Sicherungsschlüssel verwendet. • Der REST-Endpunkt der Signatur ServiceNow *api/sn_kmf/signature/certificates* gibt zusammen mit anderen in der Instanz vorhandenen Zertifikaten Build-Zertifikate für die Codesignatur zurück.	• Bei der Überprüfung sind Signaturen mit Build-Zertifikaten nicht vertrauenswürdig. • Wenn Sie beim Signieren keine Schlüssel angeben, wird das Signieren nicht ausgeführt. • Der Signatur-REST-Endpunkt *api/sn_kmf/signature/certificates* schließt ServiceNow Build-Zertifikate (San Diego, Vancouver PKI, W PKI) aus.

Auswirkung auf Ihren MID-Server

Wenn die ROT-Eigenschaft auf „false“ festgelegt ist

Wenn Sie Ihre ROT-Eigenschaft auf dem Standardwert („false“) belassen, hat dies keine Auswirkungen auf Ihren MID-Server.

Wenn Codesignatur aktiviert ist und die ROT-Eigenschaft auf „wahr“ festgelegt ist

- Die API *„isTrusted()* "gibt für Signaturen mit einem Build-Zertifikat „ `false` “ zurück.
- Die API *„isTrusted()* "gibt für Signaturen mit Ihrem Zertifikat „ `true` “ zurück.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Der REST-API-Aufruf für Zertifikate schließt Build-Zertifikate aus.
- Möglicherweise werden in den Protokollen MID-Server-Probleme angezeigt, z. B. Meldungen zu `fehlgeschlagenen Signaturvalidierungen`.

Migrieren Sie Signaturen, um ein Kundenzertifikat zu verwenden

Führen Sie einen Signierauftrag aus, um Ihre Signaturen zu einem Kunden-Root of Trust (ROT) zu migrieren.

Vorbereitungen

Erforderliche Rolle: admin, security_admin und sn_kmf.cryptographic_manager

Codesignatur muss in der Produktion und in der vertrauenswürdigen Instanz aktiviert sein. Sie können dies überprüfen, indem Sie überprüfen, ob die **Systemeigenschaft com.snc.kmf.signature.validation.flag** auf `true`festgelegt ist.

Dieses Verfahren ist Teil einer Reihe von Verfahren zum Ändern des Root of Trust (ROT) eines Kunden in Ihren Instanzen. Eine Übersicht über diesen Prozess finden Sie unter Ändern Sie Ihre Root of Trust-Konfiguration.

Prozedur

1. Melden Sie sich bei Ihrer Produktionsinstanz an.
2. Navigieren zu **Alle** > **Systemdefinition** > **Geplante Aufgaben**an.
3. Suchen und öffnen Sie **ROT – Update-Datensatz generieren, um Signaturen mithilfe der geplanten Aufgabe „Kundenzertifikat“ zu migrieren**.
4. Wählen Sie unten im Formular **Jetzt ausführen**aus.
5. Navigieren zu **Alle** > **Systemsicherheit** > **Security-Aufträge** > **Neu erstellen:**an.
6. Wählen Sie bei der Eingabeaufforderung **Signierauftrag**aus.
7. Füllen Sie im Formular **„Signierauftrag“** die Felder nach Bedarf aus.

Feld	Wert
Name	Erstellen Sie einen eindeutigen Namen für Ihren Job.
Typ	Wählen Sie **Update Set signieren aus**.
Tabelle	Wählen Sie den in den vorherigen Schritten erstellten Update Set aus. Der Name des Update Set beginnt mit `change_root_of_trust_updateSet`.

8. Klicken Sie mit der rechten Maustaste auf den Formular-Header, und wählen **Sie Speichern**, um diesen Datensatz zu speichern.
9. Klicken Sie mit der rechten Maustaste auf den Formularheader, und wählen Sie **Exportieren** > **XML (dieser Datensatz)** um diesen Datensatz als XML-Datei zu exportieren.
10. Melden Sie sich bei Ihrer vertrauenswürdigen Instanz an.
11. Navigieren zu **Alle** > **Systemsicherheit** > **Security-Aufträge** > **Alle**an.
12. Klicken Sie mit der rechten Maustaste auf den Listenheader, und wählen Sie **XML importieren**aus.
13. Wählen Sie im Formular „ **XML** importieren“ **Datei** wählen, und wählen Sie die XML-Datei aus, die Sie in den vorherigen Schritten heruntergeladen haben.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

14. Wählen Sie **Hochladen** aus.
15. Öffnen Sie in der Liste den importierten Sicherheitsauftrag.
16. Wählen Sie **„Codesignaturauftrag in Produktion exportieren“ aus**.
    Mit dieser Aktion wird der Auftrag signiert und in ein neues Update Set eingefügt, das Sie in Ihre Produktionsinstanz importieren können.

    Wichtig: Nach dem Signieren des Auftrags müssen Sie die nächsten Schritte innerhalb von 10 Minuten ausführen. Wenn Sie diesen Zeitraum überschreiten, können Sie den Auftrag mithilfe der folgenden Schritte erneut signieren, wodurch ein weiteres signiertes Update Set erstellt wird.

17. Navigieren zu **Alle** > **Systemupdate-Sätze** > **Lokale Update-Sätze**an.
18. Suchen Sie das in den vorherigen Schritten erstellte Update Set.
    Der Name beginnt mit `SIGN_UPDATE_SET_updateSet`.
19. Wählen Sie „ **XML** exportieren“, um Ihr Update Set als XML-Datei zu exportieren.
20. Melden Sie sich bei Ihrer Produktionsinstanz an.
21. Navigieren zu **Alle** > **Systemupdate-Sätze** > **Abgerufene Update-Sätze**an.
22. Wählen Sie unten in der Liste **Update Set aus XML importieren aus**.
23. Wählen Sie im Formular „ **XML** importieren“ **Datei** wählen, und wählen Sie die XML-Datei aus, die Sie in den vorherigen Schritten heruntergeladen haben.
24. Wählen Sie **Hochladen** aus.
25. Navigieren zu **Alle** > **Systemupdate-Sätze** > **Abgerufene Update-Sätze**, und öffnen Sie den Update-Satz, beginnend mit `SIGN_UPDATE_SET_updateSet`.
26. Wählen Sie **Update Set-Vorschau anzeigen aus**.
27. Wählen Sie nach Abschluss der Vorschau die **Option Update Set festlegen**aus.
28. Navigieren zu **Alle** > **Systemsicherheit** > **Security-Aufträge** > **Alle**an.
29. Öffnen Sie den importierten Sicherheitsauftrag.
30. Wählen Sie **Start** aus, um den Sicherheitsauftrag auszuführen.

    Nach Abschluss der Sicherheitsaufgabe werden im Feld **Zusammenfassung** Informationen zum Status der Aufgabe angezeigt.

    Wenn sich der Auftrag im Status „Fertig“ befindet, müssen alle Signaturen von Update-Satz-Datensätzen das vom Kunden bereitgestellte Zertifikat als Verifizierungszertifikat verwenden. Sie können dies in der Tabelle mit den KMF-Signaturdatensätzen [sn_kmf_record_signature] überprüfen.

Nächste Maßnahme
Informationen zum Fortsetzen des Root of Trust-Konfigurationsprozesses finden Sie unter Root of Trust für ServiceNow deaktivieren.

Root of Trust für ServiceNow deaktivieren

Führen Sie eine geplante Aufgabe in Ihrer vertrauenswürdigen Instanz außerhalb der Produktion aus, um Root of Trust zu deaktivieren.

Vorbereitungen
Erforderliche Rolle: admin, security_admin und sn_kmf.cryptographic_manager

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Codesignatur muss in der Produktion und in der vertrauenswürdigen Instanz aktiviert sein. Sie können dies überprüfen, indem Sie überprüfen, ob die **Systemeigenschaft com.snc.kmf.signature.validation.flag** auf `true`festgelegt ist.

Dieses Verfahren ist Teil einer Reihe von Verfahren zum Ändern des Root of Trust (ROT) eines Kunden in Ihren Instanzen. Eine Übersicht über diesen Prozess finden Sie unter Ändern Sie Ihre Root of Trust-Konfiguration.

Prozedur

1. Melden Sie sich bei Ihrer vertrauenswürdigen Instanz an.
2. Navigieren zu **Alle** > **Systemdefinition** > **Geplante Aufgaben**an.
3. Öffnen Sie die geplante Aufgabe **Root of Trust für ServiceNow deaktivieren**.
4. Wählen Sie die **Option Signierten Auftrag in Produktion exportieren aus**.
5. Navigieren zu **Alle** > **Systemupdate-Sätze** > **Lokale Update-Sätze**an.
6. Suchen und öffnen Sie das Update Set **ServiceNow Root of Trust** deaktivieren.
7. Wählen Sie „ **XML** exportieren“, um Ihr Update Set als XML-Datei zu exportieren.
8. Melden Sie sich bei Ihrer Produktionsinstanz an.
9. Navigieren zu **Alle** > **Systemupdate-Sätze** > **Abgerufene Update-Sätze**an.
10. Wählen Sie unten in der Liste **Update Set aus XML importieren aus**.
11. Wählen Sie im Formular „ **XML** importieren“ **Datei** wählen, und wählen Sie die XML-Datei aus, die Sie in den vorherigen Schritten heruntergeladen haben.
12. Wählen Sie **Hochladen** aus.
13. Navigieren zu **Alle** > **Systemupdate-Sätze** > **Abgerufene Update-Sätze**, und öffnen Sie das Update Set **ServiceNow Root of Trust** deaktivieren.
14. Wählen Sie **Update Set-Vorschau anzeigen aus**.
15. Wählen Sie nach Abschluss der Vorschau die **Option Update Set festlegen**aus.
16. Navigieren zu **Alle** > **Systemdefinition** > **Geplante Aufgaben**an.
17. Öffnen Sie die geplante Aufgabe, die im Update Set importiert wurde.
18. Wählen Sie die Schaltfläche **Jetzt** ausführen aus, um die Aufgabe auszuführen.

Ergebnisse

Durch die Ausführung der geplanten Aufgabe wird die ROT-Eigenschaft auf „true“ festgelegt. Ihre Instanz ist so konfiguriert, dass sie den Root of Trust des Kunden verwendet.

Codesignatur verwenden

Erfahren Sie, wie Sie Datensätze, Nachrichten und Anhänge signieren, um die Authentizität und Integrität Ihrer Daten zu überprüfen.

Signieren Sie die Datensätze der JDBC-Datenquelle in der Produktionsinstanz

Verwenden Sie Update-Sätze, um die JDBC-Datenquellen zu signieren und zu validieren, indem Sie die Codesignatur in der Produktion und in vertrauenswürdigen Instanzen aktivieren.

Signieren Sie die REST- und SOAP-Nachrichten in der Produktionsinstanz

Verwenden Sie Update-Sätze, um die REST- und SOAP-Nachrichten zu signieren und zu validieren, indem Sie die Codesignatur in der Produktion und in vertrauenswürdigen Instanzen aktivieren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Signieren Sie die Flows, Subflows und Aktionen in der Produktionsinstanz

Verwenden Sie Update-Sätze, um die Flows, Subflows und Aktionen zu signieren und zu validieren, indem Sie die Codesignatur in der Produktion und in vertrauenswürdigen Instanzen aktivieren.

Signieren Sie bestimmte Datensätze oder Anhänge

Erstellen Sie einen Sicherheitsauftrag, um bestimmte Datensätze oder Anhänge zu signieren und nicht alle Datensätze oder Anhänge in einer Tabelle.

Eigenständiges Signiertool

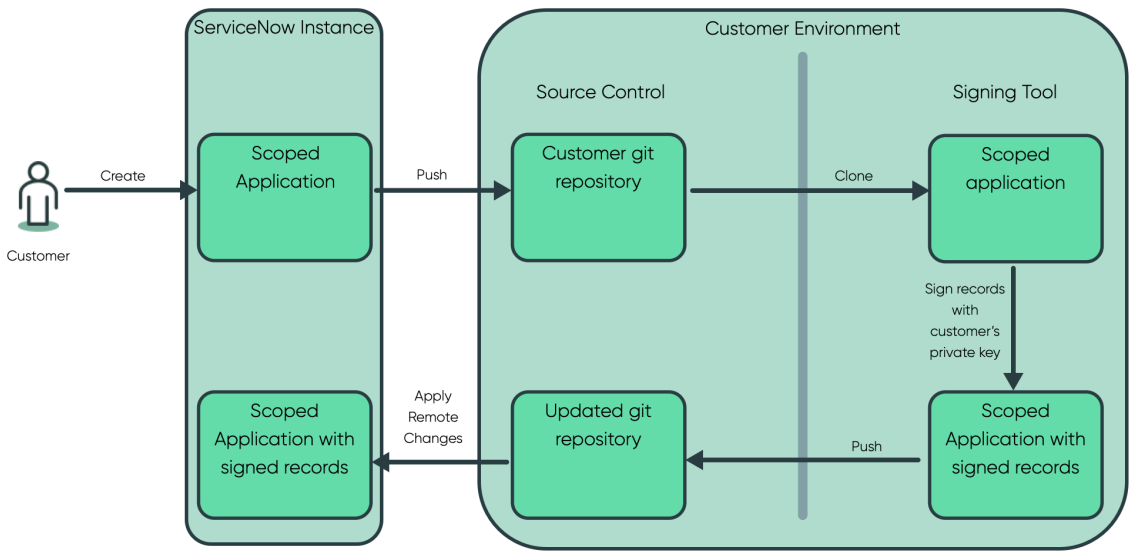
Verwenden Sie das eigenständige Signiertool, um unterstützte Datensätze in -Anwendungen ServiceNow mit Ihrem eigenen privaten Schlüssel zu signieren.

Eigenständiges Signiertool

Verwenden Sie das eigenständige Signiertool, um unterstützte Datensätze in -Anwendungen ServiceNow mit Ihrem eigenen privaten Schlüssel zu signieren.

Verwenden Sie das Signiertool zum Signieren von Datensätzen in ServiceNow -Apps. Das Tool generiert Signaturen für Datensätze in Ihrer lokalen Umgebung mit Ihrem eigenen privaten Schlüssel.

Workflow des Signaturtools



1. Erstellen oder wählen Sie eine vorhandene ServiceNow -Anwendung mit zu signierenden Datensätzen, wie z. B. Business-Regeln oder Skripteinbindungen.
2. Übertragen Sie die Anwendung in Ihr Git-Repository, das sich in Ihrer Umgebung befindet.

   Hinweis: Anwendungen können mithilfe der Quellcodeverwaltungsintegration zwischen einem Git-Repository und Ihrer -Instanz synchronisiert werden. Weitere Informationen zur Konfiguration und Verwendung dieser Integration finden Sie unter Integration der Quellcodeverwaltung .

3. Klonen Sie die Anwendung in Ihrer lokalen Umgebung.
4. Verwenden Sie das Signiertool (auch in Ihrer lokalen Umgebung), um die unterstützten Datensätze aus der geklonten Anwendung ServiceNow mit Ihrem privaten Schlüssel zu signieren. Das Signiertool erstellt Signaturdatensätze und X.509-Zertifikatdatensätze

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

[sys_certificate]. Weitere Informationen zur Verwendung des Signiertools finden Sie unter Verwenden des Signiertools.

5. Übertragen Sie die aktualisierte Anwendung in Ihr Git-Repository.
6. Importieren Sie in Ihrer -Instanz die aktualisierte Anwendung, indem Sie Remote-Changes anwenden.

Verwenden des Signiertools

Erfahren Sie, wie Sie mit dem Signiertool unterstützte Datensätze in den Anwendungen ServiceNow signieren.

Vorbereitungen

Erforderliche Rolle: admin

Um diese Schritte ausführen zu können, benötigen Sie:

- Eine Anwendung ServiceNow, die über zu signierende Datensätze verfügt.
- Ein privater Schlüssel zum Signieren von Datensätzen.
- Das Skript *signRecords.sh* in Ihrer lokalen Umgebung mit Ausführungsberechtigung.

Wichtig: Das Skript *signRecords.sh* ist in der JAR-Datei signing-tool enthalten, die Sie über anfordern müssen ServiceNow Kundensupport an.

Prozedur

1. Navigieren Sie in Ihrer lokalen Umgebung zu dem Verzeichnis, das das Skript *signRecords.sh* enthält.
2. Verwenden Sie das folgende Befehlsformat, um Ihre Datensätze zu signieren:

```
./signRecords.sh -d [Path to the root directory of the ServiceNow
 Application to Sign] -f [Path to the Keystore file]
```

   Beispiel:

```
./signRecords.sh -d /users/abc/ServiceNow-App-1
 -f /users/abc/codesigning.p12
```

3. Geben Sie das Passwort für den Schlüsselspeicher ein, wenn Sie dazu aufgefordert werden. Drücken Sie die Eingabetaste, wenn kein Passwort vorhanden ist.
4. Überprüfen Sie die Ausgabe, um eine erfolgreiche Signierung zu bestätigen.

```
Sep 26, 2022 2:41:09 PM com.snc.java.commands.ACommand start
INFO: CODESIGN: executing codesigning...
Sep 26, 2022 2:41:09 PM com.snc.core.codesigning.CodeSignerSupplier get
INFO: CODESIGN: signing record for documentId:
 65e811327702111057416efe7c5a994f
Sep 26, 2022 2:41:11 PM com.snc.java.commands.ACommand start
INFO: CODESIGN: codesigning successfully completed!
```

   Im obigen Ausgabebeispiel hat das Signiertool den Datensatz mit der angegebenen Schlüsselspeicherdatei signiert. Sie können auch Folgendes anzeigen:

   - Das Skript hat den unterstützten Datensatz `65e811327702111057416efe7c5a994f gefunden` und signiert.
   - Im Verzeichnis „ServiceNow-App-1“ wurden zwei Datensätze erstellt: `sys_certificate.xml` und `sn_kmf_record_signature.xml`.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Importieren Sie die aktualisierte Anwendung zurück in Ihre -Instanz, indem Sie Remote-Changes in Studioanwenden.
   Weitere Informationen finden Sie unter Remote-Changes übernehmen .

Argumente des Signiertools

Erfahren Sie mehr über die verfügbaren Argumente für das Signiertool.

Befehlszeilenargumente

Argument	Erforderlich	Beschreibung
-d	Ja	Stammverzeichnis des zu signierenden Projekts. Sollte ein Projektverzeichnis (zufällig 32 alphanumerisch), die Datei „sn_source_control.properties“ und<project_name> IML-Datei
-f	Ja	Der Dateipfad des Schlüsselspeichers.
-a	Nein	Alias für den Zugriff auf einen bestimmten Eintrag im Schlüsselspeicher.
-c	Nein	Verketten Sie Datensatzsignaturen in einer Datei.
-k	Nein	Passwort für den Zugriff auf den im Schlüsselspeicher gespeicherten Schlüssel. Sie können dieses Passwort auch eingeben, wenn Sie dazu aufgefordert werden, anstatt innerhalb des Arguments.
-o	Nein	Signieren Sie mit einem neuen Zertifikat anstelle aller vorhandenen sys_cert-Dateien.
-p	Nein	Passwort für den Zugriff auf den Schlüsselspeicher, wenn ein Passwort vorhanden ist. Sie können dieses Passwort auch eingeben, wenn Sie dazu aufgefordert werden, anstatt innerhalb des Arguments.
-W	Nein	Löschen Sie alle vorhandenen Signaturdatensatzdateien.
-H	Nein	Diese Hilfemeldung anzeigen und beenden.

Signieren Sie die Datensätze der JDBC-Datenquelle in der Produktionsinstanz

Verwenden Sie Update-Sätze, um die JDBC-Datenquellen zu signieren und zu validieren, indem Sie die Codesignatur in der Produktion und in vertrauenswürdigen Instanzen außerhalb der Produktion aktivieren.

- Richten Sie Circle of Trust zwischen Produktionsinstanz und vertrauenswürdigen Instanzen ein.
- Erforderliche Rolle: security_admin

Hinweis:

- MID-Server verarbeitet die Dateidatenquellen nicht, und daher sind diese Datenquellen nicht mit Code signiert.
- LDAP-Datenquellen können nicht signiert werden.

Signieren Sie vorhandene Datenquellen vom Typ JDBC

Verwenden Sie Update-Sätze, um Massensignaturaufträge in die Produktionsinstanz zu bringen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: security_admin

Prozedur

1. Konfigurieren Sie in der vertrauenswürdigen Instanz außerhalb der Produktion den KMF-Signaturauftrag, um die Datenquellen zu signieren.

   a. Navigieren zu **Systemsicherheit** > **Security-Aufträge** > **Alle**an.

   b. Klicken Sie auf **Neu**.

   c. Füllen Sie diese Werte im Formular aus.

Feld	Beschreibung
Name	Name zur Identifizierung des Datensatzes.
Typ	Typ des Verschlüsselungsauftrags. Wählen Sie **Massensignaturdatensätze aus**.
Tabelle	Tabelle, aus der die Datensätze signiert werden sollen. Wählen Sie **Datenquelle aus**.

   d. Klicken Sie **auf Codesignaturauftrag in Produktion exportieren**.
   Es wird eine Bestätigungsmeldung angezeigt, dass das Update Set signiert ist.

   e. Exportieren Sie das generierte Update Set in eine XML-Datei.

2. Importieren Sie in der Produktionsinstanz das Update Set, und legen Sie es fest, um die signierten Massenaufträge von der vertrauenswürdigen Instanz abzurufen.

   a. Navigieren zu **Systemsicherheit** > **Security-Aufträge** > **Alle**an.

   b. Öffnen Sie den Update-Satz, der aus der vertrauenswürdigen Instanz exportiert wurde.

   c. Klicken Sie auf **Start**.
   Es wird eine Bestätigungsmeldung angezeigt, dass die Datensätze signiert sind.

Signieren Sie neue Datenquellen vom Typ JDBC

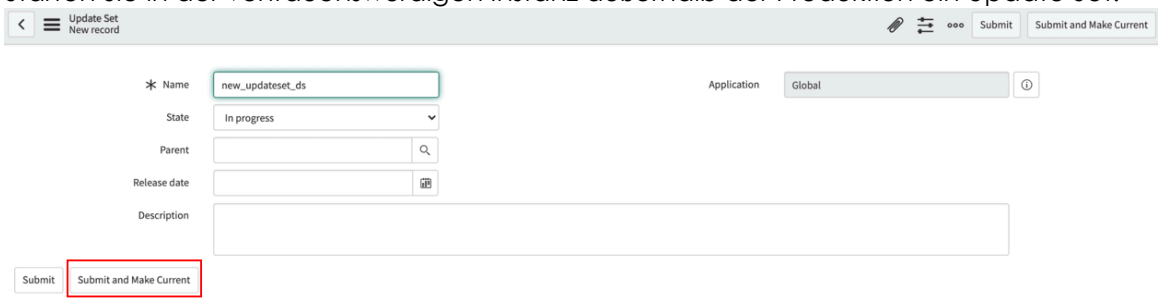
Verwenden Sie Update-Sätze, um das signierte Update Set in die Produktionsinstanz zu bringen.

Vorbereitungen
Erforderliche Rolle: sn_kmf.cryptographic_manager

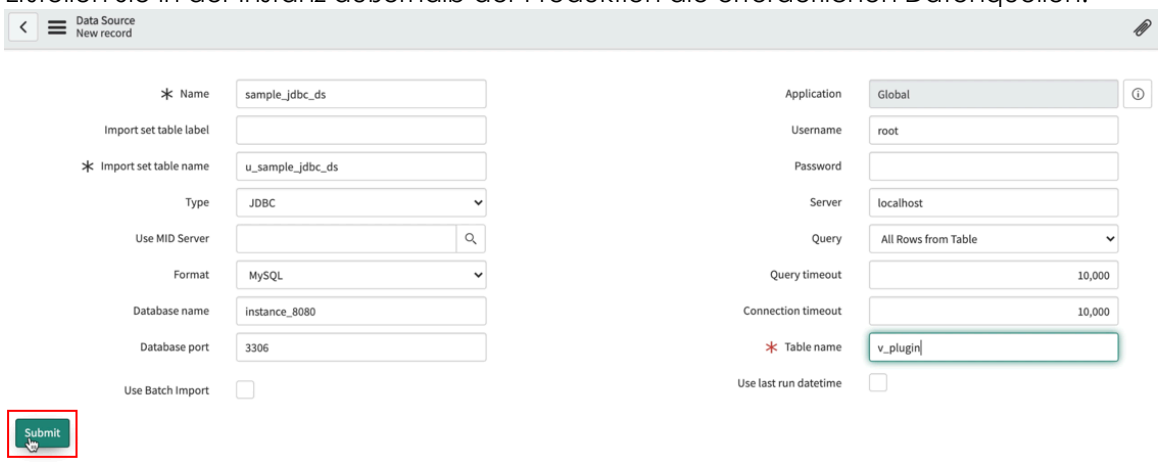
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Starten Sie in der vertrauenswürdigen Instanz außerhalb der Produktion ein Update Set.

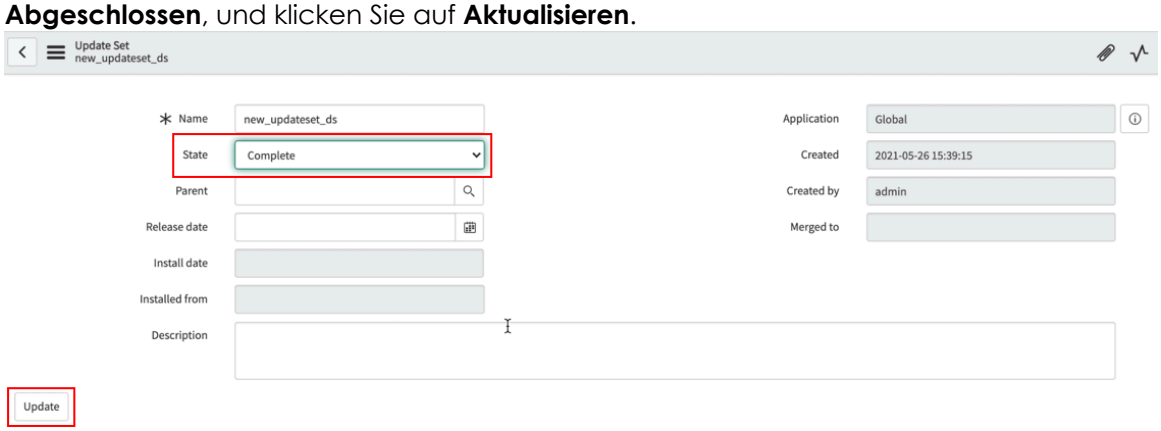


2. Erstellen Sie in der Instanz außerhalb der Produktion die erforderlichen Datenquellen.



Die Datenquellen werden dem Update Set hinzugefügt.

3. Ändern Sie in der Instanz außerhalb der Produktion den Status des Update Set in **Abgeschlossen**, und klicken Sie auf **Aktualisieren**.



4. Signieren Sie in der Instanz außerhalb der Produktion den Update-Satz, indem Sie einen Verschlüsselungsauftrag erstellen.

   a. Navigieren zu **Systemsicherheit** > **Security-Aufträge** > **Alle**an.

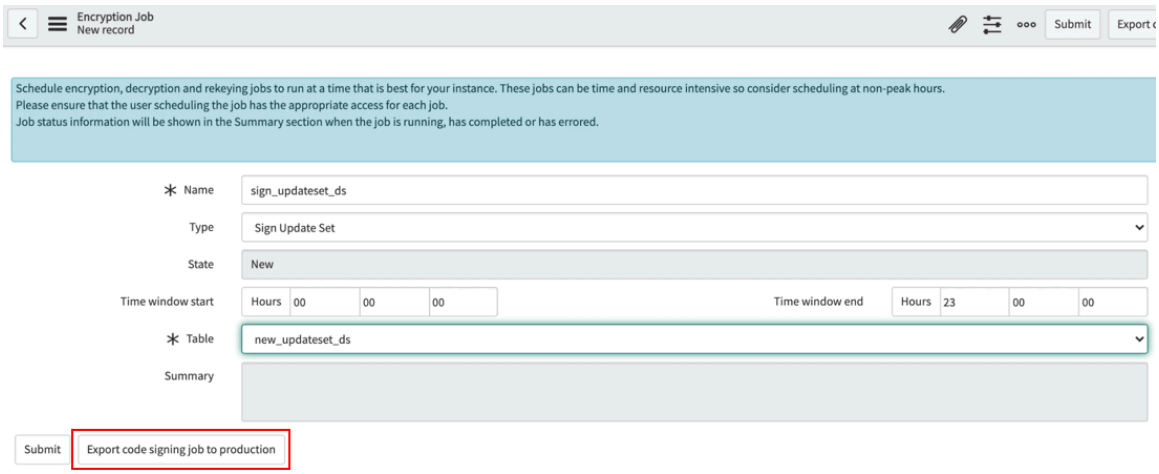
   b. Klicken Sie auf **Neu**.

   c. Füllen Sie diese Werte im Formular aus.

Feld	Beschreibung
Name	Name zur Identifizierung des Datensatzes.

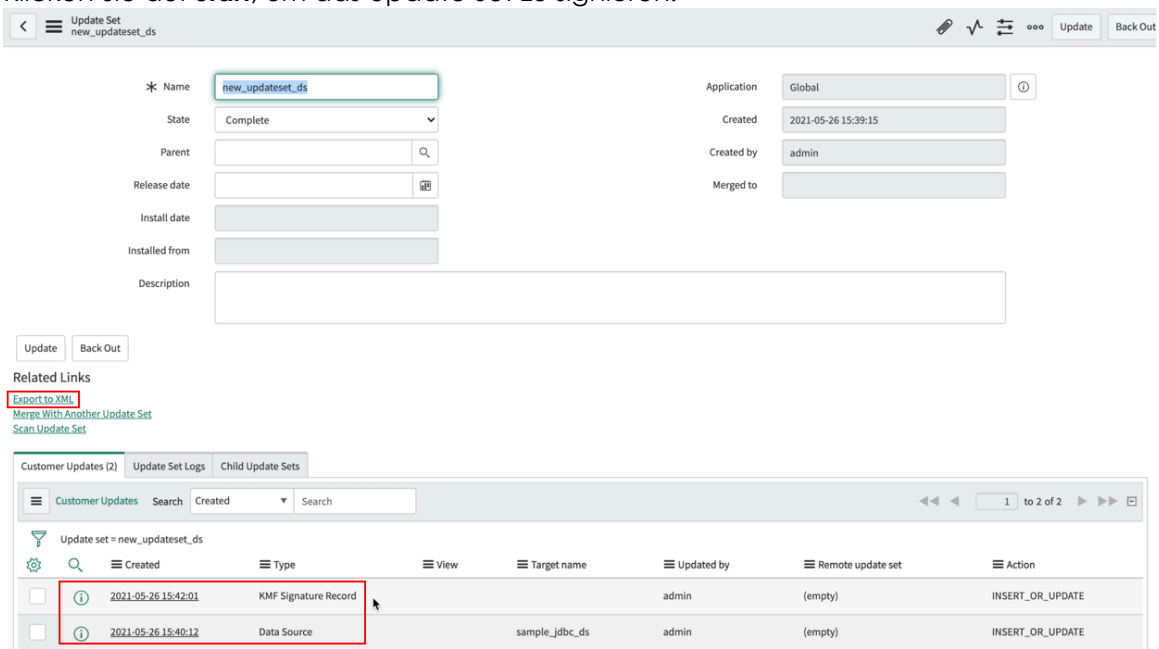
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Typ	Typ des Verschlüsselungsauftrags. Wählen Sie **Update Set signieren aus**.
Tabelle	Update Set, aus dem die Datensätze signiert werden sollen.



d. Klicken Sie auf **Absenden**.

e. Klicken Sie auf **Start**, um das Update Set zu signieren.



- Die**Zusammenfassung** wird aktualisiert, dass die Datensätze signiert sind.
- Das Update Set wird aktualisiert und enthält die Signatur.

5. Öffnen Sie in der Instanz außerhalb der Produktion den signierten Update-Satz-Datensatz, und exportieren Sie ihn in eine XML-Datei.

6. Importieren Sie das signierte Update Set in der Produktionsinstanz.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren zu **Systemupdate-Sätze** > **Update Sets abgerufen**an.

b. Klicken Sie auf den zugehörigen Link **Update Set aus XML** importieren, um das Update Set zu importieren, das aus der vertrauenswürdigen Instanz exportiert wurde.
Weitere Informationen finden Sie unter Schnellstart-Update Set importieren und festlegen .
Das Update Set wurde erfolgreich committet.

Signieren Sie die REST- und SOAP-Nachrichten in der Produktionsinstanz

Verwenden Sie Update-Sätze, um die REST- und SOAP-Nachrichten zu signieren und zu validieren, indem Sie die Codesignatur in Produktionsinstanzen und] Instanzen außerhalb der Produktion aktivieren.

Vorbereitungen

- Richten Sie Circle of Trust zwischen Produktionsinstanz und Instanz außerhalb der Produktion ein.
- Erforderliche Rolle: security_admin

Signieren Sie die vorhandenen REST- und SOAP-Nachrichten

Signieren und validieren Sie die vorhandenen REST- und SOAP-Nachrichten, indem Sie die Codesignatur in der Produktion und in vertrauenswürdigen Instanzen außerhalb der Produktion aktivieren.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_manager

Prozedur

1. Konfigurieren Sie in der vertrauenswürdigen Instanz den KMF-Signaturauftrag, um die UI-Aktionen zu signieren.

   a. Navigieren Sie zu KMF-Signaturkonfiguration.

   b. Füllen Sie diese Werte im Formular aus.

Formular „KMF-Signaturkonfiguration“.

Feld	Beschreibung
Tabellenname	Glide-Tabellenname. Wählen Sie beispielsweise **UI-Aktionen [sys_ui_action] aus**.
KMF-Signatur-Zweck	Zweck des Signierens der Datensätze. Wählen Sie **ECC-Warteschlange aus**.
Signaturerzeugungsfelder	Felder in der Datenquelle, die Sie signieren möchten. Wenn an den Werten in einem oder mehreren dieser Felder Änderungen vorgenommen werden, wird die zuvor generierte Signatur ungültig. Wählen Sie **Name** und **Skript aus**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Signaturerzeugungsfilter	Filterkriterien, die zum Signieren der Datensätze erfüllt werden müssen.
Anhang signieren	Option zum Signieren des Anhangs im Glide-Datensatz.
Instanzschlüssel	Option zur Verwendung des Instanzschlüssels.

c. Klicken Sie mit der rechten Maustaste in den Header Kopfzeile des Formulars, und wählen Sie **Speichern** aus.

2. Signieren Sie in der vertrauenswürdigen Instanz die erforderlichen Datensätze.

a. Navigieren zu **Systemsicherheit** > **Security-Aufträge** > **Alle**an.

b. Klicken Sie auf **Neu**.

c. Füllen Sie diese Werte im Formular aus.

Feld	Beschreibung
Name	Name zur Identifizierung des Datensatzes.
Typ	Typ des Verschlüsselungsauftrags. Wählen Sie **Massensignaturdatensätze aus**.
Tabelle	Tabelle, aus der die Datensätze signiert werden sollen. Wählen Sie **UI-Aktion aus**.

d. Klicken Sie **auf Codesignaturauftrag in Produktion exportieren**.
Es werden zwei lokal signierte Update Sets erstellt.

- Ein Update Set für die UI-Aktionskonfiguration.
- Ein weiteres Update Set aus dem Verschlüsselungsauftrag zum Exportieren des Codesignaturauftrags.

3. Exportieren Sie in der vertrauenswürdigen Instanz das lokale Update Set in eine XML-Datei.

a. Navigieren zu **Systemupdate-Sätze** > **Lokale Update-Sätze**an.

b. Öffnen Sie den Update-Satz, den Sie für das Massensignieren der Datensätze erstellt haben.

c. Klicken Sie **auf den zugehörigen Link In XML** exportieren, und speichern Sie die XML-Datei.

4. Importieren Sie die Update Sets in der Produktionsinstanz.

a. Navigieren zu **Systemupdate-Sätze** > **Abgerufene Update-Sätze**an.

b. Klicken Sie auf den zugehörigen Link **Update Set aus XML** importieren, um das Update Set zu importieren, das aus der vertrauenswürdigen Instanz exportiert wurde.
Weitere Informationen finden Sie unter Schnellstart-Update Set importieren und festlegen .
Das Update Set wurde erfolgreich committet.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Führen Sie in der Produktionsinstanz den Verschlüsselungsauftrag aus, den Sie zuvor in der vertrauenswürdigen Instanz erstellt hatten, indem Sie **Start**auswählen.
   Es wird eine Bestätigungsmeldung angezeigt, in der erwähnt wird, dass die Datensätze signiert sind.

Signieren Sie neue REST- und SOAP-Nachrichten

Signieren und validieren Sie die neuen REST- und SOAP-Nachrichten von der vertrauenswürdigen Instanz, indem Sie die Codesignatur in der Produktion und in vertrauenswürdigen Instanzen aktivieren.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Starten Sie in der vertrauenswürdigen Instanz außerhalb der Produktion ein Update Set.
2. Erstellen Sie in der vertrauenswürdigen Instanz außerhalb der Produktion die erforderlichen REST- oder SOAP-Nachrichten.
   Die Nachrichten werden dem Update Set hinzugefügt.
3. Ändern Sie in der Instanz außerhalb der Produktion den Status des Update Set in **Abgeschlossen**, und klicken Sie auf **Aktualisieren**.
4. Signieren Sie in der Instanz außerhalb der Produktion den Update-Satz, indem Sie einen Verschlüsselungsauftrag erstellen.

   a. Navigieren zu **Systemsicherheit** > **Security-Aufträge** > **Alle**an.

   b. Klicken Sie auf **Neu**.

   c. Füllen Sie diese Werte im Formular aus.

Feld	Beschreibung
Name	Name zur Identifizierung des Datensatzes.
Typ	Typ des Verschlüsselungsauftrags. Wählen Sie **Update Set signieren aus**.
Tabelle	Update Set, aus dem die Datensätze signiert werden sollen. Wählen Sie **Neuen REST V2-Update-Satz signieren – 1 aus**.

   d. Klicken Sie auf **Absenden**.

   e. Klicken Sie auf **Start**, um das Update Set zu signieren.
      - Die**Zusammenfassung** wird aktualisiert, dass die Datensätze signiert sind.
      - Das Update Set wird aktualisiert und enthält die Signatur.

5. Öffnen Sie in der Instanz außerhalb der Produktion den signierten Update-Satz-Datensatz, und exportieren Sie ihn in eine XML-Datei.
6. Importieren Sie das Update Set in der Produktionsinstanz.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren zu **Systemupdate-Sätze** > **Abgerufene Update-Sätze**an.

b. Wählen Sie den zugehörigen Link **Update Set aus XML** importieren aus, um das Update Set zu importieren, das aus der vertrauenswürdigen Instanz exportiert wurde.
Weitere Informationen finden Sie unter Schnellstart-Update Set importieren und festlegen .
Das Update Set wurde erfolgreich committet.

Signieren Sie die Flows, Subflows und Aktionen in der Produktionsinstanz

Verwenden Sie Update-Sätze, um die Flows, Subflows und Aktionen zu signieren und zu validieren, indem Sie die Codesignatur in der Produktion und in vertrauenswürdigen Instanzen aktivieren.

- Richten Sie Circle of Trust zwischen Produktionsinstanz und vertrauenswürdigen Instanzen ein.
- Erforderliche Rolle: security_admin

Signieren Sie den vorhandenen Flow, die Subflows und die Aktionen

Signieren und validieren Sie vorhandene Flows, Subflows und Aktionen, indem Sie die Codesignatur in der Produktion und in vertrauenswürdigen Instanzen außerhalb der Produktion aktivieren.

Vorbereitungen
Erforderliche Rolle: sn_kmf.cryptographic_manager

Prozedur

1. Signieren Sie in der vertrauenswürdigen Instanz die Datensätze in der Tabelle „Schrittinstanz“.

   a. Navigieren zu **Systemsicherheit** > **Security-Aufträge** > **Alle**an.

   b. Klicken Sie auf **Neu**.

   c. Füllen Sie diese Werte im Formular aus.

Feld	Beschreibung
Name	Name zur Identifizierung des Datensatzes.
Typ	Typ des Verschlüsselungsauftrags. Wählen Sie **Massensignaturdatensätze aus**.
Tabelle	Tabelle, aus der die Datensätze signiert werden sollen. Wählen Sie **Schrittinstanz aus**.

   d. Klicken Sie **auf Codesignaturauftrag in Produktion exportieren**.
   Es werden zwei lokal signierte Update Sets erstellt.
   - Ein Update Set für die KMF-Signatur.
   - Ein weiteres Update Set aus dem Verschlüsselungsauftrag zum Exportieren des Codesignaturauftrags.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Exportieren Sie in der vertrauenswürdigen Instanz das lokale Update Set in eine XML-Datei.
   a. Navigieren zu **Systemupdate-Sätze** > **Lokale Update-Sätze**an.
   b. Öffnen Sie den Update-Satz, den Sie für das Massensignieren der Datensätze erstellt haben.
   c. Klicken Sie **auf den zugehörigen Link In XML** exportieren, und speichern Sie die XML-Datei.
3. Importieren Sie die XML-Datei in die Produktionsinstanz.
   a. Navigieren zu **Systemupdate-Sätze** > **Abgerufene Update-Sätze**an.
   b. Klicken Sie auf den zugehörigen Link **Update Set aus XML** importieren, um das Update Set zu importieren, das aus der vertrauenswürdigen Instanz exportiert wurde.
   Weitere Informationen finden Sie unter Schnellstart-Update Set importieren und festlegen .
   Das Update Set wurde erfolgreich committet.
4. Führen Sie in der Produktionsinstanz den Verschlüsselungsauftrag aus, den Sie zuvor in der vertrauenswürdigen Instanz erstellt hatten.
   a. Navigieren zu **Systemsicherheit** > **Security-Aufträge** > **Alle**an.
   b. Öffnen Sie den Verschlüsselungsauftrag, den Sie zuvor in der vertrauenswürdigen Instanz erstellt haben.
   c. Klicken Sie auf **Start**, um den Auftrag zu starten.
   Es wird eine Bestätigungsmeldung angezeigt, in der erwähnt wird, dass die Datensätze signiert sind.

Signieren Sie neue Flows, Subflows und Aktionen

Signieren und validieren Sie neue Flows, Subflows und Aktionen, indem Sie die Codesignatur in der Produktion und in vertrauenswürdigen Instanzen außerhalb der Produktion aktivieren.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_manager

Prozedur

1. Starten Sie in der vertrauenswürdigen Instanz ein Update Set.
2. Erstellen Sie in der vertrauenswürdigen Instanz die erforderlichen Flows, Subflows oder Aktionen, und veröffentlichen Sie sie.
   Die Flows, Subflows oder Aktionen werden dem Update Set hinzugefügt.
3. Ändern Sie in der vertrauenswürdigen Instanz den Status des Update Set in **Abgeschlossen**, und klicken Sie auf **Aktualisieren**.
4. Signieren Sie in der vertrauenswürdigen Instanz das Update Set, indem Sie einen Verschlüsselungsauftrag erstellen.
   a. Navigieren zu **Systemsicherheit** > **Security-Aufträge** > **Alle**an.
   b. Klicken Sie auf **Neu**.
   c. Füllen Sie diese Werte im Formular aus.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Name zur Identifizierung des Datensatzes.
Typ	Typ des Verschlüsselungsauftrags. Wählen Sie **Update Set signieren aus**.
Tabelle	Update Set, aus dem die Datensätze signiert werden sollen.

d. Klicken Sie auf **Absenden**.

e. Klicken Sie auf **Start**, um das Update Set zu signieren.

- Die**Zusammenfassung** wird aktualisiert, dass die Datensätze signiert sind.
- Das Update Set wird aktualisiert und enthält die Signatur.

5. Öffnen Sie in der vertrauenswürdigen Instanz den signierten Update-Satz-Datensatz, und exportieren Sie ihn in eine XML-Datei.

6. Importieren Sie das signierte Update Set in der Produktionsinstanz.

a. Navigieren zu **Systemupdate-Sätze** > **Update Sets abgerufen**an.

b. Wählen Sie den zugehörigen Link **Update Set aus XML** importieren aus, um das Update Set zu importieren, das aus der vertrauenswürdigen Instanz exportiert wurde.
Weitere Informationen finden Sie unter Schnellstart-Update Set importieren und festlegen .
Das Update Set wurde erfolgreich committet.

Signieren Sie bestimmte Datensätze oder Anhänge

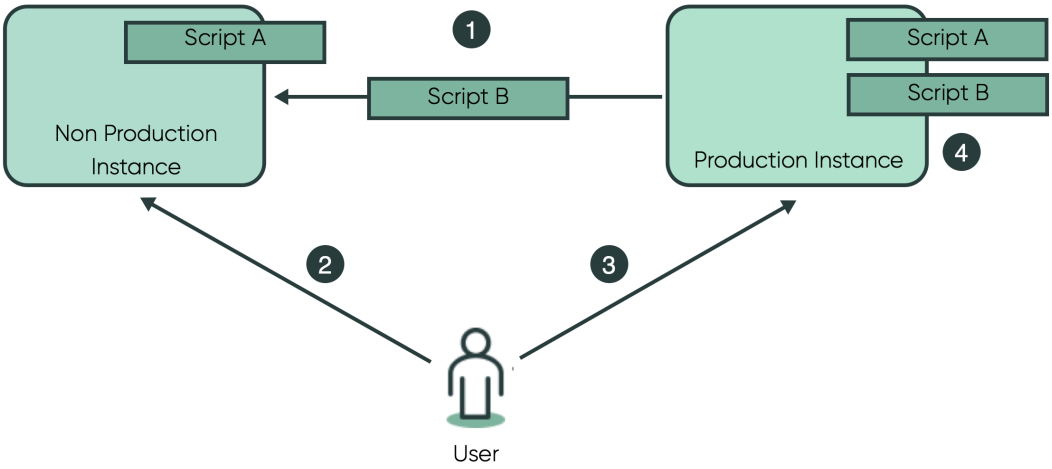
Erstellen Sie einen Sicherheitsauftrag, um bestimmte Datensätze oder Anhänge zu signieren und nicht alle Datensätze oder Anhänge in einer Tabelle.

Ab Release Vancouver können Sicherheitsadministratoren Sicherheitsaufträge verwenden, um bestimmte Datensätze in einer Tabelle anstatt aller Datensätze in einer Tabelle zu signieren. Signieren Sie bestimmte Datensätze, um ein versehentliches Signieren von nicht überprüftem Code zu vermeiden.

Diese Aufträge enthalten eine angehängte Protokolldatei, die am Ende des Signierauftrags generiert wird. Diese Protokolldatei enthält Informationen über signierte Datensätze und die verwendete Signaturkonfiguration.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Signiervorgang



Dieses Diagramm zeigt ein Beispiel für die Verwendung des Signierprozesses. In diesem Beispiel ist ein Skript mit der Bezeichnung `Skript B` nur in der Produktionsinstanz vorhanden und muss zum Signieren in eine vertrauenswürdige Instanz importiert werden. `Skript A` ist bereits in beiden Instanzen vorhanden und muss nicht signiert werden. Sie wurde entweder bereits überprüft und signiert oder wurde noch nicht überprüft und darf nicht signiert werden.

1. Importieren Sie den Datensatz in Ihre vertrauenswürdige Umgebung.
2. Erstellen Sie in der vertrauenswürdigen Instanz einen Signierauftrag, um den Datensatz zu signieren. Dieser Prozess wird in Erstellen Sie einen Auftrag zum Signieren bestimmter Datensätze oder Anhänge in einer vertrauenswürdigen Instanzdetailliert beschrieben.
3. Importieren Sie den signierten Signierauftrag mithilfe eines Update Set in Ihre Produktionsinstanz.
4. Führen Sie in der Produktionsinstanz den importierten Signierauftrag aus.

Erstellen Sie einen Auftrag zum Signieren bestimmter Datensätze oder Anhänge in einer vertrauenswürdigen Instanz

Signieren Sie einen bestimmten Datensatz oder eine Gruppe von Datensätzen, die Sie in einer vertrauenswürdigen Instanz außerhalb der Produktion definieren.

Vorbereitungen

Erforderliche Rolle: security_admin oder sn_kmf.cryptographic_manager

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Security-Aufträge** > **Neu erstellen:**an.
2. Im **Feld Welche Art von Sicherheitsauftrag möchten Sie erstellen?** Wählen Sie in der Eingabeaufforderung **Signierauftrag**aus.
   Ein neuer **Signierauftrags** -Datensatz wird angezeigt.
3. Füllen Sie im Formular die Felder nach Bedarf aus:

Signieren von Auftragsfeldern

Feld	Beschreibung
Name	Beschreibender Name für diesen Auftrag.

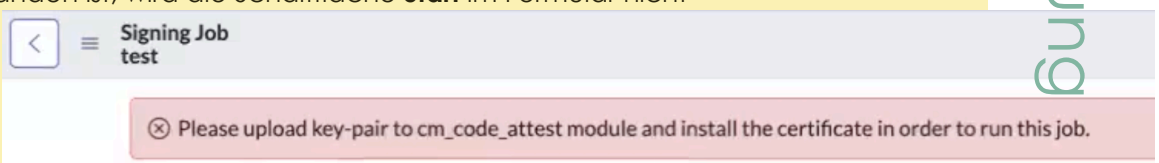
Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Typ	Typ des Sicherheitsauftrags. Um bestimmte **Datensätze** zu signieren, wählen Sie die Option Bestimmte Datensätze signieren aus. Um bestimmte **Anhänge**zu signieren, wählen Sie Bestimmte Anhänge signieren aus.
Status	Status dieses Auftrags. Dieses Feld beginnt mit dem Wert **Neu**. Dieses Feld ist schreibgeschützt.
Tabelle	Tabelle mit den Datensätzen oder Anhängen, die Sie signieren möchten. Wenn Sie Anhänge signieren, wählen Sie die Tabelle mit den Datensätzen aus, denen die Anhänge zugeordnet sind, und nicht die Tabelle „Anhang“ [sys_attachment]. **Tipp:** Überprüfen Sie die Signaturdatensatz-Tabelle des Key Management Framework (KMF) [sn_kmf_record_signature], um sicherzustellen, dass für die ausgewählte Tabelle noch keine Signaturen vorhanden sind.
Datensätze filtern	Filterbedingungen, mit denen eingeschränkt wird, welche Datensätze in der Tabelle **„Datensätze zum Signieren auswählen“ angezeigt** werden.
Datensätze zum Signieren auswählen	Liste der Datensätze in der im Feld „Tabelle“ ausgewählten **Tabelle**, eingeschränkt durch den im Feld „Datensätze filtern“ erstellten **Filter**. Verschieben Sie Datensätze aus dem Fenster **„Verfügbar** “ in das Fenster „ **Ausgewählt** “, um sie dem Signierauftrag hinzuzufügen.
Zeitfensterstart	Beginn des Zeitfensters für die Ausführung dieses Auftrags. Die Aufgabe wird nach der in diesem Feld eingegebenen Zeit ausgeführt. Ein gültiger Zeitwert ist die koordinierte Weltzeit (Coordinated Universal Time, koordinierte Weltzeit), basierend auf einer 24-Stunden-Zeitnotation.
Zeitfensterende	Das Ende des Zeitfensters für die Ausführung dieses Auftrags. Die Aufgabe wird vor der in diesem Feld eingegebenen Zeit ausgeführt. Wenn der Auftrag noch nicht abgeschlossen wurde, wird er angehalten und beim Start des nächsten Zeitfensters fortgesetzt. Die Endzeit muss nach der Startzeit liegen. Ein gültiger Zeitwert ist die koordinierte Weltzeit (Coordinated Universal Time, koordinierte Weltzeit), basierend auf einer 24-Stunden-Zeitnotation.
Zusammenfassung	Zusammenfassung der Ausführung dieses Auftrags. Dieses Feld ist schreibgeschützt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie mit der rechten Maustaste auf den Header des Formulars, und wählen **Sie Speichern**aus.
5. Wählen Sie unten im Formular die **Option Codesignaturauftrag in Produktion exportieren aus**.
   Mit dieser Aktion wird der Signierauftrag signiert, und er ist für den Export bereit.
6. Navigieren zu **Alle** > **Systemupdate-Sätze** > **Lokale Update-Sätze**
7. Suchen und öffnen Sie das Update Set für Ihren Signierauftrag.
   Auf der Registerkarte „Kunden-Updates“ können Sie sehen, dass dieses Update Set den Signierauftrag und den Signaturdatensatz enthält.
8. Wählen Sie **In XML exportieren**.
   Mit dieser Aktion wird eine XML-Datei mit dem Update Set auf Ihrem lokalen Gerät erstellt.
9. Navigieren Sie in Ihrer Produktionsinstanz zu **Alle** > **Systemupdate-Sätze** > **Abgerufene Update-Sätze** > **an.**
10. Wählen Sie unten auf der Seite **Update Set aus XML importieren aus**.
11. Wählen Sie die Schaltfläche **Datei** wählen aus, und wählen Sie die in den vorherigen Schritten erstellte XML-Datei aus.
12. Wählen Sie **Hochladen** aus.
    Ihr Update Set wird geladen und in der Liste der **abgerufenen Update Sets** angezeigt.
13. Öffnen Sie in der Liste der **abgerufenen Update-Sätze** den Datensatz für den importierten Update-Satz.
14. Wählen Sie die Schaltfläche **Vorschau auf Update Set**.
    Nachdem die Vorschau erfolgreich abgeschlossen wurde, wird die Schaltfläche **Update Set** festlegen angezeigt.
15. Wählen Sie **Update Set festlegen aus**.
16. **Alle** > **Systemsicherheit** > **Security-Aufträge** > **Alle**an.
17. Öffnen Sie Ihren Signierauftrag.
18. Wählen Sie **Start**, um den Signierauftrag auszuführen.

> ⚠ **Warnung:** Wenn das Schlüsselpaar nicht in Ihre Produktionsinstanz hochgeladen wurde, wird oben im Datensatzformular eine Warnung angezeigt. Wenn dieses Schlüsselpaar in Ihrer Instanz nicht vorhanden ist, wird die Schaltfläche **Start** im Formular nicht angezeigt.
>
> 
>

Nächste Maßnahme

Nach Abschluss werden im Feld **Zusammenfassung** die Ergebnisse des Auftrags angezeigt. An Ihren Signierauftragsdatensatz ist auch eine Protokolldatei mit dem Namen „Mass_Sign_Records-“ angehängt.<sys_id> ". Überprüfen Sie diesen Datensatz auf Details zum Auftrag und eine Liste der sys_ids für jeden signierten Datensatz.

Codesignaturreferenz

Referenzthemen enthalten zusätzliche Informationen zum Verwalten und Behandeln von Codesignaturen.

- Mit Codesignatur installierte Eigenschaften

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Codesignatur fügt die folgenden Eigenschaften hinzu.

Problembehandlung bei und Zugriff auf Protokolle

Greifen Sie auf verschiedene Protokolle zu, um Fehler zu beheben und die Fehlerursachen zu identifizieren.

Mit Codesignatur installierte Eigenschaften

Die Codesignatur fügt die folgenden Eigenschaften hinzu.

Eigenschaft	Typ	Beschreibung
com.glide.codesigning.expanded.tracking.enabled	Wahr | Falsch	Bei „wahr“ wird die Validierungslänge für den Metastapel für ecc_queue-Themen erhöht, die in der Eigenschaft **com.glide.codesigning.expanded_tracking.topic.list** aufgeführt sind. **Wichtig:** Zum Ändern dieser Eigenschaft ist erhöhte Sicherheit erforderlich.
com.glide.codesigning.expanded.tracking.length	Ganzzahl	Ebenen der Codesignaturvalidierung, die auftreten sollen, wenn Codesignatur aktiviert ist. Der Standardwert ist 3. **Wichtig:** Zum Ändern dieser Eigenschaft ist erhöhte Sicherheit erforderlich.
com.glide.codesigning.expanded_tracking.topic.list	Zeichenfolge	Kommagetrennte Liste von Themen, die einer erhöhten Metastapel-Nachverfolgung unterliegen. **Wichtig:** Zum Ändern dieser Eigenschaft ist erhöhte Sicherheit erforderlich.
com.glide.codesigning.tracking.agent.validation.exclusions	Zeichenfolge	Kommagetrennte Liste der ecc_queue-Agents, für die die Codesignatur übersprungen werden soll
com.glide.codesigning.tracking.debug	Wahr | Falsch	Bei „wahr“ ist die Debug-Protokollierung für den Codesignatur-Tracker aktiviert.
com.glide.codesigning.tracking.enabled	Wahr | Falsch	Bei „wahr“ wird die Nachverfolgung von Anrufern für die Codesignatur aktiviert. **Wichtig:** Zum Ändern dieser Eigenschaft ist erhöhte Sicherheit erforderlich.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Typ	Beschreibung
com.glide.codesigning.tracking.logging	Wahr/Falsch	Bei „wahr“ wird die Protokollierung für die Nachverfolgung von Codesignaturen aktiviert.
com.glide.codesigning.tracking.unsupported_script_tracking	Wahr/Falsch	Bei „wahr“ werden ecc_queue-Datensätze, die über nicht unterstützte Skripts eingefügt wurden (falls erkannt), nicht beglaubigt. **Wichtig:** Zum Ändern dieser Eigenschaft ist erhöhte Sicherheit erforderlich.
com.glide.codesigning.tracking.validation_fail_fast	Wahr/Falsch	Bei „wahr“ schlägt die Verifizierung der Codesignatur beim ersten Fehler bei der Skriptvalidierung fehl, anstatt alle Skripts zu überprüfen. **Wichtig:** Zum Ändern dieser Eigenschaft ist erhöhte Sicherheit erforderlich.
com.glide.event_handler.code_signing.tracking	Zeichenfolge	Definiert den Ereignishandler, mit dem sichergestellt wird, dass Kunden, die Codesignatur neu aktivieren, eine möglichst sichere Konfiguration erhalten. **Wichtig:** Zum Ändern dieser Eigenschaft ist erhöhte Sicherheit erforderlich.
com.glide.web_service_outbound.impl.codesigning.tracking	Wahr/Falsch	Bei „wahr“ wird die Nachverfolgung von SOAPMessageV2-Codesignaturen aktiviert **Wichtig:** Zum Ändern dieser Eigenschaft ist erhöhte Sicherheit erforderlich.
com.snc.csf.servicenow_root_of_trust.disabled	Wahr/Falsch	Gibt an, ob die Root of Trust-Funktion aktiv ist. Der Standardwert ist „ `false`“, was bedeutet, dass die Build-Zertifikate ServiceNow vertrauenswürdig sind.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Typ	Beschreibung
		Wichtig: Diese Eigenschaft kann nur mit einer signierten geplanten Aufgabe von einem Anwender mit den Rollen „admin“, „sicherheitsadmin“ und „KMF-Manager“ geändert werden. Weitere Informationen zum Ändern des Root of Trust finden Sie unter Ändern Sie Ihre Root of Trust-Konfiguration.
com.snc.kmf.signature.validation.optin	Wahr | Falsch	Bei „wahr“ wird Codesignatur in Ihrer Instanz aktiviert. **Wichtig:** Diese Eigenschaft kann nur über eine Anforderung in Kundenservice und Supportgeändert werden. Weitere Informationen finden Sie in KB1205749
glide.jdbcprobeloader.tracking	Wahr | Falsch	Aktiviert oder deaktiviert die Codesignatur für JDBC-Datenquellen. **Wichtig:** Zum Ändern dieser Eigenschaft ist erhöhte Sicherheit erforderlich.
glide.rest.codesigning.tracking	Wahr | Falsch	Bei „wahr“ wird die Nachverfolgung von RESTMessageV2-Codesignaturen aktiviert. **Wichtig:** Zum Ändern dieser Eigenschaft ist erhöhte Sicherheit erforderlich.

Mit Codesignatur installierte Rollen

Codesignatur enthält die folgenden Rollen.

Codesignaturadministrator [codesigning_admin]

Verwenden Sie die Administratorrolle für Codesignaturen, um anderen Anwendern die Rollen „codesigning_manager“ und „codesigning_auditor“ zuzuweisen.

Enthält die Rollen

Liste der Rollen, die in der Rolle enthalten sind.

Keine.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Keine.

Besondere Überlegungen

Vermeiden Sie das Gewähren einer Administratorrolle, wenn spezialisiertere Rollen verfügbar sind.

Codesignaturmanager [codesigning_manager]

Verwenden Sie die Codesignaturmanager-Rolle, um die Signaturkonfiguration zu erstellen und zu aktualisieren und Codesignaturaufträge zu erstellen und auszuführen.

Enthält die Rollen

Liste der Rollen, die in der Rolle enthalten sind.

Keine.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Besondere Überlegungen

Keine.

Auditor für Codesignatur [codesigning_auditor]

Verwenden Sie die Auditor-Rolle für Codesignatur, um Signaturkonfigurationen und Signieraufträge anzuzeigen. Die Auditor-Rolle hat keinen Erstellungs- oder Schreibzugriff auf Codesignatur-Assets.

Enthält die Rollen

Liste der Rollen, die in der Rolle enthalten sind.

Keine.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Besondere Überlegungen

Keine.

Problembehandlung bei und Zugriff auf Protokolle

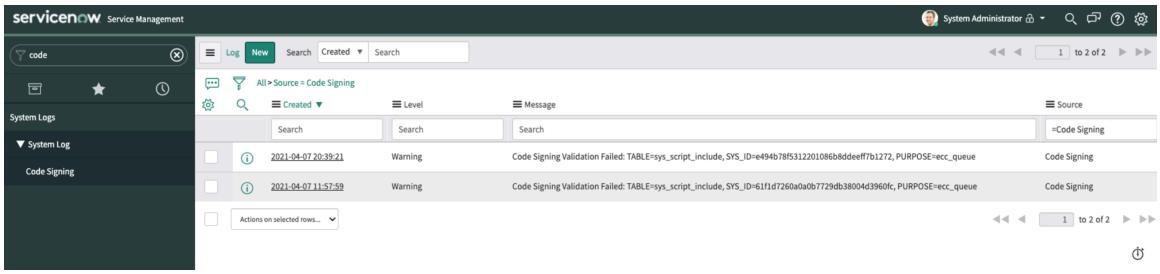
Greifen Sie auf verschiedene Protokolle zu, um Fehler zu beheben und die Fehlerursachen zu identifizieren.

Codesignaturprotokolle

Wenn einer der Datensätze der ECC-Warteschlange nicht von der Codesignatur-Tracker-API signiert ist, werden die nicht signierten Nachrichten und die erforderlichen Details im Modul

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

„Codesignatur“ angezeigt. Navigieren zu **Systemprotokolle** > **Systemprotokoll** > **Codesignatur** um auf die Liste der nicht vertrauenswürdigen Datensätze zuzugreifen.

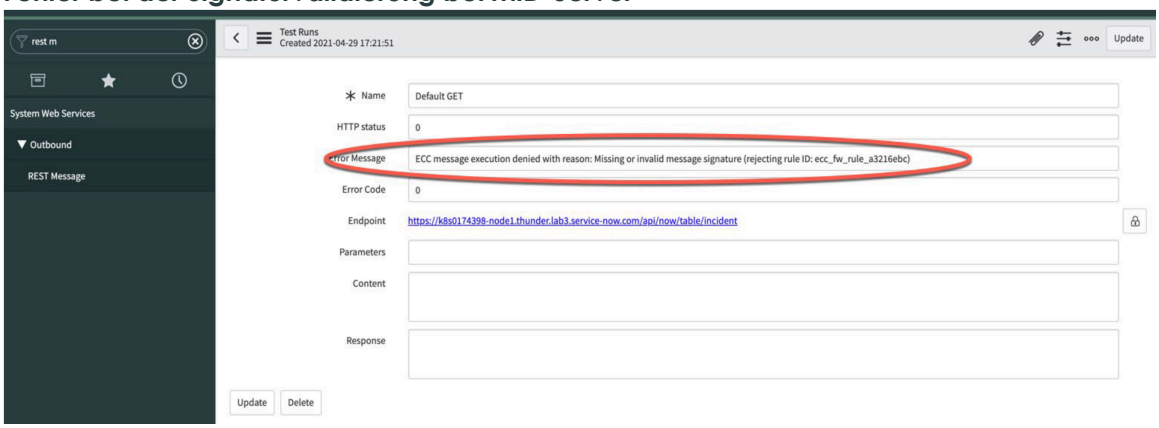


Um zusätzliche Debug-Knotenprotokolle zu erhalten, aktivieren Sie *com.glide.codesigning.tracking.debug*, und legen Sie den Wert auf `true`fest.

Fehler bei der Validierung der REST-Nachrichtensignatur bei MID-Server

Greifen Sie auf die Fehlermeldung bezüglich des Fehlers bei der Signaturvalidierung zu, , indem Sie zu navigieren **System-Webservices** > **Ausgehend** > **REST-Nachricht** und Öffnen des erforderlichen REST-Nachrichtendatensatzes.

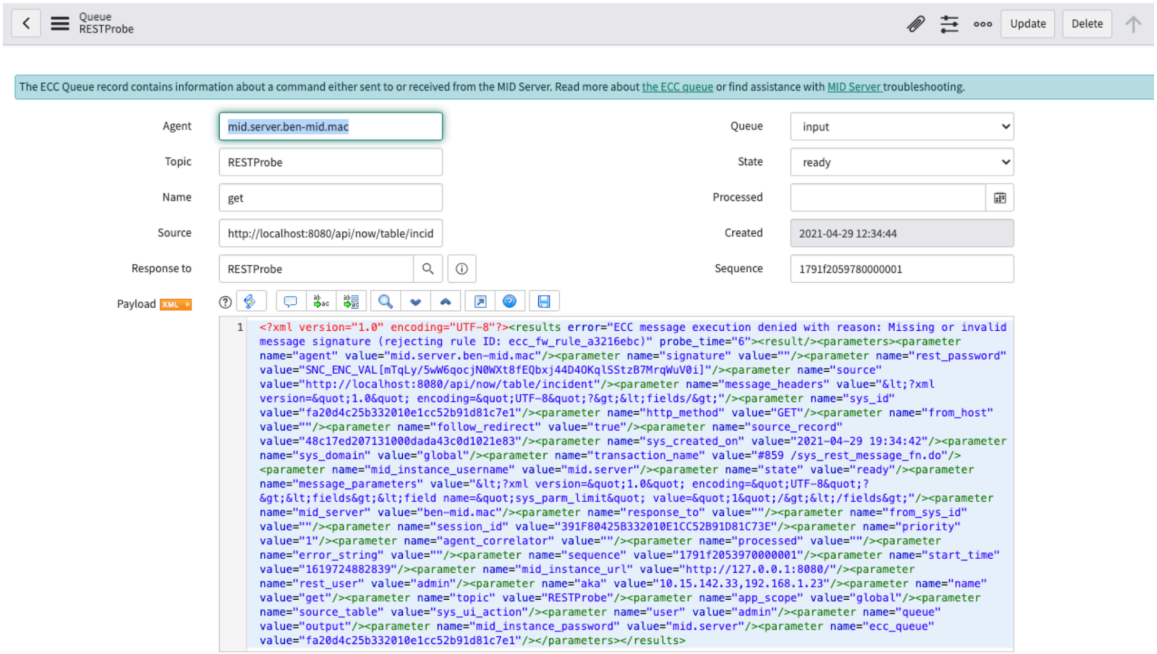
Fehler bei der Signaturvalidierung bei MID-Server



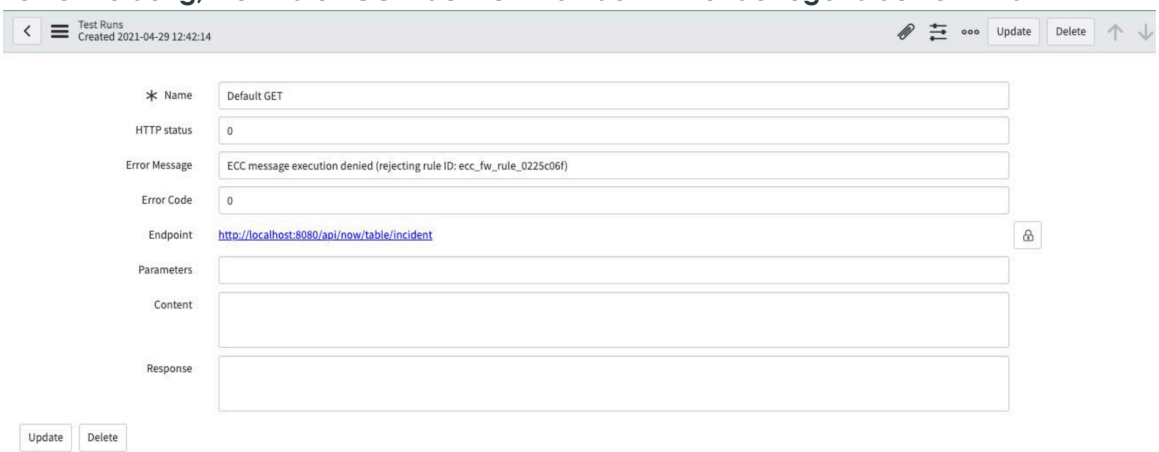
Hinweis: Fehlermeldungen im Zusammenhang mit ECC-Firewall-Ablehnungen beginnen mit `ECC-Nachrichtenausführung verweigert`.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ECC-Warteschlange, wenn die Signaturvalidierung auf fehlschlägt MID-Server



Fehlermeldung, wenn die ECC-Nachricht von der Anwenderregel blockiert wird



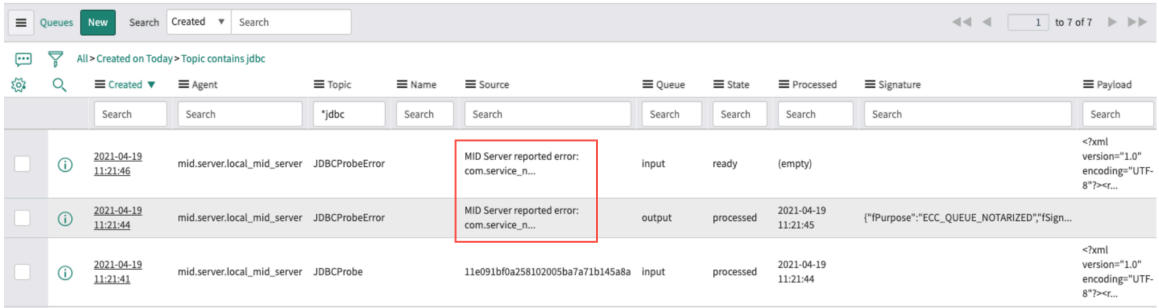
JDBC-Probe

Wenn eine JDBC-Datenquelle mit ungültiger oder fehlender Signatur auf MID-Serverausgeführt wird, wird eine Fehlermeldung mit den erforderlichen Details angezeigt.



Quelle zeigt auch die Details der Fehlermeldung an.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



MID-Server Protokolle

Um die detaillierte ECC-Firewallprotokollierung zu aktivieren, erhöhen Sie die Protokollebene, indem Sie den Wert des Konfigurationsparameters MID Server , *`mid.log.level`*, auf `TRACE` `festlegen`. Die detaillierten Protokolle enthalten Informationen über:

- Regeln, die MID-Server aus der Startkonfigurationsdatei geladen hat.
- Granularer Ausführungs-Trace von Regeln.
- Spezifische Regel, aufgrund derer eine ECC-Nachricht zu akzeptieren oder abzulehnen ist.

Hinweis: Wenn „`boot-config.xml`“ ungültig ist, kann MID-Server nicht gestartet werden, und die Fehlerdetails werden in den MID-Agent-Protokollen protokolliert.

Antivirus-Scanning

Schützen Sie mit Antivirus-Scanning Ihre Instanz vor Virusinfektionen, die durch Dateianhänge Ihrer Systemdatensätze wie Incidents, Probleme und Storys eingeschleust werden können.

Erkunden Sie Antivirus-Scans



Erfahren Sie, welchen Wert Antivirus-Scanning hat.

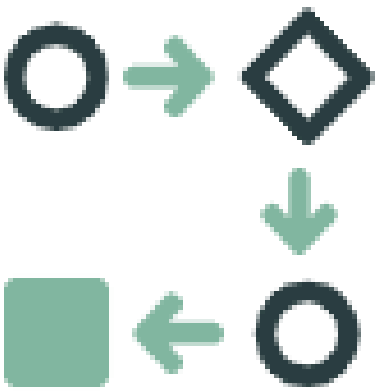
Konfigurieren Sie den Virenschutz



Erfahren Sie, wie Sie den Virenschutz konfigurieren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Infizierte Dateien auflösen



Erfahren Sie, wie Sie mit infizierten Dateien verfahren.

Referenz für Antivirus-Scans



Erfahren Sie mehr über die Wörterbuchattribute für Antivirus-Scans.

Antivirus-Scanning erkunden

Schützen Sie mit Antivirus-Scanning Ihre Instanz vor Virusinfektionen, die durch Dateianhänge Ihrer Systemdatensätze wie Incidents, Probleme und Storys eingeschleust werden können.

Antivirus-Scanning scannt Dateianhänge, die in der Anhangtabelle [sys_attachment] gespeichert sind, um Benutzer vor dem Hochladen und Herunterladen infizierter Dateien zu schützen. Alle von der Plattform unterstützten Dokumenttypen werden von Antivirus Scanning gescannt.

Das Plugin Virenschutz (com.glide.snap) ist in Ihrer -Instanz standardmäßig aktiviert. Als Administrator können Sie die Funktion Antivirus-Scanning in Ihrer Instanz per Umschalter deaktivieren und wieder aktivieren, Konfigurationsoptionen festlegen und die Virenschutzaktivität in der Instanz überprüfen.

Hinweis:

- Antivirus-Scanning ist auch für Kunden in der Government Community Cloud (GCC) und in einer geschäftlichen Umgebung verfügbar. Benutzer müssen die Eigenschaft (com.glide.snap.fed_enable_scan) auf „true“ festlegen, um die Funktion verwenden zu können.
- Die Kommunikationsprotokolle HTTP und HTTPS werden unterstützt.
- Edge-verschlüsselte Dateien sind von diesem Scan ausgeschlossen.
- Virenschutzdefinitionen werden täglich aktualisiert.
- Dateien mit einer Dateigröße von über 100 MB werden nicht gescannt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Scannen von E-Mails und Anhängen

Eingehende E-Mails werden von den E- Mail-Filtern des Systems auf Viren geprüft, nicht von Antivirus-Scanning.

Standardmäßig werden nur Anhänge gescannt, die an Tabellen „zz_yylive_profile“ angehängt sind. Um andere Tabellen mit dem Spaltentyp „ **file_attachment** “ zu scannen, erstellen Sie die Systemeigenschaft *com.glide.snap.scan.zz_yytables*, und fügen Sie den Tabellennamen ein.

Wenn die Tabellennamen zz_yyincident und zz_yycase lauten, muss der Eigenschaftswert *zz_yyincident,zz_yycase*lauten.

Nachdem diese Eigenschaft festgelegt wurde, werden Anhänge für die Tabellen „zz_yyincident“ und „zz_yycase“ gescannt.

Szenarien werden gescannt

Überprüfen Sie diese Upload- und Download-Szenarien, um zu verstehen, wie das System potenzielle Sicherheitsbedrohungen aus Dateien identifiziert, die an Ihre Datensätze angehängt sind.

Szenario 1: Laden Sie eine Datei hoch

1. Der Benutzer lädt unwissentlich eine infizierte Datei in einen Datensatz hoch.
2. Das System scannt die Datei und verschiebt sie in die Quarantäne.
3. Die Datei wird im Fenster „Anhänge“ angezeigt und dort als nicht verfügbar markiert.
4. Der Benutzer wählt die Datei aus, und die folgende Fehlermeldung wird angezeigt: `Die Datei „Infected_testing.txt“ hat die Sicherheitsprüfung nicht bestanden. Entfernen Sie die Datei aus dem Datensatz INC0000059, und versuchen Sie es erneut.`
5. Das System sendet eine E-Mail-Benachrichtigung an den Benutzer und den Antivirus-Administrator.
6. Der Benutzer schließt das Fenster „Anhänge“ und kehrt zum Datensatz zurück. Die infizierte Datei wird im Header als nicht verfügbar angezeigt. Beispiel: `infiziert_testing123.txtZ [nicht verfügbar].`

Szenario 2: Laden Sie eine Datei herunter

1. Der Benutzer öffnet einen Datensatz, um eine angehängte Datei herunterzuladen.
2. Der Benutzer weiß nicht, dass die Datei infiziert ist und wählt sie zum Download aus.
3. Das System scannt die Datei, verschiebt sie in die Quarantäne und zeigt eine ähnliche Meldung an wie `Die Datei infizierte_testing123.txt hat die Sicherheitsprüfung nicht bestanden und kann nicht heruntergeladen werden.`
4. Der Anwender schließt die Nachricht, und der Bildschirm wird aktualisiert und zeigt an, dass die Datei nicht verfügbar ist.
5. Das System sendet eine E-Mail-Benachrichtigung an den Benutzer und den Antivirus-Administrator.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Szenario 3: Laden Sie eine ZIP-Datei herunter

1. Ein Benutzer öffnet einen Datensatz und lädt eine angehängte ZIP-Datei herunter.
2. Das System scannt die ZIP-Dateien einzeln.
3. Eine Datei besteht die Sicherheitsprüfung nicht und wird als nicht verfügbar markiert. Die verbleibenden Dateien wurden komprimiert und erfolgreich heruntergeladen.
4. Der Benutzer öffnet die ZIP-Datei und sieht zusätzlich zu der erfolgreich heruntergeladenen Datei die Datei „error.txt“. Diese Datei enthält eine Fehlermeldung, die angibt, welche Datei den Scan nicht bestanden hat und daher nicht in der ZIP-Datei enthalten war.
5. Der Benutzer öffnet den Datensatz erneut und sieht, dass die nicht verfügbare Datei in den Abschnitt „ **Potenzielle Sicherheitsrisiken** “ im Fenster „Anhänge“ verschoben wurde und nicht heruntergeladen werden kann.

Antivirus-Scanning konfigurieren

Konfigurieren Sie Antivirus-Scanning in Ihrer Instanz und auf Tabellenebene.

Vorbereitungen

Erforderliche Rolle: antivirus_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Antivirus-Scanning ist standardmäßig in Ihrer Instanz aktiv und scannt dort automatisch Anhänge, um alle mit Viren infizierten Dateien zu identifizieren. Konfigurieren Sie die Funktion, indem Sie sicherstellen, dass der Scan in Ihrer Instanz aktiviert ist, und indem Sie alle Tabellen identifizieren, die Sie vom Scan ausschließen möchten.

Prozedur

1. Navigieren zu **Alle** > **Virenschutz** > **Konfiguration**an.
2. Berücksichtigen Sie bei der Konfiguration der Funktion Folgendes.

Option	Beschreibung
Antivirus-Scanning aktivieren	Das Antivirus-Scanning ist aktiv und standardmäßig für die Instanz aktiviert. Der Umschalter ist auf die Position Ein eingestellt und wird grün angezeigt. **Hinweis:** Um die Eigenschaft auf „ `falsch` “ festzulegen, wenden Sie sich an den Kundensupport.
Herunterladen von Anhängen zulassen, wenn Antiviren-Scanner nicht zur Verfügung steht	Wenn diese Option auf die Position „Ein“ festgelegt ist, wird das Antivirus-Scanning umgangen, wenn der Scanner eine Zeitüberschreitung erfährt, und es kann keine Antwort abgerufen werden. In dieser Situation wird der Dateidownload fortgesetzt, ohne den Scan abzuschließen. Wenn die Option deaktiviert ist, wird der Dateidownload

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	bis zum erfolgreichen Abschluss des Scanvorgangs verhindert.
Liste der ausgeschlossenen Tabellen	Alle Dateianhänge, die einer Tabelle in dieser Liste zugeordnet sind, werden von der Virenprüfung ausgeschlossen. Fahren Sie mit Schritt 4 fort, wenn Sie die Tabellen definieren möchten, die das System vom Scannen ausschließt.

3. Wählen Sie **Speichern**.
4. Schließen Sie Tabellen aus der Virenprüfung aus, indem Sie sie der **Liste der ausgeschlossenen Tabellen**hinzufügen.
   a. Navigieren Sie zu **Systemdefinition** → **Wörterbuch**
   b. Suchen Sie nach der Tabelle, die Sie vom Scan ausschließen möchten, und wählen Sie die Tabelle aus, deren Typ auf Sammlung festgelegt ist.
   c. Wählen Sie auf der Registerkarte **Attribute** die Option **Neu**aus.
   d. Fügen Sie `Exclude_from_antivirus_scan` im Feld Attribute hinzu, und geben Sie im Feld **Wert**`Wahr` ein.
   e. Wählen Sie **Absenden**.

Ergebnisse
Antivirus-Scanning wird in Ihrer Instanz aktiviert, und die **Liste der ausgeschlossenen Tabellen** auf der Antivirus-Konfigurationsseite wird mit allen Tabellen ausgefüllt, die Sie von der Prüfung ausgeschlossen haben.

Dateien in Quarantäne werden überprüft

Überprüfen Sie Dateianhänge in Quarantäne, und ergreifen Sie nach Bedarf weitere Maßnahmen.

Vorbereitungen
Erforderliche Rolle: antivirus_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird
Überwachen Sie auf der Seite Antivirus-Quarantäne in regelmäßigen Abständen die Einträge Ihrer Dateien in Quarantäne, um eine der folgenden Aktionen auszuführen.

Prozedur
1. Navigieren zu **Alle** > **Virenschutz** > **Quarantäne**an.
2. Aktivieren Sie das Kontrollkästchen neben jedem Eintrag in Quarantäne, für den Sie eine verfügbare Aktion ausführen möchten.
3. Wählen Sie im Banner die Dropdown-Liste **Aktionen für ausgewählte Zeilen** aus, um die Aktion auszuwählen, die für den ausgewählten Zeilen-Quarantäneeintrag ausgeführt werden soll.

Aktion	Beschreibung
Löschen	Wählen Sie diese Aktion aus, um die Datei unter Quarantäne zu löschen, wenn sie von Anwendern nicht mehr benötigt wird.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktion	Beschreibung
Wiederherstellung	Wählen Sie diese Aktion aus, um die Datei basierend auf Ihrer Bewertung des Status oder auf der Anwenderanforderung wiederherzustellen. Scannen Sie die Datei jedoch mit dem Antivirenprodukt eines Drittanbieters, bevor Sie sie wiederherstellen, um Virenbedrohungen zu minimieren. Nach der Wiederherstellung steht die Datei dem Anwender zum Download zur Verfügung.
Herunterladen	Wählen Sie diese Aktion aus, um die Datei zum weiteren Scannen und Analysieren auf Ihr lokales System herunterzuladen.

Ergebnisse
Das System fragt nach einer Bestätigung und führt die ausgewählte Aktion gemäß Ihrer Eingabe aus.

Zugehörige Informationen

Instanz-Sicherheitszentrum

Antivirus-Metriken

Virenschutz-Aktivität wird überprüft

Überprüfen Sie das Antivirus-Aktivitätsprotokoll, das alle Aktivitäten für potenziell infizierte Dateien ab dem Zeitpunkt, zu dem sie erkannt und in Quarantäne gestellt werden, nachverfolgt.

Vorbereitungen
Erforderliche Rolle: antivirus_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird
Dieses Protokoll fungiert als Bericht, der Antivirus-Aktivitäten wie Discovery, Löschung und andere mögliche Ereignisse in Quarantänedateien erfasst.

Prozedur

1. Navigieren zu **Alle** > **Virenschutz** > **Aktivität**an.
2. Überprüfen Sie das Protokoll der Dateien in Quarantäne.
   Sie können die durchgeführten Aktionen in der Spalte Ereignis für jede Datei in Quarantäne anzeigen.

Nächste Maßnahme
Bestimmen Sie, welche Datensätze Sie löschen, wiederherstellen, herunterladen oder im Protokoll behalten möchten. Siehe Dateien in Quarantäne überprüfen

Kenntnisse über Wörterbuchattribute für Antivirus-Scanning

Wörterbuchattribute ändern das Verhalten der Tabelle oder des Elements, die bzw. das durch den Wörterbuchdatensatz beschrieben wird. Als Administrator können Sie die Werte von Wörterbuchattributen festlegen, um das Verhalten der standardmäßigen Antivirus-Scanning-Konfiguration zu ändern.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wörterbuchattribute für Antivirus-Scanning

Name	Wert	Zielelement	Beschreibung
Exclude_from_antivirus_scan	wahr/falsch	eine beliebige Tabelle	Bei „wahr“ werden Dateianhänge in der Tabelle von der Virenprüfung ausgeschlossen. Siehe Antivirus-Scanning konfigurieren
Supress_antivirus_email_notification	wahr/falsch	eine beliebige Tabelle	Bei „wahr“ wird das Senden von von der Plattform generierten E-Mail-Benachrichtigungen beendet, wenn eine potenziell infizierte Datei identifiziert wird.
Supprim_antivirus_ui_notification	wahr/falsch	eine beliebige Tabelle	Bei „wahr“ werden von der Plattform generierte UI-Benachrichtigungen gestoppt, wenn eine potenziell infizierte Datei identifiziert wird.

Zugehörige Informationen

Tabellen und Felder mithilfe von Wörterbuchattributen ändern

HTML-Bereinigung

Entfernen Sie unerwünschten Code, und schützen Sie sich vor Sicherheitsbedrohungen wie Angriffen mit websiteübergreifendem Skripting, indem Sie HTML-Markup in HTML-Feldern und übersetzten HTML-Feldern bereinigen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkunden Sie die HTML-Bereinigung



Erfahren Sie, wie die HTML-Bereinigung funktioniert.

Konfigurieren Sie die HTML-Bereinigung



Konfigurieren Sie die HTML-Bereinigung.

HTML-Bereinigung aktivieren



Erfahren Sie, wie Sie die HTML-Bereinigung aktivieren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

HTML-Bereinigung erkunden

Entfernen Sie unerwünschten Code, und schützen Sie sich vor Sicherheitsbedrohungen wie Angriffen mit websiteübergreifendem Skripting, indem Sie HTML-Markup in HTML-Feldern und übersetzten HTML-Feldern bereinigen.

Verwenden Sie die HTML-Bereinigung, um sicherzustellen, dass HTML-Inhalte in Ihrer Instanz keine potenziell schädlichen Inhalte enthalten. Die HTML-Bereinigung funktioniert durch das Entfernen von HTML-Tags, die zur Gefährdung Ihrer Instanz verwendet werden könnten, z. B. <![CDATA[<script>]]>-, `<link>`- oder `<embed>` -Tags, die verwendet werden können, um unerwünschte Skripts in Ihrer Instanz auszuführen oder Ihre Benutzer auf unerwünschte Inhalte zu leiten. Sichere Tags, die die Formatierung Ihrer Inhalte steuern, bleiben erhalten. Als Administrator können Sie anpassen, welche Inhalte entfernt oder beibehalten werden. Sie können auch steuern, ob die Bereinigung für alle Inhalte oder nur für die von Ihnen angegebenen Felder gilt.

Die HTML-Bereinigung überprüft die integrierte Aufnahmeliste auf Markups, die Sie immer beibehalten möchten. Die Bereinigung stellt die *Skripteinbindung HTMLSanitizerConfig* bereit, mit der Administratoren die integrierte Aufnahmeliste ändern können. Elemente können auch der Ausschlussliste hinzugefügt werden, um HTML-Markup zu entfernen. Der Inhalt der Ausschlussliste überschreibt die Aufnahmeliste.

Die folgenden Arten von Elementen können den Einschluss- und Ausschlusslisten hinzugefügt werden:

- Globale Attribute
- Beliebige HTML-Elemente

Hinweis: Standardmäßig unterstützen URL-Attribute wie `href` und `src` nur diese Protokolle:

- `http`
- `https`
- `Mailto`
- `Daten`

Beispiel:

```
<a href="https://community.servicenow.com/community">ServiceNow
Community</a>
```

Hinweis: Weitere Informationen zur Eigenschaft *glide.html.sanitize_all_fields*, die die Verwendung der HTML-Bereinigung steuert, finden Sie unter HTML-Bereinigung unter Härtungseinstellungen für Instanzsicherheit.

Konfigurieren Sie URL-Attribute und die Protokolle

Sie können urlAttributes und ihre Protokolle in der **HTMLSanitizer** -Skripteinbindung konfigurieren. Beispiel:

```
HTML_WHITELIST : {
urlAttributes: { "protocols" : [ "file", "notes" ] },
                - -
                - -
        }
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Da sich in diesem Beispiel „ `Notizen` “ in der Aufnahmeliste befindet, wird diese URL nicht bereinigt:

```
<a title="Lotus"
 href="Notes://
ABC/X575C90019DE33/ABC594DCB76D86EB4925653E0011C4C1/ZZ90B7E2D33964749257E
EA003456FD">Lotus</a></p>
```

Standardaufnahmeliste

Hinweis: Die Standardaufnahmeliste ist eine Systemliste, auf die Benutzer in der -Instanz nicht zugreifen können.

```
BUILTIN_HTML_WHITELIST :{

    globalAttributes:{ attribute:["id","class","lang","title","style"],

                                    attributeValuePattern:{}},

    label:{ attribute:["for"]},

    font:{ attribute:["color","face","size"]},

    a:{ attribute:["href","nohref","name","shape"]},


 img:{ attribute:["src","name","alt","border","hspace","vspace","align","
height","width"},


 table:{ attribute:["border","cellpadding","cellspacing","bgcolor","backg
round","align","no resize","height","width","summary","frame","rules"]},


 th:
{ attribute:["background","bgcolor","abbr","axis","headers","scope","nowr
ap","height","width","align","valign","char
 off","char","colspan","rowspan"]},


 td:
{ attribute:["background","bgcolor","abbr","axis","headers","scope","nowr
ap","height","width","align","valign","char
 off","char","colspan","rowspan"]},

    tr:{ attribute:["background","height","width","align","valign","char
 off","char"]},

    thead:{attribute:["align","valign","char off","char"]},

    tbody:{attribute:["align","valign","char off","char"]},

    tfoot:{attribute:["align","valign","char off","char"]},

    colgroup:{attribute:["align","valign","char
 off","char","span","width"]},
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
    col:{attribute:["align","valign","char off","char","span","width"]},
    p:{attribute:["align"]},
    style:{attributeValuePattern:{"type":"text/css"}}
    canvas:{ attribute:["height","width"]},
    details:{ attribute:["open"]},
    summary:{ attribute:["open","valign","char off","char"]},
    button:{ attribute:["disabled","accesskey","type"]},
    form:{},

 input:{ attribute:["size","maxlength","checked","alt","src","type","disa
bled","readonly","accesskey","border","usemap"]},
    select:{ attribute:["disabled","multiple","size"]},

 textarea:{ attribute:["rows","cols","disabled","readonly","accesskey"]},
    option:{ attribute:["disabled","label","selected"]},
    div:{ attribute:["align"]},
    ol:{ attribute:["start","type","square"]},
    ul:{ attribute:["type","square","itemscope","itemtype","itemref"]},
    li:{ attribute:["value","fb__id","itemprop"]},

 span:{ attribute:["color","size","data-mce-bogus","itemprop","face"]},
    br:{ attribute:["clear"]},
    h3:{ attribute:["itemprop"]},
    html:{ attribute:["xmlns","lang","xml:lang"]},
    link:{ attribute:["rel","type","href","charset"]},
    meta:{ attribute:["name","content","scheme","charset","http-equiv"]},
    pre:{ attribute:["xml:space"]},
    noscript:{},    h1:{},    h2:{},      h4:{},    h5:{},    h6:{},
    i:{},    b:{},    u:{},    strong:{},    em:{},    small:{},
 big:{},
    pre:{},    code:{},    cite:{},    samp:{},    sub:{},    sup:{},
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
    strike:{},   center:{},  blockquote:{},    hr:{},      map:{},

    dd:{},    dt:{},    dl:{},  fieldset:{},    legend:{}, figure:{},
tt:{},

    body:{},   caption:{},   head:{},   title:{},  shape:{},},
```

Konfigurieren der HTML-Bereinigung

Sie müssen eine Skripteinbindung ändern, um Konfigurationsänderungen an der HTML-Bereinigung vorzunehmen.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Skripteinbindungen**an.
2. Öffnen **Sie HTMLSanitizerConfig**.
3. Um der Ausschlussliste Elemente hinzuzufügen, verwenden Sie die Klasse HTML_BLackliste.

   Um der Aufnahmeliste Elemente hinzuzufügen, verwenden Sie die Klasse HTML_WHITELIST.

   Dieses Format verwenden:

```
HTML_XXXXLIST :{
        globalAttributes :{

            attribute:[attribute-name1,...],

 attributeValuePattern:{ attribute-name2:attribute-value-regex-pattern,
...}

        },<html-element-name>:{// Same as Above},----}
```

   - *globalAttributes* enthält Attribut- oder attributeValuePattern-Elemente, die global für alle HTML-Elemente gelten.
   - *attribute* ist eine durch Kommas getrennte Liste von Attributen.
   - *attributeValuePattern* ist ein Wörterbuch von Attribut-zu-Attribut-Wert-Regulierungs-Muster-Paaren. Das Attributwert-Regex-Muster ist ein regulärer Ausdruck, der mit dem Attributwert übereinstimmen muss.

Example:

Betrachten Sie das folgende Beispiel:

```
HTML_WHITELIST:{
        globalAttributes:{
            attribute:["id","name"],},
        img:{
            attribute:["style","align"],
            attributeValuePattern:{src:".*jpeg"}},
        iframe:{},}
```

Der Aufnahmeliste werden folgende Elemente hinzugefügt:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- ID und Name der globalen Attribute. Dies ist eine Liste von Zeichenfolgen, die global auf alle Elemente angewendet werden können.
- Das Bildelement, bei dem die Attribute „Stil“ und „Ausrichtung“ sind.
- Das img-Element, bei dem das Quellattribut des Bilds eine Datei mit der Erweiterung „.jpeg“ ist. Dies ist ein Beispiel für ein Muster für reguläre Ausdrücke, das einem Attributwert entspricht.
- Das iframe-Element.

HTML-Bereinigung aktivieren

Die HTML-Bereinigung bietet eine Eigenschaft zum Aktivieren oder Deaktivieren der Bereinigung für alle HTML-Felder im System.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Standardmäßig ist diese Eigenschaft für neue Instanzen auf „true“ festgelegt.

Prozedur

1. Geben Sie im Navigationsfilter `sys_properties.list` ein.
2. Legen Sie die Eigenschaften *`glide.html.sanitize_all_fields`* und *`glide.translated_html.sanitize_all_fields`* auf **true fest**.

   Hinweis: Weitere Informationen zu dieser Eigenschaft finden Sie unter HTML-Bereinigung in Härtungseinstellungen für Instanzsicherheit.

Trouble?

Wenn die Eigenschaften in der Tabelle „Systemeigenschaften“ nicht vorhanden sind, können Sie sie hinzufügen.

Aktiviert die Bereinigung einzelner Felder

Sie können Feldattribute verwenden, um die Bereinigung für einzelne Felder zu aktivieren oder zu deaktivieren.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Sie müssen zuerst die Bereinigungseigenschaft auf „falsch“ setzen und dann die Bereinigung für jedes Formular pro Feld aktivieren.

Prozedur

1. Navigieren Sie zur Tabelle sys_properties, und legen Sie *`glide.html.sanitize_all_fields`* auf **false**fest.
   Dadurch wird die Bereinigung für alle HTML-Felder im System deaktiviert.
2. Navigieren Sie zu dem Formular, das das HTML-Feld enthält.
3. Klicken Sie mit der rechten Maustaste auf die HTML-Feldbezeichnung, und wählen Sie **Dictionary konfigurieren**aus.
   Das Formular „Wörterbucheintrag“ wird für das Feld „HTML“ geöffnet.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Geben Sie im Feld Attribute eine der folgenden Optionen ein:
   - Um die Bereinigung zu deaktivieren, geben Sie „ `html_sanitize=false` “ ein
   - Um die Bereinigung zu aktivieren, geben Sie „ `html_sanitize=true` “ ein
5. Klicken Sie auf **Aktualisieren**.
6. Um die HTML-Bereinigung für übersetzte HTML-Felder zu aktivieren, legen Sie die Eigenschaft *`glide.translated_html.sanitize_all_fields`* **auf true** fest.

Protokollierung der HTML-Bereinigung aktivieren

Wenn die HTML-Bereinigung Elemente oder Attribute entfernt, werden sie dem Systemprotokoll hinzugefügt.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können diese bereinigten Elemente überprüfen, indem Sie Ihrer Instanz-URL /syslog_list.do? sysparm_query=source%3DHTMLSanitizer hinzufügen.

Prozedur

1. Um diese bereinigten Elemente zu überprüfen, fügen `Sie /syslog_list.do? sysparm_query=source%3DHTMLSanitizer` Ihrer Instanz-URL hinzu.
2. Um die Protokollierung zu aktivieren oder zu deaktivieren, fügen Sie den Systemeigenschaften die Eigenschaft „`glide.html_sanitize.discarded_log.enable` “ hinzu, und legen Sie den Wert auf „ **wahr** “ (aktiviert) oder „ **falsch** “ (deaktiviert) fest. Diese Eigenschaft ist standardmäßig **true**.

Auditing

Verfolgen Sie Datensatzänderungen in für Auditing aktivierten Tabellen. Standardmäßig verfolgt das System unter anderem Änderungen an den Incident-, Change- und Problem-Tabellen nach.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Untersuchen



Lernen Sie die Funktionen und Geschäftswerte von Auditing kennen.

Konfigurieren



Erfahren Sie, wie Audits konfiguriert werden.

Ansicht



Überprüfen Sie die Tabellen „Sys-Audit“ und „Audit-Beziehungsänderung“.

Referenz



Erfahren Sie mehr über die Verlaufssätze.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auditing erkunden

Verfolgen Sie Datensatzänderungen in für Auditing aktivierten Tabellen. Standardmäßig verfolgt das System unter anderem Änderungen an den Incident-, Change- und Problem-Tabellen nach.

Durch das Aktivieren des Auditings wird das Erstellen, Aktualisieren und Löschen aller Datensätze in der Tabelle nachverfolgt. Wenn Sie einzelne Felder in einer Tabelle prüfen möchten, können Sie Felder, die Sie nicht nachverfolgen möchten, mithilfe eines Wörterbuchattributs ausblenden.

Audit-Informationen werden in den folgenden Tabellen gespeichert:

- Die Audit -Tabelle.
- Tabelle Wissen über Verlaufssätze

Warnung: Das Audit von Systemtabellen, die viel Datenverkehr erhalten, wie z. B. Workflow-Kontexte [wf_context] oder Ereignismanagement-Warnungen [em_alert], kann sich auf die Leistung auswirken. Aus diesem Grund können Sie die Tabelle „em_alert“ nicht als Ganzes prüfen. Auditieren Sie stattdessen ausgewählte Interessenfelder. Legen Sie *audit=true* sowohl für die Tabelle „em_alert“ als auch für die ausgewählten Felder fest. Versuchen Sie, so wenige Felder wie möglich zu prüfen.

Übergeordnete und untergeordnete Tabellen werden geprüft

Tabellen leiten die Audit-Kennzeichnungen nicht von übergeordneten oder untergeordneten geprüften Tabellen ab.

- Wenn Sie beispielsweise Auditing für die Tabelle „Konfigurationselemente“ [cmdb_ci] aktivieren, werden nur CIs geprüft, die in dieser Basistabelle gespeichert sind.
- Wenn Sie Auditing für die Tabelle „Computer“ [cmdb_ci_computer] aktivieren, werden entsprechend nur die Computer-CI-Datensätze geprüft, einschließlich aller Felder in der Tabelle „Computer“ [cmdb_ci_computer], die von der Tabelle „Konfigurationselemente“ [cmdb_ci] abgeleitet ist.

Systemtabellen werden geprüft

Standardmäßig prüft das System nicht, ob ein Datensatz aus Systemtabellen gelöscht wird. Um eine Systemtabelle zu prüfen, fügen Sie sie der Liste der Tabellen in der Eigenschaftsliste *glide.ui.audit_deleted_tables* hinzu.

Löschungen aus einem Formular oder einer Liste werden geprüft

Standardmäßig prüft das System das Löschen einzelner Datensätze aus einem Formular. Um Auditing zu verhindern, legen Sie das Wörterbuchattribut der Tabelle *no_audit_delete* fest.

Das System prüft Löschungen aus einer Liste, wenn das **Audit** für das Tabellenwörterbuch ausgewählt ist und die Tabelle nicht in der Eigenschaft *glide.db.audit.ignore.delete* aufgeführt ist.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Standardmäßig ist die Eigenschaft *glide.db.audit.ignore.delete*] in der Tabelle „Systemeigenschaft“ [sys_properties] nicht vorhanden. Um die Eigenschaft und die zugehörigen Werte zu ändern, müssen Sie sie zuerst manuell hinzufügen. Bei manuellem Hinzufügen werden jedoch die folgenden Standardwerte überschrieben:

```
glide.db.audit.ignore.delete =
sys_mutex,sys_db_cache,sys_lucene_block,sys_lucene_file,sys_lucene_directory,sys_use
cmdb_ci_windows_service, cmdb_sam_sw_install, cmdb_software_instance,
cmdb_sam_sw_usage, sam_sw_counter_detail
```

Weitere Informationen zum Hinzufügen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen

Es ist zu beachten, dass Audit-Löschungen standardmäßig aktiviert sind, unabhängig davon, ob der Datensatz aus der Formularansicht, der Listenansicht oder über ein Skript/eine geplante Aufgabe gelöscht wird.

Informationen geprüft

Beim Audit werden die folgenden Datensatzänderungen nachverfolgt:

- Eindeutiger Datensatzbezeichner (sys_id) des geänderten Datensatzes
- Feld, das sich geändert hat
- Neuer Feldwert
- Alter Feldwert
- Anzahl der Aktualisierungen dieses Datensatzes und Felds
- Datum und Uhrzeit des Change
- Benutzer, der die Änderung vorgenommen hat
- Grund für den Change (wenn dem Change ein Grund zugeordnet ist)
- Interne Prüfpunkt-ID für den Datensatz, wenn der Datensatz mehrere Versionen hat.

Informationen, die von der Auditierung befreit sind

Einige Updates werden nicht geprüft, obwohl die Überwachung für eine Tabelle aktiviert ist. Aus diesem Grund können im Verlauf eines Datensatzes 132 Updates angezeigt werden, von den geprüften jedoch nur sieben.

Auditing schließt die folgenden Informationen aus:

- Durch ein Upgrade durchgeführte Updates.
- Aktualisierungen werden über Importsätze vorgenommen.
- Datensätze in über- oder untergeordneten Tabellen.
- Felder mit dem Wörterbuchattribut „no_audit“.
- Systemtabellen sind nicht in der Eigenschaftenliste *glide.ui.audit_deleted_tables* aufgeführt.
- Felder, die mit dem Präfix sys_ beginnen (Systemfelder), mit Ausnahme der Spalten sys_class_name und sys_domain_id.
- UI-Seiten können manchmal Aktualisierungen für einen Datensatz auslösen, ohne ein Audit-Protokoll zu erstellen.
- Jedes Mal, wenn eine Inaktivitätsüberwachung einen Datensatz berührt. Dadurch wird verhindert, dass möglicherweise Hunderte von Updates für einen Incident aufgelistet werden, wobei die nützlichen Daten durch Rauschen übertönt werden.
- Manuelle Änderungen an Performance Analytics Punktzahlen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auditing einer Tabelle

Anweisungen zum Auditieren einer Tabelle finden Sie unter Auditing für eine Tabelle konfigurieren.

Standardmäßig verfolgt das System alle Felder in einer geprüften Tabelle. Sie können eine Teilmenge der Felder in einer Tabelle auf zwei Arten prüfen:

- Sie können Auditing für die gesamte Tabelle aktivieren und dann die Felder ausschließen, die Sie nicht einschließen möchten. Dies ist geeignet, wenn Sie die meisten, aber nicht alle Felder prüfen möchten. Dies wird als Ausschlusslistebezeichnet. Weitere Informationen finden Sie unter Feld von der Auditierung ausschließen (Ausschlussliste).
- Sie können Auditing für die Tabelle aktivieren, jedoch nur für bestimmte Felder. Dies ist angemessen, wenn Sie nur eine kleine Anzahl der Felder der Tabelle prüfen möchten. Dies wird als Aufnahmelistebezeichnet. Informationen zum Einschließen eines Felds mithilfe einer Aufnahmeliste finden Sie unter Ein Tabellenfeld in Auditing einbeziehen (Einschlussliste).

Nicht stornierbare Audit-Datensätze

Reduzieren Sie mit der neuen Standardeinstellung die Wahrscheinlichkeit, dass Audit-Datensätze nicht aufgezeichnet werden, wenn eine Transaktion abgebrochen wird.

Audits wurden so festgelegt, dass ein Datensatz sofort in derselben Transaktion mit den Schreibvorgängen für den Zieldatensatz erstellt wird. Wenn der Zieldatensatz gelöscht wird, wird das Audit trotzdem erstellt und im Modul **„NCA-Test-Audit** -Löschung“ aufbewahrt.

Hinweis: Der erweiterte Audit-Prozess ist standardmäßig aktiviert. Wenn die Eigenschaft `glide.db.audit.lazy` auf `True`festgelegt ist, ist der erweiterte Audit-Prozess deaktiviert.

Vor dem Release Xanadu wurden bestimmte auditierbare Vorgänge nicht erfasst, wenn eine Transaktion abgebrochen wurde. Dies liegt daran, dass die Plattform einige Vorgänge zwischen der Datensatzänderung ausführt und vor der Audit-Erstellung abgebrochen wird. Jetzt werden Audits jedoch unmittelbar nach der Änderung des Datensatzes erstellt, wodurch sich die Wahrscheinlichkeit verringert, dass eine abgebrochene Transaktion den Vorgang abbricht, bevor das Audit aufgezeichnet wurde.

Audits werden jetzt im selben Thread wie die Transaktion aufgezeichnet. Frühere Audits wurden in einem Hintergrund-Thread erstellt. Durch diese Änderung wird der Standardwert der Eigenschaft „`glide.db.audit.lazy`“ von „Wahr“ in „Falsch“ neu definiert. Diese Eigenschaft ist normalerweise nicht in der Eigenschaftentabelle definiert, da die meisten Instanzen den neuen Standardwert und das neue Standardverhalten verwenden. In einigen Instanzen ist diese Eigenschaft möglicherweise bereits vorhanden und auf „Wahr“ festgelegt. Dies bedeutet, dass diese Instanzen diese Änderung nicht zum Audit-Verhalten verwenden können.

Hinweis: Es wird empfohlen, diese Eigenschaft zu löschen, um das Update zu nutzen.

Auditing für eine Tabelle konfigurieren

Sie können die Tabellenüberwachung aktivieren, um Änderungen an allen oder einigen Feldern der Tabelle nachzuverfolgen.

Vorbereitungen

Erforderliche Rolle: admin.

Hinweis: Verschlüsselte Felder werden nicht standardmäßig geprüft. Dieses Verhalten ist nicht konfigurierbar.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Lexikon**an.
   Das System zeigt die Liste der Wörterbucheinträge an. Die Liste enthält eine Zeile für jede Tabelle sowie eine Zeile für jede Spalte (Feld) in der Tabelle.
2. Suchen Sie in der Liste der Wörterbucheinträge die Zeile, die der Tabelle entspricht, die Sie prüfen möchten, z. B. `cmdb_ci_computer`.
   Sie können die Zeile für die Tabelle selbst von einer Zeile für eine Spalte in der Tabelle unterscheiden, indem Sie die Zeile mit dem richtigen Tabellennamen, einem leeren Eintrag für den **Spaltennamen** und dem **TypSammlung**suchen.
3. Wählen Sie den Wörterbucheintrag für die Tabelle aus.
   Das System zeigt das Wörterbucheintragsformular an.
4. Aktivieren Sie die **Checkbox Audit**.
5. Wählen Sie **Aktualisieren**.

Nächste Maßnahme

Wenn Sie nur einige Felder in der Tabelle Auditing der Aufnahmeliste für eine Tabelle aktivierenüberwachen möchten. Wenn Sie die meisten Felder prüfen, einige aber ausschließen möchten, lesen Sie Feld von der Auditierung ausschließen (Ausschlussliste).

Auditing der Aufnahmeliste für eine Tabelle aktivieren

Aktivieren Sie eine Tabelle, um nur die von Ihnen explizit angegebenen Felder zu prüfen. Dies ist nützlich, wenn Sie nur eine kleine Anzahl von Feldern in einer geprüften Tabelle prüfen möchten.

Vorbereitungen

Erforderliche Rolle: admin
Die Tabelle muss für Auditing aktiviertsein.

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Lexikon**an.
   Das System zeigt die Liste der Wörterbucheinträge an. Die Liste enthält eine Zeile für jede Tabelle sowie eine Zeile für jede Spalte (Feld) in der Tabelle.
2. Passen Sie bei Bedarf die Listenansicht so an, dass die Spalte **Attribute** angezeigt wird.
3. Suchen Sie in der Liste der Wörterbucheinträge die Zeile, die der Tabelle entspricht, die Sie prüfen möchten, z. B. `cmdb_ci_computer`.
   Sie können die Zeile für die Tabelle selbst von einer Zeile für eine Spalte in der Tabelle unterscheiden, indem Sie die Zeile mit dem richtigen Tabellennamen, einem leeren Eintrag für „Spaltenname“ und dem Typ *`collection`*suchen.
4. Geben Sie im Feld **Attribute** für diese Zeile *`audit_type=whitelist`*ein.

Nächste Maßnahme

Geben Sie an, welche Felder in dieser Tabelle geprüft werden sollen.

Feld von der Auditierung ausschließen (Ausschlussliste)

Verhindern Sie, dass Now Platform eine Teilmenge von Feldern in einer geprüften Tabelle nachverfolgt, indem Sie diese Felder von einem Audit ausschließen.

Vorbereitungen

Erforderliche Rolle: admin

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um ein Feld in einer Tabelle von der Überwachung auszuschließen, müssen Sie zuerst die Überwachung für diese Tabelle aktivieren.

Warum und wann dieser Vorgang ausgeführt wird

Fügen Sie einer Ausschlussliste eine Reihe von Feldern hinzu, wenn Sie die meisten Felder in einer auditierbaren Tabelle prüfen möchten. Wenn Sie nur einige Felder prüfen möchten, befolgen Sie stattdessen das Verfahren für die Aufnahmeliste.

Hinweis: Das Deaktivieren der Überwachung von Journalfeldern kann sich auf bestimmte Funktionen wie den Aktivitätsformatierer auswirken. Weitere Informationen finden Sie unter KB0743142 .

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Lexikon**an.
2. Passen Sie bei Bedarf die Listenansicht so an, dass die Spalte **Attribute** angezeigt wird.
3. Navigieren Sie zu der Zeile, die der Tabelle und dem Feld (Spalte) entspricht, die Sie vom Audit ausschließen möchten.
4. Geben Sie in der Spalte **Attribute** für diese Zeile `no_audit`ein.

Ein Tabellenfeld in Auditing einbeziehen (Einschlussliste)

Verfolgen Sie eine Teilmenge der Felder in einer geprüften Tabelle, indem Sie diese Felder einer Aufnahmeliste hinzufügen.

Vorbereitungen

Erforderliche Rolle: admin
Um Felder in einer Tabelle zu einer Aufnahmeliste hinzuzufügen, müssen Sie zuerst Auditing für diese Tabelle und Auditing für Einschlusslisten für diese Tabelle aktiviert haben.

Warum und wann dieser Vorgang ausgeführt wird

Fügen Sie einer Aufnahmeliste eine Reihe von Feldern hinzu, wenn Sie nur eine kleine Anzahl der Felder einer geprüften Tabelle prüfen möchten. Wenn Sie die meisten Felder prüfen und nur wenige ausschließen müssen, befolgen Sie stattdessen das Ausschlusslistenverfahren.

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Lexikon**an.
2. Passen Sie bei Bedarf die Listenansicht so an, dass die Spalte **Attribute** angezeigt wird.
3. Navigieren Sie zu der Tabelle und dem Feld (Spalte), die Sie in die Aufnahmeliste aufnehmen möchten.
4. Geben Sie im Feld **Attribute** *`audit=true`*ein.

Auditing für eine Systemtabelle aktivieren

Löschungen aus Tabellen mit dem Präfix „sys_“ werden standardmäßig nicht geprüft. Um Löschungen aus diesen Tabellen nachzuverfolgen, fügen Sie den Tabellennamen der Eigenschaft *`glide.ui.audit_deleted_tables`* hinzu. Durch Aktivieren des Plugins „Gelöschte Datensätze wiederherstellen“ werden dieser Eigenschaft mehrere Standardwerte hinzugefügt.

Vorbereitungen

Erforderliche Rolle: admin

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **UI-Eigenschaften**an.
2. Suchen Sie die **Liste der Systemtabellen (beginnend mit „sys__“, kommagetrennt), die die Eigenschaft „audited löschen“ enthalten**.
3. Fügen Sie Tabellennamen hinzu, oder entfernen Sie sie. Tabellennamen müssen durch Kommas ohne Leerzeichen getrennt werden.
4. Klicken Sie auf **Speichern**.

Hinweis: Weitere Informationen zum Auditing finden Sie unter Informationen zur sys audit-Tabelle.

Sys-Audit- und Audit-Beziehungsänderungstabellen anzeigen

Now Platform verfolgt Einfügungen und Aktualisierungen für geprüfte Datensätze in den Tabellen „Sys Audit“ (sys_audit) und „Audit-Beziehungsänderung“ (sys_audit_relation).

Now Platform verfolgt Audit-Tabellen nach. Um Tabellen nachzuverfolgen, aktivieren Sie im Wörterbuchdatensatz das Kontrollkästchen **Audit**, um den Wert auf „true“ festzulegen. Standardmäßig werden keine Datensätze aus Systemtabellen geprüft, z. B. aus Update-Satz-Tabellen.

Hinweis: Um Leistungsprobleme und Endlosschleifen zu vermeiden, überspringt das System alle Geschäftsregeln oder Workflows, die durch Einfügungen in die Sys-Audit-Tabelle ausgelöst wurden.

Sys-Audit-Tabellenspalten

Die folgenden Spalten werden in den Datensätzen der Tabelle „sys_audit“ angezeigt:

Feld	Beschreibung
Tabellenname	Tabelle, für die der Audit-Datensatz gilt (z. B. „`Incident`“)
Feldname	Spalte in der Tabelle, für die der Audit-Datensatz bestimmt ist (z. B. „`assigned_to`“)
Dokumentenschlüssel	Sys_id (Unique Record Identifier) für den ursprünglichen Datensatz, der dem Audit-Datensatz zugeordnet ist.
Anwender	Name des Benutzers, der den Change erstellt hat. **Hinweis:** Einige automatisierte Prozesse verwenden das System oder Gastbenutzer, um Änderungen an Datensätzen anzuwenden und nachzuverfolgen. Weitere Informationen finden Sie unter System- und Gastbenutzer .
Alter Wert	Alter Wert der Feldänderung, die von diesem sys_audit-Datensatz dargestellt wird.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	• Referenzfelder: Eindeutiger sys_id-Wert des geänderten Datensatzes. • Felder für Datum und Uhrzeit: Wert in Coordinated Universal Time (UTC), wie in der Datenbank gespeichert.
Neuer Wert	Neuer Wert der Feldänderung, die von diesem sys_audit-Datensatz dargestellt wird. • Referenzfelder: Eindeutiger sys_id-Wert des geänderten Datensatzes. • Felder für Datum und Uhrzeit: Wert in Coordinated Universal Time (UTC), wie in der Datenbank gespeichert.

Funktionsweise der Tabelle „Audit-Beziehungsänderung“ (sys_audit_relation).

Die Sys-Audit-Tabelle [sys_audit] verfolgt Änderungen an Referenzfeldern in Tabellen, die für das Audit gekennzeichnet sind. Diese Aktivität umfasst Journalfeldeinträge und Verlaufssätze. Die Tabelle „Änderung der Audit-Beziehung“ [sys_audit_relation] verfolgt Beziehungsänderungen zwischen Datensätzen der Tabelle „sys_audit“ und den Quelltabellen, aus denen die geprüften Datensätze stammen. Außerdem wird nachverfolgt, wann ein Datensatz möglicherweise gelöscht wurde.

•

- Wenn Sie einen Datensatz in einer Tabelle auditieren, wird zwischen den verschiedenen Ursprungstabellen und dem Store, in dem die Daten aufgezeichnet werden, eine Beziehung erstellt. Diese Beziehungsinformationen werden in den Tabellen „sys_history_set“, „sys_history_line“ und „sys_journal“ gespeichert.
- Wenn Sie ein Feld löschen, das sich auf einen geprüften Tabellendatensatz bezieht, wird die Löschung in der Tabelle „sys_audit_relation“ aufgezeichnet. Mit anderen Worten: Jedes Mal, wenn Sie einen geprüften Datensatz ändern, löscht er zuerst die vorherigen Elemente und erstellt dann eine Beziehung in der Tabelle „sys_audit_relation“ mit neuen Dokument-IDs.

Wissen über Verlaufssätze

Das System generiert bei Bedarf automatisch Verlaufssatz-Datensätze aus der Audit-Tabelle, wenn ein Benutzer einen Datensatz erstellt oder seinen Verlauf anzeigt.

Wenn sich ein Datensatz in einer geprüften Tabelle befindet, wird der zugehörige Verlaufssatz generiert, wenn der Datensatz eingefügt wird oder wenn ein Benutzer den Datensatz anzeigt.

Hinweis: Verwenden Sie keine Verlaufssätze zum Generieren von Berichten.

Im Verlaufssatz-Datensatz werden mehrere Informationsfelder erfasst, die in der Listenansicht angezeigt werden.

Datensatzfelder der Listenansicht

Feld	Eingabewert
ID	Dokument-ID für den Datensatz, dessen Verlauf aufgezeichnet wird.
Tabelle	Geprüfte Tabelle für den Datensatz, dessen Verlauf aufgezeichnet wird.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datensatzfelder der Listenansicht (Fortsetzung)

Feld	Eingabewert
Ladezeit	Zeit, die zum Generieren des Verlaufssatzes benötigt wurde.

Audit-Verlaufsdatensatzfelder

Feld	Eingabewert
Bezeichnung	Die Bezeichnung des Felds, das geändert wurde.
Alt	Wert vor dem Change.
Neu	Wert nach dem Change.
Typ	Gibt an, ob der Eintrag für ein normales Feld, einen E-Mail-Datensatz oder einen Beziehungs-Change-Datensatz gilt.
Updateanzahl	Die Anzahl der Änderungen dieses Felds. Der Wert -1 gibt an, wann der Datensatz erstellt oder gelöscht wurde.
Update-Zeit	Datum und Uhrzeit des Change. **Hinweis:** Die Aktualisierungszeit für automatisch generierte Verlaufszeilen stimmt nicht mit der Erstellungs- oder Aktualisierungszeit für einen Datensatz in einer bestimmten Verarbeitungssituation überein. Wenn Sie den Verlaufssatz eines Datensatzes zum ersten Mal anzeigen, wird automatisch ein erster Satz von Verlaufszeilen-Datensätzen generiert. Da Dateiänderungen in einem Upgrade nicht geprüft werden, tritt diese Datumsabweichung in folgenden Fällen auf: • Sie zeigen einen Verlaufssatz an, nachdem an einem Datensatz eine Änderung vorgenommen wurde • Bevor in einem zukünftigen Upgrade eine weitere Änderung vorgenommen wird.
Anwendernamen	Name des Benutzers, der den Change erstellt hat.

Verlaufssätze in einer Kalenderansicht

Nachdem Verlaufssätze aktiv sind, wird die Kontextmenüauswahl für Verlauf mit Informationen aus dem Verlaufssatz und nicht aus der Tabelle `„sys_audit“ gefüllt`. Aus der Perspektive des Benutzers sind dieselben Verlaufsdaten in derselben Anwenderoberfläche verfügbar, die Informationen werden jedoch anders gespeichert.

Da die Verlaufsansicht eine Kalenderansicht enthält, aber nicht die normale Listenoberfläche zum Filtern der und Interagieren mit den Verlaufsdatensätzen verwendet, ermöglicht sie:

- Verlaufsdaten werden gesucht und gefiltert.
- Verlaufsdaten werden exportiert.

Verlaufssätze werden angezeigt

Es gibt zwei Möglichkeiten zum Anzeigen des Verlaufssatzes, auf die über die Kontextmenüaktion **Verlauf**zugegriffen werden kann.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterschiede zwischen Audit- und Verlaufssätzen

Die Tabellen „Audit“ [sys_audit], „Verlaufssätze“ [sys_history_set] und „Verlauf“ [sys_history_line] speichern dieselben Daten, dienen jedoch unterschiedlichen Zwecken und verwalten Daten unterschiedlich.

Audit-Tabelle [sys_audit]

In der Audit-Tabelle [sys_audit] speichert das System Verlaufsinformationen für alle Datensätze. Diese Datensätze sollen für immer aufbewahrt werden, damit Administratoren den Verlauf der geprüften Datensätze jederzeit nachverfolgen können. Da die Anzahl der Audit-Datensätze mit der Zeit zunimmt, wird es ineffizienter, Verlaufsinformationen direkt in der Audit-Tabelle abzufragen. Es ist viel effizienter, Abfragen nur für die kleineren Teilmengen der Datensätze auszuführen, für die Sie tatsächlich Verlaufsinformationen anzeigen möchten.

Tabelle „Verlaufssatz“ [sys_history_set].

Die Tabelle „Verlaufssatz“ [sys_history_set] gibt an, welche Datensätze aus einer geprüften Tabelle Verlaufsinformationen enthalten. In der Tabelle „Verlauf“ [sys_history_line] werden die tatsächlichen Änderungen an Feldwerten gespeichert, die vorgenommen wurden.

- Das System generiert nach Bedarf automatisch einen Verlaufssatz und Verlaufsdatensätze aus der Audit-Tabelle, wenn ein Benutzer entweder einen Datensatz erstellt oder seinen Verlauf anfordert.
- Anstatt einen vollständigen Verlauf aller Changes im System zu enthalten, enthalten Verlaufssätze und Verlaufsdatensätze nur eine aktuelle Teilmenge von Verlaufsinformationen für Datensätze, in denen Benutzer diese Informationen erstellt oder angefordert haben.
- Neben Audit-Daten enthalten Verlaufssätze auch die Informationen, die beim Einfügen des Datensatzes festgelegt werden, einschließlich Journalfeldeinträge. Journalfeldeinträge, die Sie vor dem Erstellen eines Datensatzes erstellen, werden auf die gleiche Weise behandelt wie Journaleinträge, die zum Zeitpunkt der Datensatzerstellung erstellt wurden. Diese Journaleinträge werden in Verlaufssätzen mit der gleichen Erstellungszeit und den gleichen Daten wie der zugehörige Datensatz selbst angezeigt.

Das System begrenzt Verlaufssätze und Verlaufsdatensätze durch:

- Lassen Sie die Tabellenbereinigung Verlaufssatz-Datensätze löschen, die seit 30 Tagen nicht aktualisiert wurden.
- Verwenden der Tabellenrotation, um alle sieben Tage zwischen vier Verlaufstabellen zu rotieren. Das System löscht Verlaufsdatensätze, die älter als 28 Tage sind.

Wenn jemand die Verlaufsinformationen zu einem späteren Zeitpunkt erneut benötigt, kann das System sie aus den Audit-Quelldatensätzen erneut generieren.

Nachdem das System Verlaufssatz-Datensätze generiert hat, verwendet die Kontextmenüauswahl **Verlauf** den Verlaufssatz anstelle von Audit-Datensätzen. Aus der Perspektive des Benutzers sind dieselben Verlaufsdaten in derselben Anwenderoberfläche verfügbar, die Informationen werden jedoch anders gespeichert.

Steuern Sie den Zugriff auf den Verlauf

Durch Festlegen einer Systemeigenschaft können Sie einer Rolle Zugriffsrechte für die Anzeige des Auditverlaufs gewähren.

Vorbereitungen

Erforderliche Rolle: admin

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **System**an.
2. Wählen Sie die Eigenschaft *glide.history.role* aus der Tabelle aus.
3. Wählen Sie in *List of roles (comma-separated) that can access the history of a record*die Anwenderrollen aus, auf die Sie auf den Verlauf zugreifen möchten.
4. Wählen Sie **Speichern**.

Ergebnisse

Alle Änderungen an einem Feld werden übersprungen, wenn ein Anwender ohne Lesezugriff den Verlauf eines Datensatzes anzeigt.

Ändern Sie die Anzahl der Verlaufseinträge

Standardmäßig werden im Verlauf maximal 250 Einträge angezeigt. Sie können diesen Wert jedoch ändern.

Vorbereitungen

Erforderliche Rolle: admin

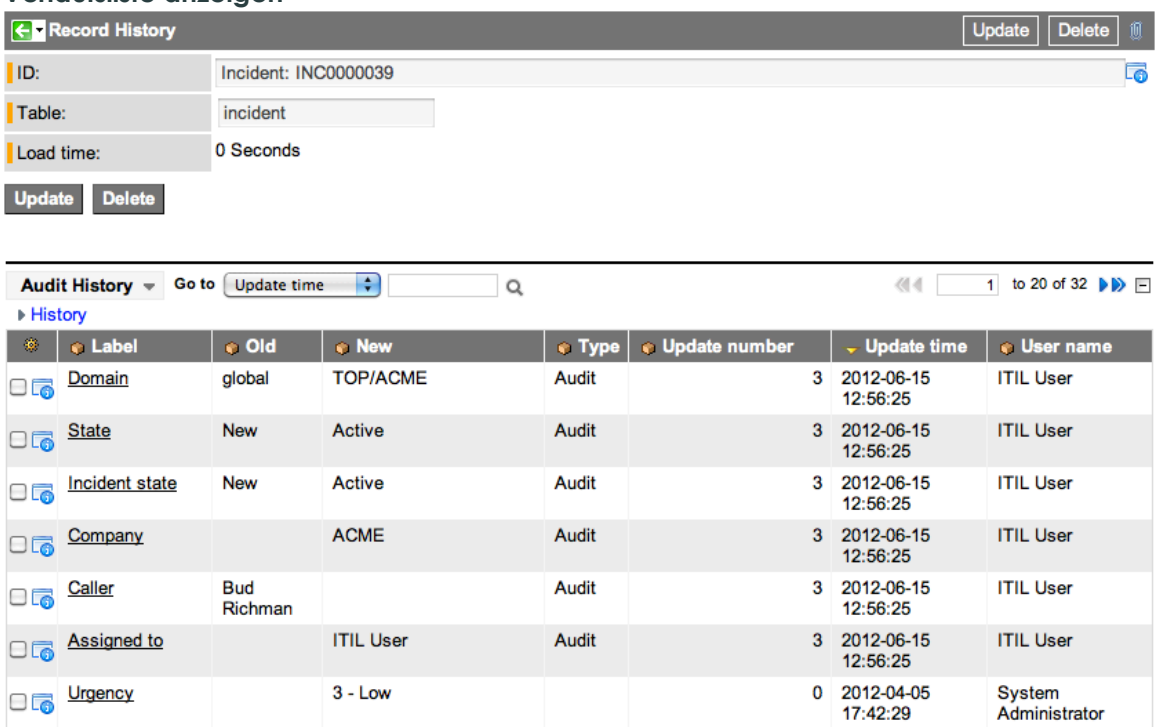
Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **System**an.
2. Wählen Sie die Eigenschaft *glide.history.max_entries* aus.
3. Legen Sie den Wert *Maximum number of field entries displayed in record history, default is 250* mit einer neuen maximalen Anzahl von anzuzeigenden Einträgen fest.

Verlaufsliste

In der Verlaufsliste wird jeder Change als eigene Zeile in der Change-Liste angezeigt.

Verlaufsliste anzeigen

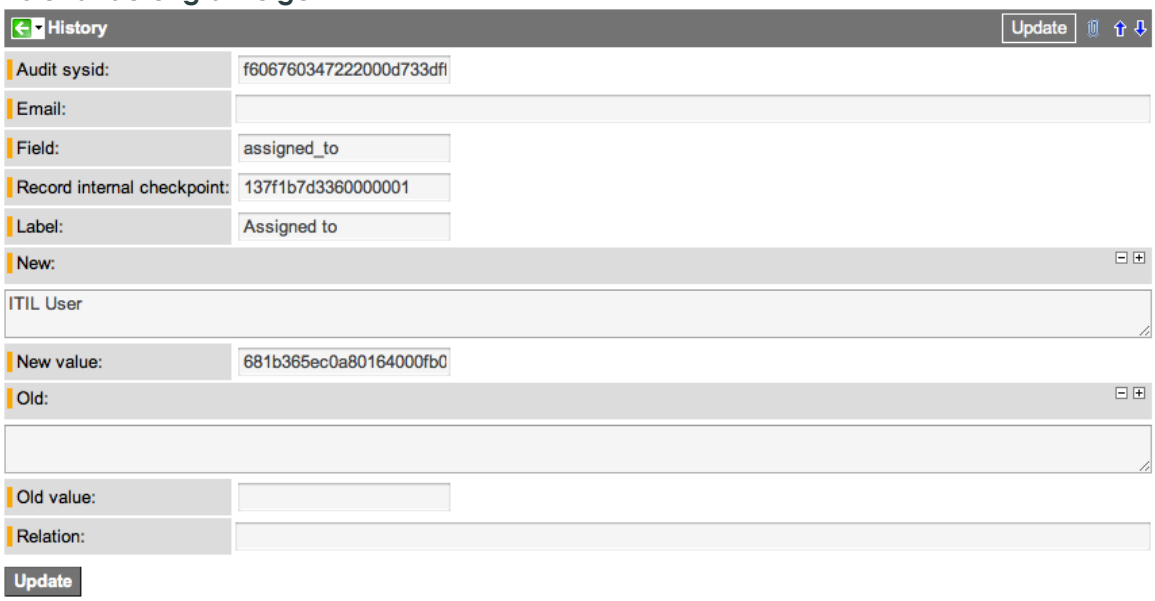


Label	Old	New	Type	Update number	Update time	User name
Domain	global	TOP/ACME	Audit	3	2012-06-15 12:56:25	ITIL User
State	New	Active	Audit	3	2012-06-15 12:56:25	ITIL User
Incident state	New	Active	Audit	3	2012-06-15 12:56:25	ITIL User
Company		ACME	Audit	3	2012-06-15 12:56:25	ITIL User
Caller	Bud Richman		Audit	3	2012-06-15 12:56:25	ITIL User
Assigned to		ITIL User	Audit	3	2012-06-15 12:56:25	ITIL User
Urgency		3 - Low		0	2012-04-05 17:42:29	System Administrator

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Klicken Sie auf ein Zeilenelement, um zusätzliche Details zum Change anzuzeigen.

Listenänderung anzeigen



Anforderungen

Um eine Verlaufsliste anzuzeigen, müssen die folgenden Anforderungen erfüllt sein.

Auditing

Auditing für die Tabelle muss aktiviert sein, um eine Verlaufsliste anzuzeigen.

ACLs

Standardmäßig ist die Option *Listenverlauf* nur für Benutzer mit der Benutzerrolle admin verfügbar. Um diese Option für Nicht-Administratoren zu aktivieren, erstellen Sie eine anwenderdefinierte ACL-Regel, die Lesezugriff auf die Tabelle „Datensatzverlauf“ [sys_history_set] gewährt.

Rollen

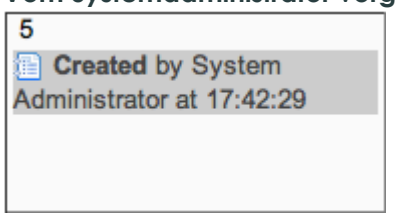
Mindestens eine der Rollen, die der Benutzer hat, muss in der Eigenschaft `glide.history.role` enthalten sein, die standardmäßig die Rolle itil enthält.

Verlaufskalender

Der Verlaufskalender zeigt die Tage an, an denen der Datensatz geändert wurde, wer die Änderung vorgenommen hat und wann.

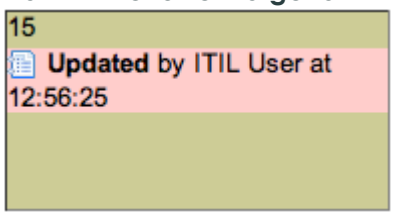
Der Verlaufskalender ist nach Updatenummer sortiert. Jedem Benutzer wird eine Farbe zugewiesen, sodass Sie auf einen Blick erkennen können, wie oft ein Datensatz von einem bestimmten Benutzer geändert wurde. Beispiel:

Vom Systemadministrator vorgenommene Änderungen



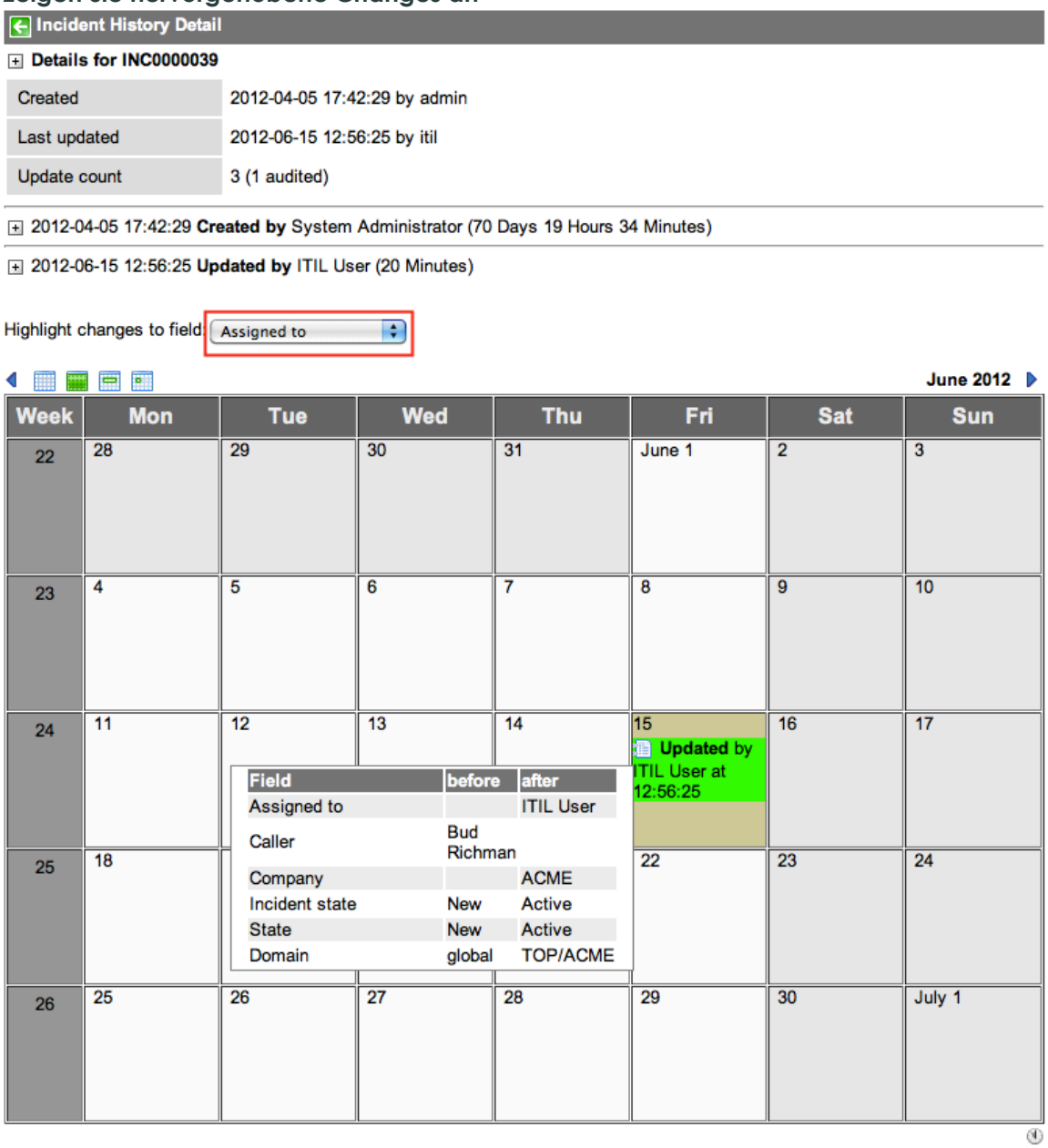
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von ITIL-Benutzer vorgenommene Changes



Um Änderungen an einem bestimmten Feld hervorzuheben, wählen Sie das Feld im Feld **Änderungen an Feld** hervorheben aus. Durch Auswahl eines Felds in diesem Auswahlfeld wird der Kalender geändert, um die Zeiten hervorzuheben, zu denen dieses Feld geändert wurde. Bewegen Sie den Mauszeiger über den Text eines hervorgehobenen Change, um den Change im Wert anzuzeigen.

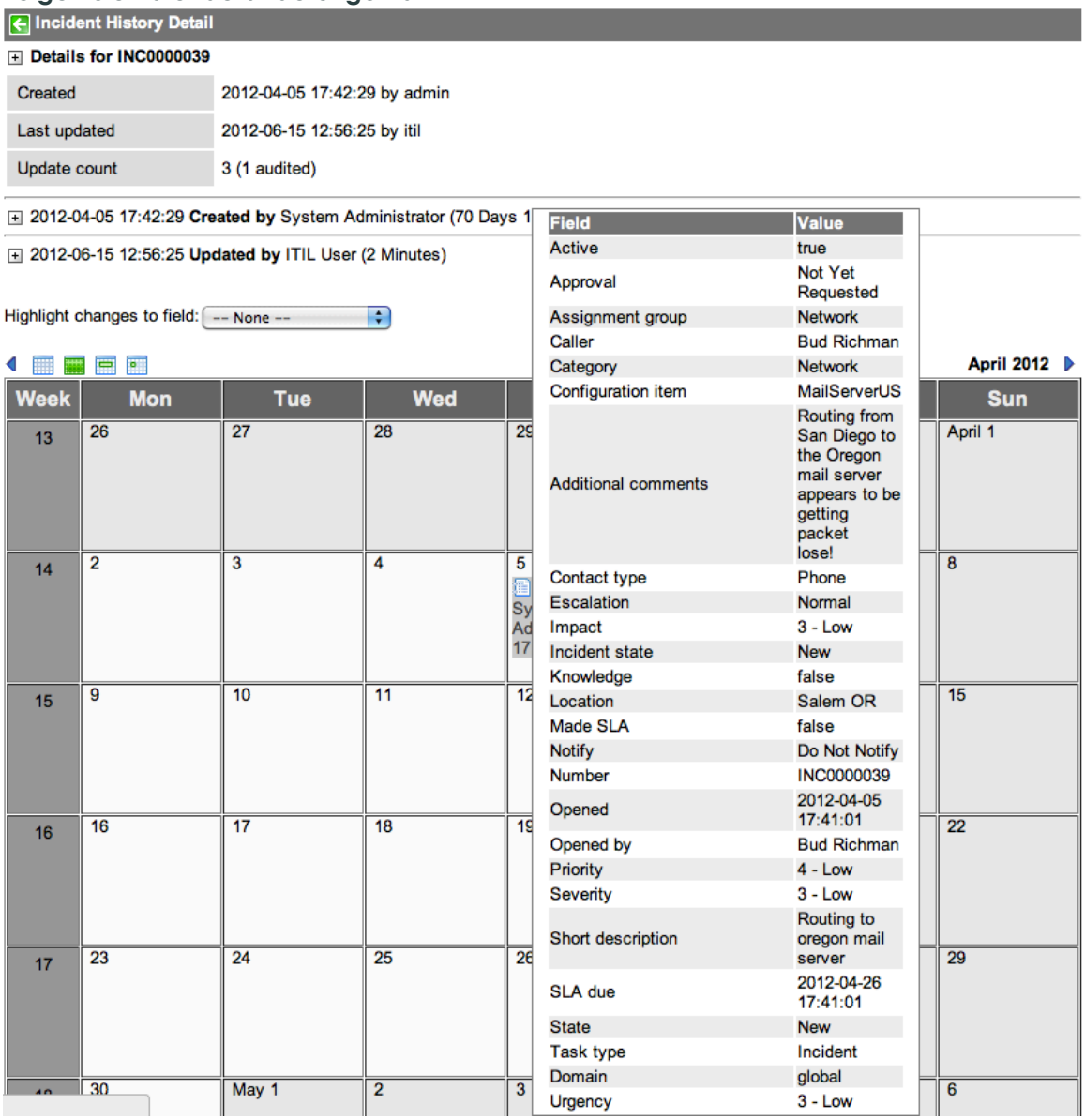
Zeigen Sie hervorgehobene Changes an



Wenn Sie den Mauszeiger über das Symbol in einem Eintrag bewegen, werden in einem Popup alle Wertänderungen angezeigt. Dies sind die gleichen Informationen, die im oberen Teil des Formulars angezeigt werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie Kalenderänderungen an



Sie können auf die Tagesnummer klicken, um eine Ansicht der Änderungen für diesen Tag zu erhalten. Sie können auch auf die Wochennummer links klicken, um die Wochenansicht zu öffnen. Sie können von Monat zu Monat und von Monat zu Monat scrollen, um Änderungen anzuzeigen.

Verlaufszeitleiste

Sie können eine Zeitleiste der Changes für ein CI und die zugehörigen Datensätze, Beziehungen, Baselines und vorgeschlagenen Changes für das CI anzeigen. Zeitleisten sind für CIs in der Tabelle „Konfigurationselement“ [cmdb_ci] oder einem untergeordneten Element dieser Tabelle verfügbar, wenn Auditing für die Tabellen aktiviert ist.

Erforderliche Rolle: Die ACL für diese Ansicht basiert auf den Rollen, die in der Systemeigenschaft *glide.history.role* definiert sind, die standardmäßig auf `itil festgelegt`ist. Außerdem muss der Benutzer über Lesezugriff auf die Tabelle „Verlaufssatz“ [sys_history_set] verfügen, die standardmäßig dem Administrator zugewiesen ist.

Sie können eine Zeitleiste öffnen, wenn Sie den Verlauf eines CI anzeigen. Sie können den Zeitraum, den Zeitraum und die Eigenschaften angeben, die in der Zeitleiste angezeigt

Automatische Übersetzung

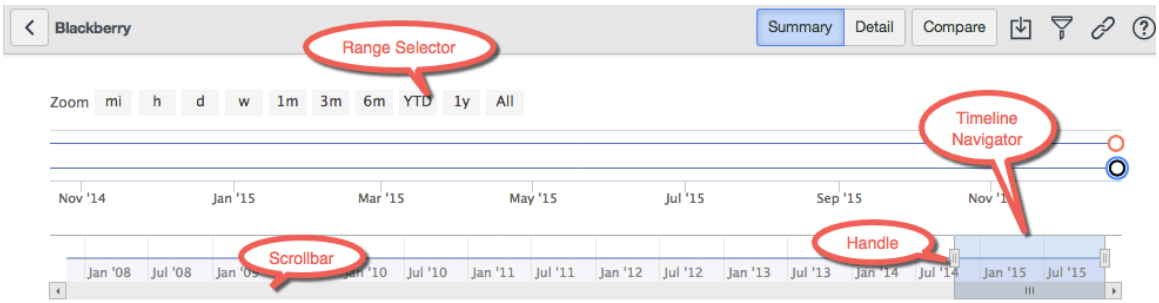
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

werden. Sie können entweder anzeigen, was sich in einem bestimmten Change Set geändert hat, oder das gesamte CI anzeigen, um Probleme besser beheben zu können. Sie können auch eine Zeitleiste der Änderungen an den zugehörigen Datensätzen des CI anzeigen und Snapshots des CI zu jedem Zeitpunkt exportieren und vergleichen.

CI-Changes werden durch Blasen in verschiedenen Formen und Farben entlang der Zeitleiste dargestellt. Die Form jeder Blase stellt eine andere Art von Change dar, und die Farbe jeder Blase gibt an, ob die Änderung gültig oder ungültig ist. CI-Baselines werden durch schwarze Kreise dargestellt, über die Sie den Mauszeiger bewegen können, um weitere Details anzuzeigen. Klicken Sie auf **?** um Definitionen der Blasenform und Farbe anzuzeigen, und zeigen Sie auf eine Blase, um Details zum Change Set anzuzeigen.

Eine Änderung an einer Beziehung gilt nur dann als gültig, wenn sie über Change-Management angewendet wurde. Wenn der Change über das Framework „Vorgeschlagene Changes“ angewendet wurde, ist er gültig. Weitere Informationen finden Sie unter Erstellen oder bearbeiten Sie ein geplantes Validierungsskript .

Ansicht der Verlaufszeitleiste



Zeitleistenblasen



Hinweis: Vorgeschlagene Changes, die kein geplantes Startdatum haben, werden zu zukünftigen Zeitpunkten platziert.

Zeitleistennavigator

Verwenden Sie die Handles an beiden Enden des Zeitleistennavigators, um den angezeigten Zeitraum zu verlängern oder zu verkürzen.

Sie können zu einem anderen Zeitraum scrollen, indem Sie auf den unteren Teil des Zeitleistennavigators klicken und den Navigator dann nach links oder rechts ziehen.

Zoom

Standardmäßig wird die Zeitleiste für den letzten Monat angezeigt. Neben der Bezeichnung **Zoom** über der Zeitleiste können Sie ein anderes Zeitintervall auswählen. Sie können Intervalle von einer Minute bis zum gesamten Datenzeitraum auswählen.

Wenn es während des Zeitraums viele Changes am CI gibt, werden die angezeigten Blasen möglicherweise zu voll. Sie können vergrößern oder verkleinern, um die Blasen mit einer der folgenden Methoden zu verteilen:

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ändern Sie das Zeitintervall auf der Zeitleiste. Wenn Sie das Zeitintervall verkürzen, vergrößern Sie die Ansicht, und wenn Sie das Zeitintervall verlängern, verkleinern Sie die Ansicht.
- Wählen Sie den Abschnitt der Zeitleiste aus, in den Sie vergrößern möchten.

Eigenschaftenfilter

Sie können die angezeigten Blasen filtern. Standardmäßig werden alle Blasen angezeigt, die Änderungen an allen Eigenschaften des CI darstellen. Sie können die Ansicht so einschränken, dass nur die Blasen angezeigt werden, in denen sich ausgewählte Eigenschaften geändert haben, und Blasen, in denen sich nur nicht ausgewählte Eigenschaften geändert haben, ausgeschlossen werden.

Die Ansichten **Detail** und **Zusammenfassung** heben Eigenschaften innerhalb Ihres Filterbereichs hervor, die sich geändert haben. Die geänderten Eigenschaften werden in Hellblau hervorgehoben.

In der **Zusammenfassungsansicht** können Sie auswählen, ob alle Eigenschaften des CI oder nur geänderte Eigenschaften einbezogen werden sollen. Wenn Sie alle Eigenschaften in der Zusammenfassungsansicht anzeigen möchten, werden die geänderten Eigenschaften vor den unveränderten Eigenschaften aufgeführt.

Zusammenfassungsansicht

In der Ansicht „ **Zusammenfassung** “ werden Snapshots der CIs angezeigt, die durch die einzelnen Blasen dargestellt werden. Jeder Snapshot zeigt die Änderungen an den Feldern und Beziehungen des CI gemäß dem Change Set an. Zeigt alte und neue Werte vor und nach dem Change und alle Beziehungen an, die hinzugefügt oder gelöscht wurden.

Verwenden Sie die Schaltflächen **>** und **<** auf beiden Seiten der Snapshot-Anzeige, um durch die nächsten und vorherigen Change Set-Datensätze in chronologischer Reihenfolge zu scrollen.

Detailansicht

In der **Detailansicht** werden Snapshots des CI angezeigt, die den Blasen entsprechen. Jeder Snapshot enthält die Felder, die sich im Eigenschaftsfilterbereich befinden, und zeigt die geänderten Eigenschaften mit einem blauen Hintergrund an. Klicken Sie auf eine Blase, um den entsprechenden Snapshot des CI anzuzeigen. Die angezeigten Daten sind schreibgeschützt.

Verwenden Sie die Schaltflächen **>** und **<** auf beiden Seiten, um durch die nächsten und vorherigen Change Set-Datensätze in chronologischer Reihenfolge zu scrollen.

Zeigen Sie die Zeitleiste der Änderungen an zugehörigen Datensätzen an

Auf der Change-Zeitleiste für einen CI-Datensatz können Sie auch eine Zeitleiste der Changes für die zugehörigen Datensätze des CI anzeigen.

Vorbereitungen

Erforderliche Rolle : admin

- Zieltabelle: Der CI-Datensatz muss sich in der Tabelle „Konfigurationselement“ [cmdb_ci] oder einem untergeordneten Element dieser Tabelle befinden.
- Auditing: muss für die Tabelle aktiviert sein, die das CI enthält.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Öffnen Sie die Zeitleiste für das CI.
2. Wählen Sie das Symbol **Zugehörige Datensätze** und dann die zugehörigen Datensätze aus der **Liste der** zugehörigen Datensätze aus, die angezeigt werden sollen.
   Klicken Sie erneut auf das Symbol Zugehörige Datensätze, um die Zeitleiste der zugehörigen Datensätze anzuzeigen.

Ergebnisse

Die Zeitleiste der Changes an den zugehörigen Datensätzen des CI wird direkt über der Zeitleiste des CI angezeigt. Wenn Sie alle zugehörigen Datensätze deaktivieren, wird die Zeitleiste der zugehörigen Datensätze ausgeblendet.

Nächste Maßnahme

Bewegen Sie den Mauszeiger über eine Change-Blase auf der Zeitleiste der zugehörigen Datensätze, um Details zum Change anzuzeigen, z. B. Datum und Anzahl der geänderten Eigenschaften. Wenn Sie das Zeitintervall im Fokus ändern oder vergrößern oder verkleinern, wirkt sich dies gleichzeitig auf die CI-Zeitleiste und die Zeitleiste der zugehörigen Datensätze aus.

Exportieren Sie einen Snapshot eines CI

Sie können einen Snapshot eines CI aus seiner Zeitleiste exportieren.

Vorbereitungen

Das CI muss sich in der Tabelle „Konfigurationselement“ [cmdb_ci] oder einem untergeordneten Element dieser Tabelle befinden. Für die Tabelle, die das CI enthält, muss Auditing aktiviert sein.
Erforderliche Rolle: admin.

Warum und wann dieser Vorgang ausgeführt wird

Sie können einen Snapshot des CI im XML-, PDF- (Portal) oder PDF-Format (Querformat) exportieren.

Prozedur

1. Öffnen Sie die Zeitleiste für das CI.
2. Wählen Sie die Blase aus, die die Zeit darstellt, für die Sie einen Snapshot des CI exportieren möchten.
3. Klicken Sie auf das Exportsymbol ( ).
4. Wählen Sie das Dateiformat aus, das für den Export verwendet werden soll.
   Sie können die Datei zur Anzeige auf Ihr System herunterladen.

Vergleichen Sie CI-Snapshots

Sie können die Eigenschaften und Beziehungen eines CI an zwei verschiedenen Punkten seiner Zeitleiste vergleichen.

Vorbereitungen

Das CI muss sich in der Tabelle „Konfigurationselement“ [cmdb_ci] oder einem untergeordneten Element dieser Tabelle befinden. Für die Tabelle, die das CI enthält, muss Auditing aktiviert sein.
Erforderliche Rolle: admin.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Öffnen Sie die Zeitleiste für das CI.
2. Klicken Sie auf **Vergleichen**.
3. Wählen Sie ein **Startdatum** und ein **Enddatum** aus.
4. Klicken Sie auf **Vergleichen**.

Änderungen an Referenzfeldern werden nachverfolgt

Administratoren können Änderungen an Anzeigewerten des Referenzfelds nachverfolgen.

Da Referenzfelder nur einen ID-Wert speichern, kann das System normalerweise nur Audits durchführen, wenn sich der ID-Wert ändert. Standardmäßig prüft das System keine Änderungen, wenn sich der Anzeigewert eines Referenzfelds ändert.

Stellen Sie sich die folgende Situation vor. Ein Benutzer ändert seinen Namen von „Jane Smith“ in „Jane Miller“. Da der Benutzername der Anzeigewert für die Tabelle „User“ ist, bezieht sich jeder vorherige Verweis auf „Jane Smith“ stattdessen auf „Jane Miller“. Wenn der Administrator nur den Namen des vorhandenen Benutzerdatensatzes aktualisiert, zeigen Audit- und Verlaufsdatensätze nur den neuen Namen „Jane Miller“ an. Standardmäßig bietet das System keine Möglichkeit, zwischen Änderungen, die unter dem ursprünglichen Benutzernamen vorgenommen wurden, und denen, die mit dem neuen Benutzernamen vorgenommen wurden, zu unterscheiden.

Wenn Ihre Audit-Richtlinie die Nachverfolgung von Benutzernamensänderungen erfordert, haben Sie folgende Möglichkeiten:

- Erstellen Sie einen neuen Anwenderdatensatz für den neuen Namen, und deaktivieren Sie den vorherigen Anwenderdatensatz. Das System speichert Audit-Datensätze für den alten Anwendernamen und erstellt zukünftige Audit-Datensätze mit dem neuen Anwendernamen.
- Erstellen Sie anwenderdefinierte Felder und eine Geschäftsregel, um den vorherigen Namen und das Datum der Namensänderung zu speichern. Das System kann diese Informationen verwenden, um die richtigen Namen in Audit- und Verlaufsdatensätzen zu erstellen.

Nachverfolgung der Einfügungen

Standardmäßig erstellt das System keine Audit-Datensätze für Einfügungen, da Einfügungen in einer typischen Instanz über 80 % der Größe der Audit-Tabelle ausmachen können.

Das Nicht-Nachverfolgen von Einfügungen ermöglicht eine bessere Leistung und eine viel kleinere Audit-Tabelle. Administratoren können die Überwachung von Einfügungen aktivieren, indem sie die Eigenschaft `glide.sys.audit_inserts` auf *true festlegen*.

Nachverfolgung von CI-Beziehungen

Änderungen an einer CI-Beziehung (CI-Beziehungen, CI-/Benutzerbeziehungen oder CI-/Gruppenbeziehungen) werden im Verlauf der Elemente auf beiden Seiten der geänderten Beziehung angezeigt, unabhängig davon, ob die Änderung manuell war oder ein Ergebnis von Discoverywar.

Wenn der Computer Alpha beispielsweise eine von CI-Beziehung mit dem Computer Beta verwendete hat, enthält der Verlauf für Alpha einen Datensatz, wann die Beziehung mit Beta hergestellt wurde, und ebenso enthält der Verlauf für Beta einen Datensatz, wann die Beziehung mit hergestellt wurde Alpha wurde eingerichtet. Dieses Beispiel veranschaulicht

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

den Verlauf, der angezeigt wird, wenn einige CI-Beziehungen hergestellt werden und dann eine der Beziehungen entfernt wird:

CI-Beziehungsverlauf

⊟ 2008-12-03 10:49:37 **Updated by** Guest (19 Hours 54 minutes ago) - CI Relationship Change

- created 2 Days 2 Hours 51 minutes earlier

Relationship	Before	After
Runs	(relationship added)	Tomcat@tomdmac
Runs	(relationship added)	MySQL Server@tomdmac

⊞ 2008-12-03 10:49:38 **Updated by** Guest (19 Hours 54 minutes ago) - Mac OS X - Disks

⊞ 2008-12-03 10:49:43 **Updated by** Guest (19 Hours 54 minutes ago) - Mac OS X - Active Connections

⊞ 2008-12-03 10:50:02 **Updated by** Guest (19 Hours 53 minutes ago)

⊟ 2008-12-04 06:43:39 **Updated by** Glide Maintenance (just now) - CI Relationship Change

- last activity was 19 Hours 53 minutes earlier
- created 2 Days 22 Hours 45 minutes earlier

Relationship	Before	After
Runs	MySQL Server@tomdmac	(relationship removed)

Der Aufzählungspunkt „Erstellt“ gibt das Datum an, an dem das CI, der Benutzer oder die Gruppe erstellt wurde. Der letzte Aktivitätsaufzählungspunkt bezieht sich auf den Zeitpunkt der letzten Änderung der Beziehungen. Wenn der CI-Beziehungsverlauf für einen oder alle CI-Beziehungstypen nicht angezeigt werden soll, können Sie ihn deaktivieren, indem Sie die Überwachung in den CI-Beziehungstabellen (CI-Beziehung [`cmdb_rel_ci`], CI-/Anwender-Beziehungstyp [`cmdb_rel_user_type`] oder Gruppe deaktivieren Beziehung [`cmdb_rel_group`]).

Strenge Sicherheitseinstellungen

Strenge Sicherheitseinstellungen schließen mehrere Sicherheitsoptionen ein, die in Ihrer Instanz verfügbar sind.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkunden Sie die Einstellung für hohe Sicherheit



Lernen Sie die Funktionen und Geschäftsnutzen von Einstellungen für strenge Sicherheit kennen.

Aktivieren Sie die Einstellungen für hohe Sicherheit



Aktivieren Sie die Einstellungen für hohe Sicherheit.

Konfigurieren Sie Einstellungen für hohe Sicherheit



Erfahren Sie, wie Einstellungen für hohe Sicherheit konfiguriert werden.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Strenge Sicherheitseinstellungen erkunden

Strenge Sicherheitseinstellungen schließen mehrere Sicherheitsoptionen ein, die in Ihrer Instanz verfügbar sind.

Das Modul „Strenge Sicherheitseinstellungen“ wird mit dem Plugin „Strenge Sicherheitseinstellungen“ aktiviert, das bei neuen Instanzen standardmäßig aktiv ist. Wenn „Strenge Sicherheitseinstellungen“ in Ihrer Instanz nicht aktiv ist, lesen Sie die Anleitung für „Strenge Sicherheitseinstellungen anfordern“. Weitere Informationen zu diesem Plugin finden Sie unter Hochsicherheits-Plugin in Härtungseinstellungen für Instanzsicherheit. Eigenschaften für diese Arten von Einstellungen für hohe Sicherheit sind verfügbar:

- Standardeigenschaftswerte: Um die Sicherheit auf Ihrer Plattform zu erhöhen, indem alle kritischen Sicherheitseinstellungen an einem zentralen Ort für die Verwaltung und Überwachung zentralisiert werden.
- Standardmäßige Deny-Eigenschaft: Stellt eine Sicherheitsmanager-Eigenschaft zur Steuerung des Standardsicherheitsverhaltens für den Tabellenzugriff bereit.
- Sicherheitsadministratorrolle: Stellt eine Rolle bereit, um die Änderung wichtiger Sicherheitseinstellungen und -ressourcen zu verhindern. Die Sicherheitsadministratorrolle wird nicht von der Administratorrolle geerbt und muss explizit zugewiesen werden.
- Erweiterte Rechte: Ermöglicht Anwendern mit der Sicherheitsadministratorrolle, im Kontext eines normalen Anwenders zu arbeiten und bei Bedarf eine höhere Sicherheitsrolle zu übernehmen.
- Zugriffssteuerungen für Eigenschaften: Ermöglicht Sicherheitsadministratoren das Festlegen der Rollen, die zum Lesen und Schreiben von Eigenschaften erforderlich sind.
- Systemprotokolle: Sind schreibgeschützt.
- Zugriffssteuerungsregeln: Steuern Sie, auf welche Daten Benutzer zugreifen können und wie sie darauf zugreifen können.

Hinweis:

- „Strenge Sicherheitseinstellungen“ aktiviert auch automatisch das Plugin „Kontextsicherheit“, wenn es nicht bereits aktiv ist. Darüber hinaus bietet Plattformsicherheitseinstellungen – Hoch Einstellungen und Funktionen zur Erhöhung der Sicherheit Ihrer Instanz.
- Der Inhalt „Härtungseinstellungen für die Instanzsicherheit“ enthält detaillierte Beschreibungen und Compliance-Werte für die sicherheitsbezogenen Systemeigenschaften und Plugins im Now Platform. Weitere Informationen zu diesen Eigenschaften finden Sie unter Härtungseinstellungen für die Instanzsicherheit.
- Weitere Informationen zu den einzelnen Eigenschaften finden Sie unter Härtungseinstellungen für die Instanzsicherheit.

Es gibt zwei Möglichkeiten, Eigenschaften für Einstellungen für hohe Sicherheit festzulegen oder zu ändern.

- Navigieren zu **Systemsicherheit** > **Strenge Sicherheitseinstellungen**an.

  Optionen auf der Seite „Strenge Sicherheitseigenschaften“ sind **Ja** oder **Nein**.

- Navigieren Sie zu **sys_properties.list** und suchen Sie nach der Eigenschaft, die Sie festlegen oder ändern möchten.

  Optionen in der Tabelle „Systemeigenschaften“ [sys_properties.list] sind **true** oder **false**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugriffssteuerung für Eigenschaften

Wenn „Strenge Sicherheitseinstellungen“ aktiv ist, werden in der Tabelle „Eigenschaften“ [sys_properties] zwei zusätzliche Spalten erstellt:

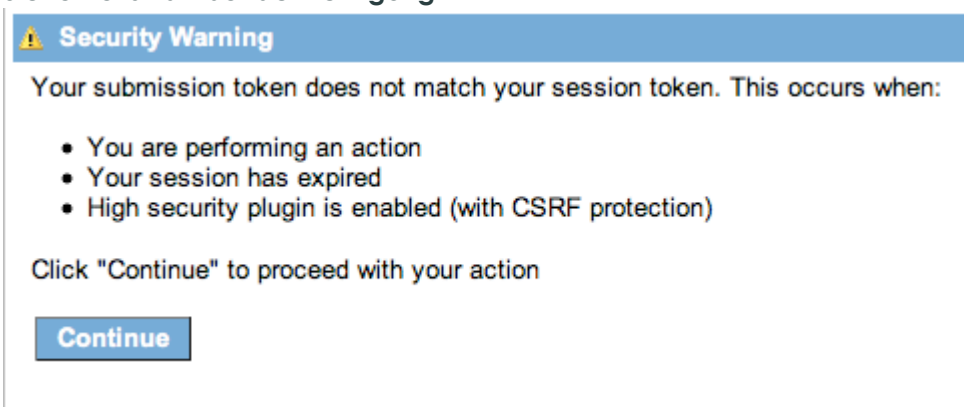
- **read_roles**: Eine durch Kommas getrennte Liste von Rollennamen, die alle Felder dieser Eigenschaft lesen dürfen.
- **write_roles**: Eine durch Kommas getrennte Liste von Rollennamen, die alle Felder dieser Eigenschaft schreiben/ändern dürfen.

Eigenschaften, die in der Tabelle „Eigenschaften“ aufgeführt sind, haben **„read_roles“** des Werts „admin“ und **„write_roles“** des Werts „security_admin“. Benutzer mit der Rolle „admin“ können die Eigenschaftswerte anzeigen und lesen, müssen jedoch zum Ändern die Eigenschaftswerte auf die Rolle „security_admin“ hochstufen.

Benachrichtigungen

Durch die Aktivierung von Einstellungen für hohe Sicherheit werden auch Sicherheitswarnmeldungen aktiviert. Im Folgenden finden Sie ein Beispiel für eine Nachricht, die nach einer Genehmigung angezeigt wird.

Sicherheitswarnbenachrichtigung



Eigenschaften von „Strenge Sicherheitseinstellungen“

Eigenschaft	Beschreibung	Standardwert	Härtungseinstellungen für die Instanzsicherheit
glide.ui.escape_text	XML-Werte auf Parser-Ebene für die Anwenderoberfläche codieren. Verhindert reflektierte und gespeicherte Cross Site Scripting-Angriffe. Diese Eigenschaft ist im Serviceportal nicht anwendbar.	Ja	XML

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung	Standardwert	Härtungseinstellungen für die Instanzsicherheit
	Hinweis: Diese Eigenschaft ist in Vancouver und späteren Releases standardmäßig auf „ **true** “ festgelegt und kann von Administratoren nicht geändert werden. Wenn Sie einen Anwendungsfall haben, bei dem die Eigenschaft geändert werden muss, wenden Sie sich an den Kundensupport.		
glide.ui.escape_all_script	Erzwingt alle Ausdrücke in Jelly-JavaScript <![CDATA[<script type="text/javascript">]]> Tags standardmäßig mit Escape-Zeichen versehen. Erzwingt die Codierung nur, wenn das Typattribut in der <![CDATA[<script>]]> Tag leer ist oder wenn der Wert `text/javascript`, `text/ecmascript`, `application/javascript`, `application/ecmascript`oder `application/x-javascript`ist.	Ja, in neuen Instanzen	Escape Jelly
glide.ui.rotate_sessions	HTTP-Sitzungs-IDs rotieren, um	Ja	HTTP-Sitzungs-Bezeichner rotieren

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung	Standardwert	Härtungseinstellungen für die Instanzsicherheit
	Sicherheitsschwachstellen zu reduzieren. Siehe: http://www.owasp.org/index.php/Session_Management#	**Hinweis:** Wenn Sie das SAML 2.0-Plugin für die Single Sign-on-Authentifizierung verwenden, setzen Sie diese Eigenschaft auf Nein. Andernfalls wird die gemeinsame Nutzung von Sitzungsinformationen zwischen der Instanz und dem Identitätsanbieter beeinträchtigt.	fiers .
glide.ui.secure_cookies	Cookies für sichere Sitzung aktivieren: Zusätzliche Cookie-Sicherheit aktivieren. Falls **Ja**, wird eine strikte Validierung des Sitzungscookies erzwungen.	Ja	Sitzungscookies schützen
glide.security.password_reset.uri	Für Mobilgeräte PasswortzurücksetzungURL, zu der der Benutzer weitergeleitet wird, wenn er auf die **Schaltfläche Passwort vergessen?** klickt. Schaltfläche.		Keine
glide.security.strict.updates	Sicherheit eingehender Transaktionen bei der Formularübermittlung nochmals überprüfen (Rechte werden immer bei der Formulargenerierung überprüft).	Ja	Überprüfen Sie die eingehenden Transaktionen noch einmal

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung	Standardwert	Härtungseinstellungen für die Instanzsicherheit
	Hinweis: Diese Eigenschaft ist in Vancouver und späteren Releases standardmäßig auf „ **true** “ festgelegt und kann von Administratoren nicht geändert werden. Wenn Sie einen Anwendungsfall haben, bei dem die Eigenschaft geändert werden muss, wenden Sie sich an den Kundensupport.		
glide.security.strict.actions	Überprüfen Sie die Bedingungen für UI-Aktionen vor der Ausführung. Normalerweise werden Bedingungen nur während des Formular-Renderings überprüft.	Ja	UI-Aktion vor der Ausführung überprüfen
glide.security.use_csrf_token	Aktivieren Sie die Verwendung eines sicheren Tokens, um eingehende Anforderungen zu identifizieren und zu validieren. Dieses Token wird verwendet, um Site-übergreifende Angriffe durch gefälschte Anforderungen zu verhindern.	Ja	Anti-CSRF-Token
glide.ui.escape_html_list_field	HTML für HTML-Felder in einer Listenansicht codieren.	Ja	Escape-Zeichen für HTML

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung	Standardwert	Härtungseinstellungen für die Instanzsicherheit
glide.html.escape_script	Escape-Zeichen für JavaScript-Tags in HTML-Feldern.	Ja	Escape-Zeichen für Javascript
glide.ui.vergissmich	Entfernen Sie das Kontrollkästchen Anwendernamen speichern von der **Anmeldeseite**.	Ja	„Anwendernamen speichern“ entfernen
glide.smtp.auth	Authentifizieren Sie sich beim SMTP-Server über die Eigenschaften Anwendername und Passwort. **Hinweis:** Diese Eigenschaft ist veraltet.	Ja	
glide.script.use.sandbox	Vom Client generierte Skripts (AJAXEvaluate- und Abfragebedingungen) in einer Sandbox mit reduzierten Rechten ausführen. Wenn **Ja**, sind nur die Business-Regeln und Skripteinbindungen verfügbar, für die das Kontrollkästchen **Vom Client aufrufbar** auf **Ja** festgelegt ist, und bestimmte Back-End-API-Aufrufe werden nicht zugelassen. Weitere Informationen finden Sie unter Sandbox-Eigenschaft für Skript konfigurieren.	Ja	Vom Client generierte Skripts in der Sandbox
glide.soap.strict_security	Strikte Sicherheit für eingehende SOAP-Anforderungen erzwingen. Erfordert, dass bei eingehenden SOAP-	Ja	Strikte Sicherheit für SOAP-Anforderungen

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung	Standardwert	Härtungseinstellungen für die Instanzsicherheit
	Anforderungen der Zugriff auf Tabellen und Felder durch den Sicherheitsmanager überprüft wird, und überprüft die SOAP-Anwender auf die richtigen Rollen für die Verwendung des Webservice.		
glide.basicauth.required.wsdl	Autorisierung für eingehende WSDL-Anforderungen anfordern. **Hinweis:** Wenn Sie keine Autorisierung für eingehende WSDL-Anforderungen vorschreiben möchten, müssen Sie die Regeln für die Zugriffssteuerung (ACL) ändern, um Gastbenutzern den Zugriff auf WSDL-Inhalt zu ermöglichen.	Ja	Autorisierung von WSDL-Anforderungen
glide.basicauth.required.csv	Standardautorisierung für eingehende CSV-Anforderungen anfordern an.	Ja	Autorisierung von CSV-Anforderungen
glide.basisauth.erforderlich.excel	Standardautorisierung für eingehende Excel-Anforderungen anfordern.	Ja	Autorisierung von Excel-Anforderungen
glide.basisauth.erforderlich.importprozessor	Standardautorisierung für eingehende Importanforderungen anfordern.	Ja	Autorisierung der Importanforderung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung	Standardwert	Härtungseinstellungen für die Instanzsicherheit
glide.basicauth.required.pdf	Standardautorisierung für eingehende PDF-Anforderungen anfordern.	Ja	Autorisierung von PDF-Anforderungen
glide.basicauth.required.rss	Standardautorisierung für eingehende RSS-Anforderungen anfordern.	Ja	Autorisierung von RSS-Anforderungen
glide.basicauth.required.scriptedprocessor	Standardautorisierung für eingehende Skriptanforderungen anfordern.	Ja	Autorisierung von Skript-Anforderungen
glide.basicauth.required.soap	Standard-Berechtigung für eingehende SOAP-Requests anfordern.	Ja	Standardauthentifizierung: SOAP-Anforderungen
glide.basicauth.required.unl	Standardautorisierung für eingehende Entlade-Anforderungen anfordern.	Ja	Autorisierung von Entlade-Anforderungen
glide.basicauth.required.xml	Standardautorisierung für eingehende XML-Anforderungen anfordern.	Ja	Autorisierung von XML-Anforderungen
glide.basisauth.erforderlich.xsd	Standardautorisierung für eingehende XSD-Anforderungen anfordern.	Ja	Autorisierung von XSD-Anforderungen
glide.cms.catalog_uri_relative	Erzwingen Sie relative Links über den URI-Parameter für /ess/catalog.do. Falls **Ja**, werden nur relative URLs über die Seite „/ess/catalog.do“ mit dem Parameter *uri* zugelassen. Bei „ **Nein**“ sind alle URLs zulässig, was auch Verknüpfungen zu externen, nicht	Ja	Relative Links erzwingen

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung	Standardwert	Härtungseinstellungen für die Instanzsicherheit
	autorisierten Inhalten zulassen kann.		
glide.set_x_frame_options	Aktivieren Sie diese Eigenschaft, um den X-Frame-Options-Antwortheader für alle UI-Seiten auf SAMEORIGIN festzulegen. Der X-Frame-Options HTTP Response Header kann verwendet werden, um anzugeben, ob der Browser eine Seite in einem <frame> oder <iframe> rendern kann. Websites können diese Eigenschaft verwenden, um Clickjacking-Angriffe zu vermeiden, indem sichergestellt wird, dass ihr Inhalt nicht in andere Websites eingebettet wird. https://developer.mozilla.org/en/the_x-frame-options_response_header	Ja	X-Frame-Options: SAMEORIGIN
glide.ui.attachment.download_mime_types	Eine Liste von kommagetrennten MIME-Typen für Anhänge, die nicht inline im Browser gerendert werden. Sie verhindert Cross Site Scripting-Angriffe. Beispielsweise erzwingt `text/html`, dass HTML-Dateien als Anhänge auf den Client heruntergeladen und nicht inline im Browser angezeigt werden.	`text/html,image/svg,image/svg+xml`	Erzwingen Sie den Download der MIME-Typen
glide.security.groupby_acl_check	Wenn diese Eigenschaft	Ja	Keine

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung	Standardwert	Härtungseinstellungen für die Instanzsicherheit
	aktiviert ist, werden ACL-Prüfungen für GroupBy-Vorgänge für die Gruppennamen basierend auf den tatsächlichen Daten der Gruppen durchgeführt.		
glide.security.diag_txns	Falls „ **Ja**“, kann nur der Administratoranwender oder ein Anwender von der zulässigen IP-Adresse auf `stats.do`, `threads.do` und `replication.do` zugreifen.	Nein	Leistungsüberwachung (ACL)
glide.ui.security.codetag.allow_script	Eingebettetes HTML (mit [code]-Tags) darf JavaScript-Tags enthalten. **Hinweis:** Diese Eigenschaft ist in Vancouver und späteren Releases standardmäßig auf „ **true** “ festgelegt und kann von Administratoren nicht geändert werden. Wenn Sie einen Anwendungsfall haben, bei dem die Eigenschaft geändert werden muss, wenden Sie sich an den Kundensupport.	Nein	Eingebetteten HTML-Code zulassen
glide.script.allow.ajaxevaluate	Aktivieren Sie den AJAXEvaluate-Prozessor. Der *`AJAXEvaluate`*- API-Aufruf ermöglicht es dem Client, beliebige	Nein	Aktivieren Sie AJAXEvaluate

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung	Standardwert	Härtungseinstellungen für die Instanzsicherheit
	Skripts auf dem Server zu senden und auszuführen.		
glide.login.autocomplete	Browsern die Verwendung der automatischen Vervollständigung für Passwortfelder in Anmeldeformularen erlauben.	Nein	Automatische Vervollständigung des Passwortfelds

Die folgenden Eigenschaften sind in der Tabelle „sys_properties“ definiert, werden jedoch nicht auf der Seite „Strenge Sicherheitseinstellungen“ angezeigt.

Eigenschaft	Beschreibung	Standardwert	Härtungseinstellungen für die Instanzsicherheit
com.glide.communications.httpclient.verify_hostname	Überprüft den Hostnamen und die Zertifikatkette, die von Remote-SSL-Hosts dargestellt werden. Schützen Sie sich vor MITM-Angriffen (Man-In-The-Middle). Weitere Informationen finden Sie unter Kubernetes-Spoke einrichten **Hinweis:** Diese Eigenschaft überschreibt die Eigenschaft com.glide.communications.trustmanager_trust_all.	wahr	Keine
glide.basicauth.required.schema	Standardauthentifizierung für eingehende Tabellenschemaanforderungen anfordern.	wahr	Keine
glide.security.csrf_previous.allow	Verwendung eines abgelaufenen sicheren Tokens zum Identifizieren und Validieren eingehender Anforderungen	falsch	Keine

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung	Standardwert	Härtungseinstellungen für die Instanzsicherheit
	zulassen Dieses Token wird verwendet, um Site-übergreifende Angriffe durch gefälschte Anforderungen zu verhindern.		
glide.security.csrf_previous.time_limit	Zeit in Sekunden, bis ein sicheres Token abläuft. Ermöglicht die Kontrolle über die Gültigkeitsdauer des vorherigen CSRF-Tokens. Wenn die Benutzersitzung abläuft, läuft auch das sichere Token ab, es sei denn, die Eigenschaft *glide.security.csrf_previous.allow* ist aktiviert und der Zeitraum liegt innerhalb des durch diese Eigenschaft beschriebenen Zeitrahmens. Dieses Token wird verwendet, um Site-übergreifende Angriffe durch gefälschte Anforderungen zu verhindern.	86400 **Hinweis:** Wert in Sekunden. Entspricht 1 Tag.	Keine
glide.security.csrf.strict_validation.mode	Erzwingt die strikte Überprüfung von CSRF-Token, wobei das erneute Übermitteln der Anforderung durch Benutzer nicht erlaubt ist, wenn das CSRF-Token nicht übereinstimmt.	falsch	Strikte CSRF-Validierung
com.glide.security.check_enforce_sanitized_html	Erzwingt das Bereinigungsverhalten von translated_html-Feldern auf globaler Ebene für Feldzuweisungen.	erzwingen	Keine

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sandbox-Eigenschaft für Skript konfigurieren

Aktivieren Sie die Skript-Sandbox-Eigenschaft (*glide.script.use.sandbox*), um vom Client generierte Skripts in einer Sandbox mit eingeschränkten Rechten auszuführen.

Es gibt zwei Fälle im System, in denen der Client Skripts zur Bewertung an den Server senden kann.

- Filter und/oder Abfragen: Es ist zulässig, einen Filter an den Server zu senden, z. `B.: assigned_to=javascript:getMyGroups()`.
- System-API: Mit dem API-Aufruf *AJAXEvaluate* kann der Client beliebige Skripts auf dem Server ausführen und eine Antwort erhalten.

Wenn Sie die Skript-Sandbox-Eigenschaft (*glide.script.use.sandbox*) aktivieren, wird das Skript, das über einen dieser beiden Einstiegspunkte ausgewertet wird, in einer Sandbox mit reduzierten Rechten mit den folgenden Eigenschaften ausgeführt:

- Nur die als vom **Client aufrufbar** markierten Business-Regeln sind in der Sandbox verfügbar.
- In der Sandbox sind nur Skripteinbindungen verfügbar, die als vom **Client aufrufbar** markiert sind.
- Bestimmte API-Aufrufe (hauptsächlich, aber nicht ausschließlich beschränkt auf Aufrufe des direkten DB-Zugriffs) sind nicht zulässig.
- Daten können in der Sandbox nicht eingefügt, aktualisiert oder gelöscht werden. Alle Aufrufe von beispielsweise *current.update()*werden ignoriert.

Hinweis: Weitere Informationen zu dieser Eigenschaft finden Sie unter Vom Client generierte Skripts in der Sandbox in Härtungseinstellungen für Instanzsicherheit.

Diese Methoden sind in vom Client generierten Skripts nicht zulässig, wenn Skript-Sandboxing aktiviert ist.

Eingeschränkte Methoden

Klasse	Methode
GlideRecord	• *löschenMehrere ()* • *löschenDatensatz ()* • *abrufenRowCount()* • *einfügen ()* • *Update ()* • *updateMultiple ()*
GlideSystem (gs)	• *hinzufügenFehlermeldung ()* • *hinzufügenInfoNachricht ()* • *hinzufügenNachricht ()* • *EreignisWarteschlange ()* • *FlushMessages ()* • *abrufenEscapedProperty()* • *abrufenEigenschaft ()*

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingeschränkte Methoden (Fortsetzung)

Klasse	Methode
	• `Protokoll ()` • `Protokollfehler ()` • `ProtokollWarnung ()` • `festlegenEigenschaft()` • `festlegenWeiterleiten ()` • `festlegenRückkehr ()` • `WorkflowFlush ()`
ScopedGlideRecord	• `löschenMehrere ()` • `löschenDatensatz ()` • `einfügen ()` • `Update ()` • `updateMultiple ()`
ScopedGlideSystem (gs)	• `hinzufügenFehlermeldung ()` • `hinzufügenInfoNachricht ()` • `debuggen ()` • `EreignisWarteschlange ()` • `ausführenNow ()` • `abrufenEigenschaft ()` • `abrufenSitzungToken ()` • `Info ()` • `festlegenWeiterleiten ()`
GlideDate GlideDateTime GlideTime	• `add()` • `addDays ()` • `addDaysLocalTime ()` • `addDaysUTC ()` • `hinzufügenMonateOrtsZeit()` • `Monate hinzufügen ()` • `Sekunden hinzufügen ()` • `hinzufügenWochen()` • `addYears()` • `vergleichenMit ()` • `getByFormat ()` • `getDate()`

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingeschränkte Methoden (Fortsetzung)

Klasse	Methode
	• `abrufenTagDerWoche ()` • `getDayOfWeekUTC` • `abrufenWochentagOrtszeit()` • `abrufenTagDesMonats ()` • `abrufenTagDesMonatsLokaleZeit()` • `abrufenTagDesMonatsNoTZ()` • `abrufenTagDerWoche ()` • `abrufenWochentagOrtszeit()` • `abrufenTagDerWocheUTC()` • `abrufenHourOfDayLocalTime()` • `abrufenUhrzeitUTC()` • `abrufenTageInMonat ()` • `abrufenTageInMonatUTC()` • `abrufenTageInMonatLokaleZeit()` • `abrufenDisplayValueInternal ()` • `abrufenAnzeigewert()` • `abrufenStundeLokaleZeit ()` • `abrufenLokales Datum ()` • `abrufenLokaleZeit ()` • `abrufenMinutenLokaleZeit()` • `abrufenMinutenUTC()` • `abrufenMonatLokaleZeit()` • `abrufenMonatNoTZ()` • `abrufenMonatUTC ()` • `abrufenNumerischerWert ()` • `getSeconds()` • `getZeit ()` • `abrufenTZOffset()` • `abrufenWert()` • `abrufenJahr ()` • `abrufenAnwenderZeitZone()` • `abrufenWocheDesJahresOrtszeit()` • `abrufenWeekOfYearUTC()` • `abrufenJahrUTC()` • `abrufenJahrLokaleZeit()` • `isDST ()`

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingeschränkte Methoden (Fortsetzung)

Klasse	Methode
	• `onOrAfter()` • `onOrBefore ()` • `festlegenTagDesMonatsUTC()` • `festlegenAnzeigewert()` • `festlegenMonat ()` • `festlegenNumerischerWert ()` • `festlegenTZ ()` • `setValue()` • `festlegenwertUTC ()` • `subtract()` • `toString()`
GlideSchedule	• `add()` • `isInZeitplan ()` • `Laden ()` • `wenn Weiter ()`

Hinweis: Die GlideSystem (gs)-Methoden `log()`, `logError()`und `logWarning()` können mit Skript-Sandboxing aktiviert werden, indem die Systemeigenschaft `glide.security.sandbox_no_logging` auf den Wert `false`festgelegt wird.

Wenn Sie das System ohne aktiviertes Skript-Sandboxing ausführen, gelten keine dieser Einschränkungen.

Hinweis: Diese Eigenschaft ist standardmäßig aktiviert, wenn Sie das Plugin „Hohe Sicherheitseinstellungen“ aktivieren. Aktivieren Sie diese Eigenschaft nicht außerhalb des Plugins.

Eigenschaft	Standard
Vom Client generierte Skripts (`AJAXEvaluate`- und Abfragebedingungen) in einer „Sandbox“ mit reduzierten Rechten ausführen. Wenn diese Option aktiviert ist, sind nur die Business-Regeln und Skripteinbindungen verfügbar, für die das Kontrollkästchen **Vom Client aufrufbar** auf wahr festgelegt ist, und bestimmte Back-End-API-Aufrufe werden nicht zugelassen.	Aktiviert (Sandbox wird verwendet).

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einstellungen für hohe Sicherheit werden aktiviert

Das Plugin „Hohe Sicherheitseinstellungen“ ist bei allen neuen Instanzen standardmäßig aktiv. Wenn es in Ihrer Instanz nicht aktiv ist, können Sie das Plugin anfordern.

Vorbereitungen

Erforderliche Rolle: keine

Bevor Sie „ Strenge Sicherheitseinstellungen“ in einer vorhandenen Instanz aktivieren :

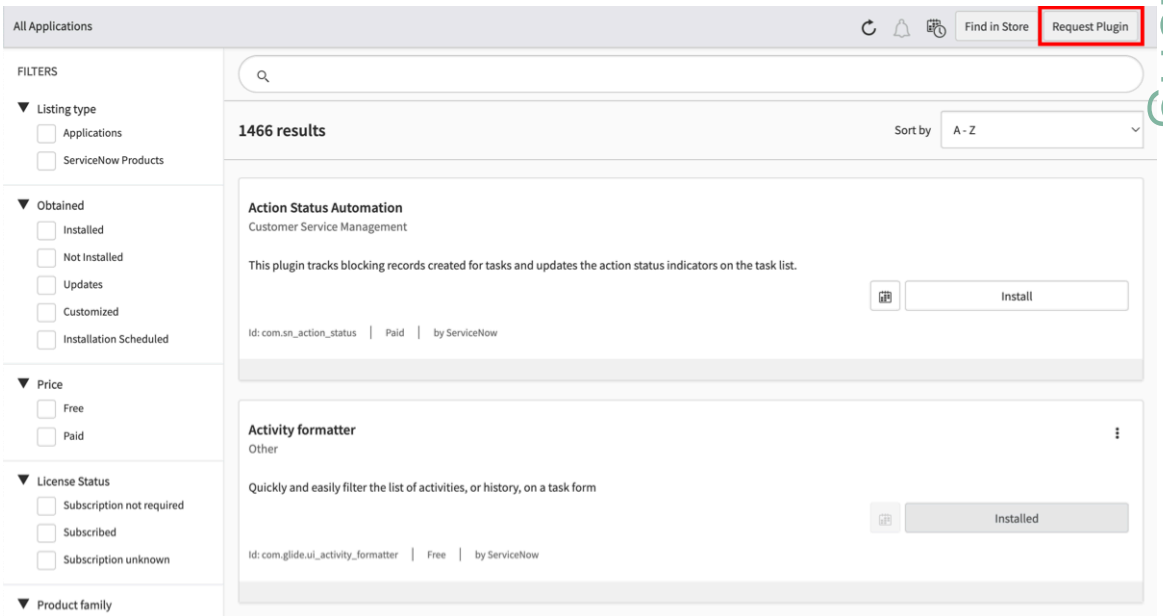
1. Lesen Sie sich die folgenden Informationen durch, um das neue Verhalten zu verstehen:
   - Regeln für Zugriffssteuerungsliste
   - Strenge Sicherheitseinstellungen
   - Standardmäßige Verweigerungseigenschaft
2. Aktivieren Sie das Plugin in einer Instanz außerhalb der Produktion. Ein aktueller Produktionsklon ist vorzuziehen.
3. Testen Sie die überarbeitete Funktionalität, insbesondere die hinzugefügten ACLs und die standardmäßig verweigern-Funktion. Setzen Sie den Test fort, bis das System wie erwartet funktioniert. Wenn Benutzer nicht auf erwartete Ressourcen zugreifen können, stellen Sie sicher, dass sie über die entsprechenden Rollen und ACL-Regeln verfügen, um ihnen Zugriff zu gewähren.
4. Erstellen Sie Update-Sätze aller erforderlichen Änderungen, damit Sie sie auf die Produktion anwenden können.

Hinweis: Weitere Informationen zu diesem Plugin finden Sie unter Hochsicherheits-Plugin in Härtungseinstellungen für Instanzsicherheit.

Erforderliche Rolle: admin

Prozedur

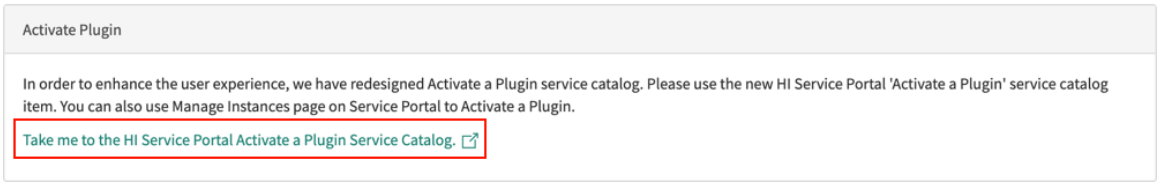
1. Navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Klicken Sie auf der Seite „Alle Anwendungen“ auf **Plugin anfordern**, um das Formular **Plugin aktivieren** auf Now Support zu öffnen.



Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie unter Now Support den Link aus, um auf Now Support Serviceportal Servicekatalog zuzugreifen.



4. Wählen Sie Ihre Instanz aus.
5. Wählen Sie **Aktionen > Plugin aktivieren** aus.
6. Geben Sie im Formular **Plugin aktivieren** die folgenden Informationen an.

Formular „Plugin anfordern“

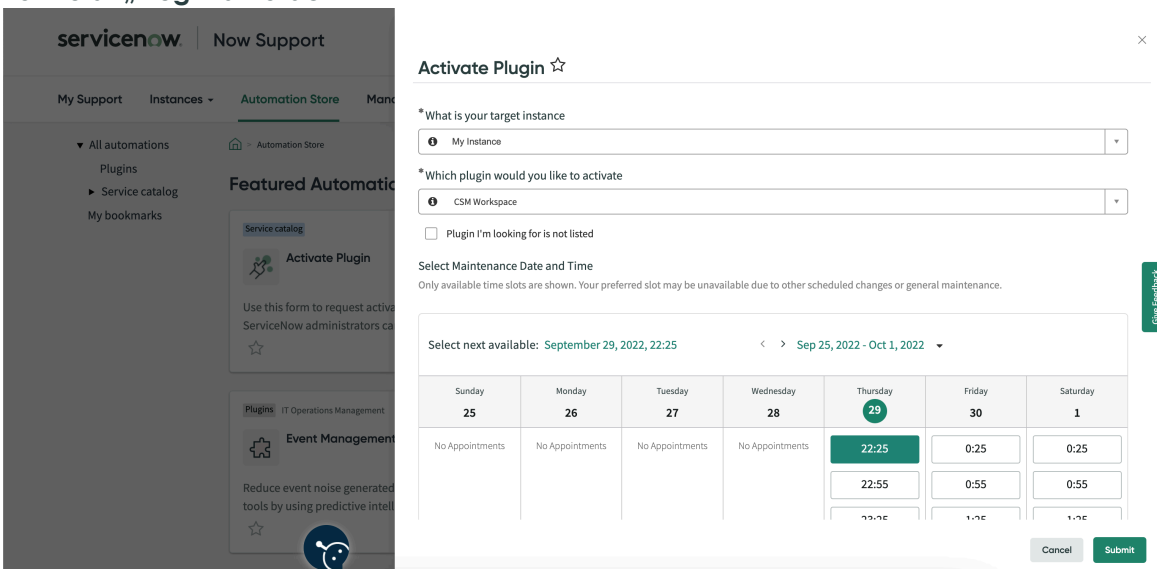
Feld	Beschreibung
What is your target instance (Ihre Zielinstanz)	Instanz, auf der das Plugin aktiviert werden soll.
Which plugin would you like to activate (Welches Plugin möchten Sie aktivieren?)	Name des zu aktivierenden Plugins **Hinweis:** Wenn das System das gewünschte Plugin nicht auflistet oder wenn Sie das Plugin auf einer OEM- oder lokalen Instanz aktivieren, aktivieren Sie das Kontrollkästchen **Plugin I'm looking for is not listed (Gesuchtes Plugin ist nicht aufgelistet)**, und geben Sie dann den Namen des Plugins ein.
Select Maintenance Date and Time (Datum und Uhrzeit der Wartung)	Datum und Uhrzeit zum Aktivieren des Plugins. **Hinweis:** Plugins werden in der pazifischen Zeitzone jeden Werktag in zwei Batches aktiviert, einmal am Morgen und einmal am Abend. Wenn das Plugin zu einem bestimmten Zeitpunkt aktiviert werden muss, geben Sie die Anforderung bei **Grund/ Kommentare** ein.

Example

Betrachten Sie beispielsweise das folgende Formular, um das Plugin „CSM Workspace“ in einer Instanz mit dem Namen „My Instance“ zu aktivieren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Plugin anfordern“



7. Wählen Sie **Absenden**.
   Weitere Informationen zum Anfordern eines Plugins finden Sie im Artikel Plugin aus dem Servicekatalog anfordern [KB0751715] in der Now Support Knowledge Base.

Virtuelles privates Netzwerk (VPN)

Verwenden Sie ein virtuelles privates Netzwerk (VPN), um Ihre Instanz mit externen Datenquellen über das Internet zu integrieren.

Erkunden	Aktivieren
	
Lernen Sie die Funktionen und Geschäftswerte von Virtual Private Network kennen.	Aktivieren Sie das virtuelle private Netzwerk.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren



Erfahren Sie, wie ein virtuelles privates Netzwerk konfiguriert wird.

Virtual Private Network (VPN) erkunden

Verwenden Sie ein virtuelles privates Netzwerk (VPN), um Ihre Instanz mit externen Datenquellen über das Internet zu integrieren.

Meine IP-Informationen

Wenn Sie eine Integration konfigurieren, die ein verschlüsseltes Protokoll verwendet, z. B. LDAP (Leichtgewichtler Verzeichniszugriff) oder HTTPS, empfiehlt es sich, das Internet als Transportmechanismus zu verwenden.

Es können jedoch Sicherheits- oder Netzwerkarchitekturanforderungen bestehen, die die Verwendung einer Site-to-Site Internet Protocol Security (IPSEC) Virtual Private Network (VPN)-Verbindung zwischen den Rechenzentren und Ihren Geschäftsnetzwerken vorschreiben. Das VPN unterstützt die erforderliche verschlüsselte Kommunikation zwischen der Instanz und Ihrem Netzwerk.

VPN-Verbindungen

Die VPN-Infrastruktur ServiceNow verwendet Paare von Cisco Adaptive Security Appliances (ASA), die als VPN-Beendigungspunkte dienen.

Das VPN zwischen der -Instanz und Ihrem Netzwerk nutzt Ihre vorhandene Netzwerkhardware, um die Kommunikation zu unterstützen. Es ist nicht erforderlich, Hardware zu installieren. Da jeder Kunde über eine einzigartige Konfiguration verfügt, verfügt die Instanz über eine flexible VPN-Lösung. Die Instanz verfügt über erstellte Tunnel zu Prüfpunkt, Juniper, Stortel und anderen IPSEC-VPN-fähigen Geräten.

Die VPN-Verbindungen zwischen der -Instanz und Ihrem Netzwerk werden erstellt, um den verschlüsselten Datenverkehr in Ihr Netzwerk zu unterstützen. Integrationen, die VPN

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

verwenden, haben häufig keine Verschlüsselung als Teil des zugrunde liegenden Protokolls. Beispiel: LDAP über VPN im Vergleich zu LDAPS über das Internet und HTTP über VPN im Vergleich zu HTTPS über das Internet.

Das Netzwerk lässt nicht zu, dass eingehender Datenverkehr zur ServiceNow-Integration oder Endanwender-zu-ServiceNow-Datenverkehr eine VPN-Verbindung durchläuft. Diese eingeschränkte Kommunikation umfasst den Zugriff von Endanwendern auf die Plattform, die Verwaltung der Plattform, Webserviceintegrationen und andere Integrationen, die für die Verwendung eines MID-Servers konfiguriert sind. Die gesamte eingehende Kommunikation für die Instanz muss über das Internet mit HTTPS erfolgen. Diese Konfiguration bietet einen verschlüsselten Kommunikationskanal. Der Verschlüsselungskanal erfüllt zusammen mit der IP-Zugriffssteuerung die Sicherheitsanforderungen für diesen Datenverkehrs-Flow.

Adressen für die VPN-Kommunikation

Um Konflikte oder Überschneidungen mit internen ServiceNow -Netzwerken oder anderen internen IP-Adressschemata in Ihrem Netzwerk zu vermeiden, muss der gesamte Datenverkehr im Tunneling-Verfahren in der Verschlüsselungsdomäne auf beiden Seiten des Tunnels Nicht-RFC-1918-Adressen verwenden.

ServiceNow stellt eine einzelne IP-Adresse für die Quelle von Abfragen in Ihrem Netzwerk bereit. Sie müssen für jeden Host, der in Ihre -Instanz integriert wird, NAT-Nicht-RFC-1918-Adressen (Network Address Translation) angeben. Diese öffentlichen Adressen müssen im Besitz Ihrer Organisation sein. Adressen von Drittparteien können nicht innerhalb von Tunnels verwendet werden. Darüber hinaus darf die Verschlüsselungsdomäne nicht die IP-Adresse des VPN-Peers enthalten.

Redundante Tunnel

Es gibt zwei Möglichkeiten, Redundanz für Ihre Tunnel zu erstellen:

- Sie verwenden dieselbe Verschlüsselungsdomäne hinter beiden Ihrer Peers. Dies ist die bevorzugte Methode.
- Verwendung einer anderen Verschlüsselungsdomäne hinter jedem Peer

Bei der ersten Methode müssen Sie hinter jedem Ihrer Peers dieselbe NAT-Adresse angeben, um mit dieser Adresse einen Verbindungspfad zu Ihrem Server zu erstellen. Der Pfad zu Ihrem Server kann derselbe physische Computer oder ein Spiegel sein, der identische Services bereitstellt. Mit dieser Methode würde Ihre Instanz dieselbe IP-Adresse verwenden, um eine Verbindung zu Ihren Servern herzustellen, unabhängig davon, ob Ihr primärer oder sekundärer Tunnel aktiv ist. Wenn Sie mehr als einen Server haben, folgen Sie diesem Schema für weitere Server. Diese Methode bietet Ihren Anwendern die meiste Transparenz und wird empfohlen.

Die zweite Methode erfordert eine Konfiguration in Ihrer Instanz, um die Redundanz bereitzustellen. Wenn der Tunnel beispielsweise für LDAP verwendet wird, können Sie redundante LDAP-Server in Ihrer Instanz bereitstellen. Beachten Sie, dass diese Methode erfordert, dass die Verbindung zum ersten konfigurierten LDAP-Server abläuft, bevor die Instanz versucht, eine Verbindung zum sekundären Server herzustellen. Aufgrund dieser zusätzlichen Zeitverzögerung sollte diese Lösung nur implementiert werden, wenn die erste Option nicht erreichbar ist. Beachten Sie auch, dass in Ihrer Instanz nicht alle Services für redundant konfiguriert werden können. Wenn Sie einen VPN-Tunnel für etwas anderes als LDAP verwenden und Redundanz erforderlich ist, überprüfen Sie, ob Ihre Konfiguration mehrere Adressen unterstützen kann, oder sehen Sie sich die erste Option oben an.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Alternativen zur Verwendung eines VPN

Diese Alternativen stellen eine einfachere Möglichkeit dar, Ihre -Instanz mit den Ressourcen in den ServiceNow -Rechenzentren zu verbinden und bieten eine bessere Verschlüsselung. Darüber hinaus können Sie Probleme vermeiden, die durch VPN-Ausfallzeiten verursacht werden, z. B. wenn Ihre Instanz für Benutzer nicht verfügbar ist, wenn ein Problem mit dem VPN-Tunnel auftritt.

Single Sign-on und MID Server

Erwägen Sie die Verwendung einer Kombination aus Single Sign-on (SSO) für die Authentifizierung und dem MID-Server für die Synchronisierung von Anwenderdaten, anstatt ein VPN für die Verbindung Ihres LDAP-Servers mit Ihrer Instanz zu verwenden. Erwägen Sie für andere Integrationen als LDAP die Verwendung von zertifikatbasierter Verschlüsselung.

Sie können den LDAP-Listener auf einem MID-Server verwenden, um Ihre Benutzertabelle nahezu in Echtzeit zu synchronisieren.

Der Vorteil dieses Ansatzes besteht darin, dass keine Firewall-Lücken, Routen, VPN-Tunnel oder andere spezielle Netzwerkeinstellungen konfiguriert und verwaltet werden müssen. Die SSO/MID-Server-Lösung ist die flexibelste, sicherste und kosteneffektivste Methode zur vollständigen LDAP-Integration.

LDAP über SSL

Eine weitere Alternative zur Verwendung eines VPN-Tunnels ist die Konfiguration von LDAP Over SSL (LDAPS) direkt über das Internet. Sie können einen schreibgeschützten Domänencontroller konfigurieren und die Instanz in Ihrer DMZ sperren, indem Sie nur die Quelladressen der Instanz und die Zielports Ihrer Wahl verwenden. Da die Ports für LDAP in Ihrer Instanz konfigurierbar sind, können Sie bei Bedarf eine Port Address Translation (PAT) durchführen. Mit LDAPS steuern Sie das Zertifikat, das über einen verschlüsselten Kanal in die Instanz hochgeladen wird (siehe Ein Zertifikat wird in eine Instanz hochgeladen). Die Pakete können ohne das Zertifikat nicht verschlüsselt oder entschlüsselt werden.

Der Vorteil dieses Ansatzes besteht darin, dass er einen stärkeren Verschlüsselungs- und Entschlüsselungsmechanismus bietet. Ein VPN kann den Datenverkehr zwischen den beiden Partnern im Internet nur mit einem koordinierten vorinstallierten Schlüssel verschlüsseln und entschlüsseln, ähnlich einem Passwort. LDAPS bietet einen längeren verschlüsselten Pfad (End-to-End) auf der Anwendungsebene und ein Zertifikat, das weitaus komplexer ist als ein vorinstallierter Schlüssel, den der IPSec-Tunnel verwendet.

VPN-Setup

Vom Zeitpunkt der Übermittlung einer VPN-Anforderung an dauert es normalerweise maximal eine Woche, bis der VPN-Build abgeschlossen ist. Zur Unterstützung der Redundanzanforderungen Ihrer Instanz und Ihrer Organisation werden mindestens zwei und maximal vier VPNs bereitgestellt (von der aktiven Site zu Ihrer aktiven Site oder der aktiven Site zu Ihrer DR-Site usw.).

Es empfiehlt sich, die Verschlüsselungsdomäne so spezifisch wie möglich anzugeben. Idealerweise enthält die Verschlüsselungsdomäne nur die spezifischen Hosts, die für die Integrationen erforderlich sind. Eine große Verschlüsselungsdomäne kann Möglichkeiten für Diskrepanzen beim Routing bieten (VPN oder Internet).

Um das VPN zu erstellen, geht die Instanz wie folgt vor:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Stellt die VPN-Peer- und Hostadressen aus jedem Rechenzentrum bereit.
2. Baut die erforderliche VPN-Konnektivität aus zwei Rechenzentren in Ihr Netzwerk auf. Zur Unterstützung der Anforderungen in Bezug auf Redundanz und Notfallwiederherstellung (DR) können die VPNs von zwei Rechenzentren aus in zwei Netzwerken bereitgestellt werden.

Die Instanz unterstützt nicht den Aufbau mehrerer VPN-Tunnel in einem Kundennetzwerk, um Verbindungen mit mehreren geografischen Regionen oder Tochterunternehmen herzustellen. Sie sollten Inter-Site-Routing, Datenverkehrsverteilung oder Traffic Shaping innerhalb Ihres eigenen internen Netzwerks durchführen, anstatt mehrere VPN-Tunnel zu verwenden.

Aktivieren eines VPN-Service

Verwenden Sie für alle VPN-Anforderungen, einschließlich Bereitstellungen, Änderungen oder allgemeine Fragen, das Formular „Servicekatalog-VPN-Anforderung“.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Navigieren Sie zu https://support.servicenow.com/now?draw=case.
2. Wählen Sie die Registerkarte **Automatisierungsspeicher**.
3. Verwenden Sie die Struktur auf der linken Seite, um zu zu navigieren **Alle Automatisierungen** > **Servicekatalog** > **Cloud-Infrastruktur**an.
4. Wählen Sie **VPN-Anforderungen aus**
5. Wählen Sie den entsprechenden VPN-Anforderungstyp aus.
6. Beantworten Sie die Fragen.
   Die Fragen variieren je nach ausgewähltem Anforderungstyp.
7. Klicken Sie auf **Absenden**.

Ergebnisse
Sobald Ihre Anforderung übermittelt wurde, arbeitet ServiceNow mit Ihren Netzwerktechnikern zusammen, um zu testen und zu validieren, ob das VPN Datenverkehr erfolgreich weiterleitet. Um sicherzustellen, dass Ihre Fragen rechtzeitig beantwortet werden, gehen Sie in diesem Prozess auf VPN-bezogene Fragen ein.

Konfigurieren einer Adresse für die VPN-Kommunikation

Um Konflikte oder Überschneidungen mit internen ServiceNow -Netzwerken oder den internen IP-Adressschemata eines anderen Kunden zu vermeiden, erfordert die Instanz, dass der gesamte Datenverkehr im Tunneling in der Verschlüsselungsdomäne auf beiden Seiten des Tunnels Nicht-RFC-1918-Adressen verwendet.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Die Instanz stellt eine einzelne IP-Adresse für die Quelle von Abfragen in Ihrem Netzwerk bereit.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

Geben Sie für jeden Host, der in die Instanz integriert wird, NAT-Nicht-RFC-1918-Adressen (Network Address Translation) an.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Plattform-Datenschutz

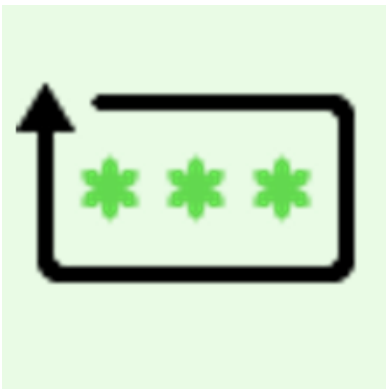
Mit Privacy können Sie vertrauliche Daten in der Instanz maskieren.

Datenschutz



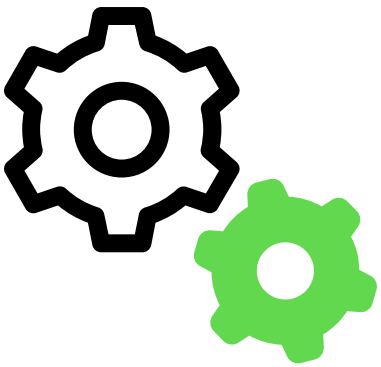
Mit Data Privacy können Sie vertrauliche Daten klassifizieren und anschließend personenbezogene Daten (PII) aus Benutzerdaten in einer Produktionsinstanz entfernen und Daten in Nicht-Produktionsinstanzen anonymisieren.

Daten-Discovery



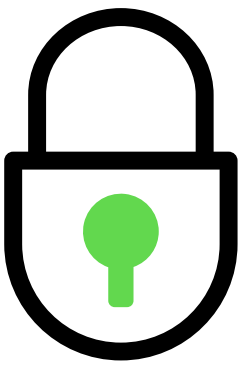
Identifizieren Sie mithilfe der Datenerkennung vertrauliche Daten innerhalb einer Instanz, um sie zu klassifizieren, zu schützen oder Berichte über sie zu erstellen.

Datenklassifizierung



Gruppieren Sie Daten mithilfe vordefinierter oder benutzerdefinierter Datenklassifizierungen nach Typ. Wenn Ihnen die Rolle „Datenklassifizierungsadministrator“ oder „Auditor“ zugewiesen wurde, können Sie verschiedene Datenklassen verwalten oder den aktuellen Status verschiedener Datentypen innerhalb der Instanz visuell analysieren.

Datenanonymisierung



Die Datenanonymisierung bietet eine Möglichkeit,

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Daten einfach umzuwandeln, sodass sie nicht identifizierbar sind und den Datenschutzbestimmungen besser entsprechen.		

Datenschutz

Mit Data Privacy können Sie vertrauliche Daten klassifizieren und anschließend personenbezogene Daten (PII) aus Benutzerdaten in einer Produktionsinstanz entfernen und Daten in Nicht-Produktionsinstanzen anonymisieren. Nachdem sie anonymisiert wurden, gelten sie nicht mehr als persönliche Daten, die Vorschriften unterliegen.

Datenschutz erkunden	Konfigurieren Sie den Datenschutz
	
Erfahren Sie mehr über Datenschutz.	Erfahren Sie, wie Sie Datenschutz konfigurieren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollen im Datenschutz



Rufen Sie Details zu Rollen im Datenschutz ab.

Erweiterte Datenschutzfunktionen



Erfahren Sie mehr über die erweiterten Funktionen von Datenschutz.

Datenschutz erkunden

Mit Data Privacy können Sie vertrauliche Daten klassifizieren und anschließend personenbezogene Daten (PII) aus Benutzerdaten in einer Produktionsinstanz entfernen und Daten in Nicht-Produktionsinstanzen anonymisieren. Nachdem sie anonymisiert wurden, gelten sie nicht mehr als persönliche Daten, die Vorschriften unterliegen.

Erklärt, wie wichtig der Datenschutz ist und welche Schritte Unternehmen unternehmen können, um vertrauliche Informationen durch Klassifizierung und Anonymisierung zu schützen. Anhand der Store-Anwendung „Datenschutz“ geben wir einen Überblick über das wichtigste Dashboard und die wichtigsten Funktionen.

Entwickler müssen mit Daten in Instanzen außerhalb der Produktion arbeiten, um sicherzustellen, dass ihre Implementierungen wie erwartet funktionieren. Das Importieren von Daten aus Ihrer Produktionsinstanz ist zwar eine nützliche Methode, um die Produktion zu simulieren, birgt jedoch auch ein Sicherheitsrisiko. Administratoren können Datenschutz verwenden, um Entwicklern Daten bereitzustellen, die keine privaten Informationen enthalten, damit sie in einer Nicht-Produktionsumgebung sicher arbeiten können.

Datenklassifizierung

Identifizieren und klassifizieren Sie Ihre vertraulichen Daten gemäß vordefinierten Kriterien, die durch den Vertraulichkeitsgrad der Datentypen in Ihrer Instanz bestimmt werden. Datenvertraulichkeitsstufen bestimmen, wie die einzelnen Arten von klassifizierten Daten behandelt werden sollen. Es gibt mehrere vordefinierte Klassen, die mit Datenschutz auf Basisebene bereitgestellt werden. Verwenden Sie den Klassifizierungsabschnitt des Datenschutzes, um Daten in Ihrer Instanz zu kennzeichnen und zu gruppieren. Klassen

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

hinzufügen, Datenklassenstruktur anzeigen und Daten klassifizieren. Gruppieren Sie Daten mithilfe vordefinierter oder benutzerdefinierter Datenklassifizierungen nach Typ.

Erklärt, wie Daten mithilfe der Store-Anwendung „Datenschutz“ klassifiziert werden.

Anonymisierung von Anwenderdaten

Als Administrator legen Sie fest, ob alle Informationen für alle Benutzer oder für eine Teilmenge von Benutzern anonymisiert werden sollen. Bei der Anonymisierung werden Daten für die ausgewählten Benutzerdatensätze durch randomisierte Werte oder von Ihnen definierte Werte ersetzt. Beim Ersetzen von Werten kann die Datenstruktur mit verschiedenen Techniken beibehalten werden.

Erklärt, wie Daten mit der Store-Anwendung „Datenschutz“ anonymisiert werden.

Datenschutzoptionen

- Datenschutz (klassisch): Verwenden Sie zuerst die Datenklassifizierungs-App, um Ihre Daten anhand vordefinierter oder anwenderdefinierter Datenklassifizierungen nach Typ zu gruppieren. Erstellen Sie dann Datenschutztechniken und -aufträge, um PII zu anonymisieren.
- Datenschutz (Store-App): Klassifizieren und anonymisieren Sie Ihre Daten innerhalb der Datenschutz-App.

Überlegungen

- Nur klassifizierte Daten können anonymisiert werden. Informationen zu Datenklassen und Klassifizierung finden Sie unter Datenklassifizierung (klassisch) oder Datenklassifizierung Store App.
- Personenbezogene Daten in Protokollen und andere Auditing-Daten werden nicht anonymisiert.
- Nur strukturierte Daten können anonymisiert werden. Unstrukturierte Daten wie Journalfelder, Kommentare, Anhänge und andere Felder, in denen Teiltext PII darstellen kann, werden nicht anonymisiert. Weitere Informationen finden Sie unter Unterstützte Feldtypen für die Anonymisierung.
- Durch Integrationen mit SSO-Systemen (Single Sign-on) können Benutzerinformationen aus ihren Quellsystemen neu synchronisiert werden. Es gibt keinen Mechanismus, um die Dauerhaftigkeit der Deidentifizierung von sys_user-Daten sicherzustellen. Informationen zur Benutzerverwaltung und zu sys_users finden Sie unter Benutzeradministration .

Domain Separation und Datenschutz

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

Support-Stufe: Kein Support

- Das Feld „Domäne“ kann in Datentabellen vorhanden sein, es ist jedoch keine Geschäftslogik zum Verwalten der Daten vorhanden.
- Diese Ebene wird nicht als domänengetrennt betrachtet.

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

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Domänentrennung für Service Provider

Unterstützte Feldtypen für die Anonymisierung

Überprüfen Sie, welche Feldtypen beim Anonymisieren von Daten unterstützt werden.

Hinweis: Nicht alle klassifizierten Feldtypen sind für die Anonymisierung verfügbar.

Einige Feldtypen mit hohem Risiko sind standardmäßig deaktiviert, wie in der Tabelle beschrieben. Weitere Informationen zu Feldern finden Sie unter Feldtypen .

Unterstützte Feldtypen für die Anonymisierung

Feldtyp	Standardmäßig verfügbar
Audio	Nein
Bedingung	Nein
Bedingung_Zeichenfolge	Nein
currency	Ja
Dezimalzahl	Ja
due_date	Ja
Float	Ja
glide_date	Ja
glide_date_time	Ja
glide_duration	Nein
glide_time	Ja
html	Nein
icon	Nein
integer	Ja
ip_adr	Nein
ip_address	Nein
Journal	Ja
„journal_input“	Ja
„journal_list“	Ja
Langer Integer	Ja
name_values	Nein
percent_complete	Nein
phone_number_e164	Ja
Preis	Ja
Zeichenfolge	Ja
Zeichenfolge_vollständig_utf8	Ja

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feldtyp	Standardmäßig verfügbar
Übersetzt_html	Nein
translate_text	Nein
URL	Nein
user_image	Nein
Video	Nein
wiki_text	Nein

Datenschutzrollen

Der Datenschutz fügt diese Rollen hinzu.

Datenschutzadministrator

Die Datenschutzadministratorrolle ist eine Administratorrolle, die zum Erstellen von Datenschutztechniken und -richtlinien verwendet wird.

Datenschutzadministrator [data_privacy_admin]

Enthält Rollen

Keine

Gruppen zugewiesen

Keine

Abonnement

Nein

Erweitert

Ja

Überlegungen

Vermeiden Sie es, Ihren Anwendern diese Rolle zuzuweisen, wenn gezieltere Rollen verfügbar sind.

Um die Rolle „Datenschutzadministrator“ zuzuweisen, heben Sie den Anwender auf die Rolle des Sicherheitsadministrators zu, um die Rolle hinzuzufügen.

Datenschutz-Auditor

Der Datenschutz-Prüfer ist eine schreibgeschützte Rolle, die zum Anzeigen von Datenschutz-Datensätzen verwendet wird.

Datenschutz-Prüfer [data_privacy_auditor]

Enthält Rollen

Keine

Gruppen zugewiesen

Keine

Abonnement

Nein

Erweitert

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nein

Überlegungen

Keine

Datenschutz-Klonprozessor

Benutzer mit der Rolle „Datenschutz-Klonprozessor“ können Datenschutzaufträge für Datenklassen erstellen und ausführen.

Datenschutz-Klonprozessor [data_privacy_clone_processor]

Enthält Rollen

Keine

Gruppen zugewiesen

Keine

Abonnement

Nein

Erweitert

Ja

Überlegungen

Keine

Datenschutzbeauftragter

Benutzer mit der Rolle „Datenschutzprozessor“ erstellen Datenschutzaufträge in der Benutzertabelle [sys_user] und führen sie aus.

Datenschutzbeauftragter [data_privacy_processor]

Enthält Rollen

Keine

Gruppen zugewiesen

Keine

Abonnement

Nein

Erweitert

Ja

Überlegungen

Keine

Datenschutz (klassisch)

Datenschutz (klassisch) ist als Familienrelease verfügbar. Die letzten Familien-Updates wurden in Tokyo veröffentlicht.

Datenschutz aktivieren (klassisch)

Sie können das Datenschutz-Plugin (com.glide.data_privacy) für Platform Security aktivieren, wenn Sie die Administratorrolle innehaben. Die Anwendung enthält Demodaten und

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

installiert zugehörige ServiceNow® Store -Anwendungen und Plugins, falls sie nicht bereits installiert sind.

Vorbereitungen
Datenschutz erfordert ein vom Rest der Now Platformgetrenntes Abonnement.

Wenden Sie sich an Ihren ServiceNow-Kundenbetreuer, um ein Abonnement zu erwerben. Wenn Sie ein Abonnement erwerben, werden bestimmte Plugins automatisch aktiviert. Wenn ein kostenpflichtiges Plugin nicht automatisch aktiviert wird, können Sie es manuell in der Liste „Alle Anwendungen“ in Ihrer Instanz aktivieren.

Hinweis: Bevor Sie ein Abonnement kaufen, können Sie Datenschutz (klassisch) und Daten-Discovery mit einer 30-tägigen Testphase testen. Nach Ablauf Ihrer Testversion können Sie in ohne Lizenz keine Daten erkennen oder Anonymisierungsaufgaben mehr ausführen.

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Die folgenden Elemente werden mit Datenschutz installiert:

- Plugins
- Rollen
- Tabellen

Weitere Informationen finden Sie unter Installiert mit Datenschutz (klassisch).

Prozedur

1. Navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie das Plugin „Datenschutz“ (com.glide.data_privacy) mithilfe der Filterkriterien und der Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: `Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.`

   Nach Abschluss der Installation wird eine Meldung angezeigt.

Installiert mit Datenschutz (klassisch)

Erfahren Sie mehr über die mit dem Datenschutz-Plugin (com.glide.data_privacy) installierten Komponenten.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installierte Tabellen

Tabelle	Beschreibung
Datenschutz-Verbundauftrag [dp_federated_job]	Föderierte Aufträge für Datenschutz
Datenschutzauftrag [dp_job]	Datenschutzaufträge
Datenschutzauftrag [dp_job_summary]	Zusammenfassungen der Datenschutzaufträge
Datenschutztechnik [dp_technique]	Datenschutztechniken
Primärer Referenzlink [dp_primary_reference]	Primäre Referenzlinks
Technik für klassifiziertes Datenschutzfeld [dp_field_technique]	Techniken für klassifiziertes Datenschutzfeld
Datenschutzkonfiguration [dp_configuration]	Datenschutzkonfigurationen
Konfiguration der Datenschutztechnik [dp_technique_with_params]	Datenschutztechniken
Parameter für Datenschutztechnik [dp_technique_with_parameter]	Datenschutztechniken mit Parametern
Parameterwert für Datenschutztechnik [dp_technique_with_parameter_value]	Parameterwerte, die in Datenschutztechniken mit Parametern verwendet werden.

Datenschutzkonfiguration (klassisch).

Erfahren Sie, wie Sie Datenschutztechniken und -richtlinien erstellen und Datenschutzaufträge erstellen und ausführen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenschutztechniken

Datenschutztechniken sind Optionen, mit denen Sie bestimmen, wie Ihre Daten anonymisiert werden. Sie müssen eine Datenschutztechnik erstellen, auf die im Datenschutzauftrag verwiesen wird. Informationen zum Zuordnen einer Datenschutztechnik zu einer zugehörigen **Konfiguration**für die Datenschutztechnik finden Sie unter Erstellen Sie eine Konfiguration für eine Datenschutztechnik.

Datenschutzrichtlinien

Konfigurieren Sie eine Datenschutzrichtlinie, um anzugeben, welche Datenschutztechniken bei der Anonymisierung Ihrer Daten verwendet werden. Details siehe Erstellen Sie eine Datenschutzrichtlinie.

Datenschutzaufträge

Datenschutzaufträge verwenden alle diese Komponenten, um Ihre Daten zu anonymisieren. Weitere Informationen zu diesen Aufträgen finden Sie unter Konfigurieren Sie eine Datenschutzaufgabe.

Erstellen Sie eine Konfiguration für eine Datenschutztechnik

Erstellen Sie eine Konfiguration für die Datenschutztechnik, um anzupassen, wie der Datenschutz Ihre Daten anonymisiert.

Vorbereitungen

Erforderliche Rolle: data_privacy_admin und admin

Prozedur

1. Führen Sie eine Hochstufung auf die Rolle **„data_privacy_admin“ durch**.
   Weitere Informationen zur Erhöhung von Rollen finden Sie unter Auf eine privilegierte Rolle hochstufen.
2. Navigieren zu **Systemsicherheit** > **Datenschutz** > **Konfiguration der Datenschutztechnik**an.
3. Klicken Sie auf **Neu**.
4. Geben Sie im Feld **Name** einen Namen für die Konfiguration Ihrer Datenschutztechnik ein.
5. **Wählen** Sie im Feld Datenschutztechnik eine Datenschutztechnik aus.

Datenschutztechniken

Technik	Beschreibung
Keine Aktion	Diese Technik ist ein Platzhalter. Bei Auswahl werden keine Felder geändert.
Zufällig ersetzen	Diese Technik tauscht Werte mit zufällig generierten Werten aus. Zeichenfolgen- und Zahlendaten können diese Technik verwenden.
Selektives Ersetzen	Diese Technik führt ein selektives Ersetzen von Zeichenfolgendaten durch. Alle Zeichen zwischen den Start- und Endindizes der Eingabe werden durch das von Ihnen gewählte Zeichen ersetzt. Sie können Zeichen angeben, die von der Maskierung ausgeschlossen werden sollen:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Technik	Beschreibung
	◦ start_index: Die Technik maskiert Daten ab dem angegebenen Zeichen. Wenn dieses Feld leer gelassen wird, beginnt die Maskierung mit dem ersten Zeichen. ◦ end_index: Die Technik maskiert Daten vom Beginn der Zeichenfolge bis zum angegebenen Zeichen. Wenn dieses Feld leer gelassen wird, endet die Maskierung mit dem letzten Zeichen. ◦ exclude_char: Definieren Sie ein Zeichen, das von der Maskierung ausgeschlossen werden soll. ◦ Ersatz_Zeichen: Definieren Sie ein Zeichen, das für die Maskierung verwendet wird. Wenn keiner angegeben ist, werden standardmäßig Sternchen (*) verwendet.
Statisches Ersetzen	Diese Technik tauscht Werte mit statischen Werten aus. Zeichenfolgen-, Zahlen- und Datumsdaten können diese Technik verwenden: ◦ date_time_value: Ersetzen Sie Datumswerte durch dieses Datum. Verwenden Sie das Format jjjj-MM-tt HH:mm:ss. ◦ date_value: Ersetzen Sie Datumswerte durch dieses Datum. Verwenden Sie das Format jjjj-MM-tt. ◦ number_value: Ersetzen Sie Zahlenwerte durch diese Zahl. ◦ Zeichenfolgenwert: Ersetzen Sie Zeichenfolgenwerte durch diesen Text.
Entfernen	Diese Technik entfernt Werte und ersetzt sie durch leere Werte (null).

Hinweis: Der zuvor unterstützte Wert „ **Ersetzen** “ ist veraltet und wurde in „ **Ersetzen-veraltet** “ umbenannt. Er darf nicht verwendet werden.

6. Klicken Sie mit der rechten Maustaste auf den Header, und klicken Sie im Kontextmenü auf **Speichern**.
   Nachdem der Datensatz gespeichert wurde, wird die Liste der **parametrisierten Datenschutzwerte** angezeigt.
7. Verwenden Sie die Datensätze in der Liste der **parametrisierten** Datenschutzwerte, um die Konfiguration Ihrer Datenschutztechnik anzupassen.
   Die verfügbaren parametrisierten Werte hängen davon ab, welche Datenschutztechnik Sie ausgewählt haben. Es gibt keine parametrisierten Werte für die Techniken **„Keine Aktion“** und „ **Entfernen** “.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parametrisierte Datenschutzwerte für selektives Ersetzen

Parameterwert für Datenschutztechnik	Beschreibung	Standardwert
char_to_replace	Zeichen, das beim Ersetzen von Werten durch eine selektive Ersetzung verwendet werden soll.	*
end_index	Die Technik maskiert Daten vom Beginn der Zeichenfolge bis zum angegebenen Zeichen. Wenn es leer gelassen wird, endet die Maskierung mit dem letzten Zeichen.	(leer)
„exclude_char“	Zeichen zum Überspringen der Maskierung. In diesem Wert kann nur ein einzelnes Zeichen verwendet werden. Wenn mehrere eingegeben werden, wird das erste Zeichen verwendet.	(leer)
start_index	Die Technik maskiert Daten ab dem angegebenen Zeichen.	1

Parametrisierte Datenschutzwerte für Ersetzen

Parameterwert für Datenschutztechnik	Beschreibung	Standardwert
date_time_value	Ersetzen Sie Datums- und Uhrzeitwerte durch dieses Datum. Verwenden Sie das Format jjjj-MM-tt HH:mm:ss.	1988-11-11 10:10:10
date_value	Ersetzen Sie Datumswerte durch dieses Datum. Verwenden Sie das Format jjjj-MM-tt.	1988-11-11
number_value	Ersetzen Sie Zahlenwerte durch diese Zahl.	1234567
Konservieren_Daten_Länge	Legen Sie den Wert auf „ **wahr** “ fest, um die Datenlänge beizubehalten. Deidentifizierte Daten haben dieselbe Länge wie die ursprünglichen Daten.	wahr
string_value	Ersetzen Sie Zeichenfolgenwerte durch diesen Text.	TEXT123

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameterwert für Datenschutztechnik	Beschreibung	Standardwert
use_random_generate_value	Legen Sie den Wert auf „ **wahr“** fest, um Daten durch zufällig generierte Werte zu ersetzen. Nur Zeichenfolgen- und Zahlendaten können durch zufällige Werte ersetzt werden. Diese Option überschreibt statische Werte.	falsch

8. Klicken Sie auf **Speichern**.

Erstellen Sie eine Datenschutzrichtlinie

Konfigurieren Sie eine Datenschutzrichtlinie, um anzugeben, welche Datenschutztechniken bei der Anonymisierung Ihrer Daten verwendet werden.

Vorbereitungen

Die Datenschutzkonfiguration definiert Tabellen, „sys_user“ und andere, sowie Spalten für die deidentifizierten, je nach Anwendungsfall, und gibt parametrisierte Typen der Techniken an, die bei der Deidentifizierung von Daten verwendet werden sollen.

Hinweis: Um eine Datenschutzkonfiguration abzuschließen, müssen Sie zuerst eine Konfiguration für eine Datenschutztechnik konfigurieren. Weitere Informationen finden Sie unter Erstellen Sie eine Konfiguration für eine Datenschutztechnik.

Erforderliche Rolle: data_privacy_admin und admin

Prozedur

1. Führen Sie eine Hochstufung auf die Rolle **„data_privacy_admin“ durch**.
   Weitere Informationen zur Erhöhung von Rollen finden Sie unter Auf eine privilegierte Rolle hochstufen.
2. Navigieren zu **Systemsicherheit** > **Datenschutz (klassisch)** > **Konfiguration der Datenschutzrichtlinie**an.
3. Wählen Sie **Neu**.
4. Geben Sie im Feld **Name** einen Namen für Ihre Datenschutzrichtlinienkonfiguration ein.
5. **Wählen** Sie im Feld Datenklasse die Datenklasse aus, die mit dieser Richtlinie verwendet werden soll.
   Datenschutzrichtlinien können nur für klassifizierte Daten gelten. Weitere Informationen zur Datenklassifizierung finden Sie unter Datenklassifizierung.
   Nach der Auswahl einer Datenklasse werden die Listen **KlassifizierteDatenschutzfeldtechniken und Primäre Referenzlinks** zum Datenschutz im Formular angezeigt.
6. Wahlweise: Wählen **Sie Auf alle Daten in Klasse** anwenden, um die Anonymisierung auf alle Daten in der ausgewählten Datenklasse anzuwenden.
   Wenn Sie dieses Feld nicht auswählen, können die Anwender Ihres Datenschutzprozessors auswählen, welche Anwender beim Erstellen von Datenschutzaufträgen anonymisiert werden sollen. Wenn Sie dieses Feld auswählen, ist diese Option nicht verfügbar.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Beim Klonen anwenden**: Diese Option wird verfügbar. Wenn diese Option ausgewählt ist, wird die Datenschutzkonfiguration während des Datenschutzklons ausgeführt.
- **Anwendungsreihenfolge**: Ein Datenschutzauftrag für die Postclone-Konfiguration mit einer höheren Anwendungsreihenfolge wird möglicherweise vor einem anderen Auftrag mit einer niedrigeren Reihenfolge gestartet.

> **Wichtig:** Vermeiden Sie das Erstellen mehrerer Datenschutzrichtlinien mit derselben Anwendungsreihenfolge, da die resultierende Verarbeitungsreihenfolge für diejenigen mit derselben Reihenfolge inkonsistent sein wird.

7. Wahlweise: Wählen Sie **Unterstützt Rollback** aus, um die Möglichkeit zur Deanonymisierung der Daten aus einem Datenschutzauftrag zu aktivieren.
   Weitere Informationen finden Sie unter Setzt einen Datenschutzauftrag zurück.
   Nachdem Sie **Unterstützt Rollback** beim Erstellen eines Datenschutzauftrags ausgewählt haben, wird die Option zum Rollback des Auftrags verfügbar.
8. Wählen Sie die Registerkarte **Techniken** für klassifiziertes Datenschutzfeld aus, um die Liste „Techniken für **klassifiziertes Datenschutzfeld** " anzuzeigen.
9. Wählen Sie einen Eintrag im Feld „ **Tabelle** " aus, um das Feld „ **Konfiguration der Datenschutztechnik** " für jeden Listeneintrag zu öffnen.
   In der Liste „ **Techniken für klassifiziertes Datenschutzfeld** " werden alle Daten angezeigt, die in der ausgewählten Datenklasse anonymisiert werden sollen. Für jeden dieser Einträge müssen Sie eine Datenschutztechnik auswählen, die angewendet werden soll.
10. Wählen Sie eine anzuwendende **Konfiguration für eine Datenschutztechnik** aus.

> **Wichtig:** Wenn Sie einen Eintrag nicht anonymisieren, wählen Sie die **DoNoThing-**Technik, anstatt den Eintrag leer zu lassen. Richtlinien mit leeren Werten im Feld **„Konfiguration der Datenschutztechnik"** können nicht ausgeführt werden, wenn sie in Datenschutzaufträgen verwendet werden.

11. Wählen Sie **Absenden** oder **Speichern**, um den Datensatz zu speichern.

Nächste Maßnahme
Konfigurieren Sie eine Datenschutzaufgabe.

Konfigurieren Sie eine Datenschutzaufgabe

Konfigurieren Sie einen Datenschutzauftrag in Ihrer Produktionsinstanz, um anonymisierte Daten in Ihrer Instanz außerhalb der Produktion für Anwender- und Datenklassenaufträge zu verwenden.

Vorbereitungen
Der Datenschutzauftrag unterstützt zwei Anwendungsfälle für die Deidentifizierung:

- Sensible Daten bestimmter sys_users
- Sensible Daten einer bestimmten Datenklasse.

Erforderliche Rolle: data_privacy_processor und admin

Prozedur

1. Führen Sie eine Hochstufung auf die Rolle **„data_privacy_processor" durch**.
   Weitere Informationen zur Erhöhung von Rollen finden Sie unter Auf eine privilegierte Rolle hochstufen.
2. Navigieren zu **Systemsicherheit** > **Datenschutz** > **Datenschutzauftrag**an.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie in der Liste der Datenschutzaufträge auf **Neu**.
4. Füllen Sie die Felder des Formulars aus.

Datenschutz-Auftragsfelder

Feld	Beschreibung
Name	Name des Jobs
Beschreibung	Beschreibung des Auftrags.
Datenschutzkonfiguration	Die für diesen Auftrag zu verwendende Datenschutzrichtlinienkonfiguration. Ausführliche Informationen zur Konfiguration von Datenschutzrichtlinien finden Sie unter Erstellen Sie eine Datenschutzrichtlinie.
Anwender	Wählen Sie die Anwender oder die Gruppe von Anwendern aus, die in diesem Auftrag anonymisiert werden sollen. Bis zu 1000 Anwender einer Gruppe können verarbeitet werden. **Hinweis:** Dieses Feld wird nur angezeigt, wenn die ausgewählte Datenschutzrichtlinienbedingung eine Auswahl von Anwenderdatensätzen erfordert.
Probelauf	Führen Sie die Aufgabe als Test aus. Von der Ausführung dieses Auftrags sind keine Datensätze betroffen. Im Feld **Zusammenfassung** werden Ergebnisse so angezeigt, als ob der Auftrag ausgeführt worden wäre. **Hinweis:** **Der Probelauf** muss deaktiviert werden, wenn ein Datenschutzauftrag mit Rollback konfiguriert wird. Details siehe Setzt einen Datenschutzauftrag zurück.
Status	Status des Datenschutzauftrags: ◦ **Bereit zum Planen**: Standardstatus für neue Aufträge. ◦ **Rollback in Bearbeitung**: Der Auftrag wurde auf ein Rollback der Anonymisierung festgelegt. ◦ **Rollback abgeschlossen**: Das Rollback des Anonymisierungsauftrags wurde erfolgreich abgeschlossen. Ein schreibgeschütztes Feld.
Geschätzte Anzahl der Datensätze	Die geschätzte Anzahl der Datensätze, auf die sich dieser Auftrag auswirkt Ein schreibgeschütztes Feld.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zusammenfassung	Ein schreibgeschütztes Feld, das die Ergebnisse des Auftrags anzeigt, wenn Sie ihn ausführen.
Zeitfensterstart	Beginn des Zeitfensters für die Ausführung dieses Auftrags. Die Aufgabe wird nach der in diesem Feld eingegebenen Zeit ausgeführt. Ein gültiger Zeitwert ist die koordinierte Weltzeit (Coordinated Universal Time, koordinierte Weltzeit), basierend auf einer 24-Stunden-Zeitnotation.
Zeitfensterende	Das Ende des Zeitfensters für die Ausführung dieses Auftrags. Die Aufgabe wird vor der in diesem Feld eingegebenen Zeit ausgeführt. Wenn der Auftrag noch nicht abgeschlossen wurde, wird er angehalten und beim Start des nächsten Zeitfensters fortgesetzt. Die Endzeit muss nach der Startzeit liegen. Ein gültiger Zeitwert ist die koordinierte Weltzeit (Coordinated Universal Time, koordinierte Weltzeit), basierend auf einer 24-Stunden-Zeitnotation.

5. Klicken Sie mit der rechten Maustaste in den Formularheader, und wählen Sie im Kontextmenü die Option **Speichern** aus.
   Nach dem Speichern des Datensatzes werden die Schaltflächen **Auftrag planen** und **Auftrag löschen angezeigt**.
6. **Klicken** Sie auf „Aufgabe planen“, um Ihre Aufgabe auszuführen.
   Die Aufgabe wird zwischen den Zeiten ausgeführt, die in den Feldern **Start des Zeitfensters** und **Ende** des Zeitfensters ausgewählt sind. Wenn der Auftrag während des Start- und Endzeitfensters nicht abgeschlossen wurde, wird der Auftrag beim Start des nächsten Zeitfensters fortgesetzt.

   Hinweis: Ein Auftrag kann nur einmal ausgeführt werden, auch wenn **Probelauf** ausgewählt ist. Um denselben Auftrag erneut auszuführen, erstellen Sie einen Datenschutzauftrag mit denselben Feldwerten.

7. Wahlweise: Wählen Sie eine der folgenden Funktionen aus:
   - Auftrag**abbrechen**: Bricht den Datenschutzauftrag ab.
   - **Pause**: Hält die Auftrags- und Rollback-Aufzeichnung an, wenn Rollback ausgewählt wurde. Nach einem Ablaufzeitraum von drei Tagen für Rollback-Kontexte wird eine Warnmeldung angezeigt. Details siehe Setzt einen Datenschutzauftrag zurück.
   - **Fortsetzen**: Startet einen angehaltenen Auftrag neu. Rollback wird für fortgesetzte Aufgaben nicht unterstützt, wenn sie angehalten sind. Brechen Sie den Auftrag ab, und erstellen Sie einen Datenschutzauftrag. Die Aufzeichnung verwendet einen nicht abgelaufenen Rollback-Kontext.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollback des Datenschutzauftrags

Datenbankänderungen werden für Aktionen wie Aufträge und Skripts erfasst, sodass die Änderungen rückgängig gemacht werden können. Führen Sie einen Datenschutzauftrag zurück, wenn menschliches Versagen versehentlich falsche Benutzerinformationen anonymisiert. Durch das Rollback werden die Daten aus dem Datenschutzauftrag deanonymisiert.

Übersicht

- Rollback ist auf einige Tage beschränkt, entsprechend der konfigurierten Ablaufdauer des RollbackContext des neuen RollbackType *REDACT*. Nach Ablauf des RollbackContext, der einem Datenschutzauftrag zugeordnet ist, ist die Rollback-Funktion für diesen Auftrag nicht mehr verfügbar.
  - Ein Rollback-Kontext von der Deanonymisierung wird standardmäßig drei Tage lang gespeichert.
  - Die standardmäßige Ablaufzeit kann vom Datenschutzadministrator im **RollbackContext** des neuen **RollbackType** *REDACT.* auf einen Wert größer als eins festgelegt werden. Legen Sie den Wert in der Glide-Systemeigenschaft *glide.rollback.expiration_days_redact*fest. Weitere Informationen finden Sie unter Führen Sie ein Rollback durch, und löschen Sie die Wiederherstellung .

    Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

    , um zusätzliche Informationen zu erhalten.
- Ein Rollback ist für Datenschutzaufträge verfügbar, die sich im Status „Abgeschlossen“, „Abgebrochen“ oder „Fehler“ befinden.
- Für jeden erfolgreichen sys_user-Deanonymisierungsauftrag, der mit einer Datenschutzrichtlinie mit aktivierter Rollback-Unterstützung konfiguriert ist, wird ein Rollback-Kontext erstellt. Pro Datenschutzauftrag kann höchstens ein Rollback-Kontext vorhanden sein.

Setzt einen Datenschutzauftrag zurück

Setzen Sie einen Datenschutzauftrag in Ihrer Instanz außerhalb der Produktion, der anonymisierte Daten aus Ihrer Produktionsinstanz verwendet, auf einen Status vor der Deidentifizierung einer Datenklasse oder eines Anwenderauftrags zurück.

Vorbereitungen

Erforderliche Rolle: data_privacy_admin oder data_privacy_processor und admin

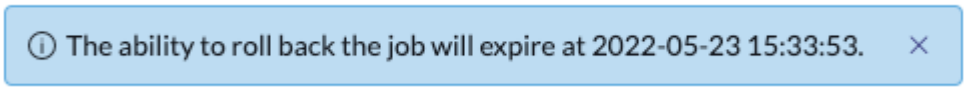
Prozedur

1. Führen Sie eine Hochstufung auf die Rolle „ **data_privacy_processor“** oder **„data_privacy_admin“ durch**.
   Weitere Informationen zur Erhöhung von Rollen finden Sie unter Auf eine privilegierte Rolle hochstufen.
2. Navigieren zu **Alle** > **Systemsicherheit** > **Datenschutz** > **Datenschutzauftrag**an.

   Hinweis: Im Voraus muss eine Datenschutzrichtlinienkonfiguration erstellt werden, die Rollback unterstützt. Erstellen Sie eine Datenschutzrichtlinie.
3. Erstellen Sie einen Datenschutzauftrag, und wählen Sie eine Datenschutzkonfiguration aus, die Rollback unterstützt.
   Weitere Informationen finden Sie unter Konfigurieren Sie eine Datenschutzaufgabe.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Planen Sie die Aufgabe für die Anonymisierung von Daten.
   - Nachdem der Auftrag ausgeführt wurde, werden die Daten für die ausgewählte Konfiguration anonymisiert.
   - Im Auftrag wird eine Nachricht angezeigt, die über die Ablaufzeit informiert. Innerhalb des Ablaufzeitraums können Sie den Auftrag rückgängig machen.



5. Führen Sie eine Hochstufung auf die Rolle **„data_privacy_processor“ durch**.
6. Öffnen Sie die Datenschutzaufgabe, für die ein Rollback durchgeführt werden soll.
7. Wählen Sie **Rollback** aus, um die Daten zu deanonymisieren.

Datenschutz-Klon

Beim Klonen von Kundendaten aus einer Quelle in eine Zielinstanz (in der Regel aus der Produktion in die Instanz außerhalb der Produktion) werden vertrauliche Daten in der Zielinstanz deidentifiziert.

Ein Datenschutzadministrator konfiguriert Richtlinien nach dem Klonen. Nachdem das Skript nach dem Klonen in der Zielinstanz abgeschlossen wurde, sehen die Benutzer deidentifizierte Daten und haben keinen Zugriff auf die ursprünglichen Daten. Datenschutzadministratoren können Deidentifizierungsrichtlinien konfigurieren, die beim Klonen auf die Zielinstanz angewendet werden, um sicherzustellen, dass die Zielinstanz keine ursprünglichen vertraulichen Daten enthält. Für die Richtlinie wird eine Reihenfolge im Verhältnis zu anderen auszuführenden Richtlinien angegeben.

Hinweis: Das Klonen von Datenschutzdaten ist für selbst gehostete Instanzen verfügbar.

Der Datenschutzklon weist die folgenden zusätzlichen Attribute auf:

- Das Datenschutz-Plugin erstellt das Skript nach dem Klonen, das in der Zielinstanz ausgeführt werden soll.
- Datenschutzaufträge, die für die PostClone-Konfiguration erstellt wurden, können parallel ausgeführt werden, wenn sie nicht dieselben Tabellen betreffen.
- Ein Datenschutzauftrag für die Postclone-Konfiguration mit einem höheren Anwendungsauftrag wird vor einem anderen Auftrag mit niedrigerem Auftrag gestartet, wenn der Auftrag mit dem höheren Auftrag keine Tabelle im Zusammenhang mit einem anderen Auftrag mit niedrigerer Reihenfolge enthält.
- Mit dem Datenschutz-Plugin befinden sich Datenschutztabellen standardmäßig im Tabellensatz „Datenerhaltungsfunktionen klonen“.
- Beim Versuch, eine Datenschutztabelle (dp_[table]) unter „Ausschlusstabellen klonen“ hinzuzufügen, wird eine Warnung angezeigt. Diese Tabelle darf nicht ausgeschlossen werden.

Konfigurieren Sie die Datenschutz-Klonanforderung

Die Integration des Datenschutzklons wird mithilfe eines PostClone-Skripts konfiguriert, um Datenschutzaufträge für konfigurierte Richtlinien im Ziel zu erstellen und auszuführen. Nach dem Ausführen des Skripts werden Anwendern deidentifizierte Daten angezeigt und sie haben keinen Zugriff auf die ursprünglichen Daten.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: data_privacy_clone_processor, data_privacy_admin und admin

Prozedur

1. Aktivieren Sie das Datenschutz-Plugin (com.glide.data_privacy) in der Quellinstanz.
   Das Plugin kann nur von Kundenservice und Supportinstalliert werden.
   Das Post-Clone-Skript für Datenschutz wird installiert.
2. Führen Sie eine Hochstufung auf die Rolle **„data_privacy_admin“ durch**.
   Weitere Informationen zur Erhöhung von Rollen finden Sie unter Auf eine privilegierte Rolle hochstufen.
3. Navigieren zu **Systemsicherheit** > **Datenschutz** > **Konfiguration der Datenschutzrichtlinie**an.
4. Erstellt eine Datenschutzrichtlinienkonfiguration.
   Wählen **Sie Auf alle in Datenklasseanwenden und Beim Klonen anwenden**aus. Weitere Informationen finden Sie unter Erstellen Sie eine Datenschutzrichtlinie.
5. Sichern Sie die Datenschutzkonfigurationen.
6. Senden Sie als Datenschutzadministrator eine Klonanforderung.

Ergebnisse
Das PostClone-Skript für Datenschutz wird in der Zielinstanz ausgeführt, und das PostClone-Skript erstellt in der Zielinstanz einen Verbundauftragsdatensatz für Datenschutz. Die verbundene Aufgabe erstellt einen Datenschutzauftrag für jede Richtlinie nach dem Klonen in der Anwendungsreihenfolge in der Zielinstanz und führt sie aus. Die Sicherungsquelle wird in die Zielinstanz geklont. Das Datenschutz-PostClone-Skript erstellt Datenschutzaufträge für konfigurierte Richtlinien in der Zielinstanz und führt sie aus.

Der Klonprozessor für erhöhte Datenschutz kann sich bei der Zielinstanz anmelden und den Status des Verbundauftrags nach dem Klonen in dp_federated_job.list und dp_job.list überwachen.

Datenschutz

Die Datenschutz-Store-App ist eine Next Experience-Aktualisierung für Datenklassifizierung und Datenschutz mit moderner Darstellung, Haptik und Benutzerfreundlichkeit. Die Store-App für Datenschutz wird in Utah und höher unterstützt.

Datenschutz besteht aus mehreren Komponenten: Übersicht, Klassifizierung und Anonymisierung.

Übersicht

Verwenden Sie den Abschnitt „Übersicht“ als Ausgangspunkt, um Ihre Daten und die Datenschutz-Compliance zu verwalten. Details siehe Übersicht über Datenschutz.

Klassifizierung

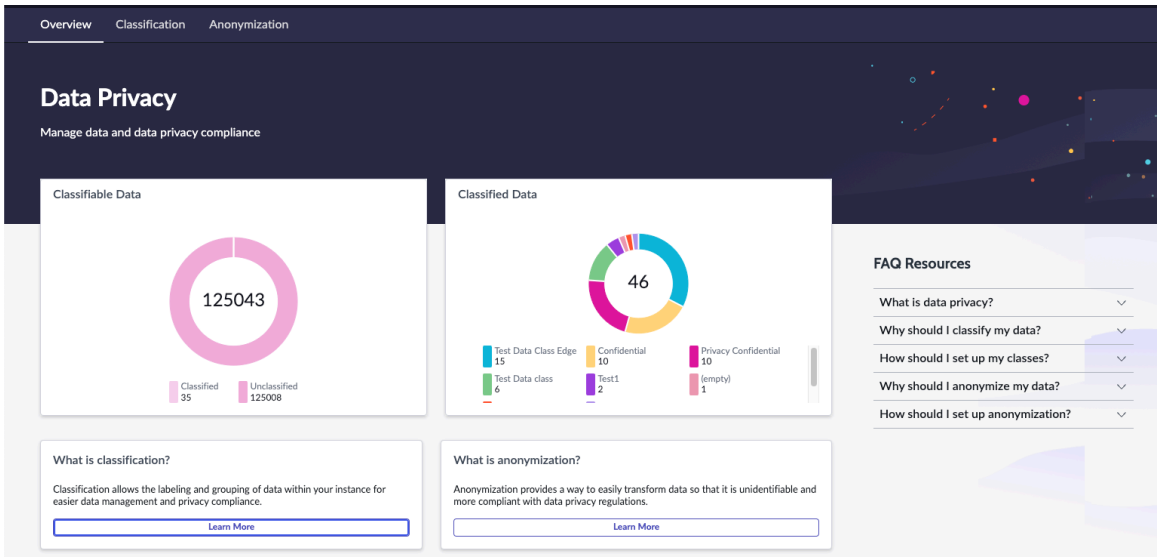
Die Datenklassifizierung ist der Prozess der Organisation von Daten in Kategorien, die das Abrufen, Sortieren und Speichern für die zukünftige Verwendung erleichtern. Die Verwendung eines Klassifizierungssystems hilft, sich auf die Anforderungen der Vertraulichkeits- und Sicherheitsrichtlinien zu konzentrieren. Klassifizieren Sie Daten, die für die Anonymisierung verwendet werden sollen. Informationen zu Datenklassen und Klassifizierung finden Sie unter Datenklassifizierung.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übersicht über Datenschutz

Die Homepage „Übersicht“ ist ein Ausgangspunkt für die Verwaltung Ihrer Daten und der Datenschutz-Compliance.

Das Dashboard „Übersicht“ informiert Sie über den aktuellen Status der Datenklassifizierungen und Anonymisierungsaufgaben in Ihrer Instanz. Sie können Ihre Daten mit dem Übersichts-Dashboard anzeigen, um zu sehen, wie viele Daten klassifiziert werden können, welche Datenklassen verfügbar sind, wie viele Daten in jeder Klasse enthalten sind und welchen Gesamtstatus die Anonymisierungsaufgaben haben. Die klassifizierten Daten sind in verschiedene Kategorien unterteilt. Durch Auswählen einer Unterkategorie in einem der Diagramme wird die Kategorie zum Gesamtdiagramm hinzugefügt oder daraus entfernt und die Anzahl angepasst.



Klassifizierbare Daten

Zeigt die Gesamtzahl der Datensätze in der Instanz an, die klassifiziert werden können. Die Anzahl wird in die Gesamtzahl der klassifizierten Daten und die Gesamtzahl der nicht klassifizierten Daten aufgeschlüsselt. Dadurch erhalten Administratoren einen schnellen Überblick über potenzielle Klassifizierungsmöglichkeiten.

Klassifizierte Daten

Zeigt die Gesamtzahl der Datensätze in der Instanz an, die klassifiziert wurden. Die Zahl wird in die Gesamtzahl der klassifizierten Daten für jede zugewiesene Datenklasse aufgeschlüsselt. So können Sie schnell nachvollziehen, wie viele Daten in jedem Bereich klassifiziert wurden.

Anonymisierungsaufgaben

Zeigt Datenschutzaufträge an, die derzeit von Aufträgen verarbeitet werden, die in Ihrer Instanz außerhalb der Produktion für Anwender- und Datenklassenaufträge abgeschlossen wurden.

Weitere Informationen

Die Abschnitte „ **Weitere** Informationen“ bieten einen schnellen Überblick über das Verständnis der Klassifizierung und Anonymisierung und bieten eine einfache Möglichkeit, mit dem Prozess zu beginnen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

FAQ-Ressourcen

Greifen Sie auf die Lernressourcen des Produkts zur Klassifizierung oder Anonymisierung zu, um zusätzliche Informationen zu den ersten Schritten zu erhalten, um Ihre Instanz mit Datenschutz zu sichern.

Aktivieren Sie den Datenschutz

Datenschutz umfasst Datenklassifizierung und Anonymisierung und wird im ServiceNow Storeinstalliert.

Vorbereitungen

Um die Datenanonymisierung zu verwenden, muss „Datenschutz (klassisch)“ zuerst mit der Berechtigung ServiceNow Vault aktiviert werden. Weitere Informationen finden Sie unter Datenschutz aktivieren (klassisch).

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle** > **Datenschutz**an.
2. Suchen Sie die Anwendung über die Filterkriterien und die Suchleiste.

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

   Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .
3. Wählen Sie eine Version aus der Liste und dann **Installieren** aus.

   Im angezeigten Dialogfeld „Installieren“ werden alle Abhängigkeiten aufgelistet, die zusammen mit der Anwendung installiert werden.
4. Wenn Sie dazu aufgefordert werden, folgen Sie den Links zum ServiceNow Store, um zusätzliche Berechtigungen für Abhängigkeiten zu erhalten.
5. Wahlweise: Wenn Demodaten verfügbar sind und Sie diese installieren möchten, aktivieren Sie das Kontrollkästchen **Demodaten laden**.

   (Optional) Demodaten sind Beispieldatensätze, die Anwendungsfunktionen für häufige Anwendungsfälle veranschaulichen. Das Laden von Demodaten wird empfohlen, wenn Sie die Anwendung zum ersten Mal auf einer Entwicklungs- oder Testinstanz installieren.

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

Datenklassifizierung

Gruppieren Sie Daten mithilfe vordefinierter oder benutzerdefinierter Datenklassifizierungen nach Typ. Wenn Ihnen die Rolle „Datenklassifizierungsadministrator“ oder „Auditor“ zugewiesen wurde, können Sie verschiedene Datenklassen verwalten oder den aktuellen Status verschiedener Datentypen innerhalb der Instanz visuell analysieren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Data Classification ermöglicht die Unterstützung von:

- Transparenz der Datentypen, die auf einer Now Platform -Instanz gehostet werden.
- Einhaltung von Datenschutzgesetzen und Erfüllung von gesetzlichen Anforderungen für Branchen wie Finanzdienstleistungen und Herstellung medizinischer Geräte.

Datenklassifizierungen

Die Datenklassifizierung ist ein eigenständiger Prozess, bei dem Sie Datenklassifizierungen manuell auf vorhandene Wörterbucheinträge in einer beliebigen Tabelle anwenden. Weitere Informationen finden Sie unter Datenwörterbuchtabellen .

- Sie klassifizieren Daten so, wie Sie es für Ihr Unternehmen für angemessen halten, und Sie können die verfügbaren Datenklassen nach Bedarf ändern.
- Wenn Sie Daten klassifizieren, können Sie die vordefinierten Datenklassifizierungen verwenden oder eigene erstellen. Obwohl die Verwendung vordefinierter Datenklassifizierungen optional ist, wird empfohlen, dies als Ausgangspunkt zu tun. Diese vordefinierten Datenklassifizierungen sind in Demodaten enthalten, die Sie in Ihrer -Instanz installieren können.
- Wenn Sie eigene Datenklassifizierungen erstellen, können Sie auch ein abgestuftes hierarchisches System mit über- und untergeordneten Datenklassifizierungen entwerfen.

Hinweis: Data Classification unterstützt Domain Separation, und die Tabelle „data_classification“ selbst ist prozessgetrennt. Weitere Informationen finden Sie unter Domänentrennung und Data Classification.

Anwendungsfälle

Die Datenschutz-Grundregel (DSGVO) ist eine Verordnung der Europäischen Union, deren Zweck darin besteht, Personen die Kontrolle über ihre eigenen personenbezogenen Daten zu geben. Sie können Datenklassifizierungen verwenden, z. B. personenbezogene Daten, um zu identifizieren, wo personenbezogene Daten in Ihrer Instanz gespeichert werden. Durch die Anwendung der entsprechenden Sicherheitsmechanismen, um diese personenbezogenen Daten vor der Weitergabe zu schützen, erfüllt Ihr Unternehmen die DSGVO-Anforderungen.

Wenn Sie Kundeninformationen in Now Platformspeichern, verwenden Sie bei Bedarf den Klassifizierungscode für personenbezogene Daten (Personal Identifiable Information, PII), um Daten nachzuverfolgen, die den Vorschriften der lokalen Datenschutzgesetze unterliegen.

Sie können eine eingeschränkte Datenklassifizierung auf Mitarbeitertabellenspalten anwenden, die vertrauliche Mitarbeiterinformationen speichern, z. B. Sozialversicherungsnummern. Administratoren und Auditoren können dann im Übersichts-Dashboard nachprüfen, ob Sie den richtigen Spalten Datenklassifizierungen zugewiesen haben. Sie können auch die Klassifizierungsdetails für eingeschränkte Informationstypen anzeigen.

Erstellen Sie Datenklassifizierungen

Erstellen Sie in der Tabelle [data_classification] eigene anwenderdefinierte Datenklassifizierungen, die Sie dann bestimmten Spalten in bestimmten Tabellen zuweisen können. Erstellen Sie neue Datenklassen, um den Klassifizierungsprozess zu starten.

Vorbereitungen
Erforderliche Rolle: data_classification_admin, admin

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Datenschutz** > **Klassifizierung**an.
2. Wählen Sie **+Datenklasse hinzufügen aus**.

   Hinweis: Im Basissystem sind mehrere Datenklassen enthalten.

3. Füllen Sie die Felder des Formulars aus.

Feld	Beschreibung
Klassenname	Name der Datenklassifizierung.
Übergeordnete Klasse	Name der übergeordneten Datenklassifizierung, der diese Datenklassifizierung untergeordnet ist. Lassen Sie das Feld leer, wenn diese Datenklassifizierung kein untergeordnetes Element einer übergeordneten Datenklassifizierung ist.
Beschreibung	Beschreibung der Datenklassifizierung.

4. Klicken Sie auf **Absenden**.
   Die neue Datenklasse wird hinzugefügt. Wenn die Datenklasse ein untergeordnetes Element ist, wird sie unter dem übergeordneten Element in der linken Navigationsleiste aufgeführt.

Daten klassifizieren

Gruppieren Sie Daten mithilfe vordefinierter oder benutzerdefinierter Datenklassifizierungen nach Typ. Weisen Sie bestimmten Tabellenspalten in der Tabelle „Wörterbuch“ [sys_dictionary] Datenklassifizierungen zu. Wenn Sie Datenklassifizierungen zuweisen, werden Einträge in der Tabelle „Wörterbuch-Datenklasse“ [m2m_dictionary_dataclass] erstellt, die Sie dann im Übersichts-Dashboard überprüfen können.

Vorbereitungen

Erforderliche Rolle: data_classification_admin, admin

Prozedur

1. Wählen Sie **Neu** aus, um Daten aus einer zu klassifizierenden Tabelle zuzuweisen.
2. Wählen Sie die Datenklasse aus der Dropdown-Liste aus.
3. Wählen Sie die Datensätze aus, die die zu klassifizierenden Tabellen und Spalten widerspiegeln.
   Wählen Sie zusätzliche Zeilen aus, die pro Seite in der Tabelle angezeigt werden sollen, um das Auffinden einer bestimmten Tabelle zu erleichtern.
4. Wählen Sie **Daten klassifizieren aus**.
   Die Daten werden unter dem Klassifizierungsnamen in der Tabelle „Klassifizierte Daten“ klassifiziert.
5. Zeigen Sie die Daten an, oder exportieren Sie sie in Excel, CSV, JSON oder PDF.
   Wählen Sie, ob Sie die Daten im ausgewählten Format herunterladen oder per E-Mail erhalten möchten.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Echtzeitanonymisierung

Verwenden Sie die RTA-Richtlinie (Real Time Anonymization), um Dateneinträge in Echtzeit zu anonymisieren.

RTA-Übersicht

Benutzer erstellen eine RTA-Richtlinie über die Seite „Anonymisierungsrichtlinien“. Spalten aus den Zieltabellen können für RTA ausgewählt werden, wobei aktive Datenmuster verwendet und ihre Richtlinien auf alle gültigen Datensatzeinträge in den Zielspalten der RTA angewendet werden. Wenn ein Eintrag mit einem aktiven Datenmuster übereinstimmt, wird die zugehörige Anonymisierungstechnik für die Anonymisierung verwendet.

Tipp: Wenn Sie die Anonymisierungstechnik ändern müssen, lesen Sie Konfigurieren Sie die Muster Datenerkennung ..

Echtzeitanonymisierungsfehler

Wenn eine RTA-Richtlinie fehlschlägt, können Sie ihren Status anhand der Tabelle Echtzeitanonymisierungsfehler überprüfen.

Echtzeitanonymisierungsfehler

Überprüfen Sie Fehler bei der Echtzeitanonymisierung (RTA).

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Datenschutz (klassisch)**an.
2. Überprüfen Sie die RTA-Fehler in der Tabelle.

Feldtitel	Beschreibung
Tabellenspalte	Die Tabellenspalte, in der der Fehler aufgetreten ist.
Fehlergrund	Kategorie der Fehlerursache.
Details zum Fehlergrund	Kurze Beschreibung, die die Ursache des Fehlers zusammenfasst.
Datenschutzkonfiguration	Die fehlgeschlagene RTA-Datenschutzkonfiguration.
Datensatz	Der spezifische Datensatz, der fehlgeschlagen ist.
Tabellenname	Tabelle, in der der Fehler aufgetreten ist.
Zeitstempel	Zeitpunkt des Fehlers.

Datenerkennung

Verwenden Sie Datenerkennung, um vertrauliche Daten innerhalb einer Instanz zu identifizieren, z. B. Kreditkarteninformationen, E-Mail-Adressen oder Sozialversicherungsnummern.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Daten-Discovery erkunden



Erfahren Sie mehr über Daten-Discovery.

Konfigurieren Sie die Daten-Discovery



Erhalten Sie Hilfe bei der Konfiguration der Daten-Discovery.

Rollen in der Daten-Discovery



Erfahren Sie mehr über Rollen in Daten-Discovery.

Daten-Discovery-Ergebnisse



Überprüfen Sie die Daten-Discovery-Ergebnisse.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenerkennung erkunden

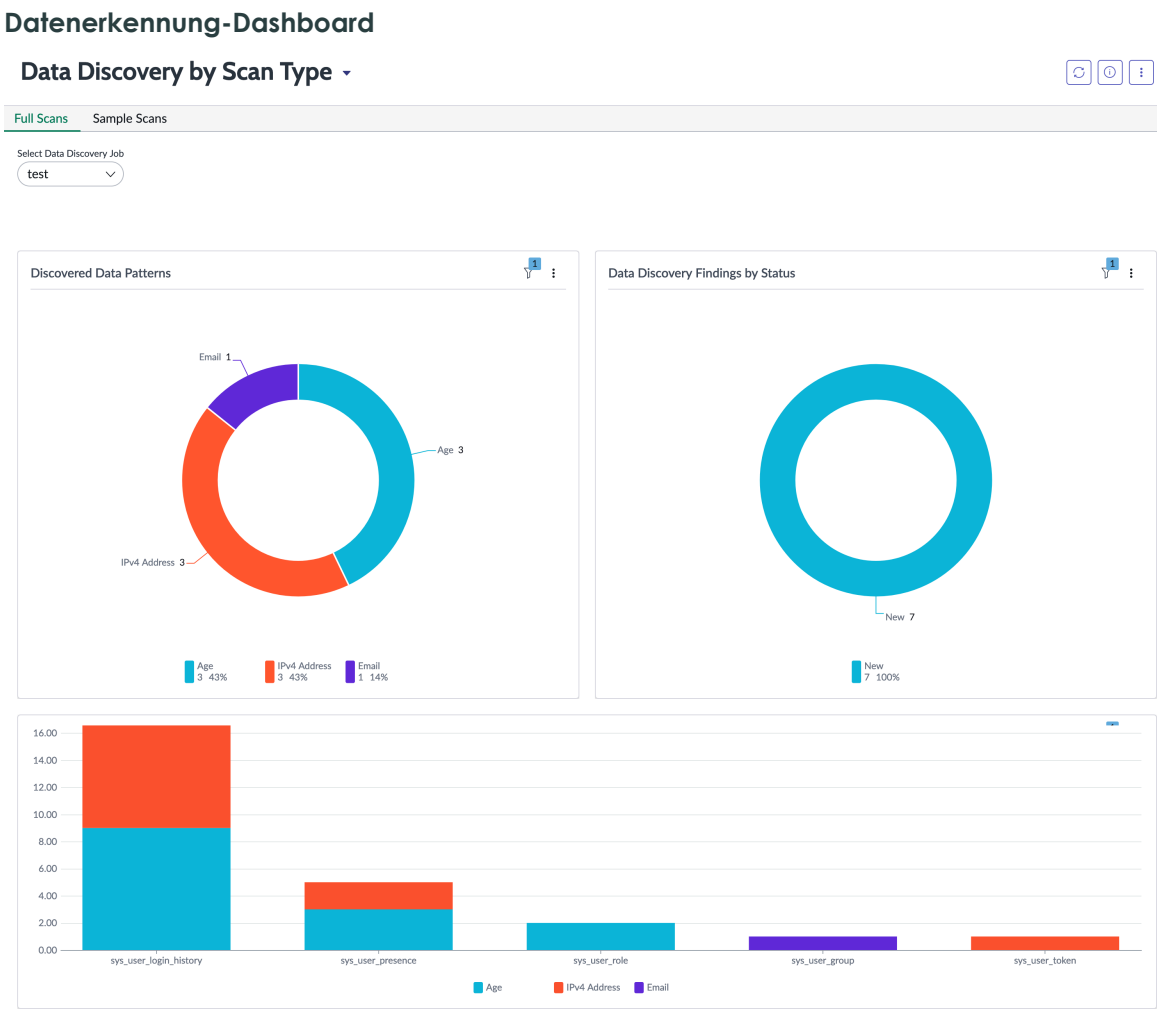
Verwenden Sie Datenerkennung, um vertrauliche Daten innerhalb einer Instanz zu identifizieren, z. B. Kreditkarteninformationen, E-Mail-Adressen oder Sozialversicherungsnummern.

Datenerkennung führt einen anwenderdefinierten Satz von Aufträgen für einen Satz von Tabellen aus. Die -Aufgaben suchen nach vertraulichen Informationen und melden sie zur Überprüfung im Dashboard Datenerkennung. Eine geplante Aufgabe verwendet bei der Ausführung automatisch alle aktiven Datenmuster und Zieltabellen.

Datenerkennung enthält auch vorab zugewiesene Rollen mit unterschiedlichen Zugriffsebenen für Daten.

Zugriff auf das Dashboard von Datenerkennung

Navigieren zu **Alle** > **Systemsicherheit** > **Daten-Discovery (klassisch)** > **Dashboard** um das Dashboard Datenerkennung anzuzeigen und Ihre aktuellen Stellenergebnisse zu überprüfen.



Erkannte Datenmuster

Tipp: Wählen Sie einen Datensatz aus, um weitere Informationen anzuzeigen und weitere Maßnahmen mit den Ergebnissen zu ergreifen. Weitere Informationen finden Sie unter Datenerkennung Auftragsergebnisse.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Diagramm „Erkannte Datenmuster“ zeigt die Anzahl und den Prozentsatz der derzeit erkannten Datenmuster an. Wählen Sie einen Abschnitt aus, um weitere Aktionen auszuführen.

Daten-Discovery-Ergebnisse nach Status

Das Diagramm „Daten-Discovery-Ergebnisse“ zeigt die Anzahl und den Prozentsatz der derzeit erkannten Datenmuster nach ihrem Status an.

Erkannte Tabellen

Die erkannten Tabellen zeigen, in welchen Tabellen sich die aktuell erkannten Daten befinden, und geben deren Datenmuster an.

Spalten mit erkannten Daten

Im Abschnitt „Spalten mit erkannten Daten“ werden die aktuell erkannten Daten anhand ihrer Spalte überprüft.

Datenerkennung aktivieren

Die Anwendung installiert Datenerkennung und zugehörige ServiceNow® Store -Anwendungen und -Plugins, falls sie nicht bereits installiert sind.

Vorbereitungen
Die Daten-Discovery erfordert ein vom Rest der Now Platformgetrenntes Abonnement.

Wenden Sie sich an Ihren ServiceNow-Kundenbetreuer, um ein Abonnement zu erwerben. Wenn Sie ein Abonnement erwerben, werden bestimmte Plugins automatisch aktiviert. Wenn ein kostenpflichtiges Plugin nicht automatisch aktiviert wird, können Sie es manuell in der Liste „Alle Anwendungen“ in Ihrer Instanz aktivieren.

Hinweis:

Bevor Sie ein Abonnement kaufen, können Sie die Funktion in einer Instanz außerhalb der Produktion kostenlos testen, indem Sie sie über den Now Support Servicekatalog anfordern.

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Die folgenden Elemente werden mit Daten-Discovery installiert:

- Rollen
- Tabellen

Weitere Informationen zu den installierten Rollen und Tabellen finden Sie unter Datenerkennung Rollen und Standarddatenmuster.

Prozedur

1. Navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie das Plugin „Data Discovery“ (sn_data_discovery) mithilfe der Filterkriterien und der Suchleiste.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.

3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: `Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.`

   Nach Abschluss der Installation wird eine Meldung angezeigt.

Klassifizieren Sie Daten auf der Seite Datenerkennung „ Ergebnisse“.

Klassifizieren Sie vertrauliche Daten, die von allen erfolgreichen Aufträgen über Datenerkennung Ergebnisse gefunden wurden.

Vorbereitungen

Erforderliche Rolle: data_discovery_admin

Ein Auftrag muss erfolgreich ausgeführt werden, bevor Ergebnisdaten anscheinend klassifiziert werden.

Warum und wann dieser Vorgang ausgeführt wird

Auf der Seite Datenerkennung „ Ergebnisse“ werden alle Dateneinträge angezeigt, die von einem -Auftrag gefunden wurden. Auf der Seite „Ergebnisse“ können Sie die Einträge überprüfen und einer Klassifizierung zuordnen.

Prozedur

1. Navigieren zu **Systemsicherheit** > **Daten-Discovery (klassisch)** > **Daten-Discovery-Ergebnisse**an.
2. Wählen Sie den Eintrag aus, den Sie klassifizieren möchten.
3. Wählen Sie in der Liste Datenerkennung Ergebnisse die **Option Klassifizieren**aus.
4. Wählen Sie die Datenklassen aus, die Sie den Tabelleneinträgen zuordnen möchten.
5. Wählen Sie **Klassifizieren aus**.

Datenerkennung Aufträge

Datenerkennung überprüft Ihre zielgerichteten Informationen anhand anwenderdefinierter Datenmuster und Zieltabellen.

Datenerkennung plant zuerst einen Auftrag im Abschnitt „ **Daten-Discovery-** Auftrag“. Wenn eine geplante Aufgabe ausgeführt wird, werden alle aktiven Datenmuster in den aktuellen Zieltabellen durchsucht. Weitere Informationen zum Erstellen und Konfigurieren eines Datenerkennung -Auftrags finden Sie unter Konfigurieren Sie einen Datenerkennung -Auftrag.

Hinweis: Beispielscanaufträge, die bis zu 10.000 Datensätze pro Tabelle und Muster scannen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnung: Wenn ein Auftrag innerhalb kurzer Zeit zweimal ausgeführt wird, kann die Anzahl der gescannten Zeilen für die zweite Ausführung 0 zurückgeben.

Datenerkennung Datenmuster

Im Abschnitt „ **Datenmuster** “ werden alle aktuellen Datenmuster angezeigt, sowohl aktive als auch inaktive. Ein Datenmuster ist ein regulärer Ausdruck, der zum Abgleichen vertraulicher Daten verwendet wird. Weitere Informationen zum Zugriff auf Datenmuster und zur Konfiguration von Datenmustern finden Sie unter Konfigurieren Sie die Muster Datenerkennung .. Im Abschnitt „ **Aktive** Datenmuster“ werden nur aktive Muster angezeigt. Inaktive Muster werden nicht angezeigt.

Zieltabellen

Im Abschnitt „ **Zieltabellen** “ werden alle Tabellen aufgelistet, die für einen Auftrag verarbeitet werden können. Um auf die Zieltabellen zuzugreifen, wählen Sie **Zieltabellen**aus.

Die folgenden Tabellen werden nicht unterstützt:

- sr
- sysx
- v
- sh$
- syslog
- ua
- Nutzungsanalysen
- ECC
- Klon
- jrobin
- pa
- sla_repair_log
- Scan
- gcf
- fm_log
- Protokoll
- np$
- sn_data_discovery
- dp_configuration
- dp_federated_job
- dp_field_technique
- dp_job
- dp_job_summary
- dp_primary_reference
- dp_technique

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- data_classification
- m2m_dictionary_dataclass

Granulare Konfiguration

Das Tool für die granulare Konfiguration ermöglicht spezifischere und präzisere Steuerungen für die Erkennung vertraulicher Daten in einer Tabelle. Es gibt jedoch wichtige Unterschiede in der Funktionsweise im Vergleich zu einem herkömmlichen Daten-Discovery-Auftrag. Eine granulare Konfiguration scannt nur bestimmte Spalten einer Tabelle für die Erkennung und meldet die Ergebnisse nach Datensatz. Für Ergebnisse aus der Prüfung von granularen Konfigurationen, die als granulare Ergebnisse bezeichnet werden, werden die Aktionen pro Datensatz angegeben, und die Rolle „data_privacy_admin“ muss anonymisiert werden.

Konfigurieren Sie einen Datenerkennung -Auftrag

Konfigurieren Sie einen Datenerkennung -Auftrag, und überprüfen Sie den Status laufender Aufträge. Ein Datenerkennung -Auftrag definiert, wann ein Muster in einer Zieltabelle ausgeführt wird.

Vorbereitungen

Erforderliche Rolle: data_discovery_admin

Prozedur

1. Navigieren zu **Systemsicherheit** > **Daten-Discovery (klassisch)** > **Daten-Discovery-Auftrag**an.
2. Wählen Sie in der Liste Datenerkennung Aufträge **Neu**aus.
3. Füllen Sie im Formular Datenerkennung Stellenfelder die Felder aus.

Datenerkennung Auftragsfelder

Feld	Beschreibung
Name	Name des Jobs
Beschreibung	Beschreibung des Auftrags.
Scantyp	Anzahl der zu scannenden Einträge. Mögliche Status: ◦ **Beispiel**: Scannt 10.000 Einträge. ◦ **Vollständig**: Scannt alle Einträge.
Kontext	Auftragsdetails zu gescannten Mustern, Zieltabelleneinträgen und verstrichener Zeit.
Status	Status des Auftrags Datenerkennung. Folgende Status sind möglich: ◦ **Bereit zum Planen**: Standardstatus für neue Aufträge. ◦ **Geplant**: Die Ausführung des Auftrags ist geplant. ◦ **In Bearbeitung**: Der Auftrag wird aktiv ausgeführt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	◦ **Abgeschlossen**: Die Ausführung des Auftrags wurde erfolgreich abgeschlossen. ◦ **Fehler**: Die Ausführung des Auftrags wurde aufgrund eines Fehlers beendet. ◦ **Abgebrochen**: Der Auftrag wurde abgebrochen. ◦ **Angehalten**: Der Auftrag wurde angehalten.
Zusammenfassung	Zeigt die Ergebnisse des Auftrags an, nachdem Sie ihn ausgeführt haben.
Startdatum	Legt das Startdatum für den Auftrag fest.
Zeitfensterstart	Beginn des Zeitfensters für die Ausführung dieses Auftrags. Die Aufgabe wird nach der in diesem Feld eingegebenen Zeit ausgeführt. Die im Feld „ **Zeitfensterstart“ eingegebene Zeit** muss vor der im Feld **„Zeitfensterende“ eingegebenen Zeit liegen**. **Hinweis:** Ein gültiger Zeitwert ist die koordinierte Weltzeit (Coordinated Universal Time, koordinierte Weltzeit), basierend auf einer 24-Stunden-Zeitnotation.
Zeitfensterende	Das Ende des Zeitfensters für die Ausführung dieses Auftrags. Die Aufgabe wird bis zu der in diesem Feld eingegebenen Zeit ausgeführt. Wenn der Auftrag dieses Mal nicht abgeschlossen wurde, wird er angehalten und beim Start des nächsten Zeitfensters fortgesetzt. Die im Feld „ **Zeitfensterende“ eingegebene Zeit** muss nach der im Feld **„Zeitfensterstart“ eingegebenen Zeit liegen**. **Hinweis:** Ein gültiger Zeitwert ist die koordinierte Weltzeit (Coordinated Universal Time, koordinierte Weltzeit), basierend auf einer 24-Stunden-Zeitnotation.

4. Wählen Sie **Absenden**.
   Die Schaltflächen **Auftrag planen** und **Aktualisieren** werden angezeigt.
5. **Wählen** Sie Auftrag planen aus, um den Auftrag auszuführen.
   Die Aufgabe wird zwischen den Zeiten ausgeführt, die in den Feldern **Start des Zeitfensters** und **Ende** des Zeitfensters ausgewählt sind. Wenn der Auftrag im Start- und Endzeitfenster

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

nicht abgeschlossen wurde, wird der Auftrag beim Start des nächsten Zeitfensters fortgesetzt.

6. Wahlweise: Wählen Sie eine der folgenden Funktionen aus:
   - Auftrag**abbrechen**: Bricht den Auftrag ab.
   - **Pause**: Hält den Auftrag an.
   - **Fortsetzen**: Startet einen angehaltenen Auftrag neu.

Konfigurieren Sie die Muster Datenerkennung .

Konfigurieren Sie ein Datenerkennung -Muster, und überprüfen Sie die aktuellen Muster. Das Muster Datenerkennung definiert den regulären Ausdruck, der zum Abgleichen von Daten mit einer Zieltabelle verwendet wird.

Vorbereitungen

Erforderliche Rolle: data_discovery_admin

Prozedur

1. Navigieren zu **Systemsicherheit** > **Daten-Discovery** > **Alle Datenmuster**an.
2. Wählen Sie in der Liste Datenerkennung Muster **Neu**.
3. Füllen Sie im Formular Datenerkennung Auftragsfelder die Felder aus.

Datenerkennung Auftragsfelder

Feld	Beschreibung
Interner Umfang	Umfang des Musters.
Beschreibung	Beschreibung des Auftrags.
Name	Name des Datenmusters.
Anwendung	Anwendungsbereich des Musters.
Ausdruck	Regulärer Ausdruck, der zum Erkennen des Datenmusters verwendet wird. **Hinweis:** Die Ausdruckslänge muss weniger als 1000 Zeichen betragen.
Stichwort (optional)	Ein bestimmtes Wort (oder durch Komma getrennte Wörter), nach dem um einen Ausdruck gesucht werden soll. Muss mit **Stichwortnähe**verwendet werden **Hinweis:** Ein Stichwort kann verwendet werden, um nach zusätzlichem Kontext für ein Muster zu suchen. Beispielsweise kann die Verwendung von Stichwörtern helfen, zwischen einem Geburtsdatum und einem Einstellungsdatum zu unterscheiden, wenn sie dieselbe Formatierung (MM/TT/JJ) haben.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Stichwortnähe (optional)	Wie weit vom Ausdruck entfernt, um nach Stichwörtern zu suchen. Muss mit **Stichwort**verwendet werden **Hinweis:** Der Standardwert ist 30, die Obergrenze 64

4. Wählen Sie **Absenden**.
   - Mit der Schaltfläche **Test** können Sie Ihren regulären Ausdruck testen, bevor Sie die Datenmusterliste absenden.

Das Datenmuster muss als aktiv festgelegt werden, um mit geplanten Aufgaben verwendet zu werden.

5. Navigieren zu **Systemsicherheit** > **Daten-Discovery** > **Aktive Datenmuster**an.
6. Wählen Sie **Bearbeiten**in der Liste Datenerkennung Aktives Muster.
7. Wählen Sie die Musterliste unter **Verfügbare Listen** aus, und verschieben Sie sie in **Ausgewählte Listen**.

Standarddatenmuster

Überprüfen Sie die in Datenerkennungenthaltenen regulären Ausdrücke für Standarddatenmuster. Diese Standarddatenmuster können zum Filtern von Tabelleneinträgen für eine weitere Klassifizierung verwendet werden.

Die folgenden sind verfügbare Standardmuster für die Daten-Discovery.

Name	Beschreibung	Regulärer Ausdruck	Stichwörter	Beispiele
Alter	Alter einer Person zwischen 0 und 99	\b([0-9] | [1-9] [0-9] | 1[012] [0-9])\b	age	Übereinstimmung 24 Keine Übereinstimmung • 103 • -2
Geburtsdatum	Geburtsdatum im Format TT/MM/JJJJ	\b[0-3]?[0-9]/ [0-3]?[0-9]/(?: [0-9]{2}})?[0-9] {2}\b	Geburtsdatum, Geburtsdatum, Geburtsdatum	Übereinstimmung • 06/18/2012 • 1/1/19
E-Mail	Standard-E-Mail-Adresse	\b[\w!#$%&'* +/=?`{\|}~^-]+(?: \.[\w!#$%&'* +/=?`{|}~^ -]+)*@(?:[a-zA-Z0-9-]+\.)+[a-zA-Z]{2,6}\b		Übereinstimmung • johndoe@emailserver.co • historyprofessor@college Keine Übereinstimmung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung	Regulärer Ausdruck	Stichwörter	Beispiele
				• notanemail.com • bademail@.org
Fahrzeugidentifikationsnummer (VIN)	Fahrzeugidentifikationsnummer	\b[A-HJ-NPR-Z0-9]{17}\b		Übereinstimmung AHUYA31581L000000
IP-Adresse	Standard-IP-Adresse	4-stellige IP \b(?:(?:25[0-5] | 2[0-4][0-9] | [01]?[0-9][0-9]?)\.){3}(?:25[0-5] | 2[0-4][0-9] | [01]?[0-9][0-9]?)\b 6-stellige IP \b(((?:[0-9A-Fa-f]{1,4}(?::[0-9A-Fa-f]{1,4})*)?::((?:[0-9A-Fa-f]{1,4}(?::[0-9A-Fa-f]{1,4})*)?)) | ((?:[0-9a-fA-F]{1,4}:){7}[0-9a-fA-F]{1,4})\b		Übereinstimmende 4-stellige IP 102.28.46.103 Übereinstimmende 6-stellige IP 914b:d45a:61ea:6346:59bc
Kreditkarte: Visa	Visa-Kreditkartennummer	\b4[0-9]{12}(?:[0-9]{3})?\b		Übereinstimmung 4444434342424242

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung	Regulärer Ausdruck	Stichwörter	Beispiele
Kreditkarte: American Express	Kreditkartennummer von American Express	\b3[47][0–9]{13}\b		Übereinstimmung 378225246366005
Kreditkarte: Mastercard	Mastercard-Kreditkartennummer	\b(?:5[1-5][0-9]{2}|222[1-9]|22[3-9][0-9]|2[3-6][0-9]{2}|27[01][0-9]|2720)[0-9]{12}\b		Übereinstimmung 5555444455554444
Kreditkarte: Gästebuch	Dynasty Kreditkartennummer	\b3(?:0[0-5]|[68][0-9])[0-9]{11}\b		Übereinstimmung 3056930009020004
Kreditkarte: Discover	Discovery-Kreditkartennummer	\b6(?:011|5[0-9]{2})[0-9]{12}\b		Übereinstimmung 6011025690875424
Kreditkarte: CCV	Prüfnummer der Kreditkarte	\b[0-9]{3,4}\b	cvv, Verifizierungscode, Sicherheitscode	Übereinstimmung 124
Kreditkarte: Ablaufdatum	Kreditkartenablauf im Format MM/JJJJ	\b(([1-9])|(0[1-9]|1[0-2]))\/?([0-9]{4}|[0-9]{2})\ b	ablaufen,exp	Übereinstimmung • 02/2027 • 04/23 Keine Übereinstimmung 03/9
USA: Sozialversicherungsnummer	Sozialversicherungsnummer für US-Bürger	\b(?!666|000|9\d{2})\d{3}-(?!00)\d{2}-(?!0{4})\d{4}\b		Übereinstimmung 001-22-111
USA: Telefonnummer	Telefonnummer aus den USA **Warnung:** Verwendet nicht den USA-Anrufcode.	\b\(?([0-9]{3})\)?[-.]?([0-9]{3})[-.]?([0-9]{4})\b		Übereinstimmung 2065550199 Keine Übereinstimmung 1 555 238 0199
USA: Reisepassnummer	9-stellige Reisepassnummer aus den USA	\b[a-zA-Z0-9]\d{8}\b		Übereinstimmung 770022122
USA: Steuerzahler-ID	US-Steuerzahler-ID-Nummer	\b(9\d{2})([\-]?)([7]\d|8[0-8])([\-]?)(\d{4})\b		Übereinstimmung 927 70 5828
USA: Führerscheinnummer	Führerscheinnummer des US-	\b[a–zA–Z]\d{7}\b		Übereinstimmung A0002144

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung	Regulärer Ausdruck	Stichwörter	Beispiele
des US-Bundesstaats Kalifornien	Bundesstaats Kalifornien			
USA: Routingnummer der Bank	US-Bankroutingnummer (ABA).	\b((0[0-9]) | (1[0-2]) | (2[1-9]) | (3[0-2]) | (6[1-9]) | (7 [0-2]) | 80) ([0-9]{7})\b		Übereinstimmung 125210305

Konfigurieren Sie die Zieltabelle Datenerkennung .

Fügen Sie eine Zieltabelle hinzu, die in Aufträgen Datenerkennung verwendet werden soll. Nur Zieltabellen werden auf Datenmuster gescannt.

Vorbereitungen
Erforderliche Rolle: data_discovery_admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn der Auftrag Datenerkennung ausgeführt wird, wird er für alle Zieltabellen mit allen aktiven Mustern ausgeführt.

Prozedur

1. Auswahlvorgang **Systemsicherheit** > **Daten-Discovery (klassisch)** > **Zieltabellen**an.
2. Wählen Sie **Neu**.
3. Wählen Sie Ihre Zieltabelle im Feld **Tabellenname** aus.
4. Wählen Sie **Absenden**.

Aktivieren Sie parallele Aufgaben für Datenerkennung

Verwenden Sie parallele Aufträge, um die Ausführungszeit des Datenerkennung -Auftrags zu verkürzen.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur
Standardmäßig führt Datenerkennung Aufträge mit einem einzelnen Thread aus. Für Datenerkennung vollständige Scans können mehrere Threads aktiviert sein.

1. Geben Sie im Navigationsfilter `sys_properties.list`ein.
2. Erstellen Sie die Eigenschaft `com.glide.data_discovery.max_concurrent_item_workers`
3. Vergewissern Sie sich, dass für den **Typ**`Ganzzahl`festgelegt ist.
4. **Wichtig:** Es wird empfohlen, mit einer kleinen Anzahl von Workern pro Knoten (2 oder 3) zu beginnen.

   Geben Sie im Feld **„Wert“** die Anzahl der parallel laufenden Mitarbeiter bis zu 5 ein.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenerkennung Rollen

Sie können Datenerkennung Rollen zuweisen, um den Benutzerzugriff auf bestimmte Datentypen zu beschränken.

Daten-Discovery-Administrator [sn_data_discovery.data_discovery_admin]

Datenmuster und zugehörige Aufgaben anzeigen, erstellen und ändern

- Datenmuster:
  - Erstellen
  - Lesen
  - Aktualisieren
  - Löschen
- Aktive Datenmuster:
  - Löschen
  - Lesen
- Aufträge:
  - Erstellen
  - Lesen
  - Aktualisieren
  - Löschen
  - Zeitplan
  - Pause
  - Fortfahren
  - Abbrechen
- Zieltabellen:
  - Erstellen
  - Lesen
  - Schreiben
- Granulare Konfiguration:
  - Erstellen
  - Lesen
  - Aktualisieren
  - Löschen
- Granulare Ergebnisse:
  - Erstellen
  - Lesen
  - Aktionen

Hinweis: Anwender mit dieser Rolle können nur die Aktion „Ignorieren“ ausführen

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Enthält die Rollen

Liste der Rollen, die in der Rolle enthalten sind.

- data_classification_auditor
- data_classification_admin
- sn_data_discovery.data_discovery_api_processor

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Besondere Überlegungen

Administratoren wird diese Rolle bei der Produktinstallation automatisch zugewiesen.

Hinweis: Vermeiden Sie das Gewähren einer Administratorrolle, wenn spezialisiertere Rollen verfügbar sind.

Auditor für Daten-Discovery [sn_data_discovery.data_discovery_auditor]

Datenmuster und Zieltabellen lesen.

- Datenmuster lesen
- Aktive Datenmuster lesen
- Lesen Sie Datenerkennung Aufträge
- Zieltabellen lesen
- Überprüfen Sie die granulare Konfiguration
- Überprüfen Sie granulare Ergebnisse

Enthält die Rollen

Liste der Rollen, die in der Rolle enthalten sind.

Keine.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Besondere Überlegungen

Keine.

Datenklassifizierungsadministrator [data_classification_admin]

Lesen Sie Datenmuster, Discovery-Aufträge und die Tabelle „data_classification“, wenn ein aktiviertes spezifisches Musterergebnis klassifiziert wird.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Enthält die Rollen

Die Rolle „Datenklassifizierung“ enthält die Liste der Rollen, die in der Rolle „data_classification_auditor“ enthalten sind.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Besondere Überlegungen

Hinweis: Weitere Informationen zur Administratorrolle für die Datenklassifizierung finden Sie unter Demodaten des Plugins Data Classification werden installiert.

Datenerkennung Auftragsergebnisse

Auf der Seite Datenerkennung „ Ergebnisse“ werden Details zu den von einem Auftrag gefundenen Daten angezeigt. Auf der Seite Ergebnisse können Sie die Ergebnisse eines Auftrags überprüfen und mit der Klassifizierung von Daten beginnen.

Auf der Seite Datenerkennung „ Ergebnisse“ werden nach einem abgeschlossenen Auftrag die folgenden Details angezeigt.

Spalte	Beschreibung
Wörterbucheintrag	Spalte der Zieltabelle, in der sich die Daten befanden
Tabelle	Zieltabelle, in der die Daten gefunden wurden
Datenmuster	Datenmuster, das zum Suchen der Daten verwendet wird
Anzahl der Übereinstimmungen von Datenmustern	Anzahl der Dateneinträge, die dem Datenmuster entsprechen
Gesamtanzahl der Zeilenscans	Anzahl der während des Auftrags gescannten Zeilen
Prozentsatz der übereinstimmenden Zeilen	Prozentsatz der Zeilen in der Zieltabelle, die dem Datenmuster entsprechen
Datenerkennung Auftrag	Auftrag, der in der Zieltabelle verwendet wird
Status	Status des Eintrags

Nachdem Sie einen Datenerkennung -Auftrag ausgeführt haben, haben die Ergebnisse den Status Neu. Wenn keine Aktion erforderlich ist, können Sie die Daten unverändert lassen, wodurch der Status automatisch auf Ignoriert festgelegt wird. Andernfalls können Sie die Daten klassifizieren, indem Sie beispielsweise anwenderdefinierte Datenklassifizierungen erstellen, um die Datenanonymisierung mit dem Tool Data Classification vorzubereiten.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Granulare Ergebnisse

Benutzer können die Aktion **Granulare Ergebnisse nachverfolgen** auswählen, um auf der Seite Granulare Ergebnisse Aktionen für bestimmte erkannte Datensätze auszuführen. Weitere Informationen finden Sie unter Granulare Ergebnisse.

Verfügbare Schutzmaßnahmen

Wählen Sie die Schaltfläche **Verfügbare Schutzmaßnahmen**, um einen Eintragssteuerungsservice, den Status, Notizen und das letzte Mal zu überprüfen. Ab Xanadu unterstützt diese Funktion nur Verschlüsselung auf Spaltenebene.

Auf Schutzservices kann auch über das Dashboard zugegriffen werden. Weitere Informationen zum Dashboard finden Sie unter Datenerkennung.

Konsolidieren Sie die Ergebnisse

Auftragsergebnisse können mit der Schaltfläche Ergebnisse konsolidieren **konsolidiert** werden. Auftragsergebnisse, die von zwei separaten Aufträgen gemeinsam genutzt werden, werden dann unter dem zuletzt ausgeführten Auftrag zusammengefasst.

Hinweis: Nur abgeschlossene vollständige Scan-Aufträge können konsolidiert werden

Klassifizieren Sie Daten auf der Seite mit Auftragsergebnissen Datenerkennung .

Klassifizieren Sie Daten in Datenerkennung direkt auf der Ergebnisseite eines Auftrags.

Vorbereitungen

Erforderliche Rolle: data_discovery_admin und admin

Ein Auftrag muss erfolgreich ausgeführt werden, bevor Ergebnisdaten anscheinend klassifiziert werden.

Prozedur

1. Gehe zu **Systemsicherheit** > **Daten-Discovery** > **Daten-Discovery-Auftrag**an.
2. Wählen Sie den Eintrag aus, den Sie klassifizieren möchten.
3. Wählen Sie in der Liste Datenerkennung Ergebnisse die **Option Klassifizieren**aus.
4. Wählen Sie die Datenklassifizierungen aus, die Sie den Tabelleneinträgen zuordnen möchten.
5. Wählen Sie **Klassifizieren aus**.

Datenerkennung unterstützte Datentypen

Überprüfen Sie, welche Feldtypen bei Verwendung von Datenerkennungunterstützt werden.

Hinweis: Nicht alle klassifizierten Feldtypen sind für Datenerkennungverfügbar.

Einige Feldtypen mit hohem Risiko sind standardmäßig deaktiviert, wie in der Tabelle beschrieben. Weitere Informationen zu Feldern finden Sie unter Feldtypen .

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterstützte Feldtypen für die Daten-Discovery

Feldtyp	Standardmäßig verfügbar
Audio	Nein
Bedingung	Nein
Bedingung_Zeichenfolge	Nein
currency	Ja
Dezimalzahl	Ja
due_date	Ja
Float	Ja
glide_date	Ja
glide_date_time	Ja
glide_duration	Nein
glide_time	Ja
html	Nein
icon	Nein
integer	Ja
ip_adr	Nein
ip_address	Nein
Journal	Ja
„journal_input“	Ja
„journal_list“	Ja
Langer Integer	Ja
name_values	Nein
percent_complete	Nein
phone_number_e164	Ja
Preis	Ja
Zeichenfolge	Ja
Zeichenfolge_vollständig_utf8	Ja
Übersetzt_html	Nein
translate_text	Nein
URL	Nein
user_image	Nein
Video	Nein
wiki_text	Nein

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Scannen mit granularer Konfiguration

Granularer Scan kann verwendet werden, um bestimmte Tabellenspalten für die Discovery zu scannen. Herkömmliche Datenerkennung -Aufträge scannen die gesamte Tabelle, um Daten zu erkennen, während granulare Scans auf bestimmte Spalten der Tabelle abzielen und dadurch mehr Kontrolle über den Discovery-Prozess bieten

Vorbereitungen

Erforderliche Rolle: admin, sn_data_discovery_admin, data_privacy_admin

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Daten-Discovery (klassisch)** > **Granulare Konfiguration**an.
2. Wählen Sie in der Liste **Granulare KonfigurationenNeu**.
3. Füllen Sie im Formular **„Granular Configuration** Fields“ (Granulare Konfiguration) die Felder aus.

Felder für granulare Konfiguration

Feld	Beschreibung
Wörterbucheintrag	Zu scannende Spalte.
Tabelle	Zu scannende Tabelle.
Spaltenbezeichnung	Bezeichnung der zu scannenden Spalte
Startpunkt des Scans	Sensible Daten werden nur für den Tag des Scan-Startpunkts und danach erkannt. **Hinweis:** Wenn der Scan-Startpunkt leer gelassen wird, werden alle Einträge in der Spalte gescannt. Wenn der Scan-Startpunkt geändert wird, wird der Scan zurückgesetzt, um mit dem neu konfigurierten Zeitstempel zu beginnen.
Aktiv	Aktivieren Sie diese Option, um die granulare Konfiguration zu aktivieren.

4. Wählen Sie **Absenden**.
   Untergeordnete Elemente von erweiterbaren Tabellen können für die Konfiguration ausgewählt werden.
5. Wahlweise: Wählen Sie die Granulare Konfiguration für die übergeordnete Tabelle aus, wählen **Sie Untergeordnete Tabellen** auswählen aus, und wählen Sie die zu scannenden untergeordneten Tabellen aus.

Ergebnisse

Die spezifische Spalte der Zieltabelle wird für die Discovery gescannt. Der granulare Scan verwendet Datenmuster aus **aktiven**Datenmustern. Unter können Sie die Ergebnisse überprüfen und Maßnahmen ergreifen **Alle** > **Systemsicherheit** > **Daten-Discovery (klassisch)** > **Granulare Ergebnisse**an. Weitere Informationen finden Sie unter Granulare Ergebnisse.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Granulare Ergebnisse

Granulare Ergebnisse können mit dem Tool „Granulare Ergebnisse“ überprüft werden.

Granulare Ergebnisse werden überprüft

Granulare Ergebnisse werden verwendet, um bis zu 500 Ergebnisse aus granularen Konfigurationenzu überprüfen. Wenn 500 Ergebnisse gefunden werden, wird das Scannen von granularen Konfigurationen angehalten, bis eine Aktion ausgeführt wird.

Spaltenbezeichnung	Beschreibung
Datensatz	Erkannter Datensatz.
Tabelle	Übergeordnete Tabelle des Datensatzes.
Spalte	Spalte des Datensatzes, in dem vertrauliche Informationen erkannt wurden.
Datenmuster	Muster, das zum Erkennen des Datensatzes verwendet wird.
Aktion	Aktion für Ergebnisse. Zum Ändern auswählen **Wichtig:** Die Rolle „data_privacy_admin“ ist erforderlich, um die Aktion „Anonymisieren“ für einen Datensatz auszuführen. Prüfen Die Überprüfung des Datensatzes steht aus. Dies ist neuen granularen Erkennungen zugewiesen. Ignorieren Für den Datensatz wird keine Aktion ausgeführt Anonymisieren Datensatz wird anonymisiert.
Status	Status des Datensatzes. Neu Status, der dem Ergebnis bei der ersten Meldung zugewiesen wird Verarbeitet Wenn die vom Anwender ausgewählte Aktion erfolgreich auf das Ergebnis angewendet wurde

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spaltenbezeichnung	Beschreibung
	Hinweis: Verarbeitete Ergebnisse werden vor dem Löschen 3 Tage lang in der Tabelle „Granulare Ergebnisse“ gespeichert Manuelle Überprüfung Beim Anwenden der vom Anwender ausgewählten Aktion ist fehlgeschlagen. **Warnung:** Ergebnisse in der manuellen Überprüfung sollten von Anwendern gelöscht werden, nachdem sie entsprechende Aktionen durchgeführt haben.

Warnung: Rollback wird für die Anonymisierung, die durch granulare Ergebnisse ausgelöst wird, nicht unterstützt.

Data Classification

Gruppieren Sie Daten mithilfe vordefinierter oder benutzerdefinierter Datenklassifizierungen nach Typ. Wenn Ihnen die Rolle „Datenklassifizierungsadministrator“ oder „Auditor“ zugewiesen wurde, können Sie verschiedene Datenklassen verwalten oder den aktuellen Status verschiedener Datentypen innerhalb der Instanz visuell analysieren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkunden Sie die Datenklassifizierung



Erfahren Sie mehr über die Datenklassifizierung.

Konfigurieren Sie die Datenklassifizierung



Erstellen und konfigurieren Sie Ihre eigenen Datenklassen.

Referenz für Datenklassifizierung



Erfahren Sie, wie die Datenklassifizierung mit Demodaten funktioniert.

Analysieren Sie Datenklassifizierungen



Erfahren Sie, wie Sie Datenklassifizierungen analysieren.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenklassifizierung erkunden

Erfahren Sie mehr über die Datenklassifizierung.

Data Classification ermöglicht die Unterstützung von:

- Transparenz der Datentypen, die auf einer Now Platform -Instanz gehostet werden.
- Einhaltung von Datenschutzgesetzen und Erfüllung von gesetzlichen Anforderungen für Branchen wie Finanzdienstleistungen und Herstellung medizinischer Geräte.

Datenklassifizierungen

Die Datenklassifizierung ist ein eigenständiger Prozess, bei dem Sie Datenklassifizierungen manuell auf vorhandene Wörterbucheinträge in einer beliebigen Tabelle anwenden. Weitere Informationen finden Sie unter Datenwörterbuchtabellen .

- Sie klassifizieren Daten so, wie Sie es für Ihr Unternehmen für angemessen halten, und Sie können die verfügbaren Datenklassen nach Bedarf ändern.
- Wenn Sie Daten klassifizieren, können Sie die vordefinierten Datenklassifizierungen verwenden oder eigene erstellen. Obwohl die Verwendung vordefinierter Datenklassifizierungen optional ist, wird empfohlen, dies als Ausgangspunkt zu tun. Diese vordefinierten Datenklassifizierungen sind in Demodaten enthalten, die Sie in Ihrer -Instanz installieren können. Weitere Informationen finden Sie unter Demodaten des Plugins Data Classification werden installiert und Mit Data Classification Demodaten installierte Komponenten.
- Wenn Sie eigene Datenklassifizierungen erstellen, können Sie auch ein abgestuftes hierarchisches System mit über- und untergeordneten Datenklassifizierungen entwerfen.

Übersichts-Dashboard

Verwenden Sie das Dashboard „Übersicht“, um zu verstehen, wie Ihre aktuellen Datentabellen verschiedenen Datenklassifizierungen zugeordnet werden. Sie können auch analysieren, wie Ihre globalen, regionalen und internationalen Anwender möglicherweise unterschiedliche Ansätze für die Datenklassifizierung benötigen, hinsichtlich der Verwendung von oder des Zugriffs auf Daten. Sie können auch den Inhalt und das Layout des Übersichts-Dashboards an Ihre Bedürfnisse anpassen.

Informationen zur Verwendung der verfügbaren geskripteten APIs und REST APIs zur Anwendung der Klassifizierungsmetadaten in vorhandenen Prozessen, Workflows und Anwendungen finden Sie unter:

- Datenklassifizierung: REST API
- DCManager: Global
- ScopedDCManager: Bereichsbezogen

Hinweis: Data Classification unterstützt Domain Separation, und die Tabelle „data_classification“ selbst ist prozessgetrennt.

Anwendungsfälle

Die Datenschutz-Grundregel (DSGVO) ist eine Verordnung der Europäischen Union, deren Zweck darin besteht, Personen die Kontrolle über ihre eigenen personenbezogenen Daten zu geben. Sie können Datenklassifizierungen verwenden, z. B. personenbezogene Daten, um zu identifizieren, wo personenbezogene Daten in Ihrer Instanz gespeichert werden. Durch die Anwendung der entsprechenden Sicherheitsmechanismen, um diese personenbezogenen Daten vor der Weitergabe zu schützen, erfüllt Ihr Unternehmen die DSGVO-Anforderungen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie Kundeninformationen in Now Platformspeichern, verwenden Sie bei Bedarf den Klassifizierungscode für personenbezogene Daten (Personal Identifiable Information, PII), um Daten nachzuverfolgen, die den Vorschriften der lokalen Datenschutzgesetze unterliegen. Wenn Sie Demodaten installieren, wird dieser Klassifizierungscode automatisch auf bestimmte sicherheitsrelevante Felder in der Tabelle „Benutzer“ [sys_user] angewendet. Weitere Informationen finden Sie unter:

- Mit Data Classification Demodaten installierte Komponenten
- Datenklassifizierungen werden Wörterbucheinträgen zugewiesen

Sie können eine eingeschränkte Datenklassifizierung auf Mitarbeitertabellenspalten anwenden, die vertrauliche Mitarbeiterinformationen speichern, z. B. Sozialversicherungsnummern. Administratoren und Auditoren können dann im Übersichts-Dashboard nachprüfen, ob Sie den richtigen Spalten Datenklassifizierungen zugewiesen haben. Sie können auch die Klassifizierungsdetails für eingeschränkte Informationstypen anzeigen.

Demodaten des Plugins Data Classification werden installiert

Wenn Sie ein Upgrade auf Xanadu (und höher) durchführen oder diese installieren, wird das Plugin Data Classification (com.glide.data_classification) automatisch aktiviert. Sie sollten die mit dem Plugin gelieferten Demodaten jedoch manuell installieren. Sie enthält mehrere wichtige vordefinierte Datenklassifizierungen, von denen eine bestimmten Benutzertabellenspalten [sys_user] in Ihrer Instanz zugewiesen wird.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Unabhängig davon, ob Sie Demodaten installieren, fügt das aktivierte Plugin Data Classification die folgenden Anwenderrollen in Ihrer Instanz hinzu:

- data_classification_admin: Kann alle Aspekte der Anwendung Data Classification verwalten, einschließlich Einrichtung und Zuweisung von Datenklassifizierung.
- data_classification_auditor: Kann Data Classification Codezuweisungen prüfen, die an Anwendertabellen und -spalten vorgenommen wurden.

Wichtig: Hinweis zur Nutzung von durch Kunden:

Alle Entscheidungen im Zusammenhang mit der Implementierung dieser Anwendung unterliegen der alleinigen Entscheidung des Kunden. Kunden erkennen an und erklären sich damit einverstanden, dass die Verwendung der Anwendung keine Erklärung von ServiceNow in Bezug auf die Einhaltung von Gesetzen oder Vorschriften darstellt und dass jede vorgeschlagene Formulierung, jedes Feld oder jede Klassifizierung, die standardmäßig mit der Anwendung bereitgestellt wird, keine Rechtsberatung durch ServiceNow darstellt.

Kunden sind allein für die Einhaltung der gesetzlichen Verpflichtungen verantwortlich, die ihnen nach geltendem Recht obliegen, einschließlich (aber nicht beschränkt auf) Datenschutz-, Sicherheitsanforderungen und Datenschutzgesetzen, und sind für die Konfiguration und die Vornahme aller erforderlichen Änderungen an dieser Anwendung verantwortlich, einschließlich (aber nicht beschränkt auf) bis) Vorlagen, um die Anforderungen der Kunden zu erfüllen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie das Plugin Data Classification mithilfe der Filterkriterien und der Suchleiste. Nachdem Sie das Plugin gefunden haben, wird die Meldung `Installiert` angezeigt.
3. Klicken Sie auf das Symbol mit den drei vertikalen Punkten, und wählen Sie **Reparieren**, um auf das Dialogfeld „Plugin aktivieren“ zuzugreifen.
4. Wählen Sie **Demodaten laden**aus, und klicken Sie dann auf **Reparieren**.

Mit Data Classification Demodaten installierte Komponenten

Wenn Sie die im Plugin Data Classification (com.glide.data_classification) enthaltenen Demodaten installieren, werden in Ihrer Instanz verschiedene Arten von Komponenten installiert. Diese Komponenten umfassen vordefinierte Datenklassifizierungen und Codezuweisungen für bestimmte Benutzerspalten [sys_user].

Datenklassifizierungen installiert

Datenklassifizierung	Beschreibung
Vertraulich	Sensible Daten, deren Gefährdung den Betrieb beeinträchtigen könnte.
Intern	Interne Daten, die nicht zur öffentlichen Offenlegung bestimmt sind.
Persönlich identifizierbare Informationen	Auch als personenbezogene Daten bezeichnet. Daten, die potenziell zur Identifizierung einer bestimmten Person verwendet werden könnten.
Öffentlich	Daten, die der Öffentlichkeit frei zugänglich gemacht werden dürfen.
Beschränkt	Hochsensible Unternehmensdaten, deren Gefährdung das Unternehmen einem finanziellen oder rechtlichen Risiko aussetzen könnte.

Data Classification Zuweisungen

Tabelle	Zugewiesene Spalte	Zugewiesene Datenklassifizierung
sys_user	Postleitzahl	Persönlich identifizierbare Informationen
sys_user	first_name	Persönlich identifizierbare Informationen
sys_user	E-Mail	Persönlich identifizierbare Informationen
sys_user	city	Persönlich identifizierbare Informationen
sys_user	Middle_name	Persönlich identifizierbare Informationen
sys_user	Straße	Persönlich identifizierbare Informationen
sys_user	mobile_phone	Persönlich identifizierbare Informationen
sys_user	last_name	Persönlich identifizierbare Informationen

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Zugewiesene Spalte	Zugewiesene Datenklassifizierung
sys_user	country	Persönlich identifizierbare Informationen
sys_user	Geschlecht	Persönlich identifizierbare Informationen
sys_user	Name	Persönlich identifizierbare Informationen
sys_user	Foto	Persönlich identifizierbare Informationen
sys_user	Staat	Persönlich identifizierbare Informationen
sys_user	home_phone	Persönlich identifizierbare Informationen

Datenklassifizierungen werden erstellt

Erstellen Sie eigene anwenderdefinierte Datenklassifizierungen in der Tabelle Data Classification [data_classification], die Sie dann bestimmten Spalten in bestimmten Tabellen zuweisen können.

Vorbereitungen

Erforderliche Rolle: data_classification_admin, admin

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Datenklassifizierung** > **Datenklassen**an.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Feld	Beschreibung
Klassifizierungsname	Name der Datenklassifizierung.
Beschreibung	Beschreibung der Datenklassifizierung.
Übergeordnet	Name der übergeordneten Datenklassifizierung, der diese Datenklassifizierung untergeordnet ist. Lassen Sie das Feld leer, wenn diese Datenklassifizierung kein übergeordnetes Element für untergeordnete Datenklassifizierungen ist.
Anwendung	Anwendungsbereich für diese Datenklassifizierung.

4. Wenn diese Datenklassifizierung ein übergeordnetes Element für untergeordnete Datenklassifizierungen sein soll, klicken Sie auf **Neu**.
   Wenn Sie keine untergeordneten Datenklassifizierungen erstellen möchten, überspringen Sie diesen Schritt.
5. Füllen Sie die Felder des Formulars aus.

Titel

Feld	Beschreibung
Klassifizierungsname	Name der untergeordneten Datenklassifizierung.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Beschreibung	Beschreibung der untergeordneten Datenklassifizierung.
Übergeordnet	Name der übergeordneten Datenklassifizierung, der diese Datenklassifizierung untergeordnet ist. Lassen Sie das Feld leer, wenn diese Datenklassifizierung kein übergeordnetes Element für untergeordnete Datenklassifizierungen ist.
Anwendung	Anwendungsbereich für diese untergeordnete Datenklassifizierung.

6. Klicken Sie auf **Absenden**.

Datenklassifizierungen werden Wörterbucheinträgen zugewiesen

Weisen Sie bestimmten Tabellenspalten in der Tabelle „Wörterbuch“ [sys_dictionary] Datenklassifizierungen zu. Wenn Sie Datenklassifizierungen zuweisen, werden Einträge in der Tabelle „Wörterbuch-Datenklasse“ [m2m_dictionary_dataclass] erstellt, die Sie dann im Übersichts-Dashboard überprüfen können.

Vorbereitungen

Erforderliche Rolle: data_classification_admin und admin

Prozedur

1. Geben Sie im Navigatorbereich `sys_dictionary.list ein`.
2. Wählen Sie unter Wörterbucheinträge alle Elemente aus, denen Sie bestimmte Datenklassifizierungen zuweisen möchten.
3. Klicken Sie nach der Auswahl der Elemente auf **Aktionen für ausgewählte Zeilen**, und wählen Sie dann **Klassifizieren**aus.

   Hinweis: Um zuvor zugewiesene Datenklassifizierungen für ausgewählte Wörterbuchelemente zu löschen, können Sie **Klassifizierung**löschen auswählen.

4. Wählen Sie im Dialogfeld „An Datenklasse zuweisen“ die Datenklassifizierungen aus, die Sie den ausgewählten Wörterbuchelementen zuweisen möchten, und klicken Sie dann auf **Klassifizieren**.

   Warnung: Dadurch werden vorhandene Klassifizierungen für die ausgewählten Wörterbuchelemente überschrieben.

   Sie können nach Bedarf mehrere Datenklassifizierungen auswählen.

   Weitere Informationen finden Sie unter Datenwörterbuchtabellen .

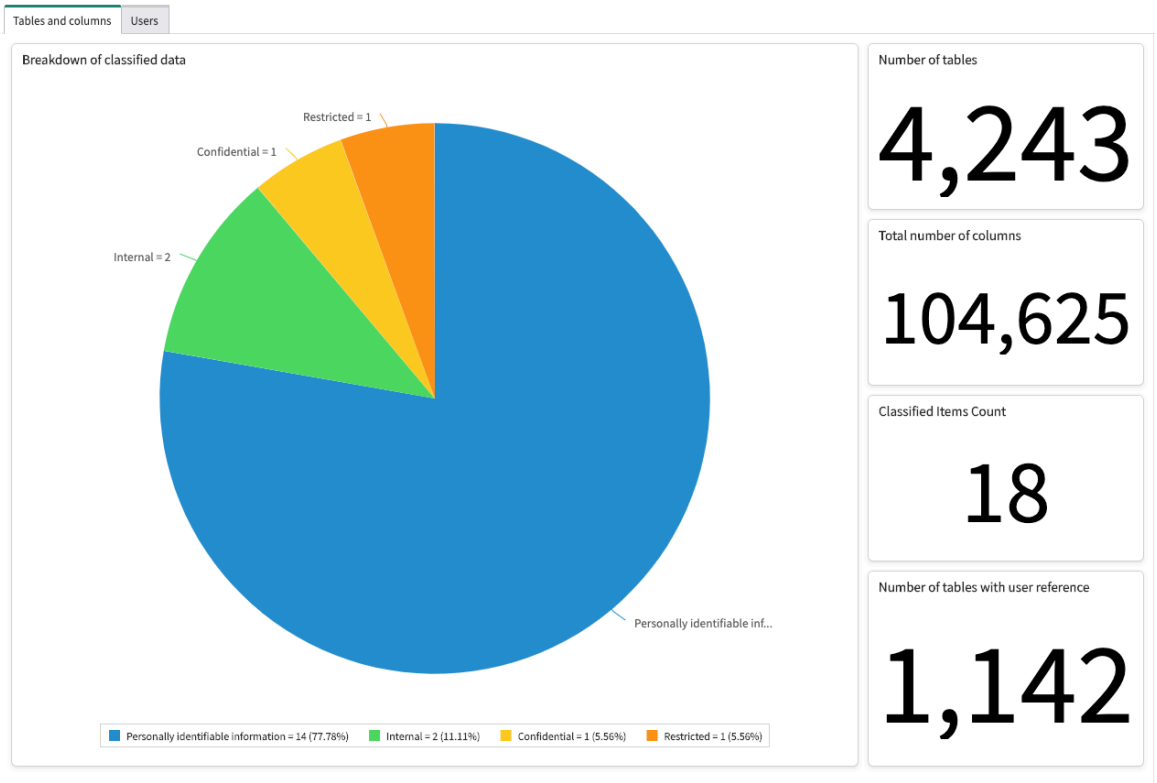
Datenklassifizierungen werden mit dem Übersichts-Dashboard analysiert

Das Dashboard „Übersicht“ informiert Sie über den aktuellen Status der Datenklassifizierungen in Ihrer Instanz und über die Verteilung der Benutzer nach Standort.

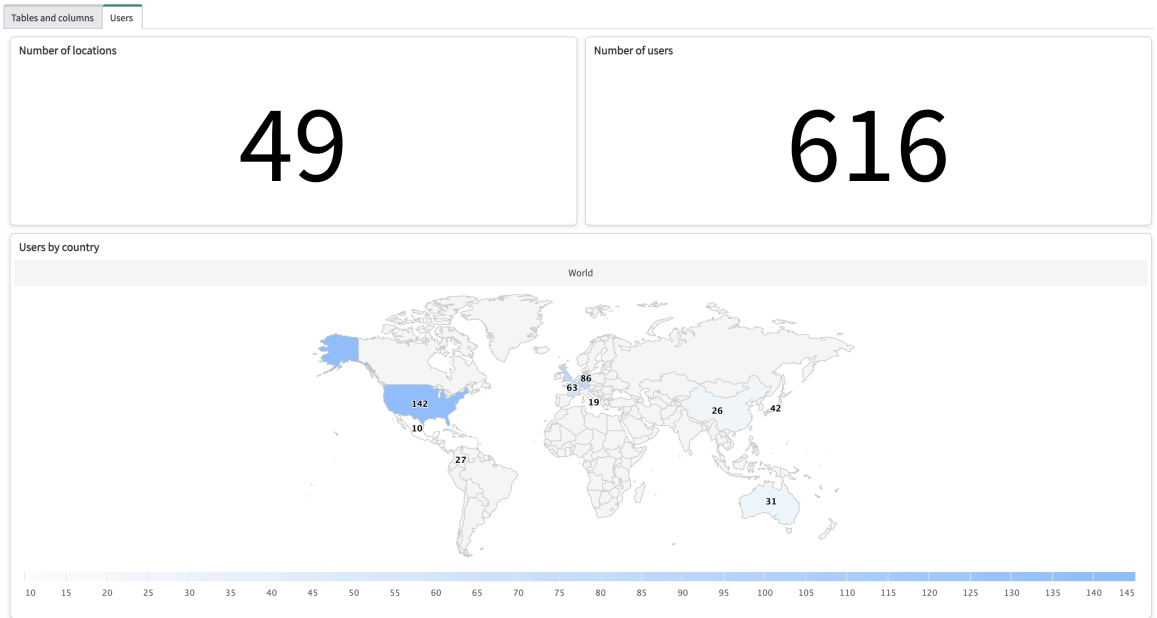
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie die Rolle „Datenklassifizierungsadministrator“ oder „Auditor“ innehaben, können Sie die aktuelle Vertraulichkeit von Instanzdaten visualisieren, was die Sicherheit und Compliance mit Datenschutzgesetzen erhöht. Mithilfe des Felds Standort in Benutzerdatensätzen können Administratoren Benutzer verschiedenen Regionen mit unterschiedlichen Datenschutzbestimmungen zuordnen.

Registerkarte Tabellen und Spalten



Registerkarte „Benutzer“.



Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Now Platform-Rollen

- data_classification_admin: Verwaltet alle Aspekte der Anwendung Data Classification, einschließlich der Einrichtung der Datenklassifizierung und der Zuweisung.
- data_classification_auditor: Audits von Codezuweisungen Data Classification.

Anwendungsfälle

Weitere Beispiele dafür, wie verschiedene Personen in Ihrer Organisation dieses Dashboard verwenden würden, finden Sie unter Anwendungsfälle in Data Classification.

Anwender	Dashboard-Verwendung
data_classification_admin	Vergewissern Sie sich, dass Sie den richtigen Feldern in Ihrer -Instanz Datenklassifizierungen zugewiesen haben.
data_classification_auditor	Überprüft die Senilität und Sicherheit von Daten in Ihrer Instanz.

Berichte

Titel	Typ	Quelltabelle	Beschreibung
Aufgliederung klassifizierter Daten	Ringdiagramm	m2m_dictionary_data_class	Stellt eine Aufgliederung der Instanzdatenklassifizierungen nach Datenklasse bereit, wobei die Gesamtzahl in der Mitte angezeigt wird.
Gesamtanzahl Tabellen	Einzelne Punktzahl	sys_dictionary	Gesamtzahl der Datentabellen im gesamten Wörterbuch.
Gesamtsummenspalten	Einzelne Punktzahl	sys_dictionary	Gesamtzahl der klassifizierten Datenspalten im gesamten Wörterbuch.
Benutzerreferenzspalten	Einzelne Punktzahl	sys_dictionary	Gesamtanzahl der Benutzerreferenzspalten im Wörterbuch.
Anzahl der Anwenderstandorte	Einzelne Punktzahl	sys_user	Gesamtzahl der verschiedenen Standorte, die für Anwender gefunden wurden
Anwenderanzahl	Einzelne Punktzahl	sys_user	Gesamtanzahl der Benutzerdatensätze in Ihrer Instanz.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Quelltabelle	Beschreibung
Anwender nach Land	Karte	sys_user	Aufgliederung der Benutzerdatensätze nach Land.

Domänentrennung und Data Classification

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

Support-Stufe: Erweitert

- Umfasst die Stufen **Basis** und **Standard**.
- Ein datengesteuerter Prozess ermöglicht es Service Provider-Kunden, die Geschäftslogik basierend auf definierten Anwendungsfällen zu ändern. Diese Konfigurationen sind UI-basiert und ausfallsicher, sodass Konfigurationen von einem Kunden sich nicht auf einen anderen auswirken können.
- Mandanten der Instanz müssen die MVP-Geschäftslogik (Minimum des lebensfähigen Produkts) und die Datenparameter für sich selbst konfigurieren können. Diese Logik und diese Parameter würden für die normale Funktion der Anwendung erwartet.

Beispiel-Anwendungsfall: Mandanten-Kunden einer gemeinsam genutzten Umgebung müssen in der Lage sein, Änderungen an der Auswirkungs-, Dringlichkeits- und Prioritätsmatrix vorzunehmen, um die Priorität in ihrer Domäne festzulegen.

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

So funktioniert Domain Separation in Data Classification

Zur Domänentrennung verwendet die Anwendung die Prozesstrennung für die Tabelle Data Classification [sys_data_classification]. Für die Tabelle „Wörterbuch-Datenklasse“ [m2m_dictionary_dataclass] wird Datentrennung verwendet. Weitere Informationen zu Daten- und Prozesstrennung finden Sie unter Domänentrennung erklärt.

Zugehörige Informationen

Domänentrennung für Service Provider

Anonymisierung von Daten

Die Anonymisierung bietet eine Möglichkeit, Daten einfach umzuwandeln, sodass sie nicht identifizierbar sind und den Datenschutzbestimmungen besser entsprechen.

Administratoren können den Anonymisierungsprozess sowohl in Produktionsinstanzen als auch außerhalb der Produktion durchführen. Datenschutz kann in Produktionsinstanzen verwendet werden, um Benutzer zu deidentifizieren. Die Anonymisierung von Datenklassen sollte nur für Nicht-Produktionsinstanzen verwendet werden. Dadurch wird sichergestellt, dass Daten wie E-Mail-Adressen oder physische Adressen durch ähnlich formatierte, aber anonymisierte Versionen ersetzt werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Administratoren können die Anonymisierung auch als Teil ihrer RTBF-Prozesse (Recht auf Vergessenwerden) verwenden, um Anwenderinformationen zu anonymisieren. Weitere Informationen finden Sie unter https://gdpr-info.eu/art-17-gdpr/ .

Verwenden Sie den Anonymisierungsabschnitt des Datenschutzes, um Datenschutzrichtlinien und -techniken zu erstellen und anzuzeigen sowie Massenzuweisungen für Datenschutz durchzuführen. Zeigen Sie alle -Aufgaben mit Beschreibung, verwendeter privater Richtlinie und Status an. Um auf den Anonymisierungsabschnitt zuzugreifen, muss ein Administrator zuerst eine Hochstufung auf die Rollen data_privacy_admin und data_privacy_processor durchführen.

Anonymisierungstechniken

Anonymisierungstechniken sind Optionen, die Sie auswählen, um zu bestimmen, wie Ihre Daten anonymisiert werden. Sie müssen eine Anonymisierungstechnik erstellen, auf die im Anonymisierungsauftrag verwiesen werden soll. Informationen zum Zuordnen einer Datenschutztechnik zu einer zugehörigen **Anonymisierungstechnik-Konfiguration finden**Sie unter Anonymisierungstechniken erstellen.

Anonymisierungsrichtlinien

Konfigurieren Sie eine Anonymisierungsrichtlinie, um anzugeben, welche Datenschutztechniken bei der Anonymisierung Ihrer Daten verwendet werden. Siehe für Details Erstellen Sie Anonymisierungsrichtlinien.

Anonymisierungsaufträge

Anonymisierungsaufgaben verwenden alle diese Komponenten, um Ihre Daten zu anonymisieren. Weitere Informationen zu diesen Aufträgen finden Sie unter Erstellen Sie einen Anonymisierungsauftrag.

Anonymisierungstechniken erstellen

Erstellen Sie eine Konfiguration für die Datenschutztechnik, um anzupassen, wie der Datenschutz Ihre Daten anonymisiert.

Vorbereitungen

Erforderliche Rolle: data_privacy_admin und admin

Prozedur

1. Führen Sie eine Hochstufung auf die Rolle **„data_privacy_admin“ durch**.
   Weitere Informationen zur Erhöhung von Rollen finden Sie unter Auf eine privilegierte Rolle hochstufen.
2. Navigieren zu **Systemsicherheit** > **Datenschutz** > **Anonymisierung**an.
3. Wählen Sie **Techniken anzeigen aus**.
   Es stehen mehrere vordefinierte Techniken zur Auswahl.

Technik	Beschreibung
Selektives Ersetzen	Diese Technik führt ein selektives Ersetzen von Zeichenfolgendaten durch. Alle Zeichen zwischen den Start- und Endindizes der Eingabe werden durch das von Ihnen gewählte Zeichen ersetzt. Sie können Zeichen angeben, die von der Maskierung ausgeschlossen werden sollen:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Technik	Beschreibung
	◦ start_index: Die Technik maskiert Daten ab dem angegebenen Zeichen. Wenn dieses Feld leer gelassen wird, beginnt die Maskierung mit dem ersten Zeichen. ◦ end_index: Die Technik maskiert Daten vom Beginn der Zeichenfolge bis zum angegebenen Zeichen. Wenn dieses Feld leer gelassen wird, endet die Maskierung mit dem letzten Zeichen. ◦ exclude_char: Definieren Sie ein Zeichen, das von der Maskierung ausgeschlossen werden soll. ◦ Ersatz_Zeichen: Definieren Sie ein Zeichen, das für die Maskierung verwendet wird. Wenn keiner angegeben ist, werden standardmäßig Sternchen (*) verwendet.
Statisches Ersetzen	Diese Technik tauscht Werte mit statischen Werten aus. Zeichenfolgen-, Zahlen- und Datumsdaten können diese Technik verwenden: ◦ date_time_value: Ersetzen Sie Datumswerte durch dieses Datum. Verwenden Sie das Format jjjj-MM-tt HH:mm:ss. ◦ date_value: Ersetzen Sie Datumswerte durch dieses Datum. Verwenden Sie das Format jjjj-MM-tt. ◦ number_value: Ersetzen Sie Zahlenwerte durch diese Zahl. ◦ Zeichenfolgenwert: Ersetzen Sie Zeichenfolgenwerte durch diesen Text. ◦ number_type: Akzeptiert eine Ganzzahl
Zufällig ersetzen	Diese Technik tauscht Werte mit zufällig generierten Werten aus. Zeichenfolgen- und Zahlendaten können diese Technik verwenden.
Entfernen	Diese Technik entfernt Werte und ersetzt sie durch leere Werte (null).
Keine Aktion	Diese Technik ist ein Platzhalter. Bei Auswahl werden keine Felder geändert.
Selektives Ersetzen durch X	Transformiert Zeichenfolgendaten und ersetzt vertrauliche Zeichen selektiv durch den Buchstaben X. **Hinweis:** Standardtechnik für Datenmuster in Datenerkennung erkunden.
Anonymisierung von Datenmustern	Anonymisiert nur erkannte Datenmuster in unstrukturierten Datenfeldern, während der zugrunde liegende Kontext intakt bleibt. **Hinweis:** Die Einstellungen für diese Technik beziehen sich auf die Technikeinstellungen für die Anonymisierung von Datenmustern in Datenerkennung erkunden.

4. Wählen **Sie Anwenderdefinierte Technik hinzufügen**, wenn Sie keine vordefinierte Technik verwenden.
5. Füllen Sie die Felder im Formular **„Technik anpassen“** aus.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld1	Beschreibung
Basistechnik	Wählen Sie eine vordefinierte Technik aus, da anwenderdefinierte Techniken auf den vordefinierten Techniken basieren.
Technikname	Geben Sie einen Namen für die Technik ein.
Technikbeschreibung	Geben Sie eine Beschreibung für die Technik ein.

6. Wählen Sie **Weiter**.
7. Geben Sie die Technikparameter ein.
   Die verfügbaren parametrisierten Werte hängen davon ab, welche Datenschutztechnik Sie ausgewählt haben. Es gibt keine parametrisierten Werte für die Techniken **„Keine Aktion“** und „ **Entfernen** “.

Parametrisierte Datenschutzwerte für die Basistechniken

Basistechnik	Parameterwert für Datenschutztechnik	Beschreibung	Standardwert
Selektives Ersetzen	end_index	Die Technik maskiert Daten vom Beginn der Zeichenfolge bis zum angegebenen Zeichen. Wenn es leer gelassen wird, endet die Maskierung mit dem letzten Zeichen.	(leer)
Selektives Ersetzen	„exclude_char“	Zeichen zum Überspringen der Maskierung. In diesem Wert kann nur ein einzelnes Zeichen verwendet werden. Wenn mehrere eingegeben werden, wird das erste Zeichen verwendet.	(leer)
Selektives Ersetzen	„replacement_char“	Zeichen, das beim Ersetzen von Werten durch eine selektive Ersetzung verwendet werden soll.	Wenn kein anderer Wert eingegeben wird, wird ein Sternchen (*****) verwendet.
Selektives Ersetzen	start_index	Die Technik maskiert Daten ab dem angegebenen Zeichen.	Wenn dieses Feld leer gelassen wird, beginnt die Maskierung beim ersten Zeichen.
Statisches Ersetzen	date_time_value	Ersetzen Sie Datums- und Uhrzeitwerte	1988-11-11 10:10:10

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Basistechnik	Parameterwert für Datenschutztechnik	Beschreibung	Standardwert
		durch dieses Datum. Verwenden Sie das Format jjjj-MM-tt HH:mm:ss.	
Statisches Ersetzen	date_value	Ersetzen Sie Datumswerte durch dieses Datum. Verwenden Sie das Format jjjj-MM-tt.	1988-11-11
Statisches Ersetzen	number_value	Ersetzen Sie Zahlenwerte durch diese Zahl.	1234567
Statisches Ersetzen	string_value	Ersetzen Sie Zeichenfolgenwerte durch diesen Text.	TEXT123
Zufällig ersetzen	Konservieren_Daten_Länge	Legen Sie den Wert auf „ **wahr** “ fest, um die Datenlänge beizubehalten. Deidentifizierte Daten haben dieselbe Länge wie die ursprünglichen Daten.	True

8. Wählen **Sie Anwenderdefinierte Technik erstellen aus**.
   Ihre anwenderdefinierte Technik wird den Anonymisierungstechniken hinzugefügt.

Nächste Maßnahme

Informationen zur Konfiguration einer Anonymisierungsrichtlinie und zur Angabe, welche Techniken bei der Anonymisierung Ihrer Daten verwendet werden, finden Sie unter Erstellen Sie Anonymisierungsrichtlinien.

Erstellen Sie Anonymisierungsrichtlinien

Konfigurieren Sie eine Anonymisierungsrichtlinie, um anzugeben, welche Techniken bei der Anonymisierung Ihrer Daten verwendet werden.

Vorbereitungen

Die Datenschutzkonfiguration definiert Tabellen, „sys_user“ und andere, sowie Spalten für die deidentifizierten, je nach Anwendungsfall, und gibt parametrisierte Typen der Techniken an, die bei der Deidentifizierung von Daten verwendet werden sollen.

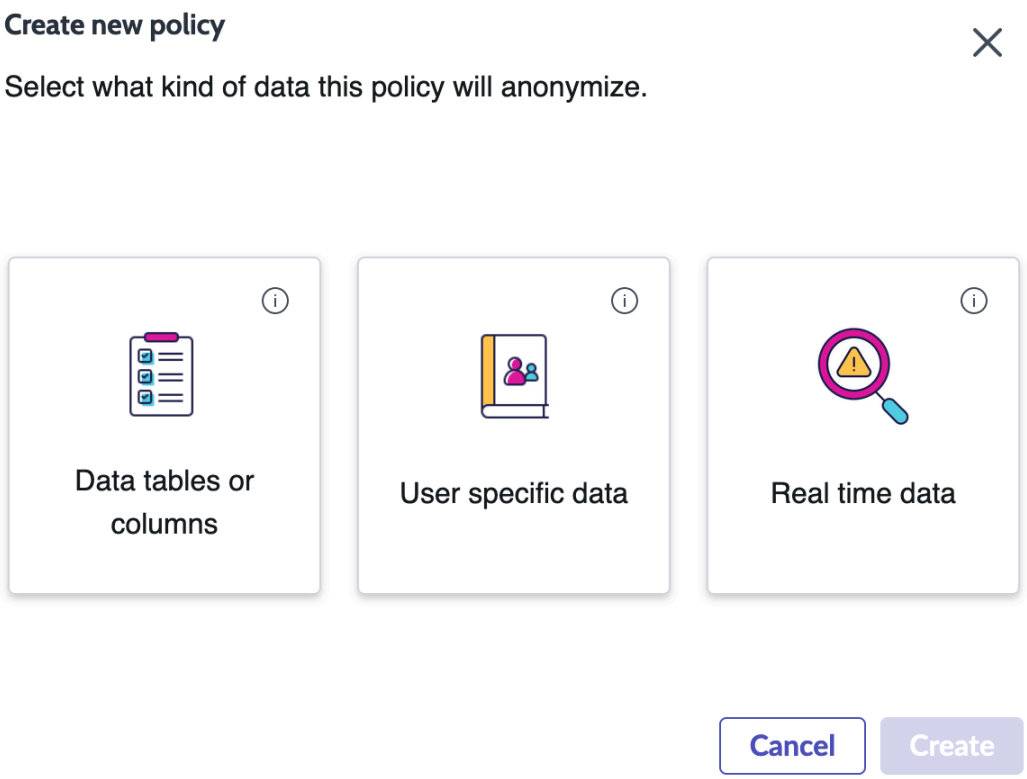
Hinweis: Um eine Datenschutzkonfiguration abzuschließen, müssen Sie zuerst eine Konfiguration für eine Datenschutztechnik konfigurieren. Weitere Informationen finden Sie unter Anonymisierungstechniken erstellen.

Erforderliche Rolle: data_privacy_admin und admin

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Führen Sie eine Hochstufung auf die Rolle **„data_privacy_admin“ durch**.
   Weitere Informationen zur Erhöhung von Rollen finden Sie unter Auf eine privilegierte Rolle hochstufen.
2. Navigieren zu **Systemsicherheit** > **Datenschutz** > **Anonymisierung**an.
   Alle Anonymisierungsrichtlinien werden angezeigt. Veröffentlichte Richtlinien sind verfügbar, um die Anonymisierungsaufgabe zu planen.
3. Wählen **Sie Neue Richtlinie erstellen aus**.
4. Wählen Sie diese Option aus, um entweder **Datentabellen oder -spalten**, **anwenderspezifische Daten**oder **Echtzeitdaten**zu anonymisieren.



Datentyp	Beschreibung
Datentabellen oder -spalten	Datensätze, die der Datenrichtlinie entsprechen, werden anonymisiert.
Bestimmte Anwenderdaten	Wählen Sie einen Satz von Anwendern oder Anwendergruppen aus, die anonymisiert werden sollen.
Echtzeitdaten	Anonymisieren Sie Echtzeiteinträge für eine Reihe von Spalten.

Datenschutzrichtlinien können nur für klassifizierte Daten gelten. Weitere Informationen zur Datenklassifizierung finden Sie unter Datenklassifizierung.

5. Wählen Sie **Erstellen** aus.
   Es sind sequenzielle Schritte erforderlich, um die Richtlinie abzuschließen, **Details zu definieren**und **Techniken zuzuweisen**. Die**Benutzerreferenz** ist auch erforderlich, wenn die Richtlinie für anwenderspezifische Daten definiert wird.

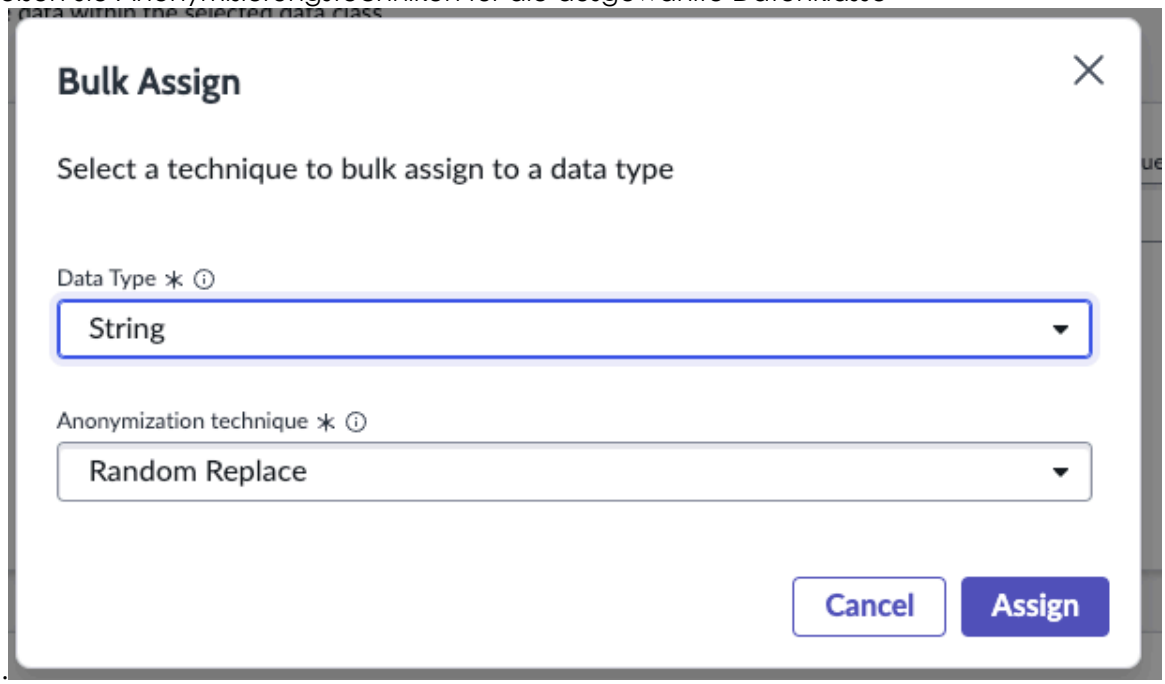
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Definieren Sie die Details für die neue Anonymisierungsrichtlinie.
   - Geben Sie den Richtliniennamen in das Feld **Name** und die Richtlinienbeschreibung in das Feld **Beschreibung** ein.
   - **Wählen** Sie im Feld Datenklasse die Datenklasse aus, die mit dieser Richtlinie verwendet werden soll.

   Hinweis: Wenn Sie einen Eintrag nicht anonymisieren, wählen Sie die **DoNoThing**-Technik, anstatt den Eintrag leer zu lassen. Richtlinien mit leeren Werten im Feld „Konfiguration der Datenschutztechnik“ können nicht ausgeführt werden, wenn sie in Datenschutzaufträgen verwendet werden.

Nach Auswahl einer Datenklasse wird das Formular „Techniken zuweisen“ für jeden Datensatz angezeigt, der für die definierte Datenklasse zurückgegeben wird.

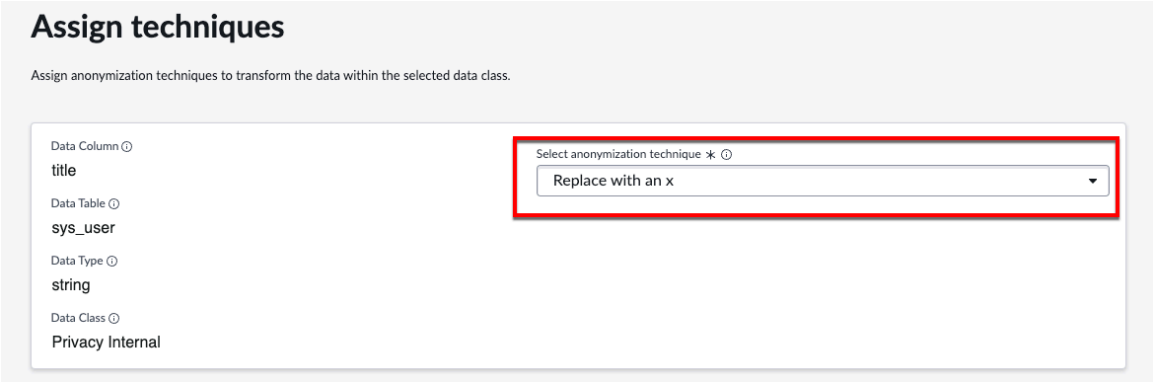
7. Weisen Sie Anonymisierungstechniken für die ausgewählte Datenklasse zu.



Option	Beschreibung
Wählen Sie **Techniken massenweise zuweisen aus**	Wendet die Anonymisierung auf alle Datensätze in der ausgewählten Datenklasse an. Wählen Sie den Datentyp und die Anonymisierungstechnik aus, die auf alle Einträge mit dem ausgewählten Datentyp angewendet werden sollen. Wiederholen Sie diesen Schritt für zusätzliche Massenzuweisungen verschiedener Datentypen. Eine Liste der Datentypen finden Sie unter Unterstützte Feldtypen für die Anonymisierung.
Wählen Sie für jeden Datenspaltendatensatz eine **Anonymisierungstechnik** aus	Die Anwender Ihrer Datenschutzbeauftragten können beim Erstellen von Datenschutzaufträgen auswählen, welche Datensätze anonymisiert werden sollen. Wenden Sie die

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	Anonymisierung einzeln auf jeden Datensatz in der ausgewählten Datenklasse an.



8. Wahlweise: Geben Sie die zu scannenden untergeordneten Tabellen ein. Untergeordnete Tabellen des übergeordneten Elements werden anonymisiert. Wenn eine Tabelle keine untergeordneten Elemente hat, ist diese Option nicht verfügbar.

   Warnung: Ein übergeordneter Auftrag schlägt fehl, wenn ein untergeordneter Auftrag fehlschlägt.

9. Wahlweise: Wenn Anonymisierung von Datenmustern ausgewählt ist, wählen Sie die zu verwendende Anonymisierungstechnik aus.
10. Wahlweise: Legen Sie die Reihenfolge für Datenmuster fest.
11. Wahlweise:

    Tipp: Verwenden Sie die Testfunktion, um Beispieleingaben zu **testen**. Sie können Metriken aus dem Ergebnis wie Scan-Zeit, Ergebnis und erkannte Muster überprüfen.

    Wählen Sie die Schaltfläche **Test** aus, um die Richtlinie zu testen.

12. **Wichtig:** Alle Tabellen müssen einen korrekten sys_dictionary-Eintrag haben.

    Wählen Sie **Speichern**.
13. Wählen Sie **Veröffentlichen** aus, um die Anonymisierungsrichtlinie für die Planung zu aktualisieren und zu Anonymisierungsrichtlinien zurückzukehren.

    Hinweis: Für die Planung von Anonymisierungsaufgaben können nur veröffentlichte Richtlinien verwendet werden.

Nächste Maßnahme
Erstellen Sie einen Anonymisierungsauftrag.

Konfigurieren Sie die Anforderung zum Klonen der Datenanonymisierung

Die Integration des Datenschutzklons wird mithilfe eines PostClone-Skripts konfiguriert, um Datenschutzaufträge für konfigurierte Richtlinien im Ziel zu erstellen und auszuführen. Nach dem Ausführen des Skripts werden Anwendern deidentifizierte Daten angezeigt und sie haben keinen Zugriff auf die ursprünglichen Daten.

Vorbereitungen
Mit der Aktivierung des Plugins „Datenschutz“ (com.glide.data_privacy) wird das Post-Clone-Skript für Datenschutz installiert. Details siehe Aktivieren Sie den Datenschutz.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: data_privacy_clone_processor, data_privacy_admin und admin

Prozedur

1. Aktivieren Sie das Datenschutz-Plugin (com.glide.data_privacy) in der Quellinstanz.
   Das Post-Clone-Skript für Datenschutz wird installiert.
2. Führen Sie eine Hochstufung auf die Rolle **„data_privacy_admin“ durch**.
   Weitere Informationen zur Erhöhung von Rollen finden Sie unter Auf eine privilegierte Rolle hochstufen.
3. Navigieren zu **Systemsicherheit** > **Datenschutz** > **Anonymisierung**an.
4. Wählen **Sie Neue Richtlinie erstellen aus**.
   Details siehe Erstellen Sie Anonymisierungsrichtlinien.
5. Wählen Sie **Datentabellen oder -spalten aus**.
6. Wählen Sie **Erstellen** aus.
7. Geben Sie einen Namen ein, und wählen Sie eine Datenklasse aus.
8. Wählen Sie diese Option, um **die Richtlinie während des Klonens zu aktivieren**.
9. Wählen Sie die auszuführende Richtlinienreihenfolge aus, wenn mehrere Klonrichtlinien vorhanden sind.
   Ein Datenschutzauftrag für die Postclone-Konfiguration mit einem höheren Anwendungsauftrag wird vor einem anderen Auftrag mit niedrigerem Auftrag gestartet, wenn der Auftrag mit dem höheren Auftrag keine Tabelle im Zusammenhang mit einem anderen Auftrag mit niedrigerer Reihenfolge enthält.
10. Wählen Sie **Fortsetzen**.
11. Schließen Sie die Richtlinienkonfiguration ab, und veröffentlichen Sie die Richtlinie.
12. Sichern Sie die Datenschutzkonfigurationen.
13. Planen Sie die Anonymisierungsaufgabe.
    Details siehe Erstellen Sie einen Anonymisierungsauftrag.
14. Senden Sie als Datenschutzadministrator eine Klonanforderung.

Ergebnisse
Das PostClone-Skript für Datenschutz wird in der Zielinstanz ausgeführt, und das PostClone-Skript erstellt in der Zielinstanz einen Verbundauftragsdatensatz für Datenschutz. Die verbundene Aufgabe erstellt einen Datenschutzauftrag für jede Richtlinie nach dem Klonen in der Anwendungsreihenfolge in der Zielinstanz und führt sie aus. Die Sicherungsquelle wird in die Zielinstanz geklont. Das Datenschutz-PostClone-Skript erstellt Datenschutzaufträge für konfigurierte Richtlinien in der Zielinstanz und führt sie aus.

Der Klonprozessor für erhöhte Datenschutz kann sich bei der Zielinstanz anmelden und den Status des Verbundauftrags nach dem Klonen in dp_federated_job.list und dp_job.list überwachen.

Erstellen Sie einen Anonymisierungsauftrag

Konfigurieren Sie einen Datenschutzauftrag in Ihrer Produktionsinstanz, um anonymisierte Daten in Ihrer Instanz außerhalb der Produktion für Anwender- und Datenklassenaufträge zu verwenden.

Vorbereitungen
Der Datenschutzauftrag unterstützt zwei Anwendungsfälle für die Deidentifizierung:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Sensible Daten bestimmter sys_users
- Sensible Daten einer bestimmten Datenklasse.

Erforderliche Rolle: data_privacy_processor und admin

Prozedur

1. Führen Sie eine Hochstufung auf die Rolle **„data_privacy_processor“ durch**.
   Weitere Informationen zur Erhöhung von Rollen finden Sie unter Auf eine privilegierte Rolle hochstufen.
2. Navigieren zu **Systemsicherheit** > **Datenschutz** > **Anonymisierung**an.
3. Wählen Sie in einer Anonymisierungsrichtlinie **Auftrag** planen für die Richtlinie aus, die für den Auftrag verwendet werden soll.
   Eine Richtlinie muss sich im Status „Veröffentlicht“ befinden, um eine Anonymisierungsaufgabe zu planen.

   ⚠ **Warnung:** Anonymisierungsaufgaben sind äußerst destruktiv und können nur bei einem Rollback rückgängig gemacht werden. Überprüfen Sie alle Informationen, z. B. verarbeitete Datensätze und Tabelle, bevor Sie einen Auftrag planen.

4. Füllen Sie die Felder des Formulars aus.

Datenschutz-Auftragsfelder

Feld	Beschreibung
Richtlinie verwendet	Schreibgeschützter Name der ausgewählten Datenschutzrichtlinienkonfiguration, die für diesen Auftrag verwendet werden soll. Bearbeiten Sie die Richtlinie, um zusätzliche Informationen zur Richtlinie anzuzeigen. Ausführliche Informationen zur Konfiguration von Datenschutzrichtlinien finden Sie unter Erstellen Sie Anonymisierungsrichtlinien.
Stellenbeschreibung	Beschreibung des Auftrags.
Startzeit	Der Beginn der Zeit für die Ausführung dieses Auftrags im **Format HH:MM:SS**.
Endzeit	Das Ende des Zeitfensters für die Ausführung dieses Auftrags im **Format HH:MM:SS**. Die Endzeit muss nach der Startzeit liegen. Die Aufgabe wird vor der in diesem Feld eingegebenen Zeit ausgeführt. Wenn der Auftrag noch nicht abgeschlossen wurde, wird er angehalten und beim Start des nächsten Zeitfensters fortgesetzt.
Probelauf	Führen Sie die Aufgabe als Test aus. Von der Ausführung dieses Auftrags sind keine Datensätze betroffen. Ergebnisse werden in

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	der Aufgabenliste so **angezeigt**, als ob der Auftrag ausgeführt worden wäre. **Hinweis:** **Der Probelauf** muss deaktiviert werden, wenn ein Datenschutzauftrag mit Rollback konfiguriert wird. Details siehe Rollback des Datenschutzauftrags.
Art der Anwenderauswahl	Wählen Sie entweder Anwender oder Gruppen aus, die anonymisiert werden sollen.
Wählen Sie Anwender/Gruppen aus	Wählen Sie den spezifischen Satz von Anwendern oder Gruppen aus, die in diesem Auftrag anonymisiert werden sollen. Unterstützt bis zu 1000 Benutzer. **Hinweis:** Dieses Pflichtfeld wird nur angezeigt, wenn die ausgewählte Datenschutzrichtlinienbedingung eine Auswahl von Anwenderdatensätzen erfordert.

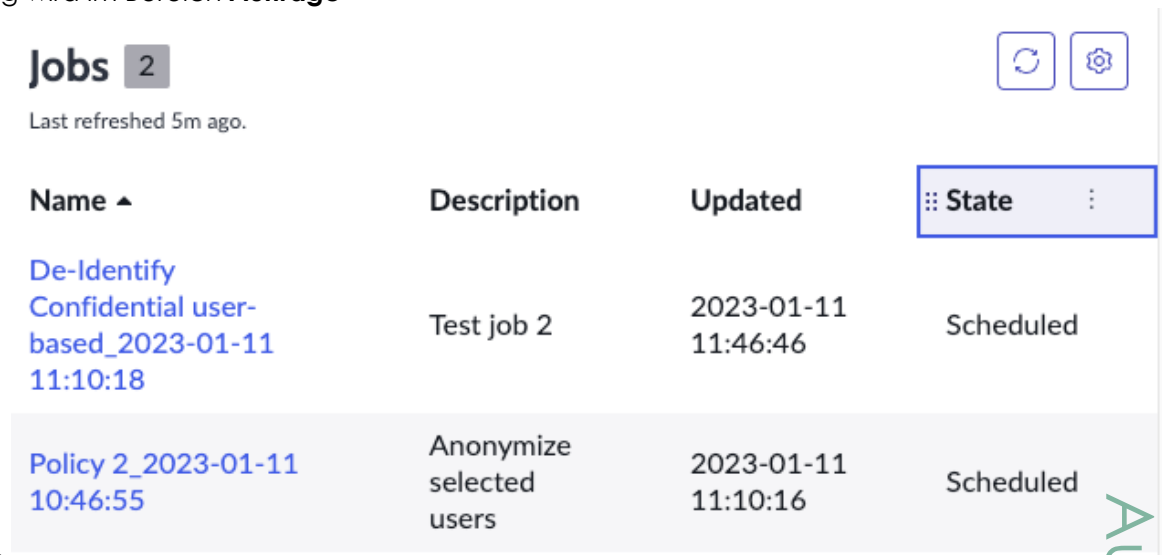
5. **Wichtig:** Alle Tabellen müssen vor der Planung und während ihrer Aufgabe einen korrekten sys_dictionary-Eintrag haben.

Wählen Sie im Formular **Auftrag** planen aus, um die Anonymisierung in die Auftragswarteschlange zu stellen.
Die Aufgabe wird zwischen den Zeiten ausgeführt, die in den Feldern **Startzeit** und **Endzeit** ausgewählt sind. Wenn der Auftrag während des Start- und Endzeitfensters nicht abgeschlossen wurde, wird der Auftrag beim Start des nächsten Zeitfensters fortgesetzt.

Hinweis: Ein Auftrag kann nur einmal ausgeführt werden, auch wenn **Probelauf** ausgewählt ist. Um einen Auftrag basierend auf derselben Richtlinie erneut auszuführen, wählen Sie **Auftrag planen** aus, und füllen Sie das Formular mit denselben Feldwerten aus.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Auftrag wird im Bereich **Aufträge**



aufgeführt.

Feld	Beschreibung
Name	Name des Anonymisierungsauftrags
Beschreibung	Beschreibung des Anonymisierungsauftrags.
Aktualisiert	Datum und Uhrzeit der letzten Aktualisierung des Auftrags.
Status	Status des Datenschutzauftrags: ◦ **Geplant**: Standardstatus für neue Aufträge. ◦ **Abgeschlossen**: Der Auftrag hat die ausgewählten Daten erfolgreich anonymisiert. ◦ **Abgebrochen**: Der Auftrag wurde manuell abgebrochen. ◦ **Fehler**: Beim Speichern des Auftrags ist ein Problem aufgetreten. Planen Sie den Auftrag neu, oder erstellen Sie einen neuen Auftrag. Wenn der Fehler weiterhin besteht, können Probleme mit der Konfiguration auftreten. ◦ **Rollback in Bearbeitung**: Der Auftrag wurde auf ein Rollback der Anonymisierung festgelegt. ◦ **Rollback abgeschlossen**: Das Rollback des Anonymisierungsauftrags wurde erfolgreich abgeschlossen. Ein schreibgeschütztes Feld.

6. Wählen Sie einen Auftrag im Bereich **Aufträge** aus, um die Auftragszusammenfassung zu öffnen.
   Nachdem ein Auftrag geplant wurde, werden in der Auftragszusammenfassung die Schaltflächen Auftrag **abbrechen** und **Pause** angezeigt.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusätzliche Felder für geplante Aufgaben

Feld	Beschreibung
Geschätzte Anzahl der Datensätze	Die geschätzte Anzahl der Datensätze, auf die sich dieser Probelaufauftrag vor der Ausführung auswirkt. Ein schreibgeschütztes Feld
Gesamtzahl der verarbeiteten Datensätze	Die Gesamtzahl der einzelnen Datensätze, die von diesem Auftrag betroffen sind. Ein schreibgeschütztes Feld.
Gesamtzahl der verarbeiteten Datentabellen	Die Gesamtzahl der von diesem Auftrag verarbeiteten Datentabellen. Ein schreibgeschütztes Feld.
Verbleibende Zeit bis zum Rollback	Die verbleibende Zeit, in der ein abgeschlossener Datenanonymisierungsauftrag zurückgesetzt und die Daten deanonymisiert werden können. Ein schreibgeschütztes Feld.
Gesamtanzahl der verarbeiteten Anwender	Die Gesamtzahl der einzelnen Benutzerdatensätze, auf die sich dieser Auftrag auswirkt. Ein schreibgeschütztes Feld.
Auftrag abbrechen	Wählen Sie diese Option, um den Anonymisierungsauftrag abzubrechen. Muss vor der Startzeit des Auftrags ausgewählt werden. Wenn diese Option ausgewählt ist, wird der Auftragsstatus in *Abgebrochen* aktualisiert.
Pause	Wählen Sie diese Option aus, um den Auftrag anzuhalten und die Aufzeichnung rückgängig zu machen, wenn Rollback ausgewählt wurde. Nach einem Ablaufzeitraum von drei Tagen für Rollback-Kontexte wird eine Warnmeldung angezeigt. Muss nach der Startzeit des Auftrags und vor der Endzeit des Auftrags ausgewählt werden. Wenn diese Option ausgewählt ist, wird der Auftragsstatus in *Angehalten* aktualisiert.
Fortfahren	Startet einen angehaltenen Auftrag neu. Rollback wird für fortgesetzte Aufgaben nicht unterstützt, wenn sie angehalten sind. Brechen Sie den Auftrag ab, und erstellen Sie einen Datenschutzauftrag. Die Aufzeichnung verwendet einen nicht abgelaufenen Rollback-Kontext. Wenn diese Option ausgewählt ist, wird der Auftragsstatus in *Geplant* aktualisiert.
Exportieren	Lädt eine PDF-Datei mit Details zur Datenschutzaufgabe herunter.

Aktivieren Sie parallele Aufgaben für die Datenanonymisierung

Verwenden Sie parallele Aufgaben, um die Ausführungszeit des Anonymisierungsauftrags zu verkürzen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur
Datenklassen- und anwenderbasierte Anonymisierungsaufgaben werden standardmäßig mit einem einzelnen Thread ausgeführt. Für datenklassen- und anwenderbasierte Aufgaben können mehrere Threads aktiviert werden. Darüber hinaus verwenden Verbundaufträge, die beim Klonen verwendet werden, standardmäßig parallele Aufträge mit 3 Workern.

1. Geben Sie im Navigationsfilter `sys_properties.list`ein.
2. Erstellen Sie die Eigenschaft `com.glide.data_privacy.max_parallel_workers`
3. Wahlweise: Um die Anzahl der parallelen Mitarbeiter für föderierte Aufträge anzupassen, bearbeiten Sie die Eigenschaft `„dp.max_concurrent_clone_item_workers“`.
4. Vergewissern Sie sich, dass für den **Typ**`Ganzzahl`festgelegt ist.
5. **Wichtig:** Es wird empfohlen, mit einer kleinen Anzahl von Workern pro Knoten (2 oder 3) zu beginnen.

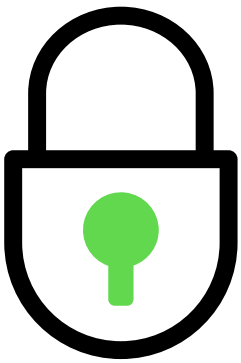
   Geben Sie im Feld **„Wert“** die Anzahl der parallel laufenden Mitarbeiter bis zu 5 ein.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verschlüsselung

Schützen Sie Ihre vertraulichen Daten, und halten Sie die gesetzlichen Anforderungen und Standards ein.

Key Management Framework



Verwenden Sie

Key Management Framework

(KMF), um die Ausführung kryptografischer Vorgänge in Ihrer Instanz von vollständig anzupassen und zu verwalten.

Zertifikate

Verwenden Sie -Zertifikate, um sichere Verbindungen herzustellen und Signaturen zu validieren.

Verschlüsselung auf Spaltenebene

Verwenden Sie die Verschlüsselung auf Spaltenebene (CLE), um den Zugriff auf verschlüsselte Daten basierend auf der Anwenderrolle zuzulassen und zu verweigern. Die Verschlüsselung auf Spaltenebene umfasst die grundlegende Schlüsselverwaltung mithilfe von Verschlüsselungsmodulen.

Column Level Encryption Enterprise

Verwenden Sie die Verschlüsselung auf Spaltenebene (CLE), um den Zugriff auf verschlüsselte Daten basierend auf der Anwenderrolle zuzulassen und zu verweigern. Die Verschlüsselung auf Spaltenebene umfasst die grundlegende Schlüsselverwaltung mithilfe von Verschlüsselungsmodulen.

Cloud-Verschlüsselung

Verschlüsseln Sie Ihre Instanzdatenbank mit Blockverschlüsselung und erweiterter Schlüsselverwaltung.

Platform Encryption-Berechtigungspaket

Führen Sie ein Upgrade auf Verschlüsselung auf Spaltenebene Enterprise, Cloud Encryption oder Database Encryption mit unbegrenzter Nutzung durch.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vollständige Datenträgerverschlüsselung (FDE)	Edge Encryption	Datenbankverschlüsselung
Die Festplattenverschlüsselung verschlüsselt das gesamte Speichersystem nur innerhalb des Datenbankservers. Weil dies die einzige Komponente ist, die Kundendaten speichert.	Verschlüsselt vertrauliche Daten in Ihrem Unternehmen, bevor Daten über das Internet an Ihre ServiceNow-Instanz gesendet werden. Daten im Ruhezustand verbleiben verschlüsselt in der Instanz.	Verschlüsseln Sie alle gespeicherten Daten in Echtzeit, um Online- und Offline-Daten ohne Verlust der Funktionalität zu schützen.

Key Management Framework

Verschlüsselung ist ein kryptografisches Verfahren, das Klartext in Geheimtext konvertiert, um die Offenlegung von Informationen zu steuern.

Übersicht

ServiceNow Die Schlüsselverwaltung umfasst die Aktivitäten im Zusammenhang mit der Handhabung von kryptografischen Schlüsseln und zugehörigen Sicherheitsparametern während des End-to-End-Schlüssellebenszyklus und ist eine effektive Kontrolle basierend auf den 800-57-Richtlinien des National Institute of Standards and Technology (NIST).

Verschlüsselung wird verwendet, um Klartextzeichenfolgen in Geheimtext zu konvertieren, der ohne Zugriff auf den richtigen Schlüssel nicht lesbar ist. Die Sicherheitsvorteile der Verschlüsselung ergeben sich aus der Kombination aus leistungsstarken Algorithmen und hochwertiger Schlüsselverwaltung.

Die Verschlüsselung aller Informationen ist möglicherweise nicht für alle Daten erforderlich und würde die Verarbeitungszeit aufgrund der großen Anzahl von Daten, die für alle Anwendungen unterstützt werden, erheblich erhöhen. Wenn Sie feststellen, dass eine Verschlüsselung von Daten erforderlich ist, sind die folgenden Now Platform -Optionen verfügbar:

Erste Schritte

Key Management Framework (KMF)	Key Management Framework (KMF)	Schlüsselverwaltungsaktionen
	Mit der API/UX (KMF) können Sie die Ausführung kryptografischer Vorgänge in Ihrer Instanz von vollständig anpassen und verwalten.	Sie können kryptografische Schlüssel anzeigen, verwalten und rotieren

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktivierungsinformationen

Das Abonnementpaket ServiceNow Platform Encryption ist eine kommerzielle Gruppenberechtigung, die Verschlüsselung auf Spaltenebene Enterprise, Cloud-Verschlüsselungund Database Encryption enthält.

Verschlüsselung auf Spaltenebene Enterprise ist die unbegrenzte Lizenz von Verschlüsselung auf Spaltenebene. Das Enterprise-Plugin Verschlüsselung auf Spaltenebene ist mit der Aktivierung des Plugins com.glide.now.platform.encryption verfügbar. Weitere Informationen finden Sie unter Abonnementpaket für Verschlüsselung und Schlüsselverwaltung.

Abonnementpaket für Verschlüsselung und Schlüsselverwaltung

Mit der Schlüsselverwaltung wird die Verschlüsselung auf Spaltenebene ohne zusätzliche Kosten auf die hoch konfigurierbaren Verschlüsselungsmodule aktualisiert. Sie haben auch die Möglichkeit, ein Upgrade auf die Lizenz mit unbegrenzter Nutzung durchzuführen. Abonnieren Sie das neue Verschlüsselungsberechtigungspaket Platform Encryption, das Verschlüsselung auf Spaltenebene Enterprise und Cloud-Verschlüsselungenthält.

Funktionen für die Verschlüsselung auf Spaltenebene

Die Verschlüsselung auf Spaltenebene mit Verschlüsselungsmodulen ist in Ihrer Instanz kostenlos enthalten und umfasst die NIST 800-57 -Schlüsselverwaltung, wobei Folgendes unterstützt wird:

- ServiceNow Verwaltete Schlüssel werden unterstützt (vom Kunden bereitgestellte Schlüssel werden nicht unterstützt).
- Der Zugriff auf Verschlüsselungsmodule ist nur rollenbasiert.
- Unbegrenzte manuelle Schlüsselrotation.
- Es können maximal fünf Verschlüsselungsmodule gleichzeitig vorhanden sein.
- Es können maximal fünf Modulzugriffsrichtlinien gleichzeitig vorhanden sein.
- Vorhandene Feldtypen werden unterstützt. (Neue Feldtypen, die in späteren Versionen erstellt wurden, werden in der Nicht-Enterprise-Version nicht unterstützt.)
- API-Unterstützung kann basierend auf dem Rollenzugriff verwendet werden.
- Verschlüsselungsaktionen werden geprüft.
- Guided Tour zur Verschlüsselung auf Spaltenebene.

ServiceNow Funktionen der Plattformverschlüsselungsgruppe

Die Plattformverschlüsselungsgruppe fügt die folgenden Funktionen und Angebote hinzu:

- Column Level Encryption Enterprise:
  - Vom Kunden bereitgestellte Schlüssel.
  - Automatische Schlüsselrotation.
  - Erweiterte Unterstützung für Feldtypen und zukünftige Updates.

    Hinweis: Die erweiterte Unterstützung für Feldtypen umfasst die Feldtypen **Journal**, **Journalliste**, **Journaleingabe**sowie **HTML und Übersetzt (Feld/Text/HTML)**.

  - Erweiterte Unterstützung für Anhänge.
  - Der Zugriff auf das Verschlüsselungsmodul kann mit einer Modulzugriffsrichtlinie auf folgender Grundlage gewährt werden:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

        - Systemanwender
        - Skript
        - Bestimmte Anwendungsbereiche
    - Unbegrenzte Verschlüsselungsmodule und Modulzugriffsrichtlinien.
    - Importieren Sie einen Schlüssel aus einem Webservice.
    - Legen Sie ein zukünftiges Rotationsdatum für Verschlüsselungsschlüssel fest.
- Cloud-Verschlüsselung mit Schlüsselverwaltung.

Zusätzliche Information

Weitere Informationen zur Schlüsselverwaltung finden Sie unter Key Management Framework.

Key Management Framework

Mit der API/UX Key Management Framework (KMF) können Sie die Ausführung kryptografischer Vorgänge in Ihrer Instanz von ServiceNow vollständig anpassen und verwalten. ServiceNow Key Management Framework bietet eine sichere und umfassende Schnittstelle für instanzseitige kryptografische Schlüsselverwaltungsservices.

Gemäß NIST 800-57- Richtlinien bietet KMF die folgenden Funktionen:

- Arbeitsteilung mit dedizierten Rollen für kryptografische Verwaltung und Vorgänge, Audits und Integration
- Kryptografische Module ermöglichen die Konfiguration von kryptografischen Spezifikationen für eindeutige kryptografische Zwecke und Schlüsseltypen
    - Symmetrischer Schlüssel: Verschlüsselung und Entschlüsselung, Packen und Entpacken von Schlüsseln und Authentifizierung
    - Asymmetrischer Schlüssel: Generierung und Verifizierung digitaler Signaturen, Verschlüsselung und Entschlüsselung, Schlüsselumschließung und -entfaltung
- Key Lifecycle Management zum Generieren, Rotieren, Widerrufen und Anhalten von Schlüsseln, einschließlich Unterstützung mehrerer Schlüssellebenszyklusstatus
- Erzwingen von Zugriffskontrollen mit Modulzugriffsrichtlinien, um sicherzustellen, dass Zugriff nur auf die in den Richtlinien konfigurierten kryptografischen Module gewährt wird.
- Schlüsselschutz: Federal Information Processing Standard (FIPS) 140-2-L3 Hardware Root of Trust (RoT), Public Key Infrastructure (PKI), Schlüsselhierarchie und Umschlagverschlüsselung
- Auditing, das Statistiken zur Schlüsselverwendung umfasst

KMF-Aktivierung

KMF ist standardmäßig aktiviert.

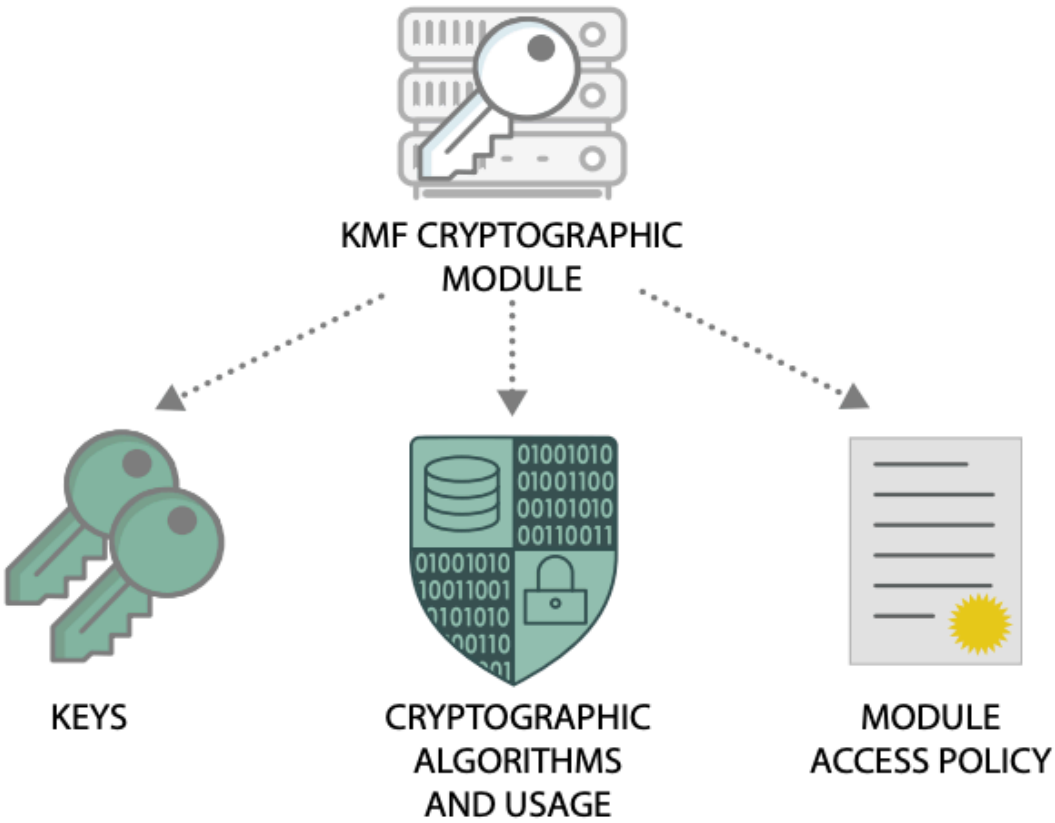
Hinweis: KMF unterstützt keine Domänentrennung, kann jedoch mit lokalen Instanzen verwendet werden.

Funktionsweise von KMF

Diese Grafik zeigt die Komponenten, aus denen KMF besteht:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die kryptografischen Module werden verwendet, um die Verschlüsselungsmethode zu definieren.
- Die kryptografische Spezifikation ist eine Konfiguration, die einen Algorithmus für die Verschlüsselung definiert.
- Mit der Spezifikation können Sie auch den Schlüssel für das Modul, einen ServiceNow -Schlüssel oder Ihren eigenen, vom Kunden bereitgestellten Schlüssel definieren.
- Eine Modulzugriffsrichtlinie ist eine Richtlinie auf Instanzebene, die die Bedingungen steuert, unter denen der Zugriff auf kryptografische Module gewährt oder verweigert wird.



Weitere Informationen zu KMF finden Sie, wenn Sie mit Übersicht über das kryptografische Modulbeginnen.

Das Key Management Framework (KMF) führt bestimmte Rollen für Konfigurationen im Zusammenhang mit kryptografischen Modulen und Schlüsselverwaltung ein. Nur KMF-Administratoren können Anwender anderen KMF-Rollen zuweisen. Weitere Informationen finden Sie unter Mit dem Key Management Framework installierte Rollen.

Weitere Informationen zum Verschlüsselungs-Framework, das der CLE-Nachfolger ist, finden Sie unter Column Level Encryption Enterprise.

Übersicht über das kryptografische Modul

Kryptografische Module sind das Herzstück von (KMF). Sie definieren die spezifischen kryptografischen Mechanismen, die für kryptografische Vorgänge für einen bestimmten Anwendungsfall verwendet werden.

Ein kryptografisches Modul wendet den kryptografischen Mechanismus Ihrer Wahl auf einen von Ihnen definierten Anwendungsfall an. Wenn Sie beispielsweise die Daten in Ihrer HR-

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendung mit einem AES-CBC mit einem symmetrischen 256-Bit-Schlüssel sichern möchten, können Sie zu diesem Zweck ein Modul erstellen.

Kryptografische Module unterstützen auch das Schlüssel-Lebenszyklusmanagement. Sie können Ihre kryptografischen Schlüssel erstellen und rotieren und Ihre Verschlüsselungsmethode definieren. Kryptografische Module bestehen aus den folgenden Komponenten:

Kryptografische Spezifikation

Definiert Aspekte Ihres Moduls, einschließlich seines kryptografischen Zwecks und der zu verwendenden Algorithmen.

Kryptografische Schlüssel

Der Schlüssel, den Ihr Modul zum Codieren oder Decodieren von kryptografischen Daten verwendet. Dies kann ein von Ihrer -Instanz generierter Schlüssel oder ein vom Kunden bereitgestellter Schlüssel sein, den Sie erstellen und hochladen.

Modulzugriffsrichtlinien

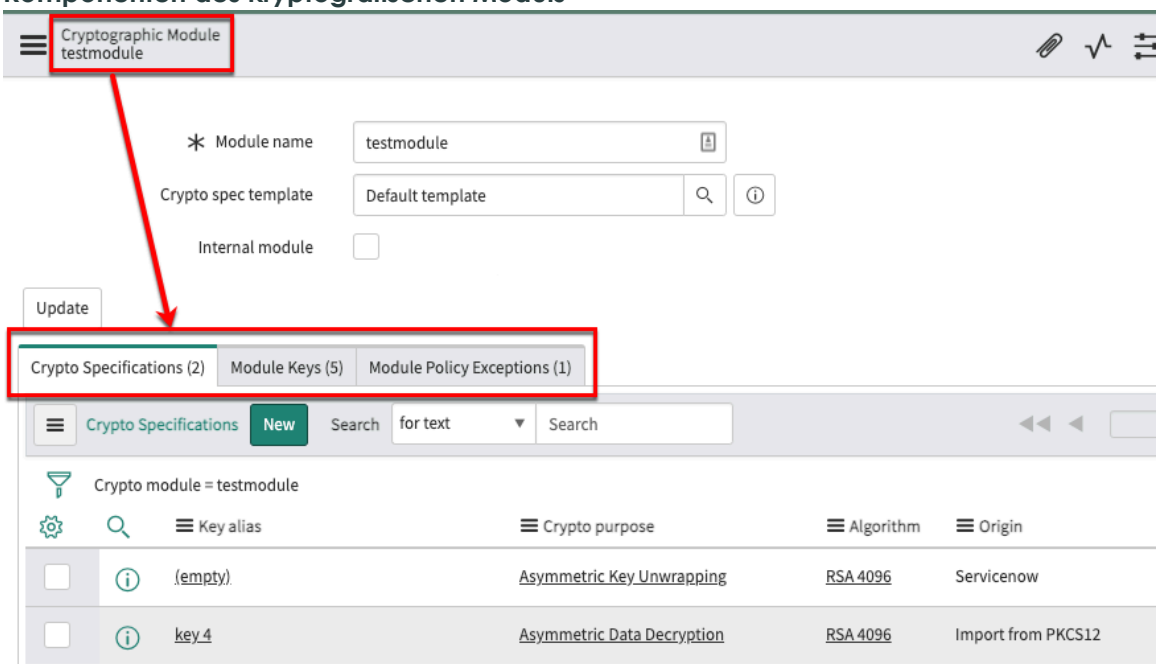
Modulzugriffsrichtlinien sind die Zugriffssteuerungsmechanismen, die einschränken, ob Daten verschlüsselt oder entschlüsselt werden können.

Modulrichtlinienausnahmen

Ein Steuerungsmechanismus zum Definieren von Ausnahmen für eine Modulzugriffsrichtlinie.

Der folgende Bildschirm zeigt diese allgemeinen Komponenten in einem kryptografischen Modul:

Komponenten des kryptografischen Moduls



Einzelheiten zum Erstellen von kryptografischen Modulen finden Sie unter Erstellen Sie ein kryptografisches Modul.

Übersicht über die Modulzugriffsrichtlinien

Modulzugriffsrichtlinien sind die Zugriffssteuerungen, die Sie auf Ihre kryptografischen Module anwenden, um Steuerungen auf Instanzebene zu definieren.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriffsrichtlinien

Modulzugriffsrichtlinien werden mit Key Management Framework (KMF) im Basissystem eingeführt.

Hinweis: Zur Verwendung der Funktion Verschlüsselung auf Spaltenebene Enterprise ist ein Abonnement erforderlich. Weitere Informationen zu [Aktivieren Sie die Verschlüsselung auf Spaltenebene Enterprise finden Sie unter Verschlüsselung auf Spaltenebene Enterprise.

Modulzugriffsrichtlinien sind eine Erweiterung der rollenbasierten Bezeichnungen, die mit den Verschlüsselungsmodulen bereitgestellt wurden. Auf folgenden Elementen können Modulzugriffsrichtlinien basieren:

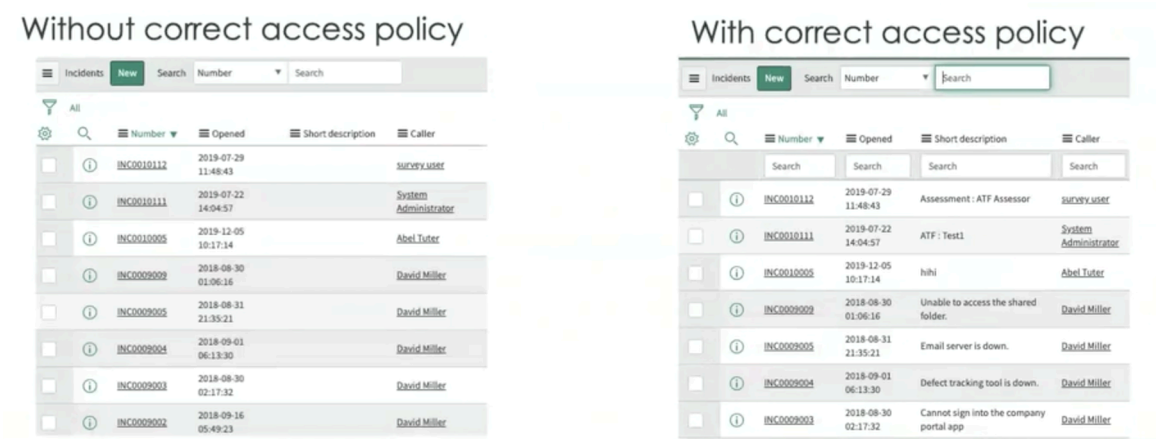
- Standard (Umfang)
- Rolle
- Systemanwender
- Skript
- Ressourcenaustausch

Hinweis: Details siehe Key Management Framework Resource Exchange.

In einem kryptografischen Modul müssen Sie die richtigen Modulzugriffsrichtlinien konfigurieren, um den Zugriff auf verschlüsselte Daten zuzuweisen. Ohne eine Modulzugriffsrichtlinie, die einem kryptografischen Modul zugeordnet ist, sind verschlüsselte Daten für Anwender nicht sichtbar, und die zugehörigen Felder und Spalten in Listen werden leer angezeigt.

In dieser Abbildung verbirgt das Fehlen einer Modulzugriffsrichtlinie im verschlüsselten Feld Kurzbeschreibung den Inhalt für alle Benutzer, die auf die Incident-Tabelle zugreifen. Wenn eine Modulzugriffsrichtlinie vorhanden ist, können Benutzer mit der zulässigen Rolle die verschlüsselten Daten anzeigen.

Verschlüsselte Kurzbeschreibungen mit und ohne Modulzugriffsrichtlinien



Hinweis: Die Daten in der Spalte erscheinen auch für Benutzer leer, ohne die richtige Rolle, die in der Modulzugriffsrichtlinie angegeben ist.

Informationen zum Setup finden Sie unter Erstellen Sie eine Modulzugriffsrichtlinie.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Autogen-Richtlinien

Autogen-Richtlinien werden automatisch vom System basierend auf der standardmäßigen Modulzugriffsrichtlinie generiert, die für das angegebene kryptografische Modul definiert ist. Dies sind Richtlinien auf globaler Ebene, die generiert und angewendet werden, wenn keine Richtlinien auf granularer Ebene definiert sind, wenn das System oder Skript versucht, auf das angegebene kryptografische Modul zuzugreifen.

Wichtig:

Autogen-Richtlinienregeln werden nicht auf geplante Aufgabentypen oder Feldverschlüsselungsmodule (Module, bei denen das übergeordnete Modul die Verschlüsselung auf Spaltenebene ist) angewendet.

Schlüssel auf Instanzebene im Key Management Framework

Die Architektur Key Management Framework (KMF) führt eine Schlüsselstruktur ein, die unter Berücksichtigung der Sicherheit entwickelt wurde. KMF verwendet ein Hardware Security Module (HSM) und nutzt eine Umschlagverschlüsselung, um sicherzustellen, dass alle Plattformschlüssel unter der Verwaltung von KMF durch eine Schlüsselkette geschützt sind. Von KMF erstellte Kundendaten-Verschlüsselungsschlüssel (Customer Data Encryption Keys, CDEKs) sind ebenfalls enthalten.

Auf Instanzebene definiert KMF mehrere Schlüssel, die intern für unterschiedliche kryptografische Zwecke im gesamten Now Platformverwendet werden.

Bei der Umschlagverschlüsselung wird ein Schlüssel mit einem anderen Schlüssel verschlüsselt. Die folgende Abbildung zeigt ein Beispiel für die Umschlagverschlüsselung. Hier werden CDEKs vom IKEK umschlagverschlüsselt, der wiederum vom IRK umschlagverschlüsselt wird, das schließlich vom RK umschlagverschlüsselt wird. Da auf die IRK nur vom HSM zugegriffen werden kann, muss das IKEK zur Entschlüsselung hochgeladen werden.

Diese Tabelle enthält Beispiele für eine Teilmenge der verfügbaren Kunden-/App-Schlüssel, die von KMFverwaltet und geschützt werden.

Key	Standort	Beschreibung
Stammschlüssel (RK)	Hardwaresicherheitsmodell (HSM)	Stammschlüssel, der zum Entschlüsseln der IRK verwendet wird.
Instanz-Stammschlüssel (IRK)	HSM	Ein für Ihre Instanz eindeutiger Schlüssel, der zum Verschlüsseln mehrerer interner Schlüssel der Instanz verwendet wird.
HMAC-Schlüssel der Instanz (IKS)	Instanz	Der pro Instanz eindeutige IIKK wird intern für HMAC-Zwecke (Hash-Based Message Authentication Code) verwendet. Die IKS trägt dazu bei, die Authentizität und Integrität von Modulschlüsseln sicherzustellen, und ist entweder in KeySecure oder

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Key	Standort	Beschreibung
		im Dateischlüsselspeicher enthalten.
Verschlüsselungsschlüssel des Instanzschlüssels (IKEK)	Instanz	Das IKEK umschließt die Modulschlüssel und wird entweder von KeySecure oder dem Dateischlüsselspeicher umschlossen.
Asymmetrischer Verschlüsselungsschlüssel der Instanz (IAEK)	Instanz	Ein für Ihre Instanz eindeutiger Schlüssel, der intern für asymmetrische Verschlüsselungszwecke verwendet wird. IAEK wird verwendet, um vertrauliche Nachrichten zwischen einer Instanz während der Verbrauchergenehmigung für Key Exchange oder Instanzübergreifende Datenreplikation zu übertragen.
Instanzsignaturschlüssel (ISK)	Instanz	Ein für Ihre Instanz eindeutiger Schlüssel, der intern zum Signieren verwendet wird.
Password2 (PW2)	Instanz	Mit KMFwird der Schlüssel für die Felder PW2 vollständig von KMFverwaltet.
Kundendaten-Verschlüsselungsschlüssel (CDEK)	Instanz	Über KMF erstellte Verschlüsselungsschlüssel werden vom IKEK umschlagverschlüsselt.
Datenverschlüsselungsschlüssel der Instanzdatenreplikation (IDR)	Instanz	Spezifische Verschlüsselungsschlüssel, die für den IDR-Prozess verwendet werden.

Kryptografischer Zweck, Algorithmen und Schlüsselinformationen

Kryptografische Spezifikationen können auf einen bestimmten kryptografischen Zweck zugeschnitten werden und decken sowohl asymmetrische als auch symmetrische schlüsselbasierte kryptografische Vorgänge ab. Die Auswahl eines kryptografischen Zwecks bietet weitere Auswahlmöglichkeiten, insbesondere für unterstützte Algorithmen und Schlüssellängenkonfigurationen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kryptografische Zwecke, Algorithmen und Schlüsselinformationen

Kryptografischer Zweck	Algorithmus	Schlüsselinformationen
Asymmetrische Datenentschlüsselung	RSA	Asymmetrisch: 2048-Bit-, 3072-Bit- und 4096-Bit-Schlüssel
Asymmetrische Datenverschlüsselung	RSA	Asymmetrisch: 2048-Bit-, 3072-Bit- und 4096-Bit-Schlüssel
Asymmetrisches Schlüssel-Entpacken	RSA	Asymmetrisch: 2048-Bit-, 3072-Bit- und 4096-Bit-Schlüssel
Asymmetrisches Key Wrapping	RSA	Asymmetrisch: 2048-Bit-, 3072-Bit- und 4096-Bit-Schlüssel
Signaturerzeugung	RSA	Asymmetrisch: 2048-Bit-, 3072-Bit- und 4096-Bit-Schlüssel
Signaturverifizierung	RSA	Asymmetrisch: 2048-Bit-, 3072-Bit- und 4096-Bit-Schlüssel
Symmetrische Authentizität	HMAC	Symmetrisch: 256-Bit-, 384-Bit- und 512-Bit-Schlüssel
Symmetrische Datenverschlüsselung/-entschlüsselung*	AES-CBC *	Symmetrisch: 128-Bit-, 192-Bit-, 256-Bit-Schlüssel
	AES-CFB	
	AES-OFB	
	AES-CTR	
	AES-GCM **	
Umschließen/Entpacken von symmetrischem Schlüssel*	AES-CBC *	Symmetrisch: 128-Bit-, 192-Bit-, 256-Bit-Schlüssel
	AES-CFB	
	AES-OFB	
	AES-CTR	
	AES-GCM **	

* AES-CBC unterstützt Optionen zur Erhaltung der Gleichheit. Verschlüsselung auf Spaltenebene Enterprise nutzt AES-CBC.

** AES-GCM verfügt über eine integrierte Datenintegrität.

Die Konfiguration dieser Parameter wird in Erstellen Sie ein kryptografisches Modulbehandelt.

Schlüssellebenszyklusstatus des Key Management Framework

KMF unterstützt mehrere Lebenszyklusstatus kryptografischer Schlüssel durch die Erzwingung bestimmter zulässiger Aktionen. Beispielsweise können nur Schlüssel, die sich im Status „Aktiv“ befinden, vollständig für ihren beabsichtigten kryptografischen Zweck verwendet werden. Die folgende Tabelle enthält weitere Details zu den verschiedenen Lebenszyklusstatus der Schlüssel.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schlüssel-Lebenszyklusstatus oder Aktion	Beschreibung
Aktiv	In einem kryptografischen Modul kann nur ein aktiver Schlüssel für eine bestimmte kryptografische Spezifikation vorhanden sein.
Gefährdet	In einem kryptografischen Modul können mehrere Schlüssel im Status „Gefährdet“ vorhanden sein, die in einer bestimmten kryptografischen Spezifikation widerrufen werden sollen. Jeder aktive oder angehaltene Schlüssel kann in einen gefährdeten Status verschoben werden. Kompromittierte Schlüssel können nicht zum Generieren neuer Inhalte verwendet werden, z. B. zum Verschlüsseln oder Signieren, sie können jedoch dennoch verwendet werden, um den Zweck vorhandener Inhalte zu identifizieren, z. B. Entschlüsseln oder Verifizieren.
Deaktiviert	Jeder aktive Schlüssel kann deaktiviert werden. Für eine bestimmte kryptografische Spezifikation können in einem kryptografischen Modul mehrere Schlüssel deaktiviert sein. Wenn Sie beispielsweise den Schlüssel drehen, wird der aktuell aktive Schlüssel deaktiviert. Deaktivierte Schlüssel können nicht zum Generieren neuer Inhalte verwendet werden, z. B. zum Verschlüsseln und Signieren, können aber dennoch verwendet werden, um Zwecke vorhandener Inhalte zu identifizieren, z. B. Entschlüsselung oder Überprüfung. **Hinweis:** Gefährdete und widerrufene Schlüssel werden als deaktivierte Schlüssel behandelt.
Zerstört	Wenn ein Schlüssel zerstört wird, wird das Schlüsselmaterial dauerhaft entfernt und kann nicht mehr für kryptografische Zwecke verwendet werden. Jeder deaktivierte Schlüssel kann mithilfe der Lebenszyklusautomatisierung gelöscht werden, wenn er im angegebenen Zeitrahmen nicht verwendet wurde. In einem kryptografischen Modul können sich für eine bestimmte kryptografische Spezifikation mehrere Schlüssel im Status „Gelöscht“ befinden. **Warnung:** Auf die Daten, die einem zerstörten Schlüssel zugeordnet sind, kann nicht mehr zugegriffen werden. Daher ist bei der Ausführung einer Schlüssellöschaktion äußerste Vorsicht geboten.
Generiert	Für eine bestimmte kryptografische Spezifikation können in einem kryptografischen Modul mehrere Schlüssel im generierten Status vorhanden sein. Ein generierter Schlüssel kann in einen aktiven Status verschoben werden, wenn für die angegebene kryptografische Spezifikation kein aktiver Schlüssel vorhanden ist. Der erste generierte Schlüssel wird automatisch auf „Aktiv“ festgelegt. **Hinweis:** Wenn die Option zum Generieren eines neuen Schlüssels besteht, wird ein neuer Schlüssel generiert und aktiviert, obwohl für die angegebene kryptografische Spezifikation Schlüssel im generierten Status vorhanden sind.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

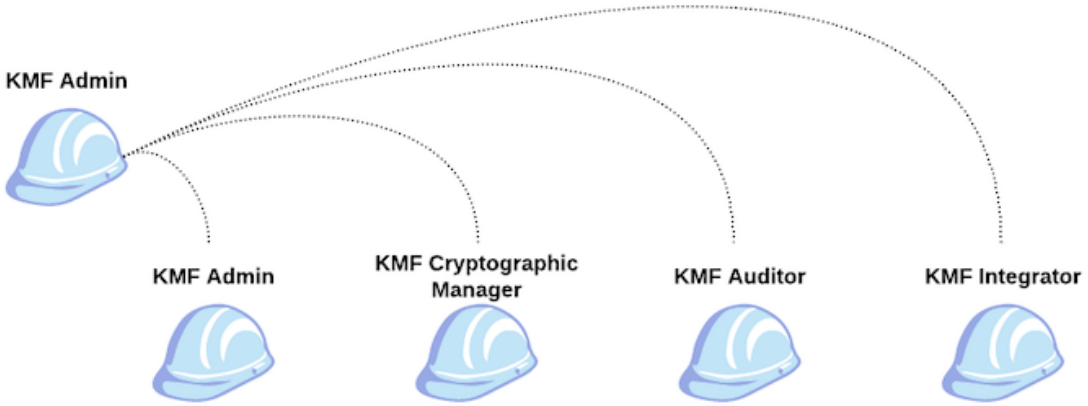
Schlüssel-Lebenszyklusstatus oder Aktion	Beschreibung
Erneuert	Ein aktiver Schlüssel mit einem Ablaufdatum kann beliebig oft verlängert werden, um den Lebenszykluszeitraum des Schlüssels zu verlängern. **Hinweis:** Die Differenz zwischen dem Aktivierungsdatum und dem Ablaufdatum wird berechnet, und das Ablaufdatum wird um diese Dauer vom aktuellen Tag verschoben.
Fortfahren	Die UI-Aktion ist für angehaltene Schlüssel verfügbar, um sie zurück in einen aktiven Status zu versetzen, wenn für die angegebene kryptografische Spezifikation kein anderer aktiver Schlüssel vorhanden ist.
Widerrufen	Jeder aktive oder angehaltene Schlüssel kann in den Status „Widerrufen“ versetzt werden. Widerrufene Schlüssel können nicht zum Generieren neuer Inhalte verwendet werden, z. B. zum Verschlüsseln oder Signieren, sie können jedoch dennoch verwendet werden, um den Zweck vorhandener Inhalte zu identifizieren, z. B. zur Entschlüsselung oder Überprüfung. Für eine bestimmte kryptografische Spezifikation können in einem kryptografischen Modul mehrere Schlüssel im Status „widerrufen“ vorhanden sein.
Rotiert	Die Schlüsselrotation führt dazu, dass der derzeit aktive Schlüssel deaktiviert und ein anderer Schlüssel aktiviert wird. Wählen Sie den neuen aktiven Schlüssel aus den folgenden Optionen aus: • Generieren eines neuen Schlüssels. • Zeigen Sie auf einen vorhandenen importierten Schlüssel. Jeder aktive Schlüssel kann rotiert werden.
Angehalten	Für eine bestimmte kryptografische Spezifikation können sich in einem kryptografischen Modul mehrere Schlüssel im Status „Angehalten“ befinden. Wenn der Schlüssel ausgesetzt ist, kann er fortgesetzt und einem aktiven Status zugewiesen werden, wenn für diese kryptografische Spezifikation kein anderer aktiver Schlüssel vorhanden ist.

Mit dem Key Management Framework installierte Rollen

Mit Key Management Framework (KMF) werden bestimmte Rollen für Konfigurationen im Zusammenhang mit der kryptografischen Modul- und Schlüsselverwaltung eingeführt.

Wichtig: Zum Zuweisen der KMF-Administratorrolle benötigen Sie die Rollen admin, security_admin und sn_kmf_admin. Verwenden Sie die KMF-Administratorrolle, um andere KMF-Rollen zuzuweisen. Weitere Informationen zum Zuweisen von KMF-Rollen finden Sie unter Weisen Sie KMF Rollen zu.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



KMF-Administrator [sn_kmf.admin]

Weist anderen Anwendern Rollen zu, um Vorgänge rund um ServiceNow Key Management Frameworkauszuführen.

Enthält die Rollen

Liste der Rollen, die in der Rolle enthalten sind.

Keine.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Besondere Überlegungen

Wichtig: Vermeiden Sie das Gewähren einer Administratorrolle, wenn spezialisiertere Rollen verfügbar sind.

- Diese Rolle wird über den in Weisen Sie KMF Rollen zugezeigten Prozess zugewiesen.
- Sie müssen über diese Rolle verfügen, um KMF-Rollen zuzuweisen. Darüber hinaus können Sie alle Funktionen des kryptografischen KMF-Managers ausführen.

Kryptografischer KMF-Manager [sn_kmf.cryptographic_manager]

Erstellungs-, Lese- und Aktualisierungsvorgänge für kryptografische Module (Zuordnung von Schlüsseln zu kryptografischer Nutzung und Algorithmuskonfigurationen) und Modulzugriffsrichtlinien. Außerdem können KMF-Kryptografiemanager Schlüsselverwaltungsvorgänge (generieren, rotieren, widerrufen) und Lebenszyklusvorgänge durchführen.

Enthält die Rollen

Liste der Rollen, die in der Rolle enthalten sind.

Keine.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Keine.

Besondere Überlegungen

Keine.

Kryptografischer KMF-Prüfer [sn_kmf.cryptographic_auditor]

Zeigen Sie Informationen zu kryptografischen Modulen, Schlüsselmetadaten und Details zum Lebenszyklus sowie Informationen zu Modulzugriffsrichtlinien (Module Access Policy, MAP) an.

Enthält die Rollen

Liste der Rollen, die in der Rolle enthalten sind.

Keine.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Besondere Überlegungen

Keine.

Kryptografischer KMF-Integrator [sn_kmf.cryptographic_integrator]

Integrieren Sie Key Management Framework mit externen Schlüsselspeichern oder Systemen.

Enthält die Rollen

Liste der Rollen, die in der Rolle enthalten sind.

Keine.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Besondere Überlegungen

Keine.

Kryptografischer KMF-Operator [sn_kmf.cryptographic_operator]

Auf Teil des ServiceNow Key Management Framework -Schlüssellebenszyklus zugreifen: Erneuerung, Rotation, Widerruf.

Enthält die Rollen

Liste der Rollen, die in der Rolle enthalten sind.

Keine.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Besondere Überlegungen

Keine.

Weisen Sie KMF Rollen zu

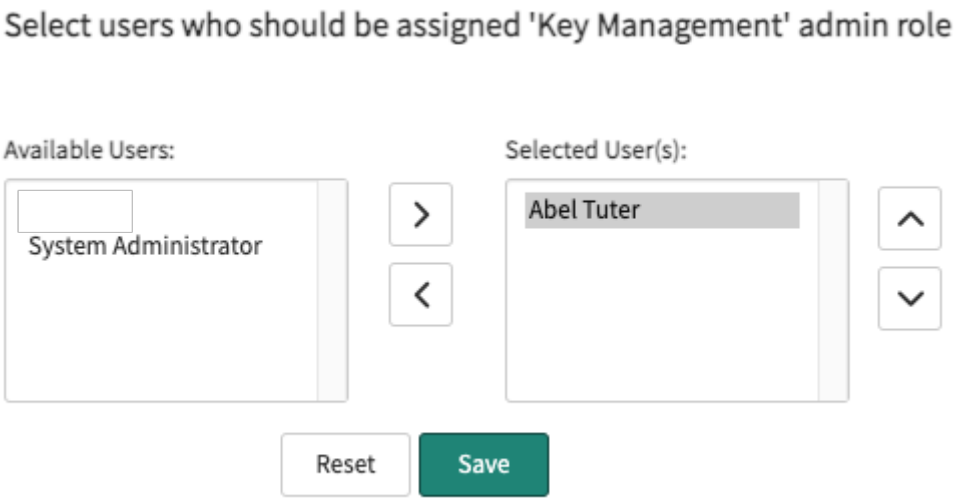
Weisen Sie Administratoren KMF -Rollen zu, die wiederum andere KMF -Rollen zuweisen können.

Vorbereitungen
Erforderliche Rolle: admin und security_admin

Sie müssen auf die Rolle security_admin hochstufen, bevor Sie die Administratorrolle KMF zuweisen. Anweisungen hierzu finden Sie unter Auf eine privilegierte Rolle hochstufen

Prozedur

1. Erhöhen Sie auf die Sicherheitsadministratorrolle.
2. Navigieren zu **Anwenderadministration** > **Anwender** und wählen Sie den Benutzer aus, der der KMF -Administrator sein soll.
3. Vergewissern Sie sich, dass der Benutzer bereits über die Rollen admin und security_admin verfügt.
   Wenn nicht, wählen Sie **Bearbeiten** in der zugehörigen Liste Rollen, und fügen Sie **admin** und **security _admin hinzu**.
4. Navigieren zu **Systemsicherheit** > **Administration der Schlüsselverwaltung**an.
5. KMF Wählen Sie in der Spalte **Verfügbare Benutzer** den Benutzer aus, der Administrator sein soll, und verschieben Sie ihn in die Spalte **Ausgewählte Benutzer**.

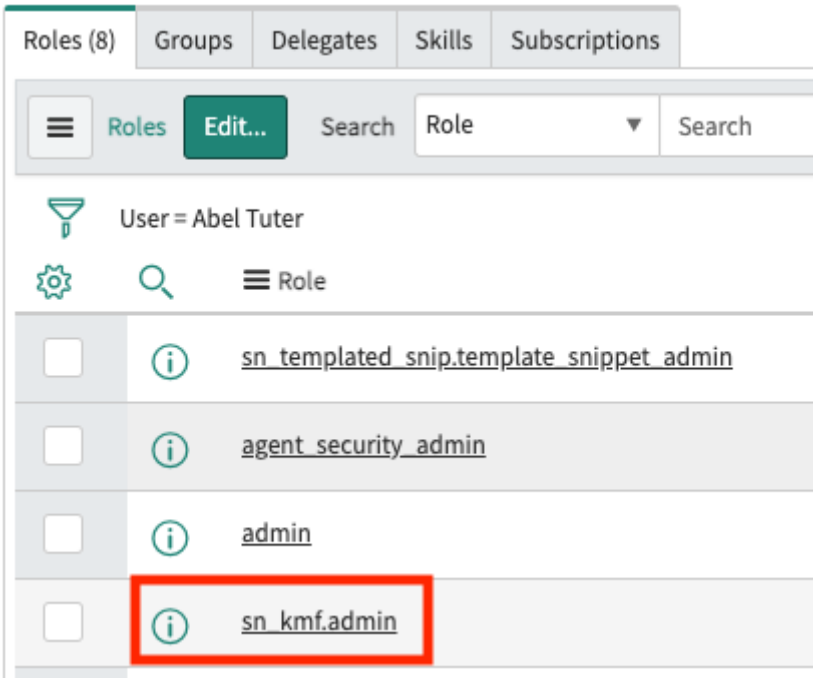


6. Wählen Sie **Speichern**.
7. Navigieren zu **Anwenderadministration** > **Anwender** und wählen Sie den Benutzer aus, dem Sie gerade die Rolle sn_kmf.admin zugewiesen haben.

Automatische Übersetzung

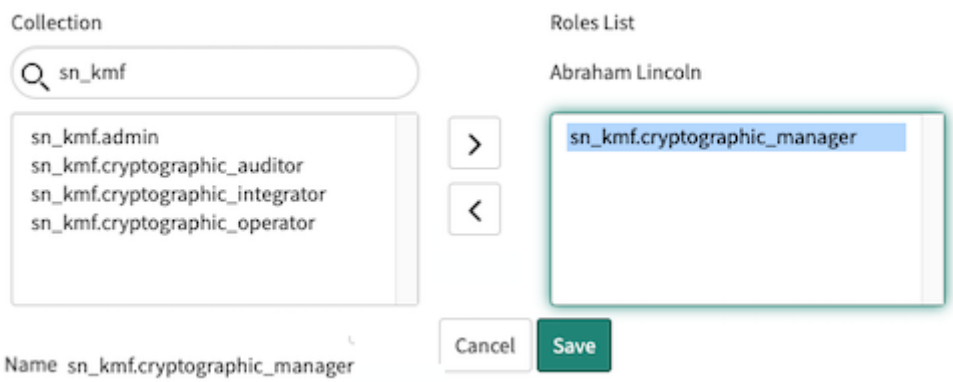
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Benutzer hat die Rolle sn_kmf.admin in der zugehörigen Liste „ **Rollen** “ und kann andere KMF-Rollen zuweisen.



Nächste Maßnahme
Wenn Sie über die KMF-Administratorrolle verfügen, führen Sie die folgenden Schritte aus, um andere KMF-Rollen zuzuweisen:

1. Navigieren zu **Anwenderadministration** > **Anwender** und wählen Sie den Benutzer aus, dem Sie eine andere KMF-Rolle zuweisen möchten, z. B. KMF Kryptografischer Manager.
2. Wählen Sie in der zugehörigen Liste „Rollen“ **Bearbeiten** aus, und wählen Sie die KMF-Rollen aus, die Sie den Anwendern zuweisen möchten. Alle KMF-Rollen beginnen mit `sn_kmf`.



Konfigurieren Sie die Feldverschlüsselungseinstellungen, um den Schlüsseltyp auszuwählen

Konfigurieren Sie Ihre Feldverschlüsselungseinstellungen so, dass von ServiceNow bereitgestellte Schlüssel oder Ihre eigenen vom Kunden bereitgestellten Schlüssel (CSK) für die Verschlüsselung auf der Now Platform verwendet werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

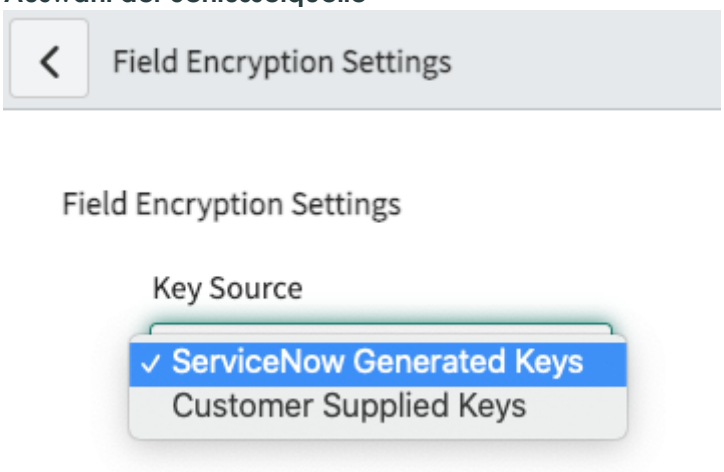
Vom Kunden bereitgestellte Schlüssel werden nur mit Verschlüsselung auf Spaltenebene Enterpriseunterstützt.

Erforderliche Rolle: sn_kmf.cryptographic_manager und security_admin

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Einstellungen für Feldverschlüsselung**an.
2. Wählen Sie in den Feldverschlüsselungseinstellungen entweder Von **ServiceNow generierte Schlüssel** oder Vom **Kunden bereitgestellte Schlüsselaus**.

Auswahl der Schlüsselquelle



Diese Option ändert die Eigenschaft `com.glide.encryption.cle_kmf.key_source` entweder in von **ServiceNow generierte Schlüssel** oder in vom **Kunden bereitgestellte Schlüssel**.

3. Wählen Sie **Speichern**.

Nächste Maßnahme

- Wenn Sie eigene, von Kunden bereitgestellte Schlüssel verwenden, finden Sie weitere Informationen unter Verwendung von vom Kunden bereitgestellten Schlüsseln mit Verschlüsselung auf Spaltenebene Enterprise.
- Wenn Sie die von ServiceNow bereitgestellten Schlüssel verwenden, beginnen Sie mit der Erstellung Ihres kryptografischen Moduls. Weitere Informationen finden Sie unter Erstellen Sie ein kryptografisches Modul.

Erstellen Sie ein kryptografisches Modul

Erstellen Sie ein kryptografisches Modul, um die für kryptografische Vorgänge verwendeten Mechanismen zu definieren. Nachdem Sie das Modul erstellt haben, erstellen Sie eine kryptografische Spezifikation, in der Sie einen Algorithmus für die Verschlüsselung definieren und einen Schlüssel generieren.

Vorbereitungen

Wenn Sie Ihre eigenen Schlüssel bereitstellen, wechseln Sie zu Konfigurieren Sie den von Ihrem Kunden bereitgestellten Schlüssel, und laden Sie ihn hoch.

Erforderliche Rolle: sn_kmf.cryptographic_manager

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Dieses Verfahren beschreibt Optionen, die mit KMF im Basissystem der Plattform ServiceNow verfügbar sind. Die Funktionalität Verschlüsselung auf Spaltenebene Enterprise ist nur verfügbar, wenn das Plugin `„com.glide.now.platform.encryption"` aktiv ist. Unter Aktivieren Sie die Verschlüsselung auf Spaltenebene Enterprise finden Sie weitere Informationen zum Abrufen von Verschlüsselung auf Spaltenebene Enterprise. Weitere Informationen finden Sie unter Erstellen Sie ein kryptografisches Modul für die Verschlüsselung auf Spaltenebene.

Hinweis: Datensätze für das kryptografische Modul [sys_kmf_crypto_module] können nicht gelöscht werden.

Prozedur

1. Navigieren zu **Alle** > **Schlüsselverwaltung** > **Kryptografische Module** > **Neu erstellen:**an.
2. Füllen Sie die Felder des Formulars aus.

Felder des kryptografischen Moduls

Feld	Beschreibung
Modulname	Alphanumerische Zeichenfolge, auf die beim Ausführen von Skripts verwiesen werden soll.
Krypto-Spezifikationsvorlage	Wählen Sie die **Standardvorlage** aus, die zum Erstellen des kryptografischen Moduls verwendet werden soll, da sie Zuordnungen unterstützter Algorithmen für Krypto-Spezifikationen enthält.
Standardwert der Modulzugriffsrichtlinie	◦ Systemstandard verwenden: ◦ Ablehnen ◦ Titel
Tatsächliches Ergebnis der Modulzugriffsrichtlinie	Ablehnen oder basierend auf dem Standardrichtlinienwert oder dem bei der Erstellung der Modulzugriffsrichtlinie ausgewählten Wert nachverfolgen.
Name	Krypto-Modulname, dem der Name des Anwendungsbereichs vorangestellt wird.
Lebenszyklusstatus des Krypto-Moduls	Der Lebenszyklus bezieht sich auf die Erstellung, Verwendung und Deaktivierung eines kryptografischen Moduls. Legen Sie die Option während der Konfiguration zunächst auf **Entwurf** fest. Wenn Sie das -Modul verwenden, legen Sie dieses Feld auf **Veröffentlicht**fest. Die Standardvorlage wird automatisch auf Veröffentlicht gesetzt.

3. Wählen Sie **Absenden**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

⚠ Warnung:

Für Benutzer mit Unterstützung der Legacy-Verschlüsselung:

Wenn Sie die Nicht-Enterprise-Version von Verschlüsselung auf Spaltenebene verwenden, sind Sie auf fünf Module beschränkt. Wenn Sie diese Grenze überschritten haben, erhalten Sie die folgende Warnung:

Diese Einfügung überschreitet den Grenzwert für die Anzahl von veröffentlichten Modulen für die Verschlüsselung auf Spaltenebene, der für das Abonnementprodukt berechtigt ist. Für zusätzliche Module ist das Enterprise-Abonnement für die Verschlüsselung auf Spaltenebene erforderlich. Wenden Sie sich an Ihr Account-Team.

Nach der erfolgreichen Übermittlung wird Ihr kryptografisches Modul in der Tabelle „Kryptografische Module“ aufgeführt. Das System stellt dem Namen den Bereich voran, um Konflikte mit anderen bereichsbezogenen Anwendungen zu vermeiden. Wenn Sie beispielsweise ein Modul mit dem Namen `my_crypto_module` im globalen Anwendungsbereich erstellt haben, wird der Name als `global.my_crypto_module gespeichert`.

Nächste Maßnahme

Erstellen Sie eine kryptografische Spezifikation

an.

Erstellen Sie eine kryptografische Spezifikation

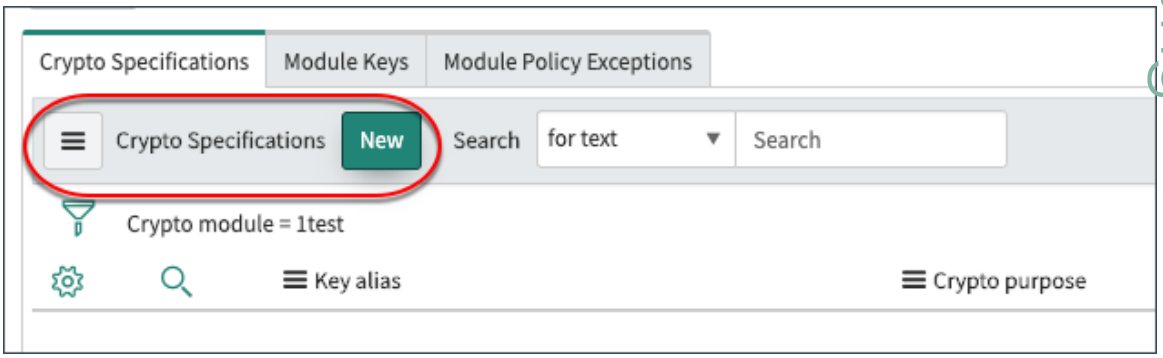
Nachdem Sie ein kryptografisches Modul erstellt haben, erstellen Sie eine kryptografische Spezifikation, um die Modulalgorithmen zu definieren.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_manager

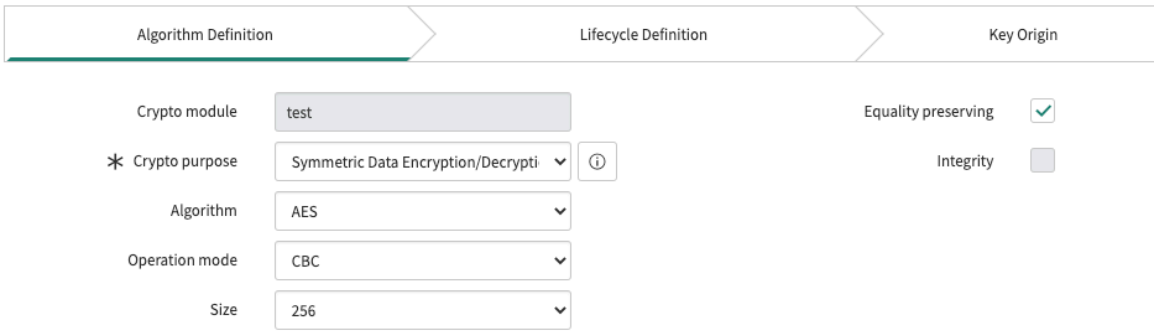
Prozedur

1. Navigieren zu **Schlüsselverwaltung** > **Kryptografische Module** > **Alle**an.
2. Wählen Sie das zu definierende kryptografische Modul aus, um die Konfigurationsoptionen zu öffnen.
3. Klicken Sie auf der Registerkarte **Krypto-Spezifikationen** auf **Neu**.



4. Füllen Sie das Formular „Algorithmusdefinition“ aus.
   Details siehe Kryptografischer Zweck, Algorithmen und Schlüsselinformationen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Der Bildschirm zur Definition des Algorithmus wird geöffnet. Wählen Sie Optionen für die Schlüsselgenerierung aus. Wiederholen Sie diesen Schritt, um mehrere Schlüssel für das ausgewählte Krypto-Modul zu generieren.

Algorithmus-Definitionsfelder

Feld	
Crypto-Modul	Schreibgeschützt. Der Name des ausgewählten kryptografischen Moduls wird angezeigt.
Kryptografischer Zweck	Wählen Sie den Zweck dieses Moduls aus. Sie können es beispielsweise für Datenverschlüsselung, Signaturgenerierung oder Key Wrapping verwenden. Die verfügbaren Algorithmen werden basierend auf dem ausgewählten Krypto-Zweck angepasst. Details siehe Kryptografischer Zweck, Algorithmen und Schlüsselinformationen.
Algorithmus	Typ des Algorithmus, der zum Erreichen des Krypto-Zwecks verwendet wird. Der Algorithmus steuert auch den Schlüsselursprung. Wird automatisch basierend auf dem ausgewählten Krypto-Zweck angepasst. Kryptografischer Zweck, Algorithmen und Schlüsselinformationen für Details.
Betriebsmodus	Dieses Feld kann basierend auf dem ausgewählten Krypto-Zweck angezeigt werden.
Größe	Wählen Sie die Bitgröße aus.
Hash	Dieses Feld wird basierend auf dem ausgewählten Algorithmus verfügbar.
Gleichstellungserhaltung	Aktiviert die nicht deterministische Verschlüsselung. Diese Option wird angezeigt, wenn Sie „ **Symmetrische Datenverschlüsselung/-**

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	
	entschlüsselung mit **AES** " und im Modus **„Cipher Block Chaining" (CBC)** auswählen. Wenn Sie diese Option auswählen, sind die codierten Daten jedes Mal dieselben, wenn dieselben Daten erneut verschlüsselt werden. Die nicht deterministische Verschlüsselung unterstützt das Filtern einer Liste verschlüsselter Daten mit Gleichheitsvergleichsoperatoren nicht.
Integrität	Der GCM-Betriebsmodus stellt Integrität bereit.

5. Klicken Sie auf **Next (Weiter)**.
   Die Krypto-Spezifikation wird in der Tabelle „Schlüssellebenszyklus" basierend auf den ausgewählten Algorithmen aufgeführt.

Nächste Maßnahme
Führen Sie einen der folgenden Vorgänge aus:

- Wählen Sie einen Eintrag in der Tabelle „Schlüssellebenszyklus" aus, um das Verhalten des Schlüssellebenszyklus zu definieren. Unter Wichtige Lebenszyklusstatus konfigurieren finden Sie Details zum Abschließen der Lebenszyklusdefinition für den Schlüssel.
- Klicken Sie auf **Weiter**, um einen kryptografischen Schlüssel zu erstellen. Sehen Sie sich eine der folgenden Aufgaben für die Schlüsselgenerierung an:
  - Generieren Sie einen kryptografischen ServiceNow-Schlüssel.
  - Konfigurieren Sie Eigenschaften für vom Kunden bereitgestellte Schlüssel.
  - Importieren Sie das Schlüsselpaar zum Packen/Entpacken.

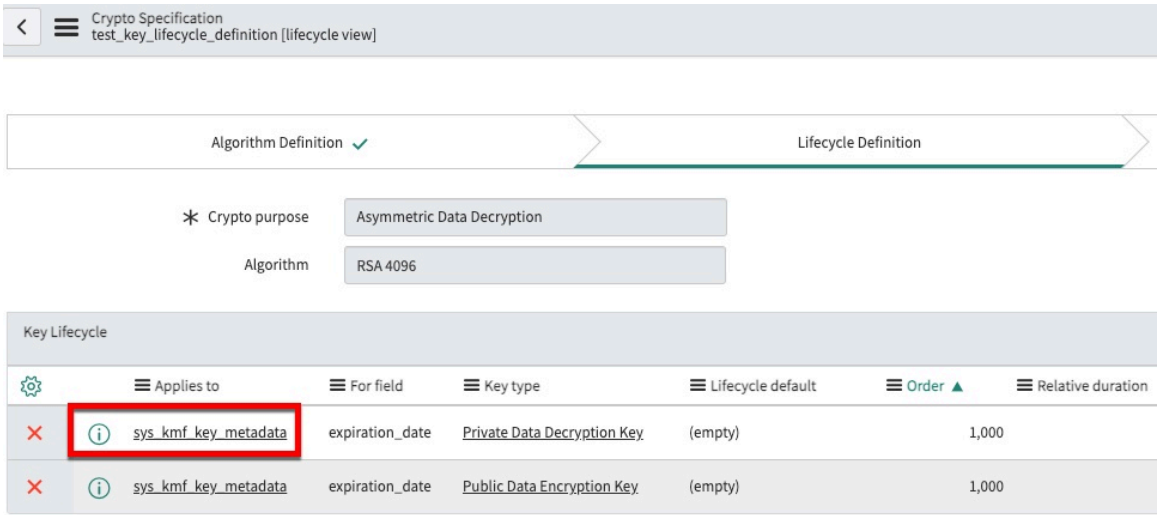
Wichtige Lebenszyklusstatus konfigurieren

Nachdem Sie eine kryptografische Spezifikation erstellt haben, können Sie die Lebenszyklusaktionen für die Schlüssel in Ihrer Instanz konfigurieren.

Vorbereitungen
Erforderliche Rolle: sn_kmf.admin

Prozedur
1. Navigieren zu **Schlüsselverwaltung** > **Kryptografische Module** > **Alle**an.
2. Wählen Sie das kryptografische Modul aus, um den Lebenszyklus eines Schlüssels zu konfigurieren.
3. Klicken Sie auf der Registerkarte Krypto-Spezifikationen auf einen Schlüssel-Alias.
   Das Formular „Algorithmusdefinition" wird für den ausgewählten Schlüssel geöffnet.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

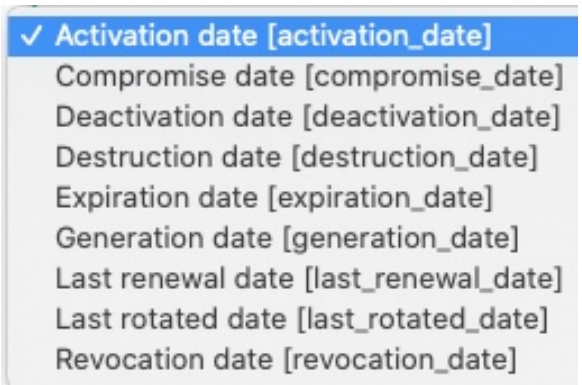


4. Klicken Sie auf **Next (Weiter)**.
   Die Feldlebenszyklus-Vorlage wird geladen. Standardwerte für den Schlüssellebenszyklus werden basierend auf den ausgewählten Algorithmen für die definierte Krypto-Spezifikation erstellt.
5. Wählen Sie im Schritt „Lebenszyklusdefinition“ für die Krypto-Spezifikation in der Spalte **Gilt für** einen Schlüssellebenszyklus aus.

Schlüssellebenszyklus-Felder

Feld	Beschreibung
Betrifft	Ausgewählter Schlüssel, für den der Lebenszyklus gilt.
Für Feld	Wählen Sie die Art der Kontrolle für den Schlüssel aus, für den der Lebenszyklus gilt. **Werte für „Für Feld“ von Key Lifecycle Management** * For field ✓ Expiration date [expiration_date] Future activation date [future_activation_date] Future destruction date [future_destruction_date] Future renewal date [future_renewal_date] Future rotation date [future_rotation_date]
Typ	Wählen Sie aus, ob die Bewertung für den Schlüssellebenszyklus ein relativer Wert oder ein absoluter Wert ist: ◦ **Relativ**: Geben Sie einen Wert ein, der von anderen Dateneinträgen im System abhängt, z. B. Schlüsselgenerierung, Aktivierung und Deaktivierung. ◦ **Absolut**: Geben Sie einen genauen Wert ein, z. B. ein Datum.
Lebenszyklusstandard	Schreibgeschützt. Zeigt einen Wert an, wenn festgelegt.
Bestellung	Geben Sie die Reihenfolge ein, in der der Schlüssellebenszyklusstatus für die Krypto-Spezifikation verarbeitet werden soll.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Typ relative Dauer	Dauer des Lebenszyklus: **Jahre**, **Monate**oder **Tage**.
Relative Dauer	Anzahl der Jahre, Monate oder Tage, die der Schlüssel gültig ist.
Relativer Betrieb	**Vor**oder **nach**.
Relativ zu	Feld, zu dem die Dauer relativ ist. Wird angezeigt, wenn eine relative Dauer oder ein Vorgang ausgewählt ist. 

Generieren Sie einen kryptografischen ServiceNow-Schlüssel

Befolgen Sie dieses Verfahren, um einen kryptografischen Schlüssel ServiceNow zum Verschlüsseln vertraulicher Daten hochzuladen und zu konfigurieren.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_manager

Warum und wann dieser Vorgang ausgeführt wird

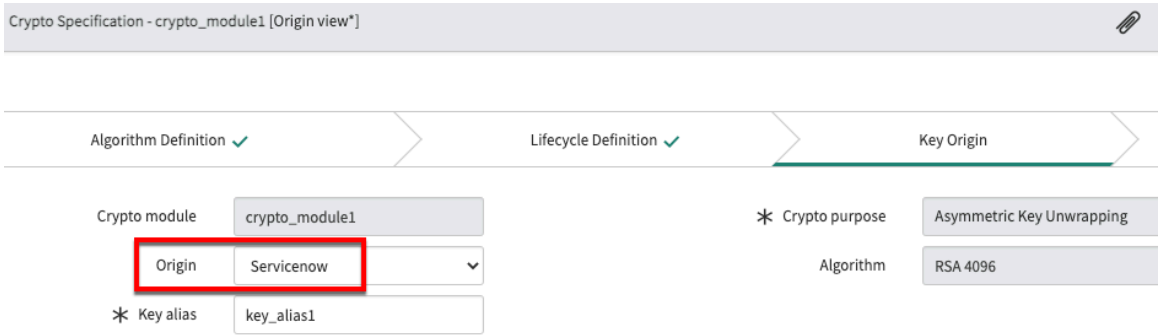
Kryptografische Manager haben die Wahl, ob von ServiceNow bereitgestellte Schlüssel oder ihre eigenen vom Kunden bereitgestellten Schlüssel (CSK) für die Verschlüsselung auf dem Now Platform mit Verschlüsselung auf Spaltenebene Enterpriseverwendet werden. Informationen zu CSK finden Sie unter Konfigurieren Sie Eigenschaften für vom Kunden bereitgestellte Schlüssel.

Prozedur

1. Legen Sie die Feldverschlüsselungseinstellungen so fest, dass von ServiceNow generierte Schlüssel verwendet werden. Details siehe Konfigurieren Sie die Feldverschlüsselungseinstellungen, um den Schlüsseltyp auszuwählen.
2. Navigieren zu **Schlüsselverwaltung** > **Kryptografische Module** > **Alle**an.
3. Wählen Sie das entsprechende Krypto-Modul aus, um die Seite mit den Details des kryptografischen Moduls zu öffnen.
4. Klicken Sie auf die Zeile für den Schlüsselalias-Eintrag auf der Registerkarte Krypto-Spezifikationen.
   Wenn noch kein Schlüssel generiert wurde, ist das Feld „Schlüsselalias“ leer.
5. Klicken Sie auf **Weiter**, um zur Registerkarte Schlüsselursprung der Komponenten Krypto-Spezifikation zu navigieren.
   Die Registerkarte Lebenszyklusdefinition wird zusammen mit der Tabelle Schlüssellebenszyklus angezeigt und kann überprüft oder bearbeitet werden. Details siehe Wichtige Lebenszyklusstatus konfigurieren.

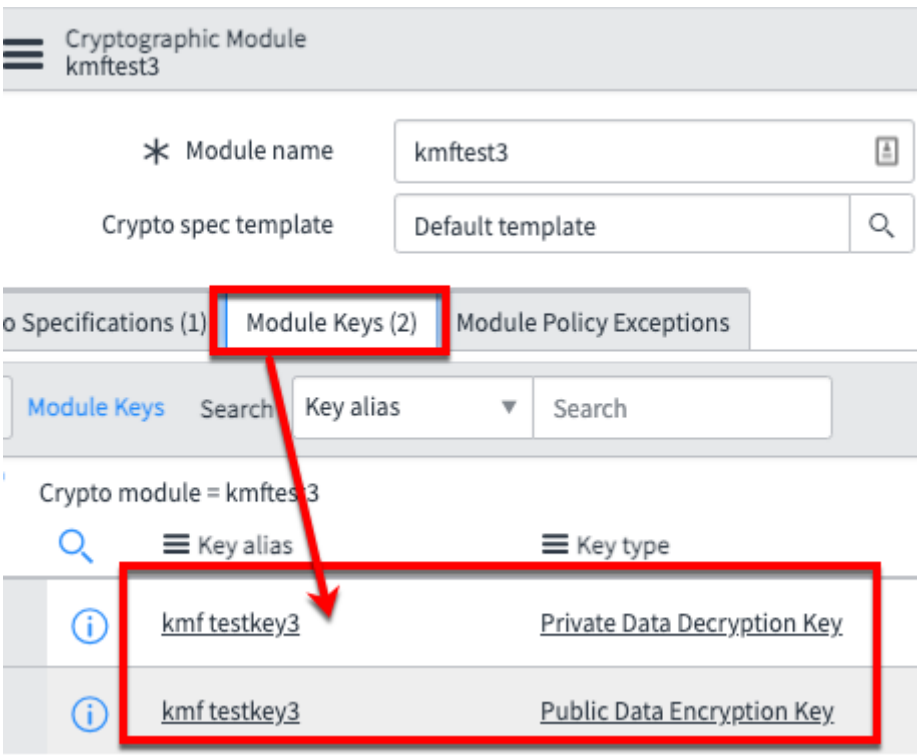
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Wählen Sie **ServiceNow** im Feld Herkunft



aus.
Dieses Feld variiert je nach den Feldverschlüsselungseinstellungen aus Schritt 1 und dem ausgewählten Algorithmus. Informationen zur Verwendung eines importierten Schlüssels finden Sie unter Importieren Sie das Schlüsselpaar zum Packen/Entpacken. Weitere Informationen finden Sie unter Konfigurieren Sie Eigenschaften für vom Kunden bereitgestellte Schlüssel, wenn Sie einen eigenen Schlüssel verwenden.

7. Geben Sie einen Anzeigenamen für den Schlüsselalias ein.
8. Klicken Sie auf **Weiter**, um zur Registerkarte Schlüsselerstellung zu wechseln.
9. Klicken Sie auf **Schlüssel generieren**.
   Nachdem Sie den Schlüssel generiert haben, wird das Formular „Kryptografisches Modul“ neu geladen und zeigt die Krypto-Spezifikation an.
10. Klicken Sie auf die Registerkarte Modulschlüssel, um die **Schlüssel** anzuzeigen.
    Sichere Informationen für den Schlüssel werden auf der Registerkarte „Modulschlüssel“ zusammen mit der Anzahl der Schlüssel gespeichert, die für die Krypto-Spezifikation vorhanden sind.



11. Wählen Sie einen Schlüssel aus, um Schlüsselverwaltungsaktionen auszuführen. Details siehe Aktionen der Schlüsselverwaltung.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie eine Modulzugriffsrichtlinie

Erstellen Sie Modulzugriffsrichtlinien, um die Verschlüsselung oder Entschlüsselung von Daten einzuschränken.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_manager oder sn_kmf.admin

Warum und wann dieser Vorgang ausgeführt wird

Die Verschlüsselung auf Spaltenebene (CLE) unterstützt rollenbasierte Modulzugriffsrichtlinien, und zusätzliche Konfigurationsoptionen werden mit der Funktionalität von (CLE_Ent) verfügbar.

- Konfigurieren Sie den spezifischen kryptografischen Vorgang in Modulzugriffsrichtlinien für kryptografische Module, die symmetrische Vorgänge unterstützen. Beispielsweise kann einem Benutzer erlaubt werden, Daten zu verschlüsseln, aber nicht zu entschlüsseln.
- Legen Sie einen Standardwert für die Modulzugriffsrichtlinie pro oder kryptografischem Modul fest.
- Ordnen Sie Skriptversionen zu, in denen Änderungen am Skript nachverfolgt werden, und machen Sie die Skriptrichtlinie ungültig, um die Sicherheit für Modulzugriffsrichtlinien vom Typ Skript zu verbessern.

CLE_Ent -Funktionen sind mit einem kostenpflichtigen Abonnement verfügbar. Informationen zu den unterstützten Funktionen und Optionen, die für die einzelnen Angebote verfügbar sind, finden Sie unter. Weitere Informationen finden Sie unter Verschlüsselung auf Spaltenebene Enterprise.

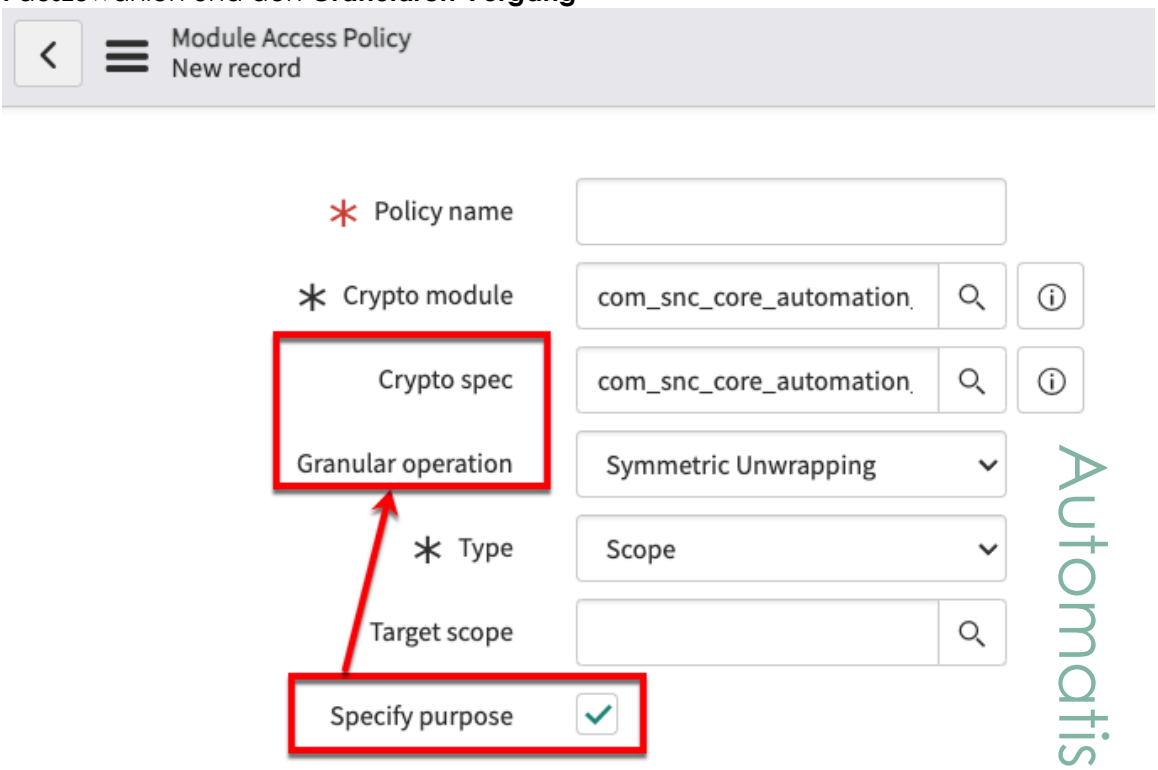
Hinweis: Das Standardverhalten der Modulzugriffsrichtlinien (Module Access Policies, MAPs) ist Ablehnen, um jeden nicht autorisierten Zugriff zu verhindern, sofern dies nicht ausdrücklich in den MAP-Datensätzen angegeben wurde.

Prozedur

1. Navigieren zu **Alle** > **Schlüsselverwaltung** > **Modulzugriffsrichtlinien** > **Alle**.
   Wenn Sie kein kryptografisches Modul erstellen, das für die symmetrische Datenverschlüsselung/-entschlüsselung konfiguriert ist, wird eine automatisch generierte Modulzugriffsrichtlinie erstellt und in der Tabelle aufgeführt.
2. Klicken Sie auf **Neu**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

◦ Wählen Sie **Zweck angeben** aus, um eine **Krypto-Spezifikation** auszuwählen und den **Granularen Vorgang**



festzulegen.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

◦ Mit den kryptografischen Spezifikationen für symmetrische Datenverschlüsselung/-entschlüsselung und symmetrisches Packen/Entpacken ist das Feld **Granularer Vorgang** verfügbar, wenn Sie das Kontrollkästchen **Zweck** angeben aktivieren.



3. Füllen Sie das Formular aus.

Felder „Modulzugriffsrichtlinien“

Feld	Beschreibung
Richtlinienname	Geben Sie einen Namen für die Richtlinie ein.
Crypto-Modul	Klicken Sie auf das Suchsymbol ( ), um ein Modul auszuwählen.
Krypto-Spezifikation	Wählen Sie eine neue kryptografische Spezifikation aus, oder erstellen Sie eine neue, während Sie die Modulzugriffsrichtlinie generieren. Dieses Feld wird verfügbar, wenn das Kontrollkästchen **Zweck** angeben aktiviert ist.
Granularer Vorgang	Wählen Sie den kryptografischen Zweck für die kryptografische Spezifikation aus. Die verfügbaren Werte hängen vom Typ der ausgewählten kryptografischen Spezifikation ab. Weitere Informationen zu Krypto-Zwecken finden Sie unter.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Typ	◦ **Bereich**: Steuert den Zugriff nach Anwendungsbereich. ◦ **Systemanwender**: Ermöglicht Systemanwendern den Zugriff auf Krypto-Module. ◦ **Skript**: Steuerung des Zugriffs nach Skript. Weitere Informationen finden Sie unter ◦ **Rolle**: Steuert den Zugriff nach Anwenderrolle. ◦ **Ressourcenaustausch**: Steuern Sie den Zugriff mit Ressourcenaustausch. Weitere Informationen finden Sie unter . **Hinweis:** Nur der Rollentyp wird mit der Verschlüsselung auf Spaltenebene unterstützt. Alle anderen Typen sind mit Verschlüsselung auf Spaltenebene Enterpriseverfügbar.
Zielbereich	Feld ist als Bezeichner für den **Umfangstyp** sichtbar. Bezieht sich auf die Funktionalität für die Richtlinie. Wählen Sie die Anwendungen aus dem Suchmenü aus. **Hinweis:** Der Zielbereich wird nicht unterstützt und kann nur mit festgelegt werden Verschlüsselung auf Spaltenebene Enterprise
Zielrolle	Das Feld ist als Bezeichner für den **Rollentyp** sichtbar. Rolle, für die diese Richtlinie gilt.
Skripttabelle Zielskript	Diese Felder werden angezeigt, wenn Sie **Skript** als Typ auswählen. Feld ist als Bezeichner für den **Skripttyp** sichtbar. Wählen Sie eine Tabelle aus, für die diese Richtlinie gilt. Dokument, für das diese Richtlinie gilt. Wählen Sie den **Tabellennamen** und dann das zugehörige Dokument für die Richtlinie aus. Wenn ein Skript ein kryptografisches Modul zum ersten Mal aufruft, wird der Zugriff auf das Modul verweigert, und der Entwickler erhält eine Fehlermeldung. Dieser Fehler gibt dem Modulbesitzer die Möglichkeit, den Zugriff auf das Modul zu gewähren oder zu verweigern.
Ressourcenaustausch: ◦ Krypto-Spezifikation ◦ Genehmigungstyp ◦ Zielinstanz-Host	Diese Optionen werden angezeigt, wenn Sie als Typ auswählen. Ressourcenaustausch wird sowohl von KMF als auch von unterstützt, wenn das übergeordnete Modul **column_level_encryption**ist. Wählen Sie die Krypto-Spezifikation, „Einmalig“ oder „Wiederkehrend“ und die URL der Zielinstanz aus. Weitere Informationen finden Sie unter .

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Identitätswechsel	In rollenbasierten Modulzugriffsrichtlinien können Benutzer mithilfe einer Identitätswechselsitzung auf verschlüsselte Daten zugreifen. Wenn Benutzer, z. B. Administratoren, die Identität anderer Benutzer annehmen, werden diese Modulzugriffsrichtlinien mit aktivierter Identität angewendet.
Zweck angeben	Wählen Sie diese Option aus, um das Feld Krypto-Spezifikation als verfügbares Feld für die Richtlinie umzuschalten.
Aktiv	Wählen Sie diese Option aus, um die Richtlinie zu aktivieren.
Ergebnis	Wählen Sie eine der folgenden Optionen aus: ◦ **StrictReject** lehnt den Zugriff unter allen Umständen ab. ◦ **Ablehnen** weist Anwender mit der **Zielrolle** oder dem **Zielbereich** zurück, auf dieses kryptografische Modul zuzugreifen, es sei denn, eine andere Richtlinie gewährt ihnen Zugriff. ◦ **Verfolgen Sie**, um den Zugriff zuzulassen und die Verwendung des Moduls zu überwachen.

4. Wählen Sie **Absenden**.

Warnung:

Für Benutzer mit Unterstützung der Legacy-Verschlüsselung:

Wenn Sie die Nicht-Enterprise-Version von Verschlüsselung auf Spaltenebene verwenden, sind Sie auf fünf Module beschränkt. Wenn Sie diese Grenze überschritten haben, erhalten Sie die folgende Warnung:

Diese Einfügung überschreitet den Grenzwert für die Anzahl von veröffentlichten Modulen für die Verschlüsselung auf Spaltenebene, der für das Abonnementprodukt berechtigt ist. Für zusätzliche Module ist das Enterprise-Abonnement für die Verschlüsselung auf Spaltenebene erforderlich. Wenden Sie sich an Ihr Account-Team.

5. Wählen Sie den Richtliniennamen aus, der dem kryptografischen Modul zugeordnet ist, das Sie untersuchen möchten.
Verwenden der Modulzugriffsrichtlinie vom Typ „Skript“:

Eine Modulzugriffsrichtlinie wird basierend auf der Standardzugriffseinstellung automatisch generiert, wenn das Skript ausgeführt wird. Dem Modulnamen wird `AutoGen-` vorangestellt. Beispielsweise wird das `Modul Module-TestPolicy` als `AutoGen-Module-TestPolicy` in der Spalte Richtlinienname aufgeführt.

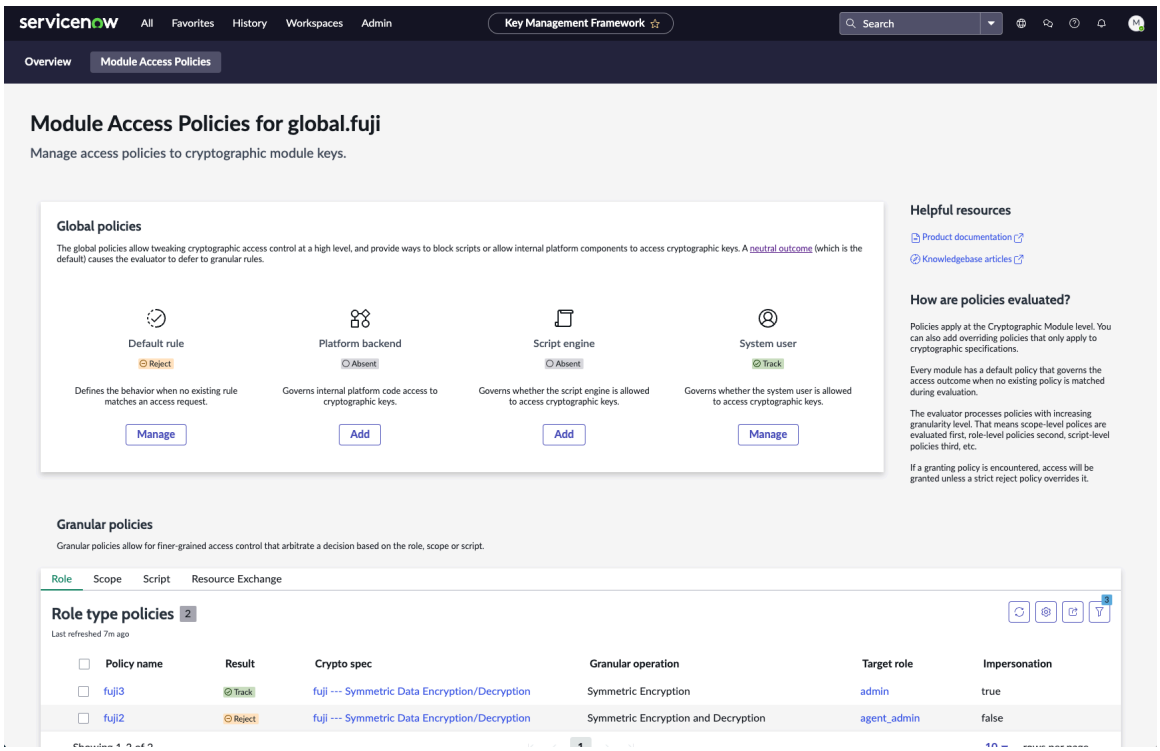
Im Formular „Kryptografische Anruferrichtlinie“ wird die von Ihnen ausgewählte Anruferrichtlinie aufgelistet. Das Feld Zielumfang gibt den Umfang des Skripts an, das versucht, das Modul zu verwenden. Weitere Informationen finden Sie unter.

Hinweis: Mit der Verschlüsselung auf Spaltenebene sind maximal fünf Modulzugriffsrichtlinien zulässig. Konfigurationsoptionen finden Sie unter.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Visualisierung von Modulzugriffsrichtlinien

Verwenden Sie die Visualisierung von Modulzugriffsrichtlinien, um alle relevanten kryptografischen Modulinformationen auf einer einzigen UI-Seite anzuzeigen.



Key Management Framework-Administratoren und Kryptografiemanager können auf der UI-Seite für Modulzugriffsrichtlinien alle Zugriffssteuerungsmechanismen für ein einzelnes kryptografisches Modul anzeigen. Bestimmen Sie anhand der auf dieser UI-Seite gesammelten Informationen schnell, wer in Ihrer Instanz Zugriff auf verschlüsselte Informationen hat.

Benutzer mit der Rolle *sn_kmf.admin* oder *sn_kmf.cryptographic_manager* können auf die UI-Seite für die Visualisierung von Modulzugriffsrichtlinien zugreifen, indem sie zu navigieren **Alle** > **Schlüsselverwaltung** > **Kryptografische Module** > **Alle**an.

Ergebnisbezeichnungen

Modulzugriffsrichtlinien enthalten ein Feld **Ergebnis**, das bestimmt, ob Zugriff auf das ausgewählte kryptografische Modul gewährt werden soll. Auf der UI-Seite wird eine Bezeichnung für Elemente auf der UI-Seite basierend auf dem Wert dieses Felds angezeigt.

UI-Bezeichnung	Ergebnisfeldwert	Definition
Track	*Track* oder *Allow*	Der Zugriff wird allen Benutzern gewährt, einschließlich Skripts.
Reject	*Reject*	Der Zugriff wird verweigert, es sei denn, eine Nachverfolgungsmodul-Zugriffsrichtlinie wird gefunden.

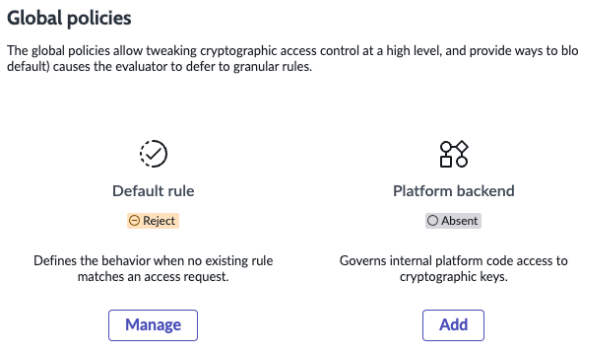
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

UI-Bezeichnung	Ergebnisfeldwert	Definition
StrictReject	*StrictReject*	Zugriff verweigert.
Absent	*N/A*	Die Modulzugriffsrichtlinie ist in der Instanz nicht vorhanden. Zugriff wird allen verweigert.

Globale Richtlinien

Verwenden Sie den Abschnitt **Globale Richtlinien**, um die Modulzugriffsrichtlinien zu überprüfen, die den Zugriff auf Plattformebene steuern.

Wählen Sie die Schaltfläche **Verwalten** unter einer der Richtlinien aus, um zu diesem Richtliniendatensatz zu navigieren. Wenn die Richtlinie nicht vorhanden ist, wird unter diesem Eintrag eine Schaltfläche **Hinzufügen** angezeigt. Wählen Sie die Schaltfläche **Hinzufügen**, um zu einem neuen Richtliniendatensatz zu navigieren, in dem Sie die Richtlinie definieren können.

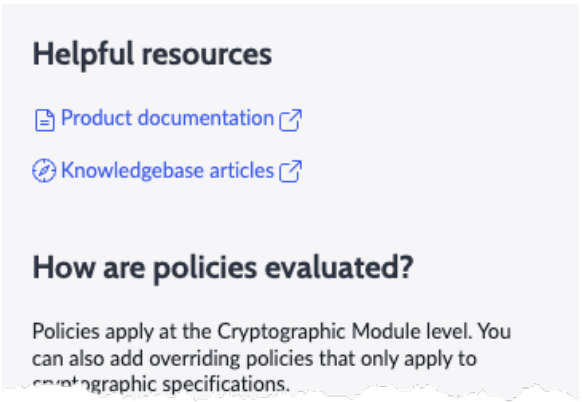


Richtlinie	Definition
Standardregel	Die Standardregelrichtlinie definiert das Verhalten, wenn keine vorhandene Regel mit einer Zugriffsanforderung übereinstimmt.
Plattform-Back-End	Die Plattform-Back-End-Richtlinie steuert den internen Plattformcodezugriff auf kryptografische Schlüssel.
Skriptmodul	Die Skript-Engine-Richtlinie steuert, ob die Skript-Engine auf kryptografische Schlüssel zugreifen darf.
Systemanwender	Die Systembenutzerrichtlinie regelt, ob der Systembenutzer auf kryptografische Schlüssel zugreifen darf.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hilfreiche Ressourcen

Im Abschnitt „ **Hilfreiche Ressourcen** “ finden Sie Links zu Produktdokumentationen, relevante Wissensartikel und eine kurze Beschreibung, wie Modulzugriffsrichtlinien auf der Plattform ausgewertet werden. Weitere Informationen zur Bewertung der Zugriffsrichtlinien für Module finden Sie unter Debugger für Modulzugriffsrichtlinien.

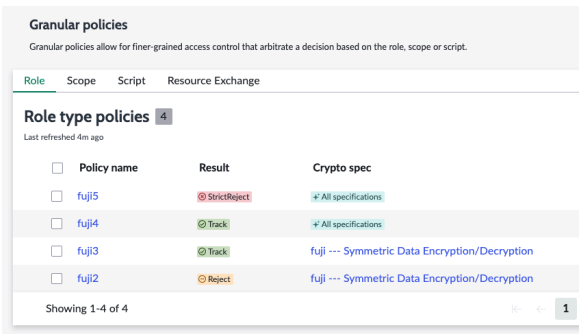


Granulare Richtlinien

Verwenden Sie den Abschnitt **Granulare Richtlinien**, um Listen von Modulzugriffsrichtlinien, getrennt nach Richtlinientyp, anzuzeigen. Verwenden Sie die Registerkarten über der Liste, um eine anzuzeigende Richtlinienkategorie auszuwählen.

- Rolle
- Umfang
- Umfang und Domäne (wenn Domain Separation aktiv ist)
- Skript
- Ressourcenaustausch (wenn das kryptografische Modul ein Password2- oder Verschlüsselung auf Spaltenebene-Untermodul ist)
- Identität (wenn Geheimnisverwaltungsunternehmen aktiv ist)

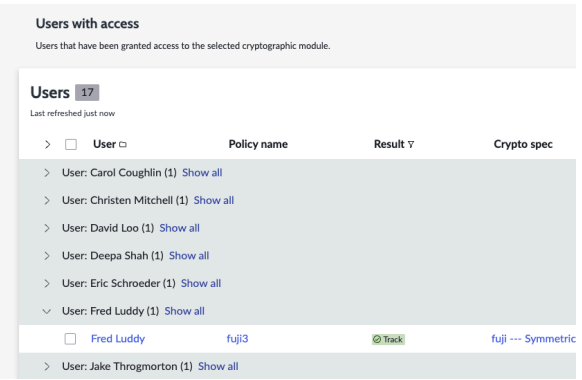
Standardmäßig werden in den Listen nur aktive Richtlinien angezeigt. Verwenden Sie das Filtersymbol, um den Standardfilter für die Liste zu ändern.



© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwender mit Zugriff

Verwenden Sie den Abschnitt **Anwender mit Zugriff**, um eine Liste aller Anwender anzuzeigen, die Zugriff auf das ausgewählte kryptografische Modul haben. Die Liste ist nach Benutzern gruppiert, da einzelne Benutzer mehrere Rollen besitzen können, die Zugriff auf ein kryptografisches Modul gewähren.

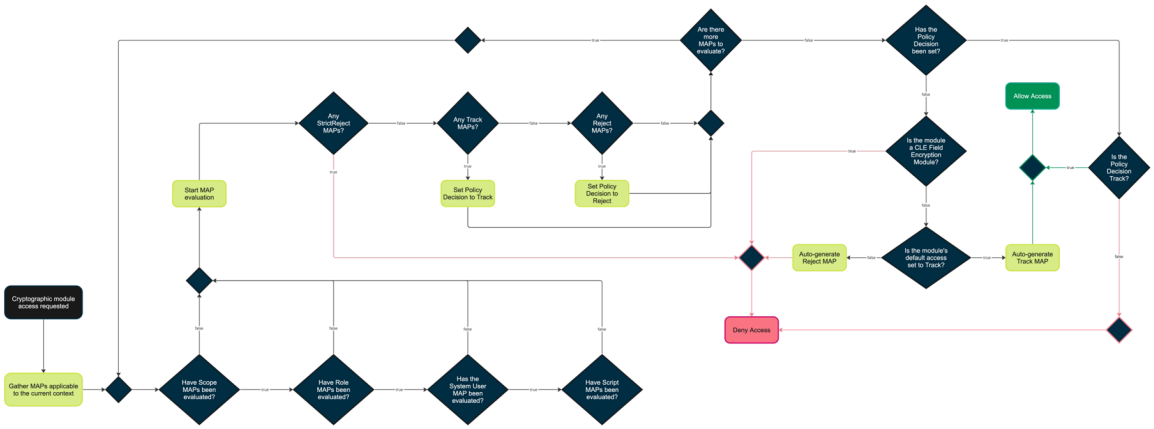


Debugger für Modulzugriffsrichtlinien

Verwenden Sie den Debugger für Zugriffsrichtlinien für das Modul, um Protokollierungsinformationen zu überprüfen und zu verstehen, warum Ihren Anwendern Zugriff auf einen Verschlüsselungskontext gewährt wird oder nicht.

Modulzugriffsrichtlinien (Module Access Policies, MAPs) definieren Steuerungen auf Instanzebene für den Zugriff auf kryptografische Module. Aufrufer (z. B. ein Benutzer oder ein Skript) benötigen expliziten Zugriff, um ein kryptografisches Modul für die Verschlüsselung und Entschlüsselung zu verwenden. Es ist nicht immer klar, welche MAPs ausgewertet werden, wenn Aufrufer versuchen, auf ein kryptografisches Modul zuzugreifen. Verwenden Sie den Debugger, um zu sehen, welche Richtlinien ausgewertet werden, wenn ein Aufrufer versucht, auf ein kryptografisches Modul zuzugreifen, und zu erfahren, warum der Zugriff gewährt oder nicht gewährt wird.

Dieses Flowchart zeigt, wie Ihre -Instanz Anforderungen für den Zugriff auf ein kryptografisches Modul auswertet.



Steuern Sie den Zugriff auf die Debug-Protokolle

Der Zugriff auf die Debug-Protokolle für den Modulzugriff wird durch die Rolle bestimmt. Benutzer mit den Rollen *sn_kmf.admin* und *sn_kmf.cryptographic_manager* haben immer Zugriff auf den Debugger. Gewähren Sie anderen Rollen mit der Systemeigenschaft *glide.kmf.module_access_policies.debugger.authorized.roles* Zugriff. Der Wert dieser Eigenschaft ist eine durch Kommas getrennte Liste von Rollen, die auf die Debug-Protokolle zugreifen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktivieren oder deaktivieren Sie den Debugger

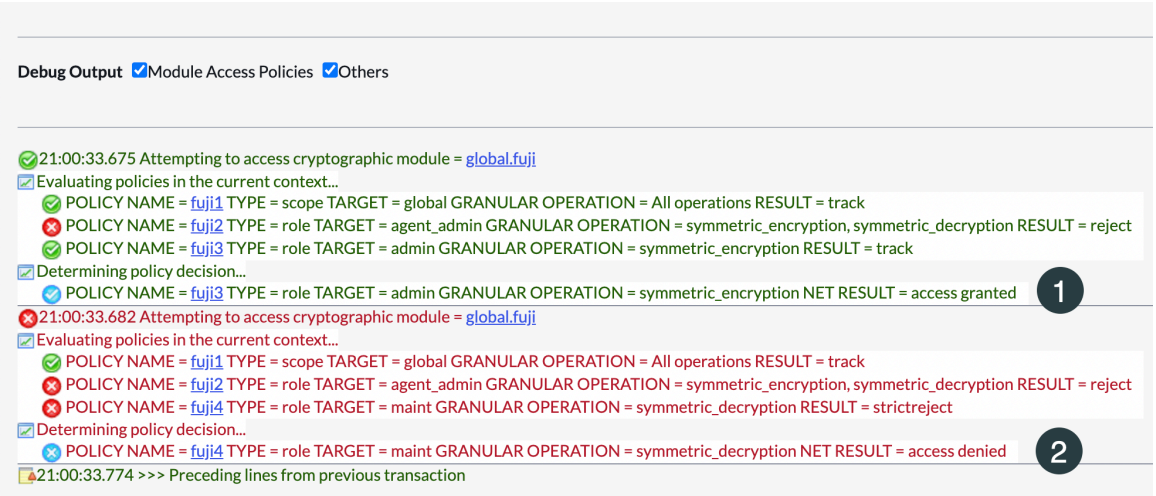
Um Debug-Protokollierungsnachrichten für Modulzugriffsrichtlinien zu aktivieren, navigieren Sie zu **Alle** > **Diagnosen** > **Sitzung debuggen** > **Modulzugriffsrichtlinien debuggen** > **an.**

Wenn Sie mit dem Debuggen fertig sind, können Sie die Protokollierungsnachrichten deaktivieren, indem Sie zu navigieren **Alle** > **Diagnosen** > **Sitzung debuggen** > **Alle deaktivieren** > **an.**

Greifen Sie auf die Protokolle zu

Navigieren Sie, nachdem Sie das Debugging aktiviert haben, zu einer Seite, die eine MAP-Bewertung auslöst, um die MAP-Debug-Protokolle anzuzeigen. Debug-Nachrichten werden unten auf der Seite angezeigt.

Tipp: Sie können den Identitätswechsel verwenden, um Zugriffsprobleme für andere Benutzer zu beheben. Weitere Informationen zum Identitätswechsel finden Sie unter Identität von Benutzern annehmen . Um die Debug-Protokolle aus der Perspektive eines anderen Benutzers anzuzeigen, stellen Sie sicher, dass für Ihre **Modulzugriffsrichtlinien** mit dem Typ *role* das Feld Identitätswechsel auf **true**festgelegt ist.



In diesem Beispiel löst ein Anrufer zwei Zugriffsanforderungen auf das kryptografische Modul `„global.fuji“ aus`. Eine symmetrische Verschlüsselung, die gewährt wird, und eine symmetrische Entschlüsselung, die abgelehnt wurde.

Protokolleinträge verstehen

Debugging-Informationen werden in diesem Format strukturiert.

1. Diese erste Zeile zeigt das kryptografische Modul an, das die Zugriffsanforderung erhält.
2. Die Zeilen zwischen der ersten und der letzten Zeile zeigen die ausgewerteten MAPs in der Reihenfolge an, in der sie ausgewertet wurden, einschließlich Name, Typ, Ziel, granularer Vorgang und Ergebnis.
3. In der letzten Zeile werden die Richtlinienentscheidung (falls zutreffend) und das Nettozugriffsergebnis für den Anrufer angezeigt (ob dem Anrufer Zugriff gewährt wird).

Jede Zeile beginnt mit einem Symbol, das den Nachrichtentyp angibt.

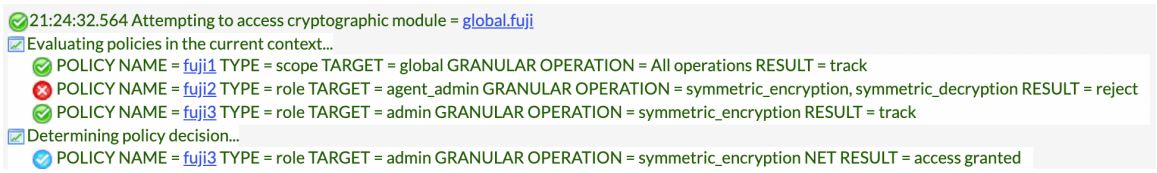
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachrichtensymbole

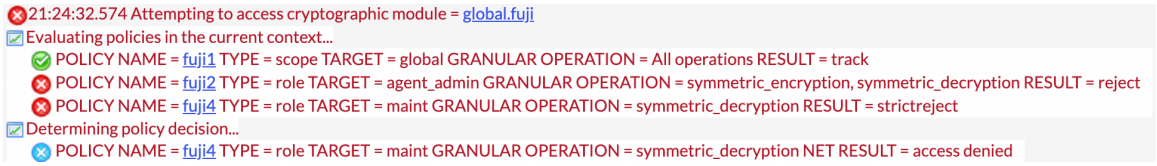
Symbol	Nachrichtentyp
	Informationsmeldung
	Die Modulzugriffsrichtlinie gewährt Zugriff
	Die Modulzugriffsrichtlinie verweigert den Zugriff
	Dem Anrufer wird Zugriff gewährt
	Anrufer hat keinen Zugriff
	Keine Modulzugriffsrichtlinie zum Auswerten

Debug-Protokollbeispiele

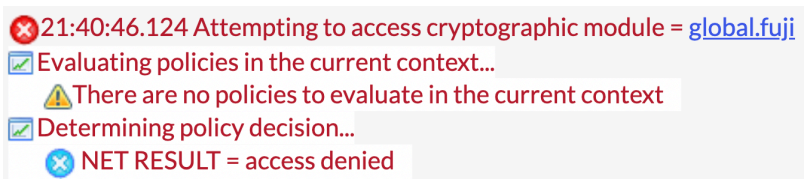
Nachricht über den gewährten Zugriff



Zugriff verweigert Nachricht



Zugriff verweigert (keine Modulzugriffsrichtlinien zum Auswerten



Zugriff verweigert (unzureichende Rechte)



Erstellt eine Lebenszyklusrichtlinie für kryptografische Module

Erstellen Sie eine Lebenszyklusrichtlinie für kryptografische Module, um Grenzwerte für kryptografische Module festzulegen, z. B. für die Gültigkeitsdauer des Schlüssels. Erstellen Sie Richtlinien, um kryptografische Module zu schützen, indem Sie deren Offenlegung begrenzen.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_manager

Warum und wann dieser Vorgang ausgeführt wird

Eine Lebenszyklusrichtlinie für ein kryptografisches Modul ist eine Richtlinie auf Instanzebene. Je mehr ein kryptografischer Schlüssel gefährdet ist, desto wahrscheinlicher ist es, dass er gefährdet wird. Schützen Sie Schlüssel, indem Sie festlegen, wie lange die Schlüssel verwendet werden können und wer sie verwenden kann.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgenden Funktionen steuern kryptografische Module:

- Instanzrichtlinien legen Grenzen für die Instanz fest. Wenn Sie beispielsweise in einer Instanzrichtlinie angeben, dass das Ablaufdatum nie mehr als zwei Jahre nach dem Aktivierungsdatum liegen darf, können Sie die Lebenszyklusregeln nicht verwenden, um ein Ablaufdatum fünf Jahre nach dem Aktivierungsdatum festzulegen.

- Mit Vorlagen für den Instanzlebenszyklus können Sie verschiedene Richtlinien für verschiedene Schlüssel festlegen. Vorlagen bieten standardmäßige Lebenszyklusregeln für kryptografische Module, sodass sie nicht für jedes Modul neu erstellt werden müssen. Beispielsweise können Sie für symmetrische Datenverschlüsselungsschlüssel andere Ablaufdaten als für öffentliche Schlüssel umschließen.

- Lebenszyklusregeln wirken sich direkt auf die Schlüssel aus. Wenn Sie beispielsweise in den Lebenszyklusregeln angeben, dass das Ablaufdatum zwei Jahre nach dem Aktivierungsdatum liegen soll, laufen Schlüssel zwei Jahre nach dem Aktivierungsdatum ab.

Prozedur

1. Navigieren zu **Alle** > **Schlüsselverwaltung** > **Lebenszyklusrichtlinien** > **Instanzrichtlinien**an.
2. Auswahlvorgang **Neu**an.
3. Füllen Sie das Formular aus.

   Felder „Kryptografische Lebenszyklusrichtlinien“.

Feld	Beschreibung
Betrifft	Schreibgeschützt. Der Schlüssel, für den der Lebenszyklus gilt.
Aktiv	Wählen Sie diese Option aus, um die Richtlinie zu aktivieren.
Richtlinienbedingung	Bedingte Anweisungen, die angeben, wann das kryptografische Modul aktiviert, verlängert, deaktiviert und gelöscht werden soll.
Ergebnis	**Ablehnen**, um den Zugriff auf das kryptografische Modul zu widerrufen, oder **nachverfolgen**, um den Zugriff zuzulassen und die Verwendung des kryptografischen Moduls zu überwachen.

Nächste Maßnahme

Wenn Sie dieser Lebenszyklusrichtlinie auf Modulebene Ausnahmen hinzufügen möchten, lesen Sie unter Erstellen Sie Richtlinienausnahmen für den Modul-Lebenszyklusnach.

Erstellen Sie Richtlinienausnahmen für den Modul-Lebenszyklus

Erstellen Sie eine Modulrichtlinienausnahme, um die Lebenszyklusrichtlinie eines Schlüssels auf Modulebene für eine Instanz zu ändern. Die Ausnahme(n) gilt nur für dieses Modul und nicht für die gesamte Instanz. Wenn der Administrator beispielsweise symmetrische Schlüssel so konfiguriert hat, dass sie auf Instanzebene auf ein Jahr beschränkt sind, kann auf Modulebene eine Ausnahme von zwei Jahren festgelegt werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_kmf.cryptographic_manager und sn_kmf.admin

Prozedur

1. Navigieren zu **Alle** > **Schlüsselverwaltung** > **Kryptografische Module Alle**an.
2. Wählen Sie das kryptografische Modul aus, das die Richtlinienausnahmen verwendet.
3. Wählen Sie in der Tabelle „Kryptografisches Modul“ das aus **Modulrichtlinienausnahmen** Registerkarte
4. Klicken **Neu**an.
5. Füllen Sie das Formular aus.

Felder „Modulrichtlinienausnahmen“.

Feld	Beschreibung
Krypto-Modul	Schreibgeschützt, Name des ausgewählten Moduls.
Betrifft	Der angegebene Schlüssel wird automatisch ausgefüllt.
Tastentyp	Wählen Sie den Schlüsseltyp aus, da sich die Ausnahmerichtlinien auf einen bestimmten Schlüssel beziehen. Pro Krypto-Modul können mehrere Ausnahmerichtlinien erstellt werden.
Richtlinienbedingung	Wählen Sie die Qualifizierungsbedingungen aus der Dropdownliste aus, und füllen Sie die zusätzlichen Einschränkungskriterien aus.
Neue Kriterien	Wählen Sie nach Bedarf zusätzliche Richtlinienbedingungen aus.
Ergebnis	Wählen Sie **Ablehnen**, um die Verwendung des Schlüssels abzulehnen, oder **verfolgen** Sie, um die Verwendung zuzulassen, wenn die Kriterien erfüllt sind.

6. Klicken **Übermitteln** an die Tabelle „Kryptografisches Modul“ zurückgegeben werden.

Aktionen der Schlüsselverwaltung

Eine der Kernfunktionen von KMF besteht in der Verwaltung von Schlüsseln (z. B. Widerrufen oder Rotieren von Schlüsseln). KMF sichert vertrauliche Daten ordnungsgemäß mit den neuesten Verschlüsselungsmaterialien und Lebenszyklusvorgängen.

Die folgende Tabelle enthält eine Zusammenfassung der wichtigsten Lebenszyklusvorgänge und Verwaltungsaktionen. Der Zweck des kryptografischen Moduls wird mit der Konfiguration des kryptografischen Moduls auf die Daten angewendet und hat keine Auswirkungen auf die Daten.

Aktion der Schlüsselverwaltung	Beschreibung
Schlüssel generieren	Generiert einen neuen Schlüssel für das angegebene kryptografische Modul. Ein zuerst generierter Schlüssel wird auf *active*festgelegt.
Schlüssel rotieren	Deaktiviert den aktuellen Schlüssel und generiert einen neuen. Der neue Modulschlüssel ist auf „Aktuell“ (aktiv) festgelegt.
Schlüssel widerrufen	Markiert den aktuellen Schlüssel- und Lebenszyklusstatus als widerrufen. Das kryptografische Modul generiert automatisch einen neuen Schlüssel für neue Daten und setzt den Schlüsselstatus auf „Aktiv“. Widerrufen

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktion der Schlüsselverwaltung	Beschreibung
	bedeutet, dass der Schlüssel nicht mehr für die Verschlüsselung verwendet wird. Er kann jedoch weiterhin zur Entschlüsselung verwendet werden. Sie können keinen Schlüssel löschen.
Schlüssel aussetzen	Markiert den aktuellen Schlüssel als angehalten. Setzen Sie den ausgesetzten Schlüssel manuell fort, oder widerrufen Sie den ausgesetzten Schlüssel, um einen neuen Modulschlüssel zu generieren, bevor Sie das kryptografische Modul erneut verwenden.
Schlüssel zum Fortsetzen	Markiert einen angehaltenen Schlüssel als aktiven Schlüssel.
Erneuern Sie den Schlüssel	Verlängert die Lebensdauer des aktuellen Schlüssels. Die **Schaltfläche** Verlängern ist unter den folgenden Umständen verfügbar: • Ihnen ist die Kryptografiemanagerrolle zugewiesen. • Der Lebenszyklusstatus ist entweder mit **Aktiv** oder **Erneuert**markiert. • Ein Ablaufdatum ist in der Definition des Modullebenszyklus festgelegt.

Zeigen Sie Schlüssel an, und verwalten Sie sie

Überprüfen Sie den Status eines Schlüssels, um weitere Schlüsselaktionen zu bestimmen, z. B. wann ein aktueller Schlüssel verlängert, rotiert, angehalten, deaktiviert oder gelöscht werden soll.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_manager

Prozedur

1. Navigieren zu **Alle** > **Schlüsselverwaltung** > **Kryptografische Module** > **Alle**an.
2. Wählen Sie ein kryptografisches Modul aus.

   Das kryptografische Modul<module-name> Formular wird angezeigt.
3. Wählen Sie auf der Registerkarte „Modulschlüssel“ den Schlüsselalias aus, um den Schlüsselstatus im Lebenszyklus zu überprüfen<key name> Formular.
4. Überprüfen Sie das Formular, da alle Felder schreibgeschützt sind.

Schlüsselfelder des kryptografischen Lebenszyklus

Feld	Beschreibung
Generierungsdatum	Zeigt das Datum an, an dem der Schlüssel generiert wurde.
Aktivierungsdatum	Zeigt das Datum an, an dem die Taste aktiviert wurde.
Letztes Verlängerungsdatum	Zeigt das Datum an, an dem der Schlüssel zuletzt verlängert wurde.
Letztes Rotationsdatum	Zeigt das Datum an, an dem der Schlüssel zuletzt rotiert wurde.
Deaktivierungsdatum	Zeigt das Datum an, an dem der Schlüssel deaktiviert wurde.
Zerstörungsdatum	Zeigt das Datum an, an dem der Schlüssel vernichtet wurde.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Schlüssel-Lebenszyklusstatus	Zeigt den Schlüssel-Lebenszyklusstatus an.
Künftiges Aktivierungsdatum	Zeigt das zukünftige Datum der Schlüsselaktivierung an.
Künftiges Verlängerungsdatum	Zeigt das zukünftige Datum der Schlüsselverlängerung an.
Künftiges Rotationsdatum	Zeigt das zukünftige Datum für die Schlüsselrotation an.
Künftiges Zerstörungsdatum	Zeigt das Datum in der Zukunft an, an dem der Schlüssel zerstört wird.
Ablaufdatum	Zeigt das Datum an, an dem der Schlüssel abläuft.

5. Um eine Aktion für den Schlüssel auszuführen, wählen Sie eine der folgenden Optionen aus, damit sie sofort wirksam wird:
   - **Schlüssel widerrufen**: Auswählen, um den Schlüssel zu deaktivieren und einen neuen Schlüssel zu generieren. Geben Sie den Grund ein, warum Sie den Schlüssel widerrufen.
   - **Schlüssel rotieren**: Wählen Sie diese Option, um den aktuellen Schlüssel zu deaktivieren und stattdessen einen neuen Schlüssel zu generieren. Der neue Schlüssel wird in der Tabelle „Modulschlüssel“ aufgeführt, und die Schlüsselversionsnummer wird um 1 erhöht. Weitere Informationen finden Sie unter.
   - **Schlüssel aussetzen**: Auswählen, um den aktuellen Schlüssel zu deaktivieren.
   - **Schlüssel fortsetzen**: Wählen Sie diese Option, um einen angehaltenen Schlüssel als aktiven Schlüssel zu markieren. Diese Option ist erst verfügbar, nachdem der aktive Schlüssel angehalten wurde.

Schlüssel rotieren

Um die Sicherheit zu erhöhen, können Sie Ihre kryptografischen Schlüssel nach einem festgelegten Zeitplan rotieren. Bei der Schlüsselrotation löschen Sie einen Verschlüsselungsschlüssel und ersetzen den alten Schlüssel durch Generieren eines neuen kryptografischen Schlüssels.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_manager

Warum und wann dieser Vorgang ausgeführt wird

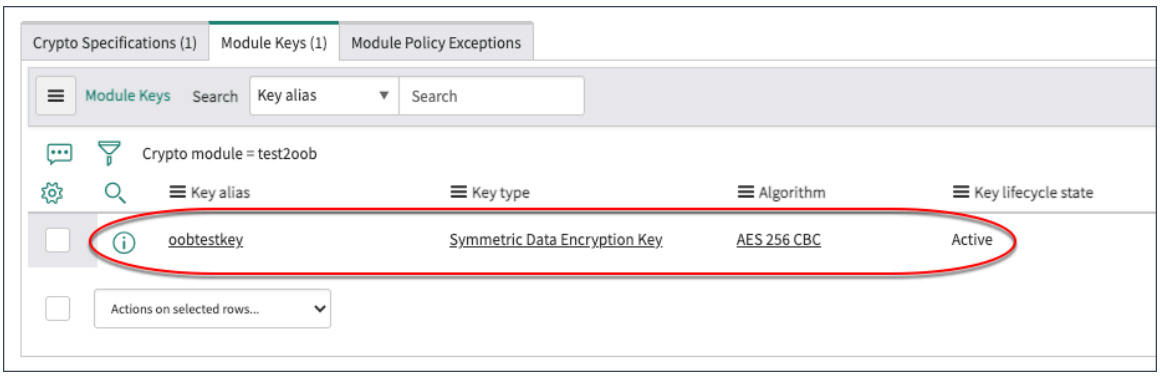
Verschlüsselungsmodule unterstützen im Gegensatz zu Verschlüsselungskontexten eine Neuschlüsselung von Datensätzen für die erneute Verschlüsselung mit einem neuen Schlüssel. Im Folgenden wird gezeigt, wie Sie einen Schlüsselrotationsvorgang manuell für ein kryptografisches Modul durchführen.

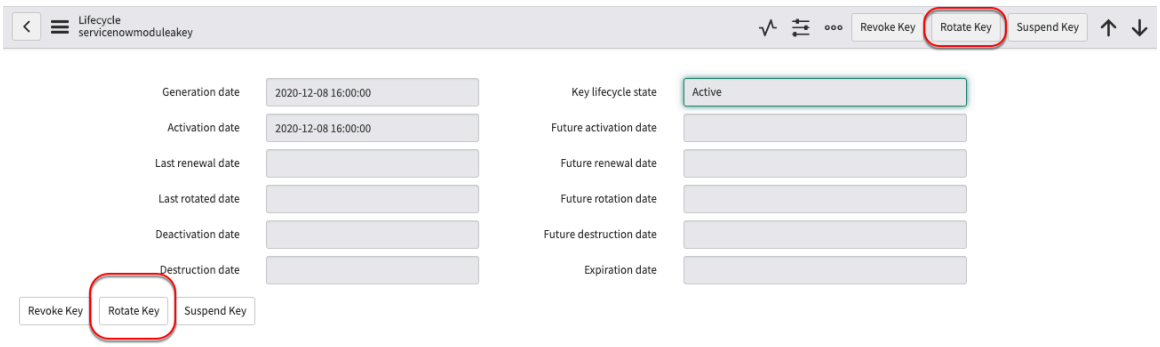
Prozedur

1. Navigieren zu **Schlüsselverwaltung** > **Kryptografische Module** > **Alle**an.
2. Wählen Sie das kryptografische Modul für die Schlüsselrotation aus.
3. **Wählen** Sie auf der Registerkarte Modulschlüssel den Schlüssel Aktiv aus.

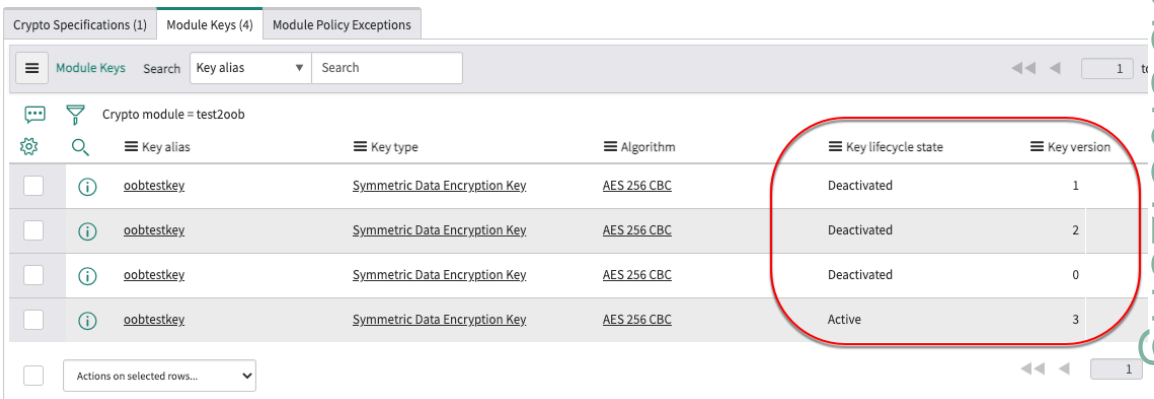
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wählen Sie den aktiven Schlüssel aus





4. Wählen Sie **Schlüssel rotieren aus**.
   Der Schlüssel-Lebenszyklusstatus ändert sich in „Deaktiviert“. Die Felder werden mit dem **Datum der letzten Rotation**, dem **Deaktivierungsdatum**und der **Schlüsselversion** aktualisiert.
5. Zurück zu **Kryptografisches Modul** > **Modulschlüssel**.



In der Tabelle ist ein zusätzlicher Modulschlüssel aufgeführt. Der neu rotierte Schlüssel wird auf „Aktiv“ und der letzte Schlüssel auf „Deaktiviert“ gesetzt.

Importieren Sie einen Schlüssel aus einem Webservice

Laden Sie einen externen Kundenschlüssel sicher in Ihre Instanz hoch, indem Sie einen Schlüssel aus einem Webservice importieren (z. B. die Schlüssel-REST-API). Sowohl symmetrische als auch asymmetrische öffentliche Schlüssel können in ein kryptografisches Modul des Ziels KMF importiert werden.

Der zu importierende Schlüssel (der Zielschlüssel) muss mit einem umschließenden Schlüssel verschlüsselt werden, bevor er in das kryptografische Zielmodul der Instanz hochgeladen

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

wird. Dieser Wrapping-Schlüssel ist die öffentliche Komponente eines öffentlichen/privaten Schlüsselpaars, das in der Instanz vorhanden sein muss. Der Schlüssel ist eine Voraussetzung, damit der umschlossene Zielschlüssel über Aus Webservices importieren hochgeladen werden kann.

Diese beiden separaten Verfahren (Importieren des umschließenden Schlüsselpaars und Importieren des umschlossenen Zielschlüssels aus einem Webdienst) werden in der folgenden Dokumentation beschrieben. Dieses Schlüsselpaar muss generiert und hochgeladen werden, damit es im internen kryptografischen Modul für den Schlüsselimport der Instanz verfügbar ist.

Hinweis: In diesem Beispiel werden OpenSSL für die Schlüssel- und Zertifikatgenerierung und das Postman-API-Testtool verwendet, um die Verwendung der REST-API zu zeigen. Ersetzen Sie andere vergleichbare Tools basierend auf Ihren Unternehmensanforderungen.

Importieren Sie das Schlüsselpaar zum Packen/Entpacken

Konfigurieren Sie die Importeinstellungen für Key Management Framework, bevor Sie einen Schlüssel importieren.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_manager

Warum und wann dieser Vorgang ausgeführt wird

In diesem Beispiel wird OpenSSL für die Schlüssel- und Zertifikatgenerierung verwendet. Ersetzen Sie andere vergleichbare Tools basierend auf Ihren Unternehmensanforderungen.

Prozedur

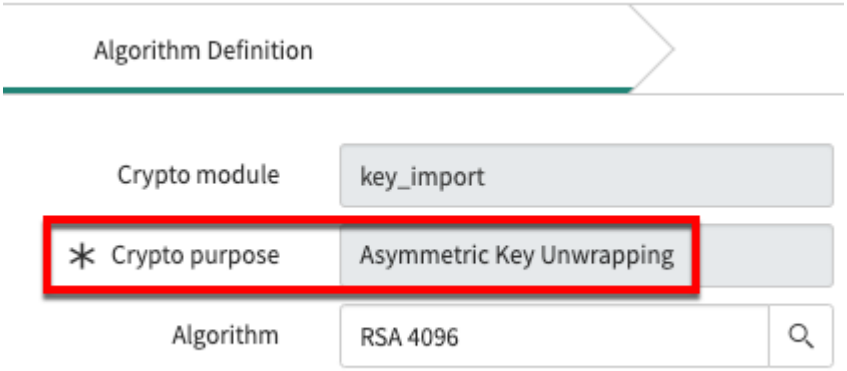
1. Verwenden Sie in Ihrer lokalen Umgebung das Terminal, um ein -Zertifikat zu erstellen.
   Beispiel: `openedsl req -x509 -sha256 -nodes -days 365 -newkey rsa:4096 -keyout Wrapping_private.key -out Wrapping_public.crt`

   Dieses Zertifikat ist eine öffentliche Komponente, die einen Schlüssel enthält. Das Zertifikat wird zum Wrapping eines symmetrischen AES-Schlüssels verwendet.

2. Verwenden Sie in Ihrer lokalen Umgebung das Terminal, um einen Schlüsselspeicher zu erstellen, der ein öffentliches Zertifikat (mit dem Packenschlüssel) und einen privaten Entpackenschlüssel enthält.
   Beispiel:`openedsl pkcs12 -export -in Wrapping_public.crt -inkey Wrapping_private.key -name "wrapping_key_alias" -out Wrapping_keystore.p12`
3. Navigieren Sie in Ihrer -Instanz zu **Alle** > **Schlüsselverwaltung** > **Einstellungen importieren** > **Schlüsselimporteinstellungen**an.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Überprüfen Sie im Abschnitt „Algorithmusdefinition“, ob das Feld **Krypto-Zweck** auf Entpacken des *asymmetrischen Schlüssels festgelegt ist*.



5. Wählen Sie einen geeigneten Algorithmus aus, der am asymmetrischen Schlüsselmaterial für den importierten Schlüsselspeicher ausgerichtet ist.
   Weitere Informationen finden Sie unter Kryptografischer Zweck, Algorithmen und Schlüsselinformationen.
6. Wählen Sie **Weiter**.
7. Wählen Sie im Abschnitt „ **Lebenszyklusdefinition** “ **Weiter**, um fortzufahren.
8. Wählen Sie im Abschnitt „ **Schlüsselursprung** “ im Feld **Herkunft** entweder **Aus PKCS12 importieren** oder **Aus BCFKS importieren aus**.

   Hinweis: Wenn Sie den Beispielschlüsselspeicher aus Schritt 1 verwenden, wählen Sie **Aus PKCS12 importieren aus**.

9. Geben Sie einen **Schlüsselalias** ein, um den Schlüssel zu identifizieren.
   Dieser Alias muss mit dem Schlüsselalias (oder dem „Anzeigenamen“) übereinstimmen, der beim Generieren des hochzuladenden Zertifikats oder Schlüsselspeichers angegeben wurde. In Fortsetzung des obigen Beispiels wäre dies `Wrapping_key_alias`.
10. Wählen Sie **Weiter**.
    Der Abschnitt „ **Schlüsselerstellung** “ enthält den Link **Schlüssel** importieren, über den ein Dialogfeld zum Hochladen des Schlüsselspeichers angezeigt wird. Um das Beispiel fortzusetzen, wäre dies `Wrapping_keystore.p12`.

Importieren Sie einen umschlossenen Schlüssel aus einem Webservice

Laden Sie Ihren umschlossenen Schlüssel mit der Funktion zum Importieren von Schlüsseln aus der Webservice-Funktion in ein kryptografisches Modul hoch. Im Beispiel wird ein symmetrischer Schlüssel verwendet. Ähnliche Schritte können verwendet werden, um einen asymmetrischen Schlüssel zu importieren.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_manager (Modulkonfiguration), sn_kmf.cryptographic_operator (REST-Vorgang Standardauthentifizierung)

Warum und wann dieser Vorgang ausgeführt wird

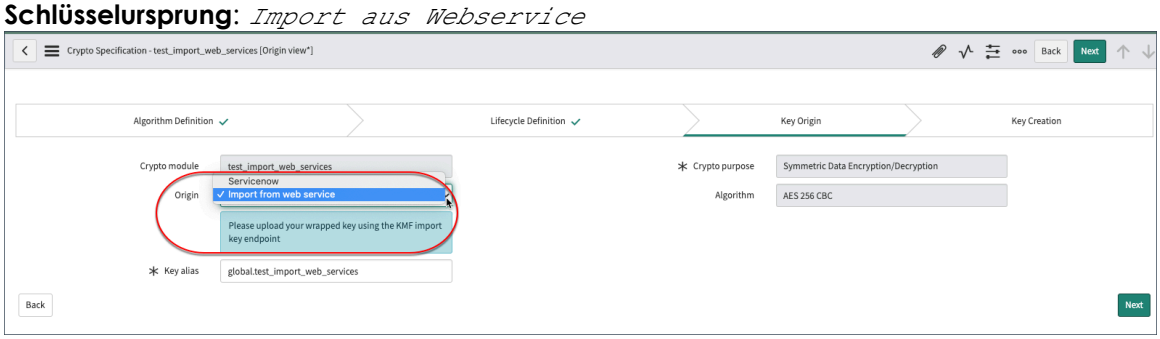
KMF Zum Abschließen des Schlüsselimportvorgangs ist der Zugriff auf den Importschlüssel-Endpunkt erforderlich.

In diesem Beispiel wird OpenSSL zum Generieren von Schlüsseln und Zertifikaten verwendet. Sie können andere vergleichbare Tools basierend auf Ihren Anforderungen ersetzen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Verwenden Sie das Terminal auf Ihrem lokalen Gerät, und umschließen Sie Ihren symmetrischen Schlüssel mit dem Public Key Wrapping-Schlüssel des Moduls Key Import (Schlüsselimportmodul).
   Beispiel: `openedsl pkeyutl -encrypt -pubin -inkey public_wrapping_key.pem -in metric_key.bin -pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256 -out Wrapped_metric_key.txt`
   In diesem Beispiel wird eine umschlossene Schlüsseldatei mit dem Namen `umschlossener_symmetrischer_schlüssel.txt erstellt`.
2. Erstellen Sie ein kryptografisches Modul, das an die API gebunden werden soll.
   Weitere Informationen finden Sie unter oder.
3. Fügen Sie eine kryptografische Spezifikation mit der folgenden Auswahl hinzu.
   - **Kryptografischer Zweck**: *Symmetrische Datenverschlüsselung/-entschlüsselung*.
   - **Schlüsselursprung**: *Import aus Webservice*



   Weitere Informationen finden Sie unter oder.

4. Führen Sie eine *HTTP POST-Anforderung* an den Import von einem Webservice-REST-Endpunkt aus.

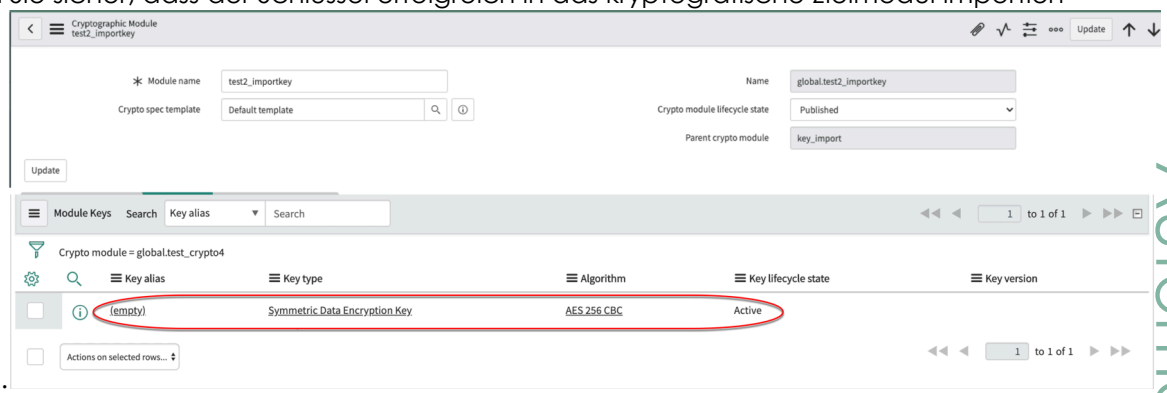
Option	Wert/Format
URL des Endpunkts	*https://*<instance> /api/sn_kmf/key/import?cryptoSpecSysID=<sys_id_of_crypto_spec> .
CryptoSpecSysID-Parameter	Die *sys_id* der neu erstellten Krypto-Spezifikation. **Tipp:** Klicken Sie mit der rechten Maustaste auf den Header der Krypto-Spezifikation, um die *sys_id* zu kopieren.
Header-Inhaltstyp	Anwendung/Oktett-Stream.
Textkörper	Muss eine binäre Anhangdatei und den zu importierenden öffentlichen Schlüssel (wrapped_metric_key.txt) enthalten.
Import aus Webservice-REST-Endpunkt	Verwendet die Standardauthentifizierung von<username/password> .

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Wert/Format
	Hinweis: Vergewissern Sie sich, dass der angegebene Benutzer über die Rolle sn_kmf_cryptographic_operator verfügt.

Der erfolgreiche Import des öffentlichen Schlüssels führt zu einer HTTP-Antwortnachricht mit dem *Status 200*.

5. Stellen Sie sicher, dass der Schlüssel erfolgreich in das kryptografische Zielmodul importiert wurde.



Key Management Framework Gesundheit

Greifen Sie bei Bedarf auf Integritätsstatusinformationen für Key Management Frameworkzu. Warnungs- und Funktionsfehler enthalten eine detaillierte Meldung.

Vorbereitungen

Erforderliche Rolle: sn_kmf_cryptographic Auditor oder sn_kmf_admin oder sn_kmf_cryptographic_manager

Warum und wann dieser Vorgang ausgeführt wird

Jede Komponente von Key Management Framework ist umrissen und meldet die folgenden Status und Farben:

- Grün/Funktionsfähig: Die Komponente ist betriebsbereit, keine Fehler zu melden.
- Grau/Deaktiviert: Die Komponente ist inaktiv, daher wird keine Integritätsprüfung durchgeführt.
- Gelb/Verschlechtert: Warnung, die Komponente funktioniert, es können jedoch Verzögerungen/vorübergehende Probleme auftreten.
- Rot/Funktionsstörung: Ein schwerwiegender Fehler verhindert den Betrieb der Komponente, was wahrscheinlich zu Teilausfällen führt.

Komponenten können Unterkomponenten mit einzelnen Berichten enthalten. Ihr eigener Integritätsstatus wirkt sich wie folgt auf das übergeordnete Element aus:

- Wenn alle Unterkomponenten inaktiv sind, wird das übergeordnete Element als inaktiv angezeigt. Inaktive Unterkomponenten haben keine Auswirkungen auf die Integrität ihrer übergeordneten Komponenten.
- Wenn eine oder mehrere Unterkomponenten beschädigt sind oder eine Fehlfunktion aufweisen, wird die übergeordnete Integrität als verschlechtert angezeigt.
- Wenn alle Unterkomponenten eine Fehlfunktion melden, meldet auch das übergeordnete Element eine Fehlfunktion.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zu Unterkomponenten finden Sie unter Schlüssel auf Instanzebene im Key Management Framework.

Hinweis: Integritätsprüfungen werden alle 15 Sekunden durchgeführt. Aktualisieren Sie die Integritätsseite, um den Bericht erneut auszuführen.

Prozedur

1. Navigieren zu **Alle** > **Schlüsselverwaltung** > > **Diagnosen**an.
2. Überprüfen Sie die folgenden Integritätsstatusinformationen:

Diagnoseinformationen

Kategorie	Details
Schlüssel sicher	Prüft, ob eine Verschlüsselung versucht wird.
Dateischlüsselspeicher	Überprüft, ob ein Versuch zum Abrufen des Instanz-Root-Schlüssels (IRK) auftritt. **Hinweis:** Der Dateischlüsselspeicher ist eine Offline-Alternative zu Key Secure, die für lokale Instanzen und Entwicklerinstanzen verwendet wird.
GlideEncrypter	Überprüft, ob ein GlideEncrypter-Kryptografiemodul, eine Spezifikation und ein Schlüssel auf Instanzebene vorhanden sind. **Hinweis:** GlideEncrypter ist eine skriptfähige Komponente, die die transparente Verschlüsselung von Feldern Password2 und andere Legacy-Verschlüsselungsanwendungen über Key Management Frameworkermöglicht.
Verschlüsselungsschlüssel des Instanzschlüssels (IKEK)	Überprüft, ob der Schlüssel aus dem Dateischlüsselspeicher oder KeySecure abgerufen werden kann.
HMAC-Schlüssel der Instanz	Überprüft, ob der Schlüssel aus dem Dateischlüsselspeicher oder KeySecure abgerufen werden kann.
Vault-PKI	Überprüft die Tresorkonnektivität, um zu überprüfen, ob der asymmetrische Verschlüsselungsschlüssel der Instanz (IAEK) und der Signaturschlüssel der Instanz (ISK) verwendbar sind und aus dem Tresor abgerufen werden können.
EJBCA PKI	Überprüft die LDAP-Konnektivität, um zu verifizieren, ob IAEK und ISK verwendbar sind und aus dem Cache und LDAP abgerufen werden können.
Instanz-PKI	Überprüft den Dateischlüsselspeicher und KeySecure auf einen Schlüssel und ob das Zertifikat vorhanden ist und mit dem symmetrischen Schlüssel übereinstimmt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kategorie	Details
	Hinweis: Instanz-PKI ist nur für Instanzen innerhalb eines ServiceNow -Rechenzentrums verfügbar.

Wenn Sie Unterstützung bei der Problembehandlung benötigen, wenden Sie sich an Kundenservice und Support.

Bereiten Sie Ihre -Instanz auf die Einstellung von GlideEncrypter vor

Verwenden Sie ein Instanzscanskript, um GlideEncrypter-API-Aufrufe in Ihrer Instanz zu suchen und zu entfernen. Das Entfernen dieser Aufrufe ist ein notwendiger Schritt, um die 3DES-Verschlüsselung in Ihrer Instanz als veraltet festzulegen.

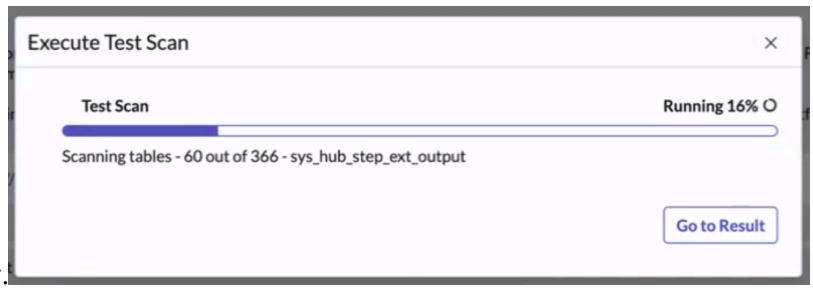
Vorbereitungen

Erforderliche Rolle: admin

Die GlideEncrypter-API wird voraussichtlich ab dem Zürcher Release von ServiceNoweingestellt. Das Entfernen von GlideEncrypter-Aufrufen aus Ihrem Skript ist ebenfalls ein notwendiger Schritt, bevor Sie die 3DES-Verschlüsselung in Ihrer Instanz als veraltet festlegen.

Prozedur

1. Navigieren zu **Alle** > **Instanz-Scan** > **Suites**an.
2. Wählen Sie in der Liste **Suites** die **Option GlideEncrypter aus, um die Datensätze mit GlideEncrypter-Nutzungen zu identifizieren**
3. Wählen Sie im Datensatz **Suites** die **Option GlideEncrypter aus, um die Datensätze mit GlideEncrypter-Nutzungen** aus der zugehörigen Liste **Prüfungen** zu identifizieren.
   Die **Überprüfung** des Spaltentyps wird angezeigt. Dieser Datensatz enthält eine Beschreibung der Prüfung sowie Informationen zu und Links zum Aktualisieren der von der Prüfung gefundenen Datensätze.
4. **Wählen Sie** im Datensatz **Überprüfung des Spaltentyps die Option Testüberprüfung** aus, um den Scan auszuführen.
   Während der Ausführung des Scans vom **Typ Testscan**ausführen wird in einem Fenster der Fortschritt des Scans angezeigt.

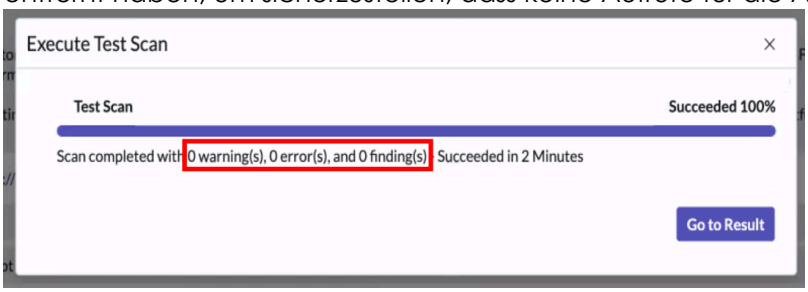


   Hinweis: Diese Prüfung prüft nur Datensätze, die vom Kunden erstellt oder geändert wurden.

5. Wählen Sie nach Abschluss des Scanvorgangs **Zu Ergebnis wechseln**, um den Datensatz **Scan-Ergebnis** anzuzeigen.
   Im Datensatz **Scan** - **Ergebnis** zeigt die Liste Scanfunde eine Liste der Datensätze in Ihrer Instanz an, die die **GlideEncrypter-** API verwenden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Wählen Sie in der Liste „ **Scanfunde** “ das Feld **Anzahl** aus, um zu einem Datensatz zu navigieren.
7. Ändern Sie alle Skripts im Datensatz, die die **GlideEncrypter-** API verwenden. Details zu Alternativen für **GlideEncrypter**finden Sie unter Alternativen zu veralteten GlideEncrypter-APIs .
8. Führen Sie den Scan erneut aus, nachdem Sie die **GlideEncrypter-** Aufrufe aus Ihren Skripts entfernt haben, um sicherzustellen, dass keine Aufrufe für die API mehr vorhanden sind.



Nächste Maßnahme
GlideEncrypter-Nutzung von 3DES für Passwort2-Felder einstellen

GlideEncrypter-Nutzung von 3DES für Passwort2-Felder einstellen

Stellen Sie die Nutzung des 3DES-Verschlüsselungsstandards durch GlideEncrypter in Ihrer Instanz außer Kraft. Stellen Sie sicher, dass Ihre Instanz ausschließlich den sichereren Advanced Encryption Standard (AES) für die Verschlüsselung und Entschlüsselung Ihrer Passwort2-Daten verwendet.

Ab Romewerden Passwort2-Daten mit Key Management Frameworkgeschützt, das den moderneren AES-Algorithmus (Advanced Encryption Standard) verwendet. Einige Konfigurationen und Fallbacks in Passwort2-Logik können jedoch weiterhin den 3DES-Algorithmus zur Verschlüsselung und Entschlüsselung verwenden.

Im Release Vancouver können Administratoren den 3DES-Algorithmus vollständig als veraltet festlegen. Nach Abschluss dieser Änderung verwendet Ihre Instanz ausschließlich die AES-Verschlüsselung für alle Verschlüsselungs- und Entschlüsselungsaufgaben im Zusammenhang mit Passwort2-Daten. Dieser Change bietet eine bessere Instanzsicherheit als im Vergleich zur 3DES-Verschlüsselung und ist erforderlich, um die NIST-Konformität zu gewährleisten.

Überlegungen vor der Einstellung

Passwort2-Daten werden zwischen Instanzen übertragen

Wenn Sie mit Passwort2 verschlüsselte Texte in andere Instanzen übertragen, müssen Sie sicherstellen, dass KMF Key Exchange zwischen Quell- und Zielinstanzen aktiviert ist. Diese Konfiguration stellt sicher, dass die zum Verschlüsseln von Passwort2-Texten verwendeten Schlüssel in beiden Instanzen verfügbar sind, um die mit Passwort2 verschlüsselten Texte zu entschlüsseln. Berücksichtigen Sie vor dem Ablegen von 3DES die folgenden Anwendungsfälle, die sich auf Passwort2-Daten zwischen Instanzen auswirken können.

- Wenn Sie in Ihrer Instanz Anwendungen haben, die Passwort2-Daten verwenden, stellen Sie sicher, dass KMF Ressourcenaustausch in dieser Instanz installiert ist. KMF Ressourcenaustausch stellt sicher, dass Schlüssel auf Instanzebene, die zum Verschlüsseln der Passwort2-Daten in der Quellinstanz verwendet werden, in den Zielinstanzen zur Entschlüsselung verfügbar sind. Weitere Informationen finden Sie unter Key Management Framework Resource Exchange.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn Sie Passwort2-Daten über XML oder Datenquellen exportieren möchten, stellen Sie sicher, dass für die Zielinstanz KMF Key Exchange aktiviert ist. Diese Konfiguration stellt sicher, dass die Schlüssel auf Instanzebene, die zum Verschlüsseln der Passwort2-Daten in der Quellinstanz verwendet werden, in den Zielinstanzen zur Entschlüsselung verfügbar sind. Einzelheiten zu dieser Konfiguration finden Sie unter Key Management Framework Key Exchange.

> **Wichtig:** Die obigen Beispiele zeigen allgemeinere Szenarien. Wenn Sie jedoch andere Mittel zur Übertragung von mit Passwort2 verschlüsseltem Text zwischen Instanzen verwenden, müssen Sie KMF Ressourcenaustausch konfigurieren, um sicherzustellen, dass die Zielinstanz Passwort2-Daten entschlüsseln kann.

Downgraden einer Instanz nach der 3DES-Einstellung

Das Folgende gilt nur für Instanzen mit Passwort2-Feldern mit Eingabelängen von mehr als 125 Zeichen, und Sie haben die 3DES-Verschlüsselung bereits eingestellt.

Um eine Instanz mittels Klonen einer Instanz auf einen früheren Release als Vancouver herunterzustufen, führen Sie die folgenden Schritte aus, bevor Sie den Klon initiieren.

1. Überprüfen Sie, ob die Datenspeicherung so konfiguriert ist, dass Daten im Feld „password2“ erhalten bleiben.
2. Wenn ja, wenden Sie sich vor dem Anfordern eines Klons an den Support von ServiceNow, um die 3DES-Einstellung zu deaktivieren. Verwenden Sie im Feld „ **Grund** “ die Option „Downgrade-Voraussetzung für Passwort2-Unterstützung klonen“ aus.

Legacy-Passwort2-Felder

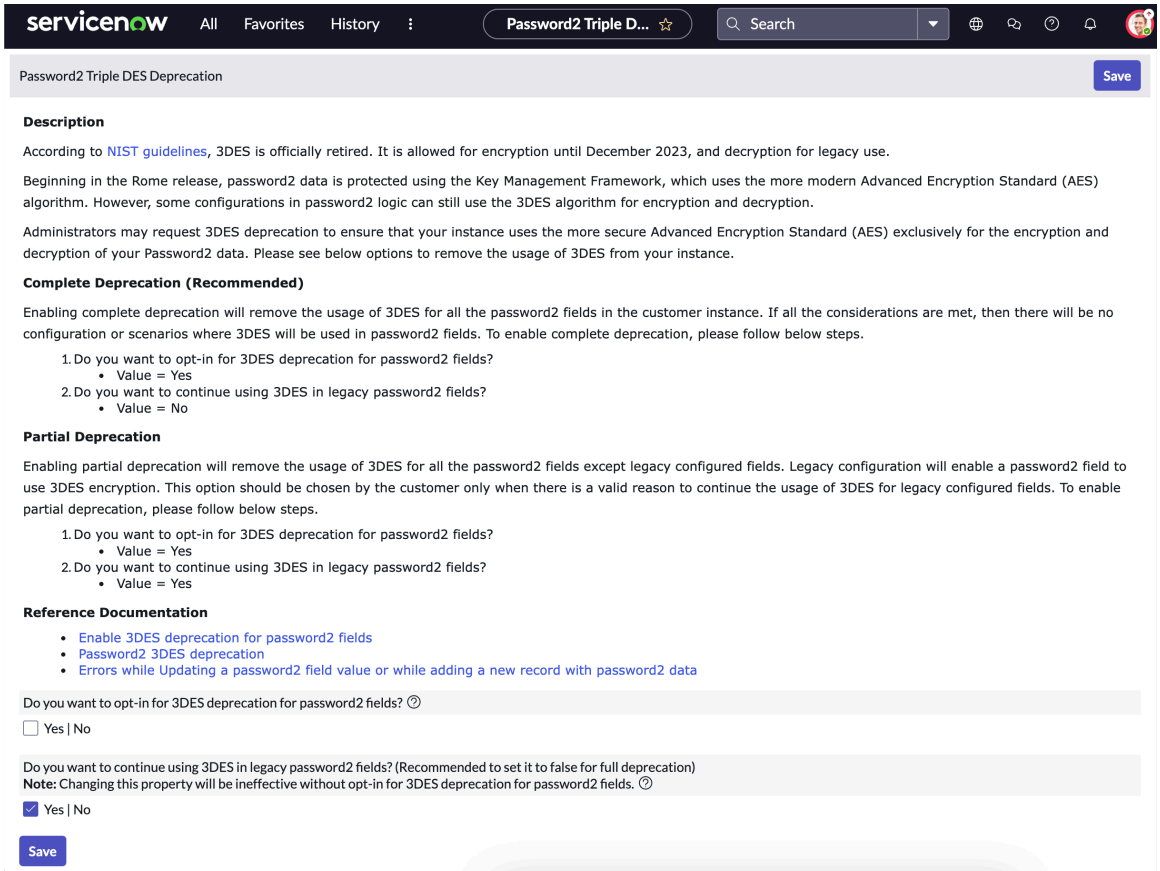
Ihre Instanz von verwendet die 3DES-Verschlüsselung, um Passwort2-Daten in Passwort2-Daten (vorRome) zu konvertieren. Nach Einstellung der 3DES-Verschlüsselung ist diese Option nicht mehr verfügbar. Wenn Sie diese Funktion weiterhin benötigen, fordern Sie eine teilweise Einstellung an (Details finden Sie im nächsten Abschnitt).

Anleitung zum Ablegen von 3DES

Nachdem Sie sich die vorangegangenen Anwendungsfälle angesehen haben, aktivieren Sie je nach Bedarf entweder die teilweise oder die vollständige Einstellung. Bei beiden Optionen können Sie auf das Formular zugreifen, um die Ablehnung zu steuern, indem Sie zu navigieren **Alle** > **Systemsicherheit** > **Sicherheitscompliance** > **Einstellung von Dreifach-DES für Passwort2**an.

> **Wichtig:** Sie müssen eine Hochstufung zum Sicherheitsadministrator durchführen, um das Modul „ **Sicherheits-Compliance“** anzuzeigen und diese Schritte auszuführen. Details zu diesem Prozess finden Sie unter Auf eine privilegierte Rolle hochstufen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Das Formular **„Passwort2-Dreifach-DES-Einstellung“** enthält Informationen zum Prozess der vollständigen und teilweisen 3DES-Einstellung. Wählen Sie die Optionen für eine vollständige oder teilweise Einstellung und anschließend **Speichern**aus.

Vollständige Einstellung

Wenn Sie die vollständige Einstellung aktivieren, wird die Verwendung von 3DES für alle Passwort2-Felder in Ihrer Instanz entfernt. Wenn alle Voraussetzungen erfüllt sind, gibt es keine Konfigurationen oder Szenarien, in denen 3DES in Passwort2-Feldern verwendet wird.

So aktivieren Sie die vollständige Einstellung:

- Wählen **Sie Möchten Sie die 3DES-Einstellung für Passwort2-Felder aktivieren?**
- Deaktivieren Sie die Option **Möchten Sie 3DES in Passwort2-Feldern von Vorgängerversionen weiterhin verwenden?**

Teilweise Einstellung

Durch das Aktivieren der teilweisen Einstellung wird die Verwendung von 3DES für alle Passwort2-Felder mit Ausnahme der in Vorgängerversionen konfigurierten Felder entfernt. Für Passwort2-Felder aus Legacy-Konfigurationen wird weiterhin die 3DES-Verschlüsselung verwendet. Wählen Sie diese Option nur aus, wenn Sie 3DES für in der Vorgängerversion konfigurierte Felder weiterhin verwenden müssen.

So aktivieren Sie eine teilweise Einstellung:

- Wählen **Sie Möchten Sie die 3DES-Einstellung für Passwort2-Felder aktivieren?**
- Wählen **Sie Möchten Sie 3DES in Passwort2-Feldern von Vorgängerversionen weiterhin verwenden?**

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nach der Einstellung von GlideEncrypter

Nach Abschluss des Abkündigungsprozesses gelten die folgenden Informationen für Ihre Instanz.

- password2-Felder unterstützen weiterhin die Entschlüsselung (aber nicht die Verschlüsselung) von mit 3DES verschlüsselten Daten.
- Vorhandene verschlüsselte 3DES-Daten in Passwort2-Feldern bleiben unverändert, bis der Feldwert von einem Anwender oder Workflow aktualisiert wird.
- Bei jeder Aktualisierung des Werts eines Passwort2-Felds wird mit 3DES verschlüsselter Text entfernt und durch den von KMF mit AES verschlüsselten Text ersetzt.
- In einigen Situationen zeigt Ihre Instanz beim Speichern der Passwortdaten möglicherweise einen Fehler an:

  ```
  Aktion abgebrochen: Der Passwortwert kann aufgrund eines technischen
  Problems nicht gespeichert werden. Hilfe finden Sie in KB1296997.
  ```

  Wenn dieser Fehler angezeigt wird, lesen Sie die Support-Informationen im Knowledge Base-Artikel KB1296997 .

Key Management Framework Resource Exchange

ServiceNow® Ressourcenaustausch ist eine Funktion von KMF, mit der Sie auf sichere Weise Ressourcen zwischen Instanzen austauschen können.

Terminologie

Wenn Sie Ressourcenaustauschverwenden, beachten Sie die folgende Terminologie:

Ressourcenaustausch Terminologie

Name	Beschreibung
Ressourcenaustausch	Der Prozess zum Austausch von Ressourcen zwischen Instanzen.
Key Exchange (KE)	Der Prozess zum Austausch von Schlüsseln über Instanzen hinweg.
Schlüsselquellinstanz (Schlüsselquelle)	Die Instanz, die die Schlüssel besitzt.
Schlüsselzielinstanz (Schlüsselziel)	Die Instanz, die die Schlüssel anfordert.

Übersicht

Ressourcenaustausch nutzt die kryptografischen APIs von KMF, um Vertraulichkeit, Integrität, Authentifizierung und Nachweisbarkeit bereitzustellen. Derzeit unterstützt RessourcenaustauschKey Exchange die Funktionalität []. Weitere Informationen finden Sie unter Key Management Framework Key Exchange.

Key Management Framework Key Exchange

KMF Key Exchange ist eine Teilmengenfunktion von KMF Ressourcenaustausch. Key Exchange überträgt verschlüsselte Daten sicher über mehrere Instanzen hinweg.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übersicht über Key Exchange

Key Exchange ermöglicht die sichere Übertragung von Schlüsseln zwischen Instanzen.

KMF Key Exchange bietet Kunden eine sichere Möglichkeit, KMF -Schlüssel zwischen Instanzen auszutauschen. Ein Anwendungsfall ist das Klonen von Daten. Mit Key Exchangewerden kryptografische Modulschlüssel während des Datenklons von KMF -Komponenten kopiert. Kryptografische Module, Modulschlüsselspezifikationen und Modulzugriffsrichtlinien sind im Klonierungsprozess enthalten. Schlüsselübertragungen sind nicht enthalten.

Key Exchange verwenden

Administratoren, die KMF für die Verschlüsselung auf Spaltenebene verwenden, können mit Key Exchange die Schlüssel zwischen Produktionsinstanzen klonen, wenn Daten geklont werden. Beim Klonen von Daten kann der -Administrator/Kryptografiemanager KMF :

- Tauschen Sie alle Schlüssel mit den anderen Instanzen aus.
- Tauschen Sie bestimmte Schlüssel einmal oder regelmäßig mit der anderen Instanz aus.
- Senden Sie bedarfsgesteuerte Anforderungen von der Zielinstanz an die Schlüsselquellinstanz.
- Tauschen Sie Schlüssel von der Quelle in das Ziel aus, um den Geheimtext neu zu schlüsseln.
  - Verwalten Sie die Ablaufzeit der Anforderung mit der Möglichkeit, Schlüssel zu löschen oder die Schlüsselaustauschanforderung abzulehnen, wenn die Anforderung abgelaufen ist.
  - Nachdem die Anforderung abgeschlossen und der Schlüssel importiert wurde, wird der verwendete Schlüssel als abgelaufen und mit einem Zeitstempel versehen.
  - Schlüsseltext in der Zielinstanz neu schlüsseln, der mit Schlüsseln aus der Quelle verschlüsselt wurde.

Unterstützte Modi

Key Exchange unterstützt mehrere Modi auf der Krypto-Spezifikationsebene des Verschlüsselungsmoduls:

Modus	Beschreibung
Automatisch (keine Konfiguration, Standardverhalten)	Alle Schlüssel werden während des Datenklonierungsprozesses ohne zusätzliche Konfiguration automatisch gesendet.
Konfigurierbar (einmaliges Konfigurations-Setup)	Der Administrator konfiguriert die Schlüssel, die während des Datenklonierungsprozesses gesendet werden sollen.
Manuell (Person in der Schleife)	Der Administrator sendet in der Zielinstanz eine bedarfsgesteuerte Anforderung an die Quelle. Die Anforderung muss von einem Administrator in der Schlüsselquellinstanz genehmigt werden.
Schlüssel erneut geben (automatisierte Anforderung)	Der Administrator wählt während des Setup-Prozesses für das Klonen die Option zur Schlüsselerneuerung aus.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie den Schlüsselaustausch

Key Management Framework (KMF) generiert während der Neuinstallation oder des Upgrades der Instanz einen automatischen Schlüsselaustausch für unterstützte kryptografische Module. verwaltet lokal den Datenverschlüsselungsschlüssel für die Instanz.

Vorbereitungen

Vor der Verwendung von Key Exchangemuss sowohl in der Ziel- als auch in der Quellinstanz ein kryptografisches Modul mit einem Schlüssel erstellt werden.

Erforderliche Rolle: sn_kmf.cryptographic_manager

Warum und wann dieser Vorgang ausgeführt wird

Key Exchange -Anforderungen werden von der Zielinstanz aus initiiert.

Der automatische Schlüsselaustausch ist beim Klonen einer Instanz standardmäßig aktiv, wobei die Eigenschaft in die Zielinstanz geklont wird. Konfigurieren Sie zusammen mit KMFSystemeigenschaften, um zu verwalten, wie Schlüssel während eines Instanzklons behandelt werden:

- **Automatischen Schlüsselaustausch deaktivieren:** Legen Sie die Eigenschaft *glide_encryption.auto_key_exchange.enabled* für wiederkehrende Klonanforderungen auf „ **falsch** “ fest.
- **Anforderungen zum automatischen Schlüsselaustausch senden**: Legen Sie diese Eigenschaft auf **„wahr“ fest**.

Wichtig: Die Basissystemeigenschaft ist standardmäßig auf „ **true** “ festgelegt. Dies bedeutet, dass der automatische Schlüsselaustausch beim Klonen einer Instanz aktiviert ist. Dieser Wert muss auf „ **false** “ festgelegt werden, wenn Sie die Funktion Schlüsseltext mit Schlüsselaustausch neu schlüsseln oder den wiederkehrenden Schlüsselaustausch verwenden. Weitere Einzelheiten erhalten Sie unter Tour zum Austausch wiederkehrender Schlüssel.

Prozedur

1. Navigieren zu **Alle** > **Schlüsselverwaltung** > **Ressourcenaustausch-Anforderungen** > **Neu**an.
2. Füllen Sie die Felder des Formulars aus.

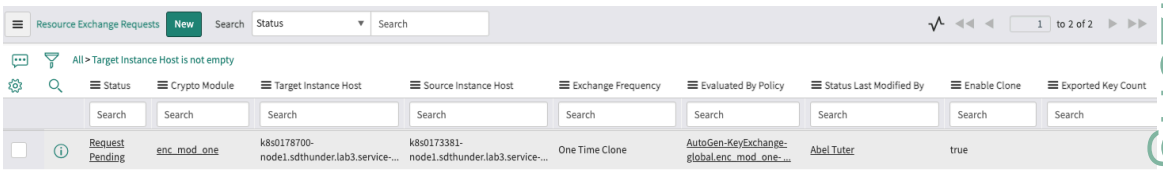
Ressourcenaustausch Anforderungsformularfelder

Name	Beschreibung
Austauschhäufigkeit	◦ **Ad**-hoc: Sendet Anforderungen von der wichtigsten Zielinstanz an die Quellinstanz. Geben Sie die sys_id der Instanz und die Hostinformationen für die Quelle ein. Wird mit „Rekey of Key Exchange“ nicht unterstützt. ◦ **Einmaliger Klon**: Einmaliger Austausch der Schlüssel von den Krypto-Quellspezifikationen zur Zielinstanz. ◦ **Wiederkehrender Klon**: Tauscht Schlüssel aus den ausgewählten Quell-Krypto-Spezifikationen mit der Zielinstanz in einem definierten wiederkehrenden Klon aus.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
<Source or Target> sys_id der Instanz	◦ Ad-hoc: Geben Sie die**sys_id**für die Quellinstanz ein, von der die Schlüssel angefordert werden sollen. ◦ **Einmaliger Klon**, **Wiederkehrender Klon**: Geben Sie die sys_id für die Zielinstanz ein, die die Anforderungen sendet. **Tipp:** Geben Sie im Anwendungsnavigator `stats.do` ein, um die Instanz-ID zu finden.
<Source or Target> Instanz-Host	Geben Sie den Hoststandort oder den Namen der Quell- oder Zielinstanz ein. **Tipp:** Beispiel : `instanceA.service-now.com`
Krypto-Spezifikationen	Die Schlüssel aus der Krypto-Spezifikation in einem Krypto-Modul definieren die zu klonenden Schlüssel. Sowohl für einmalige als auch für wiederkehrende Klonanforderungen erstellt Ihre -Instanz automatisch eine **Resource Exchange** -Modulzugriffsrichtlinie. Sie müssen eine Richtlinie nicht manuell konfigurieren. **Hinweis:** Wählen Sie das Symbol „), um die verfügbaren kryptografischen Spezifikationen zu durchsuchen.
Erneute Schlüsselerstellung nach importiertem Schlüssel aktivieren	Option zum Aktivieren der automatischen Schlüsselerstellung.

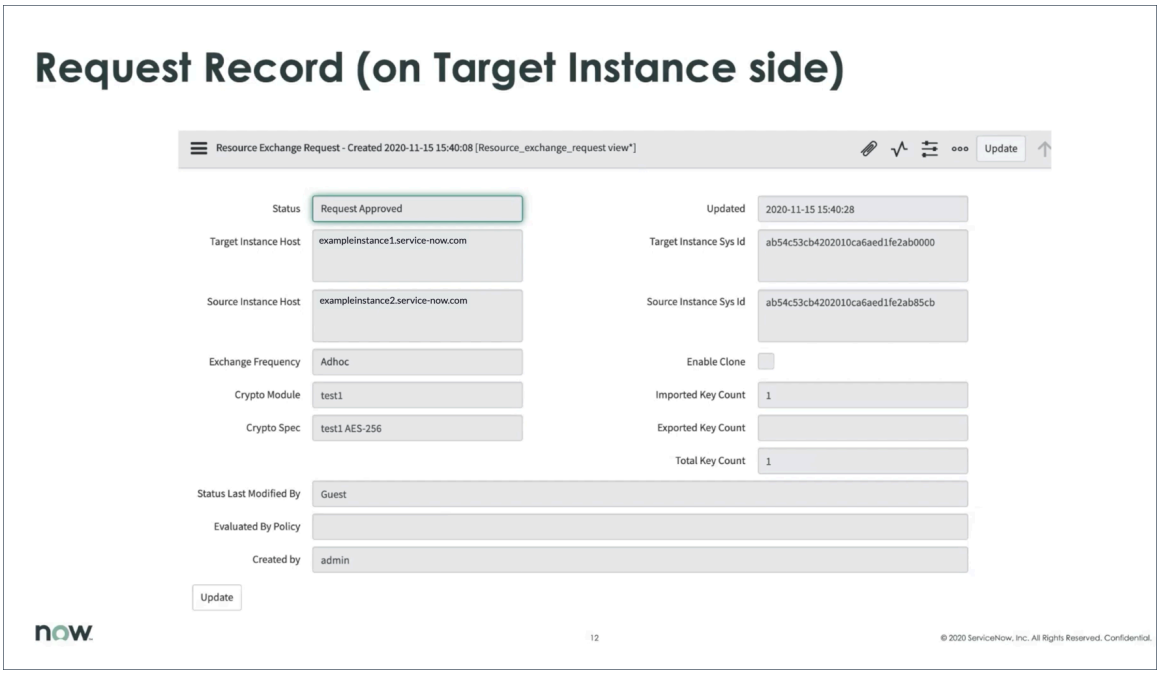
3. Wählen Sie **Absenden**.
   Bei Erfolg wird oben im Formular eine Bestätigung angezeigt. Die Tabelle „Anforderungen“ wird mit dem Eintrag „ **Anforderung ausstehend** “ sowohl in der Quellinstanz als auch in der Zielinstanz aktualisiert. Öffnen Sie den Anforderungsdatensatz, um den Status der Anforderung, die Anzahl der importierten Schlüssel und die Gesamtanzahl der Schlüssel auf dem Ziel- oder Quellhost anzuzeigen.



4. Die ausstehende Anforderung wird in der Quellinstanz akzeptiert, um den Austausch abzuschließen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zum Zeitpunkt des Klonens wird die Modulzugriffsrichtlinie in der Quellinstanz aufgerufen, um die Anforderung automatisch zu genehmigen und Schlüssel an das neu geklonte Ziel zu senden.



Ergebnisse
Nachdem ein Schlüsselaustausch versucht wurde, aktualisiert Ihre Instanz außerhalb der Produktion die Systemeigenschaft *`protected.script.values.kmf.rekeyed`*. Diese Eigenschaft ist in der Tabelle „Systemeigenschaften“ [sys_properties] sichtbar, nachdem versucht wurde, einen Schlüssel auszutauschen. Wenn die Verschlüsselung mit dem ausgetauschten Schlüssel erfolgreich ist, hat diese Eigenschaft den Wert **true**. Andernfalls hat die Eigenschaft den Wert **false**. Wenn der Wert „false“ ist, versucht die Instanz am nächsten Tag erneut, zu verschlüsseln.

Schlüsseltext mit Schlüsselaustausch neu schlüsseln

Ressourcenaustausch unterstützt die Neuschlüsselung von Geheimtext in der Zielinstanz, der mit Schlüsseln aus der Quelle verschlüsselt wurde. Die Aktivität zur erneuten Schlüsselerstellung wird im Schlüssellebenszyklus nachverfolgt.

Übersicht

Administratoren, die KMF für die Verschlüsselung auf Spaltenebene verwenden, können mit Key Exchange kryptografische Schlüssel zwischen Produktionsinstanzen beim Klonen von Daten neu schlüsseln. Ein aktiver Schlüssel muss zuerst in der Zielinstanz für die Neuschlüsselung verfügbar sein, da die Neuschlüsselung einen aktiven Schlüssel erfordert. Ein Verschlüsselungsauftrag wird automatisch vom System erstellt und ausgeführt, um den Quellschlüssel zu rotieren, neu einzugeben und den Geheimtext erneut zu verschlüsseln.

Mit Key Exchange können Sie:

- Legen Sie einen Ablaufzeitrahmen für die erneute Schlüsselerstellung fest.

  Wenn die Anforderung abgelaufen ist, wird die Anforderung abgelehnt und der Schlüssel gelöscht.

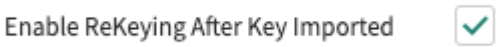
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Automatisieren Sie die Neuschlüsselung von Geheimtext, der mit Schlüsseln aus Quellinstanzen verschlüsselt wurde.

  Ein neuer geklonter Kryptoschlüssel wird verwendet, um den Geheimtext in der Zielinstanz erneut zu verschlüsseln.

- Der Zweck für die erneute Schlüsselerstellung wird während des Klonvorgangs eingerichtet und im Rahmen des Klonvorgangs automatisiert.
- Die Aktivität zur erneuten Schlüsselerstellung wird auf der Registerkarte „ **Module Key** “ (Modulschlüssel) des kryptografischen Moduls nachverfolgt. Greifen Sie auf den Lebenszyklusstatus des Schlüssels und die Schlüsselversion für die Schlüsselaktivität zu. Weitere Informationen finden Sie unter Schlüssel rotieren.

Konfigurieren Sie Key Exchange, und aktivieren Sie das Kontrollkästchen **Erneute Schlüsselerstellung nach Schlüsselimport** aktivieren, um zu aktivieren. Details siehe Konfigurieren Sie den Schlüsselaustausch.



Tour zum Austausch wiederkehrender Schlüssel

Verwenden Sie diese Tour, um einen wiederkehrenden Schlüsselaustausch in Ihrer -Instanz mit und Ressourcenaustauscheinzurichten.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_manager

Warum und wann dieser Vorgang ausgeführt wird

Dieses Beispiel zeigt, wie eine Zielinstanz Schlüssel von einer Hostinstanz anfordert.

- Bevor Sie dieses Verfahren ausführen können, müssen Sie eine Instanz klonen. Weitere Informationen finden Sie unter Systemklon .
- **Automatischer Schlüsselaustausch**: Die Basissystemeigenschaft *glide_encryption.auto_key_exchange.enabled*ist standardmäßig auf „ **wahr** “ festgelegt. Dies bedeutet, dass der automatische Schlüsselaustausch beim Klonen einer Instanz aktiviert wird. Die Eigenschaft wird in die Zielinstanz geklont.
- Deaktivieren Sie die automatische Einstellung, indem Sie die Eigenschaft auf **false festlegen**.

Prozedur

1. Erstellen Sie in der Quellinstanz ein Kryptomodul, oder greifen Sie mit column_level_encryption auf ein vorhandenes Kryptomodul zu, und richten Sie die verschlüsselten Feldkonfigurationen für die Geheimtextverschlüsselung für Key Exchangeein.
   Weitere Informationen finden Sie unter und.

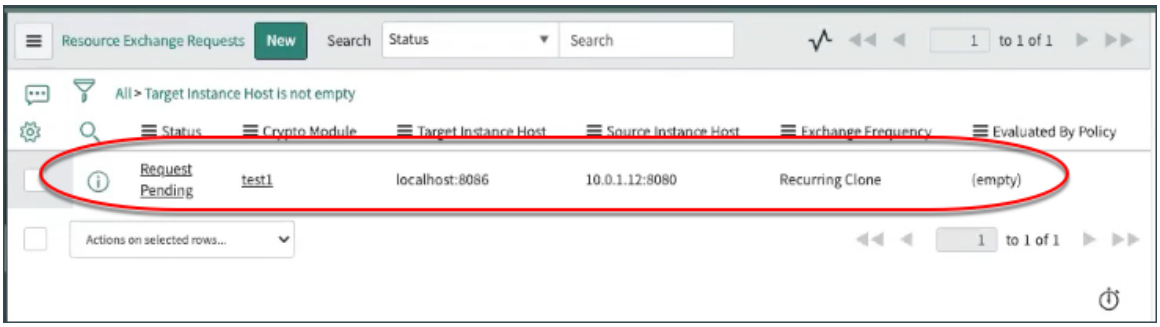
   a. Stellen Sie sicher, dass im Kryptomodul Schlüssel generiert wurden.

   Hinweis: Ihre -Instanz erstellt bei der Ausführung der Klonanforderung automatisch eine Modulzugriffsrichtlinie.

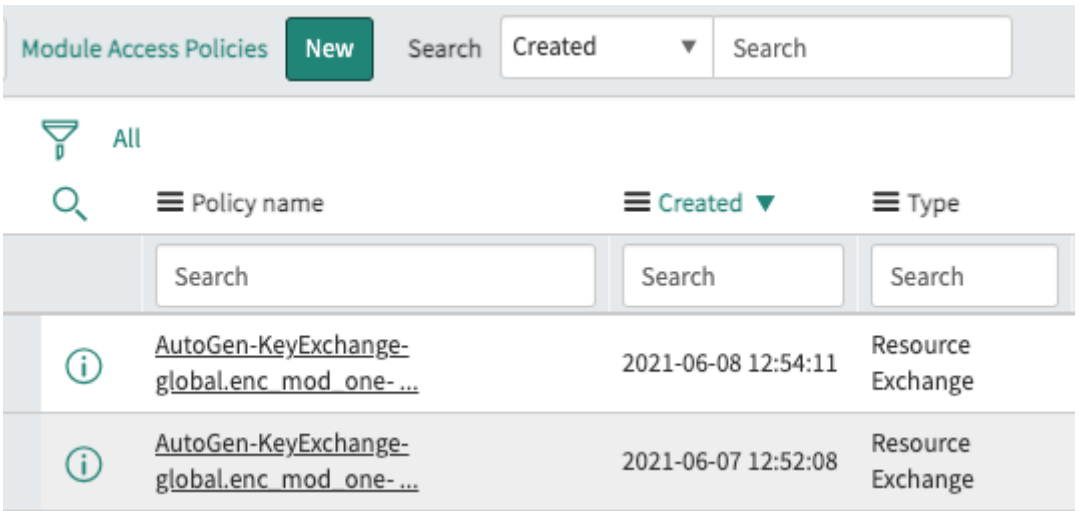
2. Navigieren Sie in der geklonten Instanz zu **Schlüsselverwaltung** > **Ressourcenaustausch-Anforderungen** > **Neu**an.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Füllen Sie das Formular aus, und wählen Sie **Wiederkehrender Klon** als Austauschhäufigkeit aus.
4. Navigieren Sie von der Zielinstanz des Klons zu **Schlüsselverwaltung** > **Ressourcenaustausch-Anforderungen**an.
   Die Anforderung von der Hostinstanz wird in der Tabelle angezeigt.

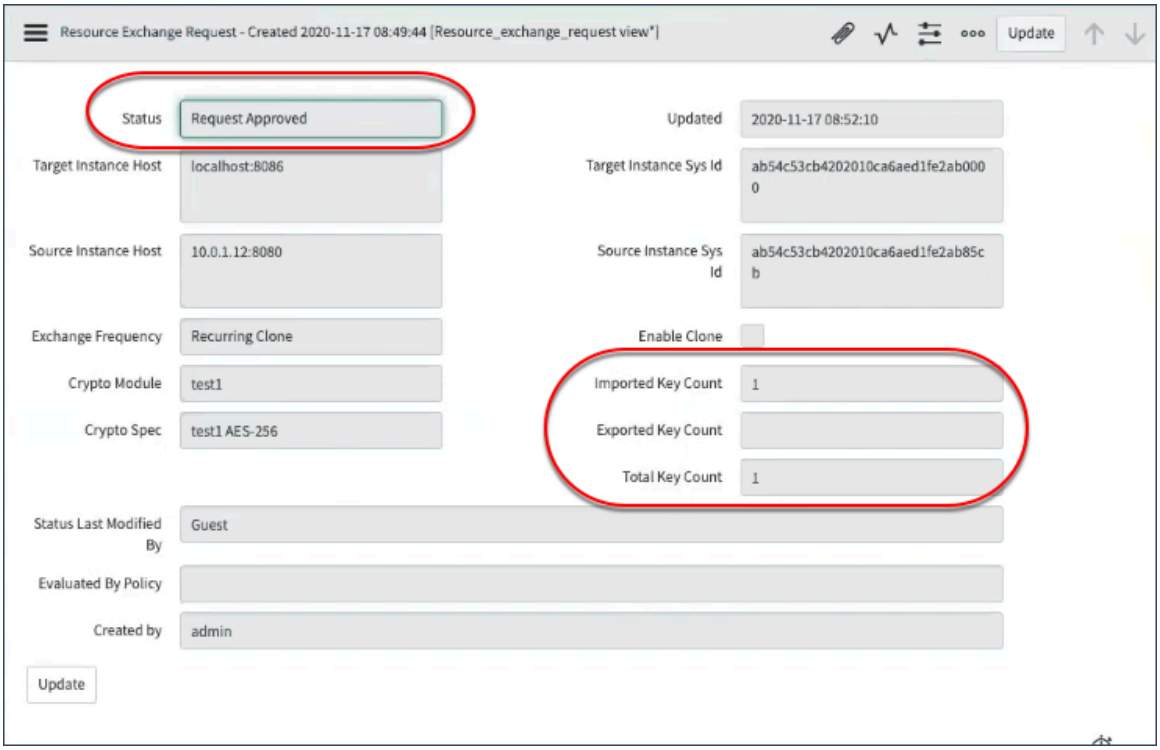


Wichtig: Für einmalige und wiederkehrende Klonanforderungen erstellt Ihre Instanz automatisch eine Modulzugriffsrichtlinie. Sie müssen eine Richtlinie nicht manuell konfigurieren. Zum Zeitpunkt des Klonens wird diese Richtlinie in der Quellinstanz aufgerufen, um die Anforderung automatisch zu genehmigen und Schlüssel an das neu geklonte Ziel zu senden.

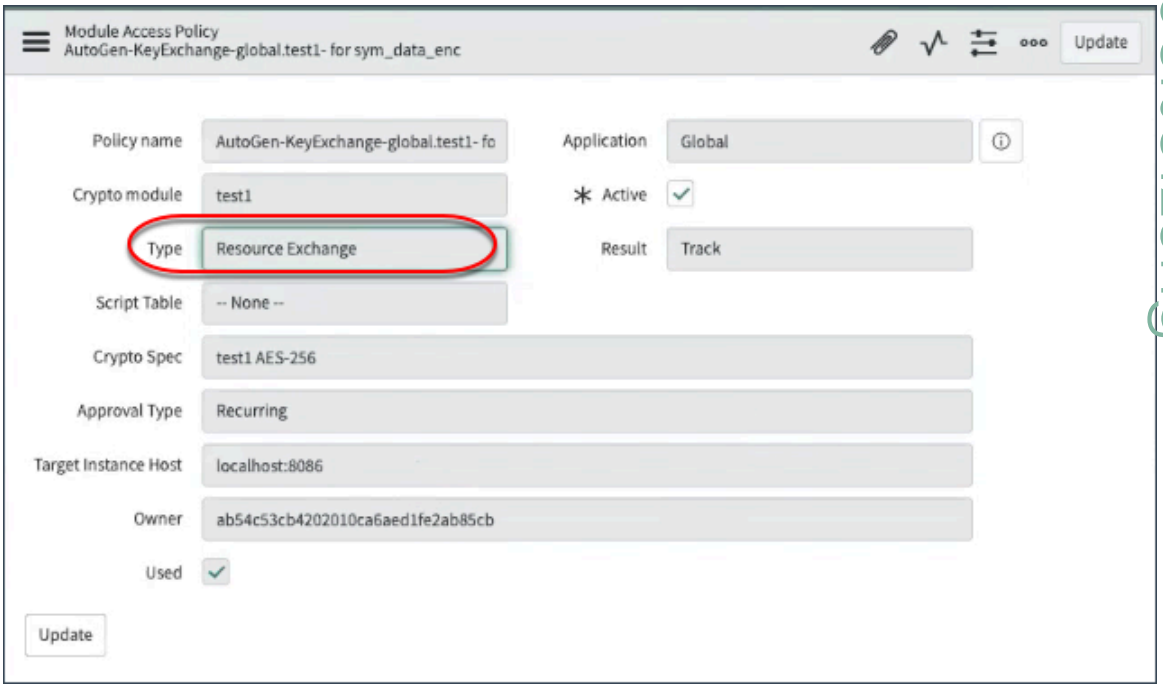


Im Formular „Anforderungen“ wird der Status auf „ **Anforderung genehmigt** “ aktualisiert, und im Datensatz wird das Feld Anzahl **importierter Schlüssel** angezeigt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Kehren Sie zur Hostinstanz zurück.
6. Zeigen Sie den Anforderungsdatensatz an, um die Anzahl der exportierten Schlüssel anzuzeigen.
7. Zeigen Sie den Datensatz „Modulzugriffsrichtlinie“ an, um zu sehen, dass der **Typ**Ressourcenaustauschist.



Hinweis: Ressourcenaustausch unterstützt auch die Neuschlüsselung von Geheimtext in der Zielinstanz. Siehe für Details.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse
Nachdem ein Schlüsselaustausch versucht wurde, aktualisiert Ihre Instanz außerhalb der Produktion die Systemeigenschaft *protected.script.values.kmf.rekeyed*. Diese Eigenschaft ist in der Tabelle „Systemeigenschaften“ [sys_properties] sichtbar. Wenn die Verschlüsselung mit dem ausgetauschten Schlüssel erfolgreich ist, hat diese Eigenschaft den Wert **true**. Andernfalls hat die Eigenschaft den Wert **false**. Wenn der Wert „false“ ist, versucht Ihre Instanz am nächsten Tag erneut, zu verschlüsseln.

Infrastruktursicherheit

Verwenden Sie Tools für die Infrastruktursicherheit, um Zertifikate zu erstellen, hochzuladen und zu verwalten, die Ihre Instanz zum Verschlüsseln des Datenverkehrs von Client zu Server verwendet.

Das Plugin „Infrastructure Security“ bietet Tools, mit denen Sie TLS-Verschlüsselungen und -Zertifikate (Transport Layer Security) verwalten können. Ihre Instanz von verwendet TLS, um den Datenverkehr vom Client zum Server zu verschlüsseln.

Wählen Sie die in Ihrer Instanz verwendeten Verschlüsselungen aus

Auf der **Seite TLS**können Administratoren konfigurieren, welche Rechenzentrums-Verschlüsselungen auf ihrer Instanz verwendet werden sollen, und die Reihenfolge auswählen, in der die Verschlüsselungen getestet werden.

Generieren Sie eigene Zertifikate, und laden Sie sie hoch

Verwenden Sie die Sicherheitstools der Infrastruktur, um eigene Zertifikatsignaturanforderungen zu generieren, die von der Zertifizierungsstelle Ihrer Wahl signiert werden können. Anschließend können Sie das signierte Zertifikat mit den -Tools in das Lastenausgleichsmodul Ihrer Instanz hochladen.

Überwachen Sie den Status Ihrer Verschlüsselungen und Zertifikate

Verwenden Sie die Seiten **TLS-Einstellungen** und **SYOC-Einstellungen**, um den Status der Änderungen anzuzeigen, die Sie an Ihren Verschlüsselungen und Zertifikaten vorgenommen haben.

Installieren Sie das Plugin „Infrastructure Security“.

Installieren Sie das Plugin ServiceNow „ Sicherheitseinstellungen für die Infrastruktur“ (com.glide.infrastructure_security), um diese Funktionen zu verwenden. Weitere Informationen zur Aktivierung von Plugins finden Sie unter Plugins aktivieren .

Aktivieren Sie nach der Installation des Plugins die SYOC-Funktion (Sign Your Own Security), indem Sie die Systemeigenschaft *sn_infra_sec.syoc.enabled*auf den Wert `true`festlegen.

Hinweis: Wenn die Eigenschaft *sn_infra_sec.syoc.enabled*in Ihrer Instanz nicht verfügbar ist, müssen Sie sie erstellen. Details zu diesem Vorgang finden Sie unter Systemeigenschaft hinzufügen .

Generiert eine Zertifikatsignaturanforderung

Verwenden Sie die Seite „Certificate Signing (CSR) generieren“, um eine Zertifikatsignaturanforderung zur Unterstützung von vom Kunden signierten Zertifikaten für Ihr Instanz-Lastenausgleichsmodul zu erstellen.

Vorbereitungen
Erforderliche Rolle: admin

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Plugin „Infrastructure Security“ (com.glide.infrastructure_security) muss installiert sein, um diese Schritte auszuführen. Weitere Informationen zu diesem Plugin finden Sie unterInfrastruktursicherheit.

Informationen zur Verwendung von anwenderdefinierten URLs mit ServiceNowfinden Sie unter Legen Sie eine anwenderdefinierte URL als Instanz-URL fest.

Prozedur

1. Navigieren zu **Alle** > **Sicherheitseinstellungen der Infrastruktur** > **CSR generieren**an.
2. Fügen Sie Ihrer Anforderung eine oder mehrere Domänen hinzu.

   a. Klicken Sie unter der Überschrift **Domänen** auf die Schaltfläche **Hinzufügen**.

   b. Geben Sie im Popup-Fenster die Domäne ein, und wählen Sie **OK**.

   c. Wiederholen Sie diese Schritte nach Bedarf, um weitere Domänen hinzuzufügen.

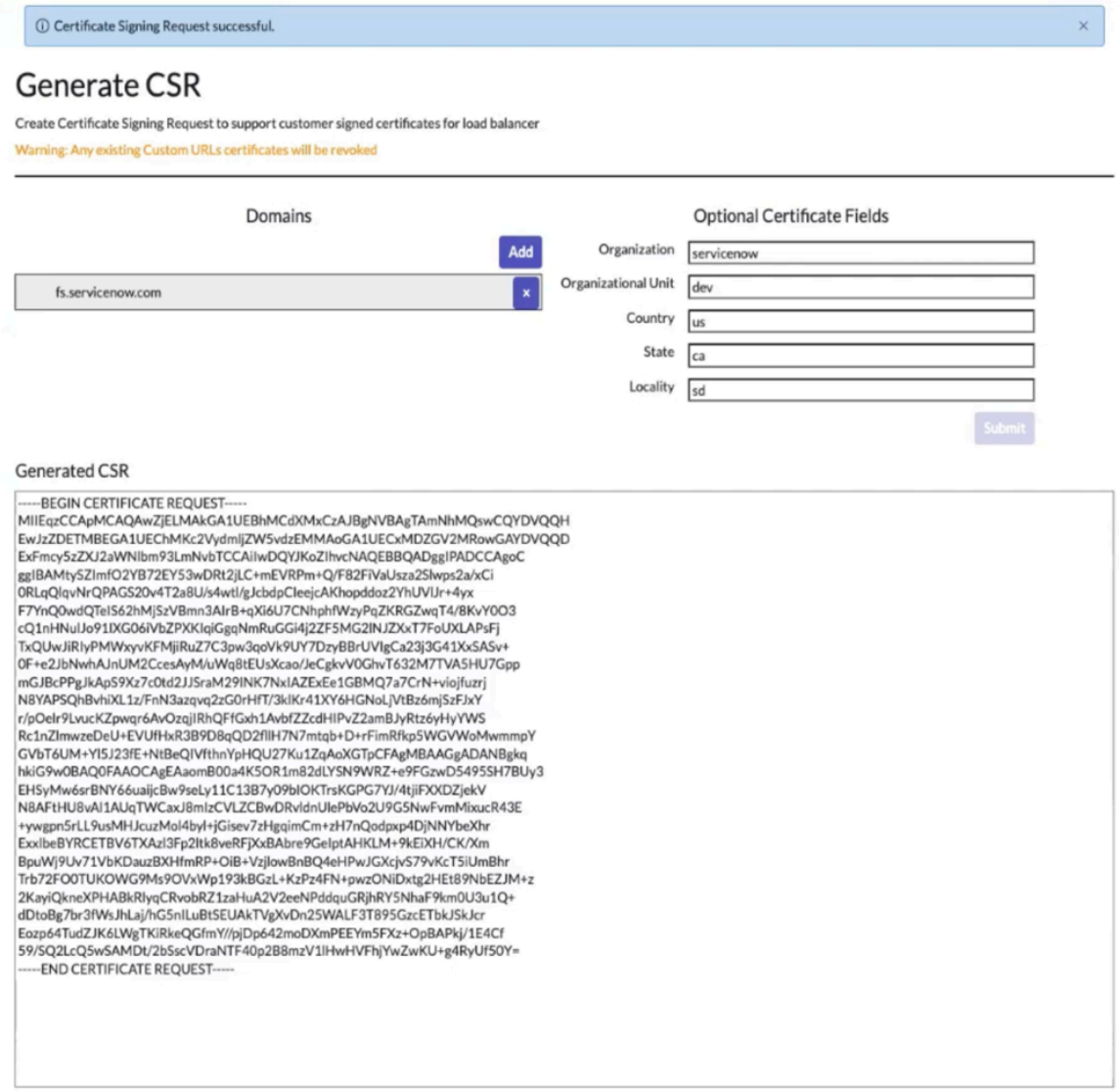
   > **Hinweis:** Domänen können entfernt werden, indem Sie links neben dem jeweiligen Domäneneintrag auf die Schaltfläche X klicken.

3. Geben Sie in die **optionalen Zertifikatfelder**alle Informationen ein, die Sie in Ihrer Anforderung enthalten möchten.
4. Wählen Sie **Absenden**.

> **Warnung:** Sie können keine Anforderung senden, während eine andere Anforderung generiert wird. Wenn dieses Problem auftritt, wird der Fehler „Ressource in Konflikt“ angezeigt. Zum Verarbeiten brechen Sie die aktuelle Anforderung ab, oder warten Sie, bis die aktuelle Anforderung verarbeitet wird, bevor Sie eine weitere senden.

Nachdem Sie Absenden ausgewählt haben, generiert Ihre **-Instanz**die Zertifikatsignaturanforderung. Die Anforderung wird im Feld **Generierte CSR** angezeigt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Kopieren Sie den Inhalt des Felds **Generierte CSR**.

Password2-Verschlüsselung mit dem Key Management Framework (KMF)

Unterstützt von Key Management Frameworkverwenden Sie den Password2 Feldtyp (zweifach verschlüsselt), um anwenderdefinierte Felder mit Aufgabentrennung, Schlüsselschutz und Lebenszyklusverwaltung zu verschlüsseln und zu entschlüsseln. Es erfüllt die Richtlinien NIST 800-57 und bietet Schutz gemäß FIPS 140-2-L3.

Password2 ist ein Textfeld, in dem Passwörter mit bidirektionaler Verschlüsselung gespeichert werden. Die bidirektionale Verschlüsselung speichert Passwörter als sicheren verschlüsselten Wert, der innerhalb der Instanz entschlüsselt werden kann.

Tipp: Ab Release Vancouver können Administratoren die 3DES-Verschlüsselung für Password2-Felder durch den neueren Advanced Encryption Standard (AES) ersetzen. Details finden Sie unter GlideEncrypter-Nutzung von 3DES für Password2-Felder einstellen.

Aktivierung

Password2 -Funktionalität ist standardmäßig aktiviert. Sie wird durch die Eigenschaft *glide.kmf.encrypter.enabled* gesteuert, die für alle neuen Instanzen und Upgrades

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

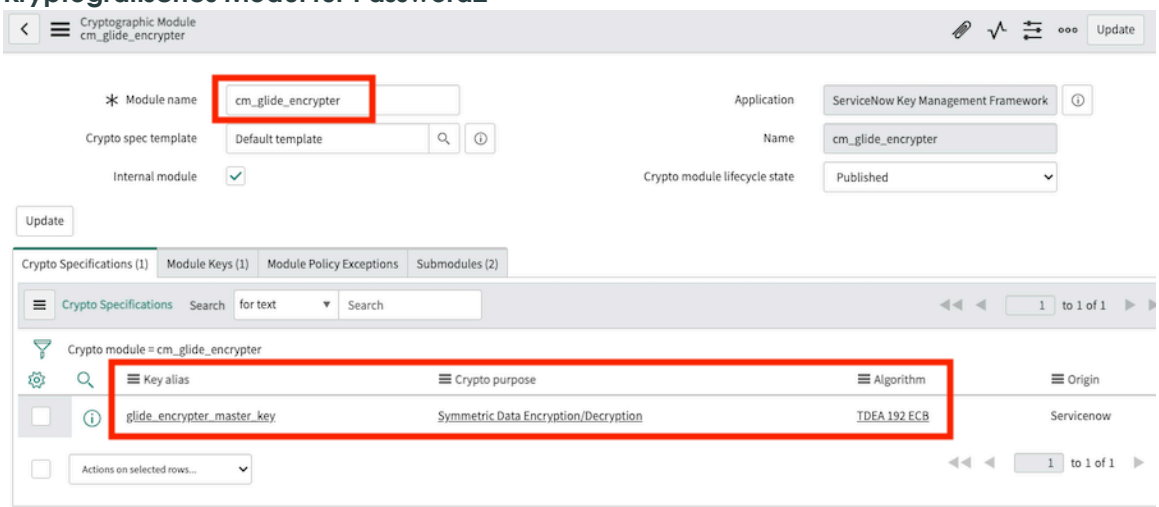
Automatische Übersetzung

auf „ **true** “ festgelegt ist. Sie müssen [] nicht aktivieren, um Password2Verschlüsselung auf Spaltenebene Enterprise zu verwenden.

Funktionsweise von Password2

Key Management Framework stellt das übergeordnete kryptografische **Basissystemmodul cm_glide_encrypter bereit**. Dieses Modul stellt eine kryptografische Spezifikation und einen Schlüssel bereit, mit dem veraltete Password2 -Felder entschlüsseln kann.

Kryptografisches Modul für Password2



Dieses cm_glide_encrypter-Modul kann Submodule mit jeweils einem eigenen Modulschlüssel und einer eigenen Spezifikation haben. Wenn ein Submodul mit demselben Anwendungsbereich wie die Anwendung im Feld Password2 vorhanden ist, verwendet das System das Submodul. Wenn beispielsweise eine Tabelle in der Anwendung ServiceNow® Kundenservice ein Submodul aufweist und Sie Informationen in ein Feld Password2 in einer Tabelle im Anwendungsbereich Kundenservice] schreiben, ruft der kryptografische Prozess das Submodul Kundenservice auf. Der Prozess verwendet auch den Schlüssel dieses Submoduls für die Verschlüsselung und Entschlüsselung mit einem eindeutigen AES 256 GCM-Verschlüsselungsschlüssel. Pro Anwendungsbereich ist ein Submodul zulässig. Das übergeordnete Modul wird nicht immer für den globalen Bereich verwendet. Im Allgemeinen verwenden neue Felder „instance_level_glide_encrypter“.

Hinweis: Sie können keine eigenen Submodule in Xanaduerstellen. Submodule werden in verschiedenen Anwendungs-Plugins auf Now Platformbereitgestellt. Sie können Schlüssel in Untermodulen rotieren, aber nicht im übergeordneten cm_glide_encrypter-Modul.

Domain Separation und On-Premise-Kunden

KMF Password2 unterstützt keine Domänentrennung. Sie können Password2 mit lokalen Instanzen verwenden.

Legacy- Password2 und aktueller Password2

In Xanaduwurde das vorhandene Feld Password2 aktualisiert.

Die aktuelle Implementierung von Password2:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Verwendet Key Management Framework gemäß den NIST 800-57 -Richtlinien zum Packen von Schlüsseln und bietet FIPS 140-2-L3- Schutz für die gesamte Schlüsselhierarchie.
- Enthält Funktionen zum Erstellen dedizierter und eindeutiger KMF Password2 -Submodule für bestimmte -Anwendungen, die Kontrolle über den gesamten Anwendungsbereich bieten. Jedes Submodul verfügt über einen eigenen eindeutigen AES 256 GCM-Verschlüsselungsschlüssel.

Passwort2-Felder in Skripts

Wenn Sie mit einem Skript auf Felder Password2 zugreifen, führen Sie das Skript im gleichen Umfang wie der Tabellenbereich aus. Verwenden Sie `setDisplayValue ()`, um Password2 -Werte zu verschlüsseln, und `getDecryptedValue ()`, um den Wert zu entschlüsseln und zu lesen.

Hinweis: Verwenden Sie die `GlideEncrypter()` – API nicht für Felder Password2.

Dieses Beispielskript zeigt, wie „ `my@Password` “ in der Spalte „password2“ der Tabelle „table_xyz“ verschlüsselt wird.

```
var  gr =  new GlideRecord('table_xyz');
gr.setDisplayValue('pwd2column_name', 'my@Password');
gr.insert();
```

Wichtig: Sie können die API „ `setValue()` “ nicht für das Feld Password2 verwenden.

Dieses Beispielskript zeigt, wie Sie dasselbe Feld entschlüsseln, um den Wert abzurufen:

```
var  gr =  new GlideRecord('table_xyz');
gr.query();
gr.next();
var ge=gr.getElement('pwd2column_name');
var ged1 = ge.getDecryptedValue();
```

Wichtig: Die `getDecryptedValue()` – API ist nicht bereichsbezogen. Es ist global verfügbar.

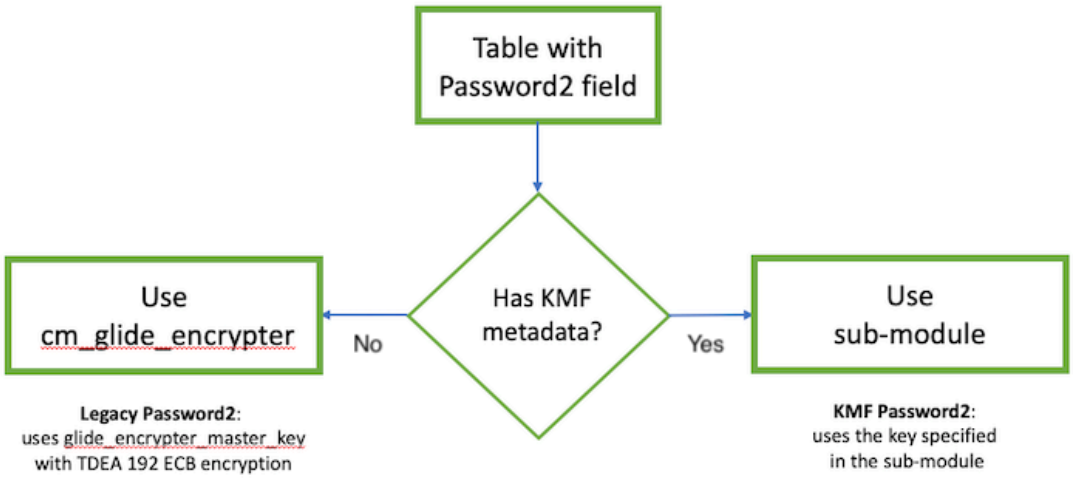
1. Wenn Sie Daten in einem Feld Password2 verschlüsseln, bestimmt das System den Anwendungsbereich, in dem sich das Feld Password2 befindet.
2. Das System sucht dann nach einem Submodul des übergeordneten Moduls **cm_glide_encrypter** mit demselben Umfang wie die Anwendung, wenn die Eigenschaft auf *true* festgelegt ist.

   Hinweis: Wenn ein Submodul mit demselben Umfang vorhanden ist, verwendet es die Submodulspezifikation und den Schlüssel zur Verschlüsselung.

In der folgenden Abbildung wird erläutert, wie Ihre -Instanz Daten in Feldern Password2 entschlüsselt:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Password2-Entschlüsselungs-Flow



KMF Password2 -Migrationsauftrag

Für Kunden, die ein Upgrade von früheren Releases durchführen, wird ein Migrationsauftrag bereitgestellt. Es nimmt Daten, die mit einer veralteten Password2 -Verschlüsselung verschlüsselt sind, und verschlüsselt sie mit dem Schlüssel in einem KMF Password2 -Submodulschlüssel erneut. Die erneute Verschlüsselung gilt nur für Tabellen mit Feldern Password2 in Anwendungsbereichen, für die auch Submodule für diesen Bereich erstellt wurden. Beispielsweise wird ein Legacy-Feld Password2 in der Anwendung **XYZ_example** (mit Anwendungsbereich **XYZ_example**) nur dann erneut verschlüsselt, wenn ein Submodul für den Anwendungsbereich **XYZ_example** unter dem übergeordneten Modul cm_glide_encrypter vorhanden ist.

Die Verschlüsselungsschlüssel KMF Password2 im Submodul sind in der Schlüsselhierarchie KMF geschützt (umschlagverschlüsselt).

Zertifikate

Ihre Instanz von benötigt Zertifikate, um sichere Verbindungen herzustellen und Signaturen zu validieren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Untersuchen



Lernen Sie die wichtigsten Funktionen und den Geschäftsnutzen von Zertifikaten kennen.

Konfigurieren



Planen Sie Ihre Kernkonfigurationen.

Hochladen



Planen und richten Sie die Anwendung ein.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zertifikate erkunden

Ihre Instanz von benötigt Zertifikate, um sichere Verbindungen herzustellen und Signaturen zu validieren.

Zertifikate werden für folgende Funktionen verwendet:

- LDAPS
- Gegenseitige Authentifizierung für ausgehenden Webservice
- Webservice – Sicherheit
- MID Server

Um ein Zertifikat zu verwenden, müssen Sie ein Zertifikat für den gesicherten Server oder Client generieren oder erwerben und in eine Instanz hochladen.

LDAP-Zertifikate

Ein SSL-Zertifikat ist erforderlich, damit die Instanz eine LDAP-über-SSL-Verbindung (LDAPS-Protokoll) mit einem LDAP-Server herstellen kann.

Die Instanz akzeptiert zwei Arten von LDAP-Zertifikaten:

Zertifikat	Typ	Erforderlich für
LDAP-Serverzertifikat	Jeder unterstützte Typ	Alle LDAP-Konfigurationen
LDAP-Client-Zertifikat	Java-Schlüsselspeichertyp	Gegenseitige Authentifizierung

Wenn mehrere Serverzertifikate vorhanden sind, probiert die Instanz jedes Serverzertifikat nacheinander aus, bis der LDAP-Server die Verbindung zulässt. Wenn Sie mehrere LDAP-Server verwenden, müssen Sie das SSL-Zertifikat für jeden LDAP-Server einbeziehen.

Die gegenseitige Authentifizierung erfordert, dass der Client zusätzlich zum Server ein Zertifikat vorlegt. Wenn Ihr LDAP-Server eine gegenseitige Authentifizierung erfordert, müssen Sie auch das Client-Zertifikat Ihres LDAP-Servers in einem Zertifikat des Java-Schlüsselspeichertyps bereitstellen.

Zertifikatkriterien

Ein gültiges Zertifikat muss die folgenden Kriterien erfüllen:

- Das Zertifikat kann eine Schlüsselgröße von bis zu 2048 Bits haben.
- Das -Zertifikat muss eine der folgenden Dateierweiterungen aufweisen:

Erweiterung	Beschreibung
DER	Das Format für differenzierte Codierungsregeln ist eine binäre Nachrichtenübertragungssyntax. Dieses Format unterstützt auch die Dateierweiterungen .cer und .CRT.
cer	Zertifikatdateierweiterungen für Zertifikate, die das Format „Distinguished Encoding Rules“ verwenden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterung	Beschreibung
CRT	Zertifikatdateierweiterungen für Zertifikate, die das Format „Distinguished Encoding Rules“ verwenden.
PEM	Das erweiterte E-Mail-Format für Datenschutz ist ein base64-codiertes DER-Zertifikat, das zwischen den Textzeichenfolgen „------BEGIN CERTIFICATE------“ und „-----END-CERTIFICATE-----“ eingeschlossen ist.

Zertifikatvertrauen

Standardmäßig vertraut Ihre -Instanz nur Zertifikaten einer Zertifizierungsstelle (Certificate Authority, CA), die in der Java Virtual Machine (JVM) anerkannt ist. Selbst- und unternehmenssignierte Zertifikate sind nicht vertrauenswürdig.

Hinweis: Weitere Informationen zu den Eigenschaften, die sich auf die Verwendung von Zertifikaten auswirken, finden Sie unter Sichere Kommunikation unter Härtungseinstellungen für Instanzsicherheit.

Generieren eines LDAP-Client-Zertifikats

Generieren Sie ein LDAP-Client-Zertifikat für die gegenseitige Authentifizierung mit OpenSSL. Die endgültige Ausgabe ist ein PKCS#12-Zertifikat, das in einem Java-Schlüsselspeicher gespeichert ist.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Weitere Informationen zum Generieren von Zertifikaten finden Sie in der OpenSSL-Dokumentation . Diese Schritte setzen voraus, dass Sie Zugriff auf OpenSSL haben.

Geben Sie diese Befehle in eine Befehlszeilenschnittstelle ein.

Prozedur

1. Generieren Sie ein selbstsigniertes Client-Zertifikat.

   Example

   Beispiel: Mit diesem Befehl wird das Client-Zertifikat „test1-cert.crt“ basierend auf dem privaten Schlüssel „test1-key.key“ erstellt.

   ```
   openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
    test1-key.key -out test1-cert.crt
   ```

2. Konvertieren Sie sowohl die Zertifikatdatei als auch den privaten Schlüssel in PKCS#12 (eine Datei mit der Erweiterung „.pfx“ oder „.p12“).

   Example

   Beispielsweise konvertiert dieser Befehl das Client-Zertifikat und den privaten Schlüssel in ein PKCS#12-Zertifikat mit der Bezeichnung test1-certificate.pfx.

   ```
   openssl pkcs12 -export -out test1-certificate.pfx -inkey test1-key.key
    -in test1-cert.crt
   ```

3. Generieren Sie den Java Key Store, und importieren Sie die pkcs12-Datei in den Java Key Store.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Example
Beispiel: Dieser Befehl importiert das Zertifikat in den Java-Schlüsselspeicher test1.jks.

```
keytool -importkeystore -srckeystore test1-certificate.pfx
 -srcstoretype PKCS12 -destkeystore test1.jks
```

4. Laden Siedas Zertifikat aus der Schlüsselspeicherdatei (`test1.jks`) in die Instanz hoch.

Hinweis:

Wenn Sie zum Hochladen in eine lokale Instanz ein Zertifikat mit der Erweiterung „.jks“ verwenden und die Fehlermeldung „Kein gültiges Zertifikat für die Verarbeitung des Anwendungsuploads gefunden“ angezeigt wird, verwenden Sie stattdessen ein Zertifikat mit der Erweiterung „.pfx“.

Nächste Maßnahme
Ein Zertifikat wird in eine Instanz hochgeladen

Ein Serverzertifikat wird generiert

Sie können mit dem Schlüsseltool eine neue Java-Schlüsselspeicherdatei generieren, eine Zertifikatsignaturanforderung (Certificate Signing Request, CSR) erstellen und den privaten Schlüssel, das öffentliche Zertifikatpaar und signierte Zertifikate in den Schlüsselspeicher importieren.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Weitere Informationen zum Generieren von Schlüsseln und CSRs finden Sie in der Java-Keytool-Dokumentation .

Geben Sie diese Befehle in eine Befehlszeilenschnittstelle ein:

Prozedur

1. Generieren Sie einen Java-Schlüsselspeicher und ein Schlüsselpaar.

Example
Beispiel: Dieser Befehl erstellt einen Schlüsselspeicher mit der Bezeichnung my.keystore und generiert innerhalb des Schlüsselspeichers einen privaten Schlüssel mit der Bezeichnung mydomain.

```
keytool -genkey -alias mydomain -keyalg RSA -keystore my.keystore
```

2. Generieren Sie eine CSR für einen vorhandenen Java-Schlüsselspeicher.

Example
Beispielsweise generiert dieser Befehl eine CSR namens mydomain.csr oder den Schlüssel mydomain.

```
keytool -certreq -alias mydomain -keystore my.keystore -file
 mydomain.csr
```

3. Importieren Sie ein Zertifikat einer Stamm- oder Zwischenzertifizierungsstelle (Certificate Authority, CA) in den Java-Schlüsselspeicher.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Example
Dieser Befehl importiert beispielsweise das CA-Zertifikat für Thawte. Dieser Befehl geht davon aus, dass die Zertifizierungsstelle die Zertifizierungsinstanz unterzeichnet hat.

```
keytool -import -trustcacerts -alias root -file Thawte.crt -keystore
 my.keystore
```

4. Importieren Sie ein signiertes primäres Zertifikat in den Java-Schlüsselspeicher.

Example
Beispiel: Dieser Befehl importiert das signierte Zertifikat mydomain.crt in den Schlüsselspeicher.

```
keytool -import -trustcacerts -alias mydomain -file mydomain.crt
 -keystore my.keystore
```

5. Laden Sie das Zertifikat in der Schlüsselspeicherdatei (my.keystore) in die Instanz hoch.

Nächste Maßnahme
Ein Zertifikat wird in eine Instanz hochgeladen

Ein Zertifikat wird in eine Instanz hochgeladen

Fügen Sie der Instanz ein Zertifikat aus dem Modul Zertifikate hinzu.

Lädt ein Zertifikat in eine Instanz hoch

Lädt ein Zertifikat in eine Instanz hoch.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn ein Zertifikat auf dem ADFS-Server aktualisiert wird, müssen Sie auch ein aktualisiertes Zertifikat in die Instanz hochladen.

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Zertifikate**an.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular aus.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen Namen für das Zertifikat an.
Ablaufbenachrichtigung	[Optional] Wählen Sie aus, ob Sie eine Benachrichtigung senden möchten, wenn das Zertifikat abläuft.
Aktiv	Wählen Sie aus, ob die Instanz dieses Zertifikat für sichere Kommunikation und Signaturanforderungen verwenden soll.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Kurzbeschreibung	[Optional] Geben Sie eine Textbeschreibung des Zertifikats ein, z. B. den Anforderer oder den Servernamen.
Format	Wählen Sie das Zertifikatformat aus. Die Instanz unterstützt die Formate PEM und DER.
Typ	Wählen Sie den Zertifikatcontainer aus. Die Instanz von erkennt Zertifikate aus Truststores, Java-Schlüsselspeichern und PKCS#12-Schlüsselspeichern.
PEM-Zertifikat	Geben Sie den base64-codierten PEM-Formatierten Text ein, der das DER-Zertifikat enthält. Die Instanz decodiert das Zertifikat, um die Felder **Gültig ab**, **Läuft**ab, **Läuft ab in Tagen**, **Ausstellerund** **Betreff** aus.

4. Wählen Sie **Absenden**.

   Während des Uploads extrahiert das Modul die schreibgeschützten Eigenschaften des -Zertifikats und zeigt sie in den folgenden Feldern an:

   - Gültig ab Datum
   - Ablaufdatum
   - Bearbeiter
   - Betreff des Zertifikats

5. Wählen Sie **Validate Stores/Zertifikate** (Speicher/Zertifikate validieren) aus, um zu überprüfen, ob das Zertifikat korrekt ist.
   Wenn bei der Instanz Fehler beim Zertifikat oder Schlüsselspeicher auftreten, wird eine Fehlermeldung angezeigt.

Ein vertrauenswürdiges Serverzertifikat wird hochgeladen

Durch das Hochladen des vertrauenswürdigen Serverzertifikats des Service Providers stellt die Instanz sicher, dass eine Verbindung zu einem gültigen und sicheren Service hergestellt wird.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Die Instanz validiert ausgehende Webservice-Aufrufe mithilfe des vom Service Provider bereitgestellten Zertifikats.

Prozedur

1. Erstellen Sie einen neuen Zertifikatdatensatz mit dem Typ **Truststore**-Zertifikat.
2. Führen Sie eine der folgenden Aktionen aus:
   - Hängen Sie das DER-formatierte Zertifikat des Service Providers an.
   - Kopieren Sie das PEM-Formatzertifikat des Service Providers, und fügen Sie es in das Feld **PEM-Zertifikat** ein.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verschlüsselung auf Spaltenebene

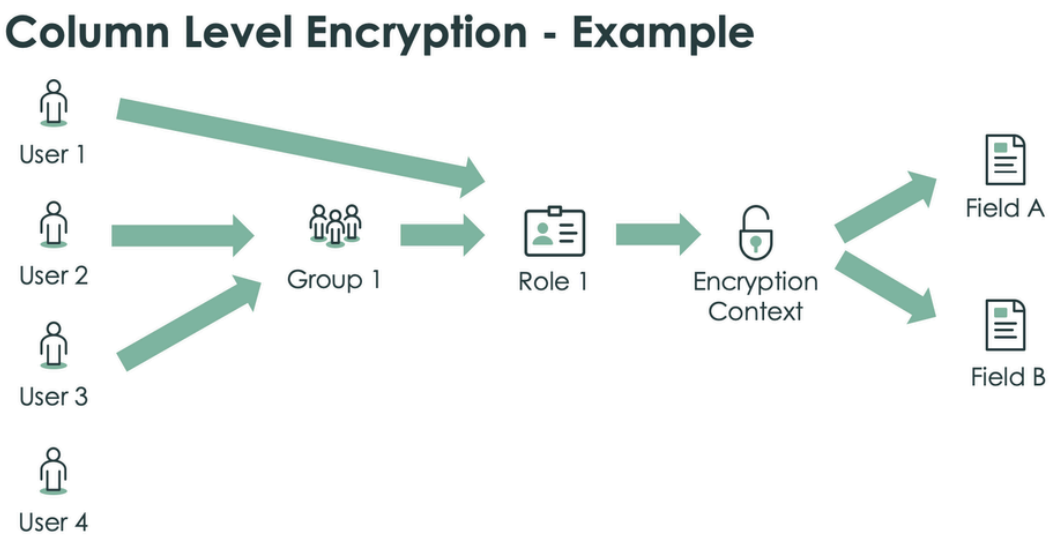
Verschlüsselung auf Spaltenebene (CLE) ermöglicht und verweigert den Zugriff auf verschlüsselte Daten basierend auf der Anwenderrolle. Die Verschlüsselung auf Spaltenebene umfasst die grundlegende Schlüsselverwaltung mithilfe von Verschlüsselungsmodulen.

Übersicht

Mit der Verschlüsselung auf Spaltenebene können Sie bestimmte Datenspalten in Ihren Tabellen verschlüsseln, anstatt die gesamte Tabelle oder Datenbank zu verschlüsseln. Verwenden Sie diese Methode, um sicherzustellen, dass Ihre vertraulichen Daten geschützt bleiben, ohne dass die gesamte Tabelle verschlüsselt werden muss. Die Möglichkeit, nur die Teile Ihrer Tabellen zu verschlüsseln, die dies erfordern, hilft, den Zeitaufwand für das Verschlüsseln und Entschlüsseln von Daten zu reduzieren.

CLE gewährt Zugriff auf verschlüsselte Daten basierend auf der Rolle eines Benutzers. Aufgrund dieses Ansatzes müssen Benutzer einer Rolle zugeordnet werden, um mit CLE verschlüsselte Daten anzuzeigen. Benutzer können direkt einer Rolle zugeordnet oder einer Gruppe zugewiesen werden, die einer Rolle zugeordnet ist. Dieser rollenbasierte Ansatz vereinfacht den Prozess, um sicherzustellen, dass Ihre Daten nur für Benutzer sichtbar sind, die sie benötigen.

Beispiel für rollenbasierte Verschlüsselung

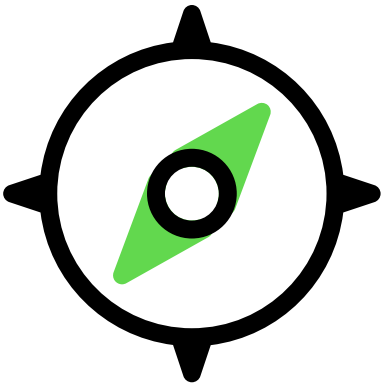
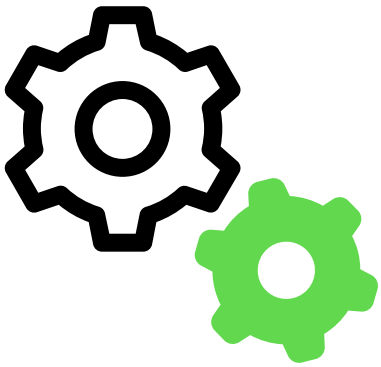
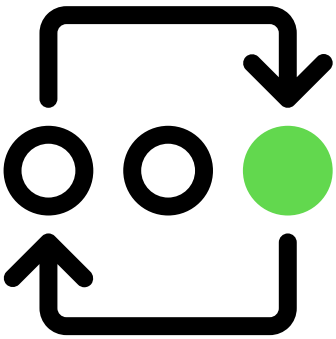


In diesem Beispiel versuchen vier Benutzer, auf Daten zuzugreifen, die in zwei Feldern eines Formulars gespeichert sind. Diese Felder werden durch einen Verschlüsselungskontext verschlüsselt, auf den nur Benutzer zugreifen können, die einer bestimmten Rolle (Rolle 1) zugeordnet sind.

- Anwender 1 ist Mitglied der Rolle 1, die Zugriff auf das Verschlüsselungsmodul 1 bietet. Anwender 1 kann den Inhalt von Feld A und Feld B sehen.
- Anwender 2 und Anwender 3 sind Mitglieder von Gruppe 1. Gruppe 1 ist ein Mitglied von Rolle 1, wodurch jeder in Gruppe 1 auf das Verschlüsselungsmodul 1 zugreifen kann und Anwender 2 und Anwender 3 den Inhalt von Feld A und Feld B sehen können.
- Anwender 4 ist kein Mitglied einer Gruppe oder Rolle und hat keinen Zugriff auf Verschlüsselungsmodul 1. Anwender 4 notiert den Zugriff auf Feld A oder Feld B. Anwender 4 sieht diese Felder auch nicht in einem Formular. In einer Listenansicht sind diese Felder sichtbar, die Werte sind jedoch leer.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erste Schritte

Untersuchen	Konfigurieren	Verwenden
		
Lernen Sie die Vorteile der Standard- und Enterprise-Editionen von Verschlüsselung auf Spaltenebene kennen.	Erfahren Sie, wie Sie Verschlüsselung auf Spaltenebene Enterprise aktivieren und konfigurieren und die Migration über den Verschlüsselungssupport verwalten	Verwenden Sie die Verschlüsselung auf Spaltenebene, um den Zugriff auf verschlüsselte Daten in Ihren Instanzen zu verwalten

Problembehandlung und Hilfe

- Entwicklerforum der ServiceNow-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Verschlüsselung auf Spaltenebene erkunden

Erfahren Sie mehr über die Verschlüsselung auf Spaltenebene.

Übersicht über die Verschlüsselung auf Spaltenebene

Verschlüsselung auf Spaltenebene (CLE) ist eine Basissystemfunktion, die die Verschlüsselung von Daten ermöglicht, die in einer Instanz mit AES128 oder AES256 gespeichert werden.

Mit CLE können Sie ausgewählte Datenbankfelder und gespeicherte Dateien mithilfe von Verschlüsselungskontexten verschlüsseln. In diesen Kontexten definieren Sie, was verschlüsselt wird, wählen den zu verwendenden Algorithmus aus und stellen den Verschlüsselungsschlüssel bereit, der in Ihrer -Instanz gespeichert wird.

Nachdem der Kontext erstellt wurde, können Sie ihn einer Anwenderrolle zuordnen. Anwender, die dieser Rolle zugewiesen sind, können entweder direkt oder über eine Gruppe auf die verschlüsselten Daten zugreifen.

Da der Zugriff auf Daten von CLE auf der Zuweisung von Rollen basiert, ist es wichtig, mit der Verwaltung von Rollen in Ihrer Instanz vertraut zu sein. Weitere Informationen finden Sie unter Rollen verwalten .

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Workflow für die Verschlüsselung auf Spaltenebene

Vorteile der Verschlüsselung auf Spaltenebene

Vorteil	Funktion	Erforderliche Rollen
Konfigurieren Sie den Zugriff auf Ihre verschlüsselten Daten basierend auf zugewiesenen Anwenderrollen.	Rollenbasierter Zugriff auf verschlüsselte Daten	Sicherheitsadministrator
Schützen Sie Ihre Daten mit dem Advanced Encryption Standard (AES). Sie können entweder den AES-128- oder den AES-256-Verschlüsselungsalgorithmus verwenden.	AES-Verschlüsselung	Sicherheitsadministrator
Erstellen Sie bis zu 5 Module und Modulzugriffsrichtlinien (Module Access Policies, MAP) mit der Standardversion von CLE. MAPs erweitern den rollenbasierten Zugriff, um Überlegungen zu ermöglichen für: • Systemanwender • Skripts • KMF-Ressourcenaustausch CLE Enterprise unterstützt zusätzliche MAPs.	Unterstützung für bis zu 5 Module und Modulzugriffsrichtlinien (Module Access Policies, MAP).	Sicherheitsadministrator
Verschlüsseln Sie allgemeine Feldtypen mit der Standardversion von CLE. CLE Enterprise unterstützt zusätzliche Feldtypen.	Verschlüsselung für Zeichenfolgentext, Felder für Datum und Datum/Uhrzeit, Anhänge und URLs	Sicherheitsadministrator
Wählen Sie zwischen standardmäßiger und gleichheitserhaltender Verschlüsselung. Wenn diese Option aktiviert ist, stellt die gleichheitserhaltende Verschlüsselung sicher, dass der verschlüsselte Wert eines Felds derselbe ist, wenn der Feldwert gleich bleibt. Diese Art der Verschlüsselung ermöglicht Gleichheitsvergleiche und Gruppierung nach Vorgängen in einem Feld. **Hinweis:** Nicht deterministische Verschlüsselung wird nicht unterstützt.	Unterstützung für gleichheitserhaltende Verschlüsselung	Sicherheitsadministrator
Verwenden Sie die APIs `getDisplayValue()` und `setDisplayValue()`, um Klartextwerte zurückzugeben und verschlüsselte Daten für verschlüsselte Felder einzufügen.	`getDisplayValue()`- und `setDisplayValue()`-APIs	Sicherheitsadministrator, Entwickler

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorteile von Verschlüsselung auf Spaltenebene für Unternehmen

Verschlüsselung auf Spaltenebene Enterprise baut auf dem vorhandenen CLE-Framework auf und bietet nach dem Kauf eines Abonnements die folgenden zusätzlichen Funktionen:

Vorteil	Funktion	Erforderliche Rollen
Zusätzliche Feldtypen verschlüsseln.	Unterstützung für zusätzliche Feldtypen: • HTML • Journal • Übersetzt	Sicherheitsadministrator
CLE Enterprise unterstützt mehr als 5 Module und Modulzugriffsrichtlinien, um mehr Optionen für den Zugriff auf gesicherte Daten bereitzustellen.	Unterstützung für zusätzliche Module und MAPs	Sicherheitsadministrator
Schlüssel aus einem Schlüssel Tresor können nach einem von Ihnen konfigurierten automatisierten Zeitplan rotiert werden. Die Verwendung der automatischen Schlüsselrotation kann die Sicherheit verbessern und gleichzeitig den Verwaltungsaufwand reduzieren.	Konfigurierbare automatische Schlüsselrotation	Sicherheitsadministrator
Verwalten Sie den gesamten Lebenszyklus Ihrer Datenverschlüsselungsschlüssel. Optional können Sie in Ihrer Umgebung generierte Datenverschlüsselungsschlüssel sicher austauschen.	Vom Kunden bereitgestellte Schlüssel	Sicherheitsadministrator
Flüchtige Schlüssel sind kryptografische Schlüssel, die für jede Ausführung eines kryptografischen Prozesses generiert werden. Diese Schlüssel sind sicherer, da sie für die Verwendung in einer einzigen Sitzung generiert werden.	Flüchtige kryptografische Schlüssel	Sicherheitsadministrator
Die aktualisierten APIs `setDisplayValue()` und `setDisplayValue()` können verschlüsselte Daten für verschlüsselte Felder einfügen.	`getDisplayValue()`- und `setDisplayValue()`-APIs aktualisiert	Sicherheitsadministrator, Entwickler

Guided Tour zur Verschlüsselung auf Spaltenebene

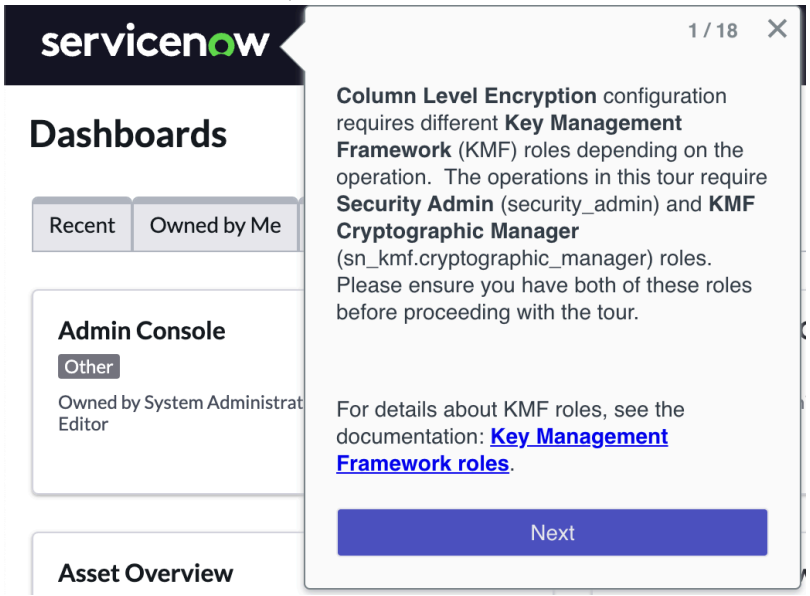
Die Tour bietet einen kurzen Überblick über das Setup der Spaltenebenenverschlüsselung (CLE), das zum Verschlüsseln von Tabellenfeldern oder Anhängen erforderlich ist. Schritte für die Erstellung von Feldverschlüsselungsmodulen, Modulzugriffsrichtlinien und verschlüsselten Feldkonfigurationen werden ebenfalls behandelt. Die Tour enthält Links zu einer detaillierten Dokumentation und zum Kurs „Übersicht über die Now Learning-Spaltenebenenverschlüsselung“.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_kmf.crypto_manager oder security_admin

Hinweis: Die Guided Tour ist noch nicht verfügbar, wenn Next Experience aktiviert ist.

Prozedur
1. Navigieren Sie zur UI-Seite **$pa_dashboards_overview.do** in Ihrer -Instanz.
   Beispiel: `http://ihrunternehmen.servicenow.com/nav_to.do?uri=%2F$pa_dashboards_overview.do ErsetzenSie Ihr Unternehmen` durch den Namen Ihrer Instanz.
2. Öffnen Sie das Symbol „Hilfe anzeigen“ (**Zeigt** das ein/aus“ in der oberen linken Ecke an.
3. Wählen **Sie Tour** starten unten in der Sidebar aus.
4. Wählen Sie **Weiter** aus, um mit der Tour fortzufahren.



Verschlüsselung auf Spaltenebene konfigurieren

Erfahren Sie, wie Sie die Verschlüsselung auf Spaltenebene aktivieren und konfigurieren und die Migration über den Verschlüsselungssupport verwalten.

Aktivierung

Verschlüsselung auf Spaltenebene

Das Plugin „Verschlüsselung auf Spaltenebene“ (com.glide.encryption) erfordert kein Abonnement und kann in Ihrer Instanz von einem Administrator aktiviert werden. Weitere Informationen zur Installation von Plugins finden Sie unter Plugins aktivieren .

Column Level Encryption Enterprise

Verschlüsselung auf Spaltenebene Enterprise ist eine erweiterte Version von Verschlüsselung auf Spaltenebene, die ein Abonnement erfordert.

- Weitere Informationen zum Produkt finden Sie unter Column Level Encryption Enterprise.
- Einzelheiten zur Installation von Verschlüsselung auf Spaltenebene Enterprise finden Sie unter Aktivieren Sie die Verschlüsselung auf Spaltenebene Enterprise.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Migration von Verschlüsselungsunterstützung

Verwenden Sie geplante Aufgaben, um Ihre Schlüssel und verschlüsselten Daten von Legacy- Encryption Support zu Verschlüsselung auf Spaltenebene Enterprisezu migrieren. Details zu diesem Prozess finden Sie unter Migration zu Verschlüsselung auf Spaltenebene Enterprise

Ändern Sie die Verschlüsselungseinstellungen für Anhänge

Verbessern Sie die Sicherheit, indem Sie verhindern, dass Benutzer unverschlüsselte Dateien anhängen. Einzelheiten finden Sie unterVerhindern, dass Anwender unverschlüsselte Dateien anhängen.

Aktivieren Sie die Verschlüsselung auf Spaltenebene Enterprise

Mit dem Abonnement von Verschlüsselung auf Spaltenebene Enterprisekann ein -Administrator das Plugin „com.glide.now.platform.encryption“ aktivieren.

Vorbereitungen

Erforderliche Rolle: admin

Wenden Sie sich an Ihren ServiceNow-Kundenbetreuer, um ein Abonnement zu erwerben. Der Account Manager sorgt in der Regel innerhalb weniger Tage für die Aktivierung des Plugins in den Produktionsinstanzen und Instanzen außerhalb der Produktion.

Warum und wann dieser Vorgang ausgeführt wird

Durch die Aktivierung des Plugins Verschlüsselung auf Spaltenebene Enterprise (`com.glide.now.platform.encryption`) werden folgende Änderungen an Ihrer -Instanz vorgenommen:

- Das Plugin „Encryption Support“ (com.glide.encryption) ist ebenfalls aktiviert.

  Hinweis: Das Plugin Key Management Framework (com.glide.kmf.global) ist standardmäßig bereits aktiv.

- Die Eigenschaft „`glide_encryption.set_value_support_cle.disabled`“ ist auf „ **false**“ festgelegt, wodurch die Funktion „Wert festlegen“ aktiviert wird. Mit der SetValue-Unterstützung können die APIs `setDisplayValue()` und `setValue()` verschlüsselte Daten unterstützen. Außerdem können `getDisplayValue()` und `getValue()` Klartextwerte zurückgeben.
- Zwei geplante Aufgaben sind aktiviert:
  - **autoKeyMigration**: Migriert Verschlüsselungskontextschlüssel zu Key Management Framework (KMF) kryptografische Modulschlüssel.
  - **autoDataMigration**: Migriert Daten, die Sie bereits verschlüsselt haben, um den kryptografischen Modulschlüssel KMF zu verwenden.

  Administratoren können ändern, wann diese geplanten Aufgaben ausgeführt werden, und sie jederzeit anhalten oder neu starten.

Prozedur

1. Navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie das Plugin *`Platform Encryption - com.glide.now.platform.encryption`* mithilfe der Filterkriterien und der Suchleiste.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.

3. Wählen Sie **Installieren** und wählen Sie dann im Dialogfeld „Plugin aktivieren“ die Option **Aktivieren**.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: `Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.`

Migration zu Verschlüsselung auf Spaltenebene Enterprise

Geplante Aufgaben migrieren Ihre Schlüssel und verschlüsselten Daten von Verschlüsselungsunterstützung zu Verschlüsselung auf Spaltenebene Enterprise.

Sie können die geplanten Aufgaben überprüfen, indem Sie zu navigieren **Systemsicherheit** > **Strenge Sicherheitseinstellungen** > **Security-Aufträge**:

- **autoKeyMigration**: Migriert Verschlüsselungskontextschlüssel zu Key Management Framework (KMF) kryptografische Modulschlüssel.
- **autoDataMigration**: Migriert Daten, die Sie bereits verschlüsselt haben, um den kryptografischen Modulschlüssel KMF zu verwenden.

Sie können ändern, wann diese geplanten Aufgaben ausgeführt werden, und sie jederzeit anhalten oder neu starten.

Stellen Sie sicher, dass die verschlüsselten Feldkonfigurationen Ihre neu migrierten Modulschlüssel verwenden, indem Sie zu navigieren **Systemsicherheit** > **Feldverschlüsselung** > **Verschlüsselungsfeld-Konfigurationen**an. Suchen Sie nach den folgenden Elementen:

- Das Feld **Methode** lautet **Einzelnes Modul**.
- Das Feld **Krypto-Modul** wird mit dem Namen des kryptografischen Moduls gefüllt, das das System automatisch erstellt. Sie können dieses Modul und die Modulzugriffsrichtlinie überprüfen, die beide aktiv und veröffentlicht sind.

Verschlüsselung auf Spaltenebene Unternehmens- und Systemklone

Wenn Verschlüsselung auf Spaltenebene Enterprise in Ihrer Instanz installiert ist, wird im Rahmen des Klonvorgangs automatisch ein neuer Verschlüsselungsschlüssel des Feldverschlüsselungsmoduls in der Zielklon-Instanz generiert. Diese Schlüssel werden für alle Module generiert, auf die der Benutzer Zugriff hat und die noch keinen Schlüssel haben.

Aus diesem Grund können Feldverschlüsselungsmodule in der Zielklon-Instanz über zwei Modulverschlüsselungsschlüssel verfügen:

- Ein aktiver Modulverschlüsselungsschlüssel. Dies ist der neue Schlüssel, der nach dem Klonen generiert wird, solange das Modul für den Anwender zugänglich ist und keine vorherigen Schlüssel hat.
- Ein deaktivierter Verschlüsselungsmodulschlüssel (aus der automatisierten Schlüsselaustauschübertragung).

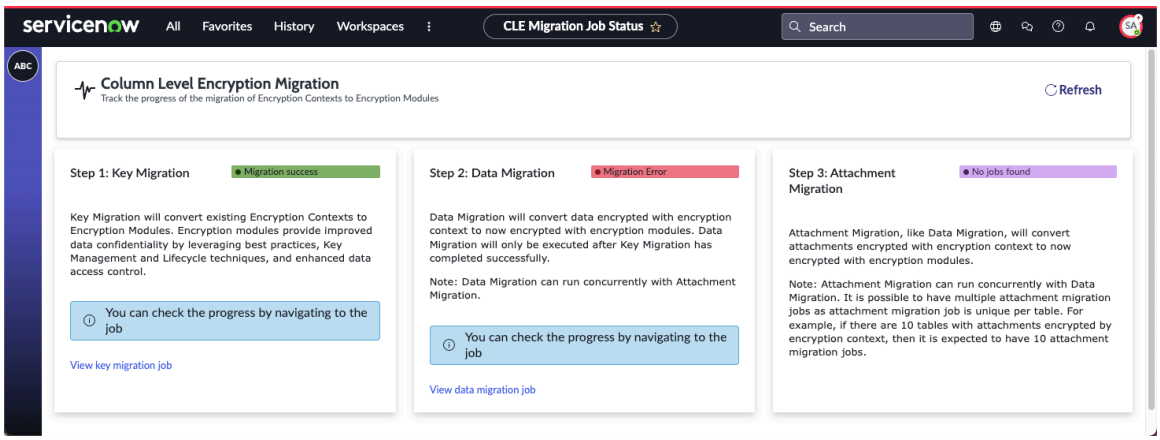
  Der Verschlüsselungsschlüssel des aktiven Moduls wird verwendet, um eingefügte Daten nach Bedarf in der Zielklon-Instanz zu verschlüsseln. Das deaktivierte Modul wird verwendet, um vorhandene Daten zu entschlüsseln, die als Teil des Systemklons geklont wurden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um einen einzigen Schlüssel zum Entschlüsseln und Verschlüsseln aller Daten zu verwenden, können Sie einen Modul-Neuschlüsselungsauftrag ausführen. Weitere Informationen zur Neuschlüsselung von Modulaufträgen finden Sie unter Massenverschlüsselungs-, Entschlüsselungs- und Neuschlüsselungsaufträge planen.

Statusseite der Migration der Verschlüsselung auf Spaltenebene

Verwenden Sie die Migrationsstatusseite, um die Migration von Verschlüsselungskontexten zu Verschlüsselungsmodulen zu verfolgen.

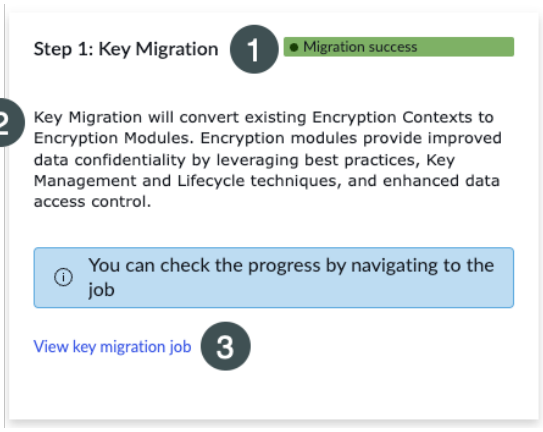


Auf der Seite Verschlüsselung auf Spaltenebene Migration wird der Status der Schritte angezeigt, die an der Migration von Verschlüsselungskontexten zu Verschlüsselungsmodulen beteiligt sind. Jeder der drei Abschnitte zeigt den Status eines bestimmten Schritts im Prozess an.

Seitenabschnittskarten

Die Seite enthält drei Karten, die die Schritte im Migrationsfortschritt darstellen. Auf diesen Karten wird Folgendes angezeigt:

- (1) Der Status des aktuellen Schritts. Dieser Status zeigt an, ob der Schritt erfolgreich abgeschlossen wurde oder ob keine Aufträge zur Verarbeitung vorhanden sind.
- (2) Eine Beschreibung des aufgeführten Schritts.
- (3) Ein Link zum entsprechenden Verschlüsselungsauftrags-Datensatz [sys_mass_encryption_job].



Verhindern, dass Anwender unverschlüsselte Dateien anhängen

Ändern Sie die Eigenschaft com.glide.encryption.enable_attachment_key_ui, um zu verhindern, dass Ihre Benutzer mit Zugriff auf einen Verschlüsselungsmodulschlüssel unverschlüsselte Anhänge anhängen.

Vorbereitungen

Erforderliche Rolle: security_admin

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie müssen auf die Rolle „security_admin“ hochstufen, um diese Schritte auszuführen. Anweisungen hierzu finden Sie unter Auf eine privilegierte Rolle hochstufen

Standardmäßig können Benutzer, die Zugriff auf einen Verschlüsselungsmodulschlüssel haben, unverschlüsselte Anhänge hochladen. Verwenden Sie die Systemeigenschaft *com.glide.encryption.enable_attachment_key_ui*, um dieses Verhalten zu ändern.

Beim Anhängen wird Ihren Anwendern eine UI-Auswahl für Datensätze angezeigt, die über eine verschlüsselte Feldkonfiguration mit mehreren Modulen verfügen. Wenn diese Eigenschaft auf „false“ festgelegt ist, wird Anwendern die Option nicht mehr angezeigt, einen Anhang nicht zu verschlüsseln.

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**an.
2. Suchen und öffnen Sie in der Liste der Systemeigenschaften die Systemeigenschaft.
3. Legen Sie den **Wert** der Eigenschaft auf `false fest`.

Mithilfe der Verschlüsselung auf Spaltenebene

Verwenden Sie die Verschlüsselung auf Spaltenebene, um den Zugriff auf verschlüsselte Daten in Ihren Instanzen zu verwalten.

Zugehörige Informationen

- Erstellen Sie ein kryptografisches Modul für die Verschlüsselung auf Spaltenebene
- Verwendung mehrerer Verschlüsselungsmodule
- Erstellen Sie eine kryptografische Spezifikation für die Verschlüsselung auf Spaltenebene
- Erweiterte Algorithmen für Verschlüsselung auf Spaltenebene Enterprise konfigurieren
- Konfigurieren Sie Eigenschaften für vom Kunden bereitgestellte Schlüssel
- Felder und Anhänge werden verschlüsselt
- Enterprise-Beispiele für Verschlüsselung auf Spaltenebene

Erstellen Sie ein kryptografisches Modul für die Verschlüsselung auf Spaltenebene

Erstellen Sie ein kryptografisches Modul für die Verschlüsselung auf Spaltenebene, um die für kryptografische Vorgänge verwendeten Mechanismen zu definieren.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_manager oder sn_kmf_admin, security_admin, admin

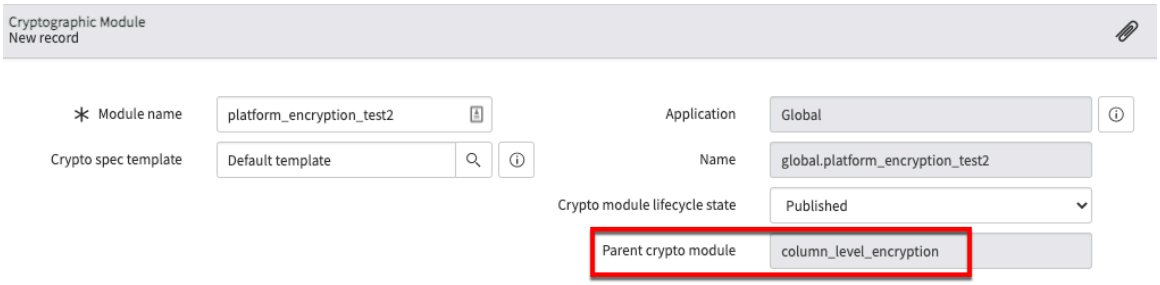
Warum und wann dieser Vorgang ausgeführt wird

Dieses Verfahren beschreibt Optionen, die bei der Verschlüsselung auf Spaltenebene (CLE) mit dem Basissystem verfügbar sind, und zusätzliche Konfigurationsoptionen, die mit der Funktionalität Verschlüsselung auf Spaltenebene Enterprise (CLE_Ent) verfügbar werden. Verschlüsselung auf Spaltenebene Enterprise ist mit einem kostenpflichtigen Abonnement verfügbar. Informationen zu den unterstützten Funktionen und Optionen, die für die einzelnen Angebote verfügbar sind, finden Sie unter Abonnementpaket für Verschlüsselung und Schlüsselverwaltung. Unter Aktivieren Sie die Verschlüsselung auf Spaltenebene Enterprise finden Sie weitere Informationen zum Abrufen von Verschlüsselung auf Spaltenebene Enterprise.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Feldverschlüsselungsmodule** > **Neu**an.



2. Füllen Sie die Felder des Formulars aus.

Formular „Kryptografisches Modul“.

Feld	Beschreibung
Modulname	Alphanumerische Zeichenfolge, auf die beim Ausführen von Skripts verwiesen werden soll.
Krypto-Spezifikationsvorlage	Standardvorlage, die zum Erstellen des kryptografischen Moduls verwendet wird, das Zuordnungen vieler Krypto-Zwecke zu Krypto-Spezifikationen und empfohlenen Algorithmen enthält.
Anwendung	Der ausgewählte Anwendungsbereich.
Name	Dem Namen des Verschlüsselungsmoduls wird der Name des Anwendungsbereichs vorangestellt, um Konflikte mit anderen bereichsbezogenen Anwendungen bei der Modulerstellung zu vermeiden. Wenn Sie beispielsweise ein Modul mit dem Namen `my_crypto_module` im globalen Anwendungsbereich erstellt haben, wird der Name als `global.my_crypto_module gespeichert`.
Lebenszyklusstatus kryptografisches Modul	Der Begriff Lebenszyklus bezieht sich auf die Erstellung, Verwendung und Deaktivierung eines kryptografischen Moduls. Legen Sie die Option während der Konfiguration zunächst auf **Entwurf** fest. Wenn Sie das -Modul verwenden, legen Sie es auf **Veröffentlicht**fest. Die Standardvorlage wird automatisch auf **Veröffentlicht**festgelegt.
Übergeordnetes kryptografisches Modul	Das übergeordnete Element wird automatisch als **column_level_encryption ausgefüllt**.

3. Klicken Sie auf **Absenden**.

   Nach der erfolgreichen Übermittlung wird Ihr kryptografisches Modul in der Tabelle „Kryptografische Module“ aufgeführt.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnung:

Für Benutzer mit Unterstützung der Legacy-Verschlüsselung:

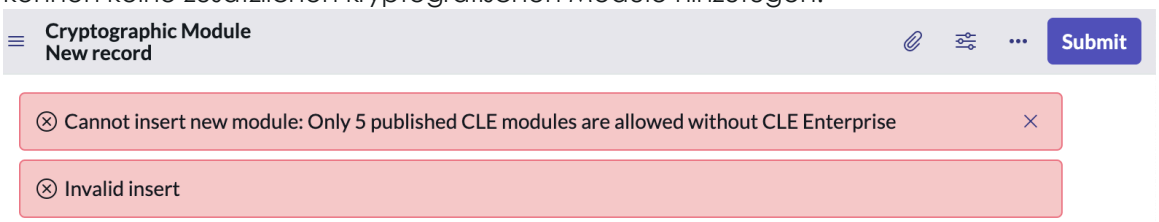
Wenn Sie die Nicht-Enterprise-Version von Verschlüsselung auf Spaltenebene verwenden, sind Sie auf fünf Module beschränkt. Wenn Sie diese Grenze überschritten haben, erhalten Sie die folgende Warnung:

Diese Einfügung überschreitet den Grenzwert für die Anzahl von veröffentlichten Modulen für die Verschlüsselung auf Spaltenebene, der für das Abonnementprodukt berechtigt ist. Für zusätzliche Module ist das Enterprise-Abonnement für die Verschlüsselung auf Spaltenebene erforderlich. Wenden Sie sich an Ihr Account-Team.

Eine standardmäßige kryptografische Spezifikation wird erstellt, wobei der Krypto-Zweck auf „Symmetrische Datenverschlüsselung/-entschlüsselung“ und der Algorithmus als „AES 256 CBC“ festgelegt ist. Wählen Sie den Algorithmus für Aktualisierungen aus.

4. Um die Konfigurationsoptionen zu öffnen, klicken Sie auf das neu erstellte kryptografische Modul.

Hinweis: Vor dem Upgrade auf Verschlüsselung auf Spaltenebene Enterprisesind maximal fünf Verschlüsselungsmodule auf Spaltenebene zulässig. Eine Fehlermeldung wird angezeigt, und Sie können keine zusätzlichen kryptografischen Module hinzufügen.



Nächste Maßnahme

Erstellen Sie eine kryptografische Spezifikation für die Verschlüsselung auf Spaltenebene.

Verwendung mehrerer Verschlüsselungsmodule

Mehrere Verschlüsselungsmodule ermöglichen die Verschlüsselung von Daten mit mehr als einem Verschlüsselungsmodul. Wenn jedes Modul über eine eigene Zugriffsrichtlinie verfügt, die beispielsweise auf einer Rolle basiert, können Benutzer mit unterschiedlichen Rollen Daten in derselben Tabelle verschlüsseln, können aber weiterhin daran gehindert werden, die verschlüsselten Daten der jeweils anderen anzuzeigen.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_manager oder sn_kmf.admin

Warum und wann dieser Vorgang ausgeführt wird

Hinweis: Nur die Verschlüsselung in Spalten unterstützt mehrere Module. Anhangverschlüsselung nicht. Massenverschlüsselung ist bei Verwendung der Methode mit mehreren Verschlüsselungsmodulen nicht verfügbar.

Sie können ein Feld, das mehrere Verschlüsselungsmodule verwendet, nicht ändern, um ein einzelnes Verschlüsselungsmodul zu verwenden.

Das Feld wird vom Verschlüsselungsmodul des ersten Benutzers verschlüsselt, der Daten eingibt. Da das Verschlüsselungsmodul pro Datensatz festgelegt wird, können Felder in einer

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Liste unterschiedliche Verschlüsselungsmodule aufweisen. Innerhalb eines Datensatzes kann das Feld nur von einem Modul verschlüsselt werden.

Prozedur

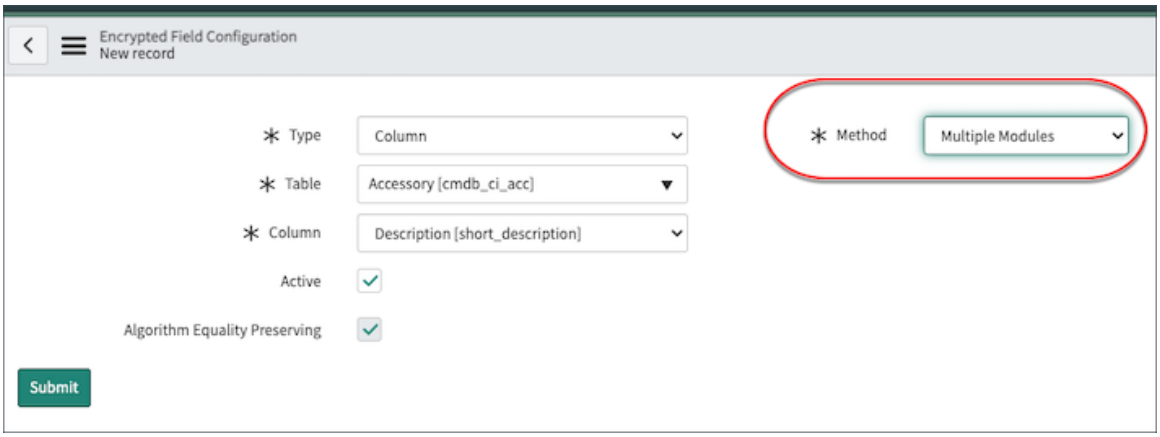
1. Erstellen Sie mehrere kryptografische Module und eine Zugriffsrichtlinie für jedes Modul.

   Stellen Sie sicher, dass Sie den verschiedenen kryptografischen Modulen über die Zugriffsrichtlinien unterschiedliche Rollen zuweisen.

2. Navigieren zu **Systemsicherheit** > **Feldverschlüsselung** > **Verschlüsselungsfeld-Konfigurationen**an.

   Weitere Informationen zu Konfigurationen verschlüsselter Felder finden Sie unter Legen Sie Konfigurationen für verschlüsselte Felder fest.

3. Im Feld **Typ** müssen Sie **Spalte**auswählen.
   Die Anhangsverschlüsselung unterstützt nicht mehrere Module.
4. Wählen Sie im Feld **Methode** die Option **Mehrere Module** aus.



5. Wählen Sie die **Tabelle** und die **Spalte** in der Tabelle aus, die Sie verschlüsseln möchten.
6. Klicken Sie auf **Absenden**.

Ergebnisse

Neu erstellte Daten für das angegebene Feld werden mit dem Schlüssel des entsprechenden Moduls verschlüsselt. Wenn ein Benutzer mit der in der Zugriffsrichtlinie von Modul A angegebenen Rolle in die angegebene Tabelle schreibt, werden die Daten mit dem Schlüssel von Modul A verschlüsselt. Nur Benutzer mit derselben Rolle können die Daten lesen.

Example:

Zum Verschlüsseln der Spalte „Kurzbeschreibung“ in der Incident-Tabelle. Sie würden wie folgt vorgehen:

1. Erstellen Sie die beiden kryptografischen Module A und B.
2. Erstellen Sie für jedes Modul eine Modulzugriffsrichtlinie.

   Gewähren Sie für Modul A Benutzern mit einer HR-Rolle Zugriff. Gewähren Sie für Modul B Benutzern mit einer Vertriebsrolle Zugriff.

3. Erstellen Sie einen Verschlüsselten Feldkonfigurations-Datensatz, indem Sie die Spalte „Kurzbeschreibung“ in der Incident-Tabelle angeben, und stellen Sie sicher, dass Sie **Mehrere Module** im Feld **Methodeauswählen**.

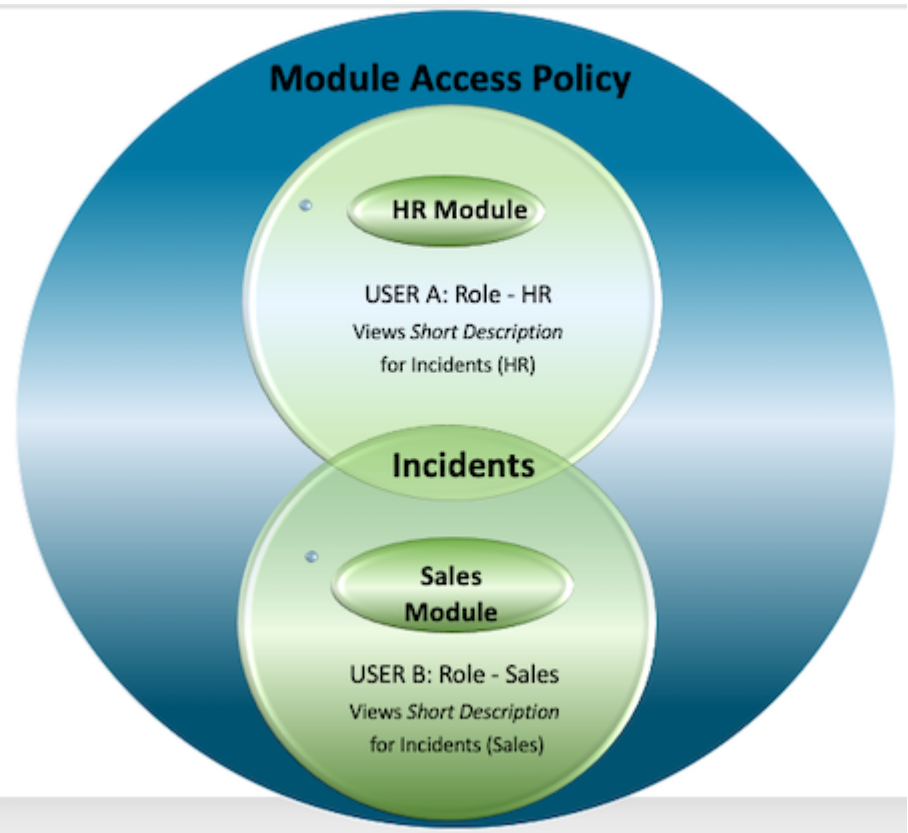
Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Lassen Sie zwei Benutzer, einen mit der HR-Rolle (Benutzer A) und einen mit der Rolle „Vertrieb“ (Benutzer B), einen Incident mit einer kurzen Beschreibung erstellen, und lassen Sie dann beide Benutzer die Liste der Incidents anzeigen.

   Die Kurzbeschreibung für den Incident, die vom Benutzer mit der HR-Rolle erstellt wurde, wird mit dem Schlüssel für Modul A verschlüsselt. Ebenso wird die Kurzbeschreibung für den Incident, der vom Benutzer mit der Rolle „Vertrieb“ erstellt wurde, mit dem Schlüssel für Modul B verschlüsselt.

   Obwohl alle Benutzer mit den Rollen HR und Vertrieb Zugriff auf Incidents haben, können nur Benutzer mit der Rolle HR die Kurzbeschreibungen der Incidents entschlüsseln und anzeigen, die von Benutzer A erstellt wurden, der die Rolle HR innehatte. Ebenso können nur Benutzer mit der Rolle „Vertrieb“ die Kurzbeschreibungen für Incidents entschlüsseln und anzeigen, die von Benutzer B erstellt wurden, der die Rolle „Vertrieb“ innehatte.



Erstellen Sie eine kryptografische Spezifikation für die Verschlüsselung auf Spaltenebene

Nachdem Sie ein kryptografisches Modul erstellt haben, greifen Sie auf die entsprechende kryptografische Spezifikation zu, um den Algorithmus zu definieren.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_manager oder sn_kmf_admin und security_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Dieses Verfahren beschreibt Optionen, die bei der Verschlüsselung auf Spaltenebene (CLE) mit dem Basissystem verfügbar sind, und zusätzliche Konfigurationsoptionen, die mit der Funktionalität Verschlüsselung auf Spaltenebene Enterprise (CLE_Ent) verfügbar werden. Die Funktionalität Verschlüsselung auf Spaltenebene Enterprise ist mit einem kostenpflichtigen Abonnement verfügbar. Informationen zu den unterstützten Funktionen und Optionen,

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die für die einzelnen Angebote verfügbar sind, finden Sie unter Abonnementpaket für Verschlüsselung und Schlüsselverwaltung. Unter Aktivieren Sie die Verschlüsselung auf Spaltenebene Enterprise finden Sie weitere Informationen zum Abrufen von Verschlüsselung auf Spaltenebene Enterprise.

Eine kryptografische Spezifikation wird vom System erstellt, wenn Sie ein kryptografisches Modul für die Verschlüsselung auf Spaltenebene erstellen.

an.

Prozedur

1. Navigieren zu **Systemsicherheit** > **Feldverschlüsselungsmodule** > **Alle**an.
2. Wählen Sie das kryptografische Modul aus, um die Konfigurationsoptionen zu öffnen. Informationen zum kryptografischen Modul werden oben auf dem Bildschirm angezeigt. Eine Kryptospezifikation für die symmetrische Datenverschlüsselung/-entschlüsselung wird automatisch mit einem AES 256 CBC-Algorithmus erstellt.
3. Wählen Sie die Krypto-Spezifikation aus der Tabelle aus, um die Algorithmusdefinition zu öffnen.
   Für Verschlüsselung auf Spaltenebene Enterprise siehe Erweiterte Algorithmen für Verschlüsselung auf Spaltenebene Enterprise konfigurieren.
4. Klicken Sie auf **Weiter**, um auf den Schlüssellebenszyklus zuzugreifen.

Nächste Maßnahme

Führen Sie einen der folgenden Vorgänge aus:

- Wählen Sie einen Eintrag in der Tabelle „Schlüssellebenszyklus“ aus, um das Verhalten des Schlüssellebenszyklus zu definieren. Unter Wichtige Lebenszyklusstatus konfigurieren finden Sie Details zum Abschließen der Lebenszyklusdefinition für den Schlüssel.
- Klicken Sie auf **Weiter**, um einen kryptografischen Schlüssel zu erstellen. Details zu diesem Vorgang finden Sie unter Generieren Sie einen kryptografischen ServiceNow-Schlüssel.

Erweiterte Algorithmen für Verschlüsselung auf Spaltenebene Enterprise konfigurieren

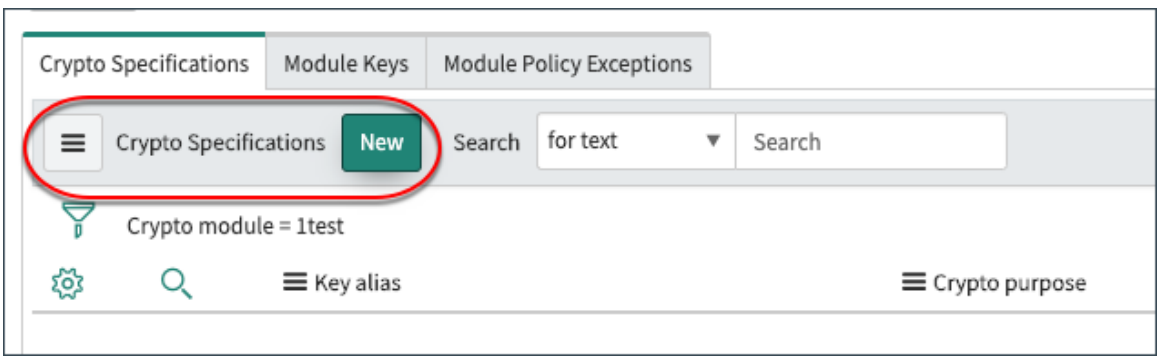
Erstellen Sie eine kryptografische Spezifikation, um den Algorithmus für ein kryptografisches Modul zu definieren. Passen Sie die Verschlüsselungsspezifikationen mit den erweiterten Optionen an, die für Verschlüsselung auf Spaltenebene Enterpriseverfügbar sind.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Klicken Sie auf der Registerkarte **Krypto-Spezifikationen (#)** auf **Neu**.



© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Füllen Sie die Felder des Formulars aus.

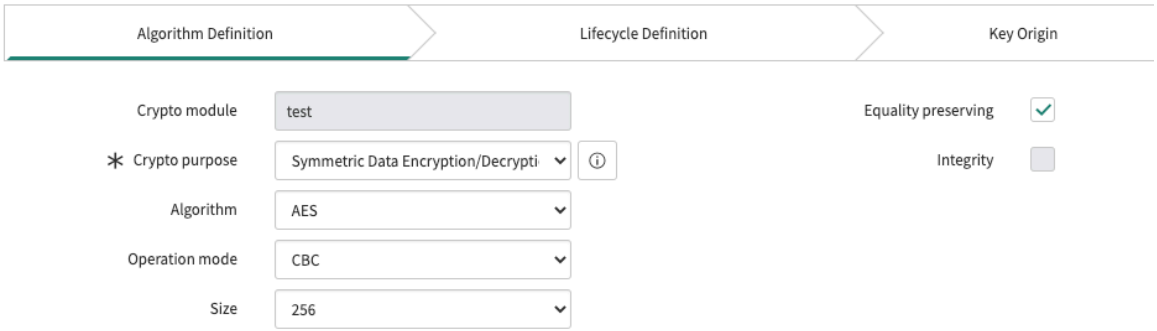
Formular „Algorithmusdefinition“.

Feld	Beschreibung
Crypto-Modul	Der Name des ausgewählten kryptografischen Moduls wird ausgefüllt.
Kryptografischer Zweck	Der Wert ist „ **Symmetrische Datenverschlüsselung/-entschlüsselung** “ für Verschlüsselung auf Spaltenebene Enterprise.
Algorithmus	Der Wert ist **AES** für Verschlüsselung auf Spaltenebene Enterprise.
Betriebsmodus	Der Wert ist **CBC** für Verschlüsselung auf Spaltenebene Enterprise.
Größe	Mögliche Werte sind **256** und **128**. **Hinweis:** Eine Größe von 256 Bit ist am sichersten für die Verschlüsselung und wird für die symmetrische Datenverschlüsselung/-entschlüsselung für Verschlüsselung auf Spaltenebene Enterpriseverwendet.
Gleichstellungserhaltung	Option zum Aktivieren der deterministische Verschlüsselung. **Hinweis:** Wenn Sie diese Option auswählen, sollte der verschlüsselte Wert eines Felds derselbe sein, wenn der Feldwert gleich bleibt. Option zum Aktivieren der **symmetrischen Datenverschlüsselung/-entschlüsselung** mit **AES** im **CBC-Modus (Cipher Block Chaining)**.
Integrität	Option zum Bereitstellen von Integrität im GCM-Vorgang und gilt nicht für die Funktionalität Verschlüsselung auf Spaltenebene Enterprise.

3. Klicken Sie auf **Absenden**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das folgende Beispiel zeigt die AES CBC-256-Verschlüsselung. Wenn Verschlüsselung auf Spaltenebene Enterprise aktiv ist und das übergeordnete Modul „column_level_encryption“ ist, gilt als Krypto-Zweck nur die symmetrische Datenverschlüsselung/-entschlüsselung AES CBC-256. Details siehe Kryptografischer Zweck, Algorithmen und Schlüsselinformationen.



Nächste Maßnahme
Führen Sie einen der folgenden Vorgänge aus:

- Wählen Sie einen Eintrag in der Tabelle „Schlüssellebenszyklus“ aus, um das Verhalten des Schlüssellebenszyklus zu definieren. Unter Wichtige Lebenszyklusstatus konfigurieren finden Sie Details zum Abschließen der Lebenszyklusdefinition für den Schlüssel.
- Klicken Sie auf **Weiter**, um einen kryptografischen Schlüssel zu erstellen. Sehen Sie sich eine der folgenden Aufgaben für die Schlüsselgenerierung an:
  - Generieren Sie einen kryptografischen ServiceNow-Schlüssel.
  - Konfigurieren Sie Eigenschaften für vom Kunden bereitgestellte Schlüssel.
  - Importieren Sie das Schlüsselpaar zum Packen/Entpacken.

Verwendung von vom Kunden bereitgestellten Schlüsseln mit Verschlüsselung auf Spaltenebene Enterprise

Sie können anstelle der vom System ServiceNow® generierten Schlüssel auch Ihren eigenen, vom Kunden bereitgestellten Schlüssel verwenden.

Wichtig: Diese Themen beziehen sich nur auf Instanzen, die Verschlüsselung auf Spaltenebene Enterpriseverwenden, was nur mit dem Plugin `com.glide.now.platform.encryption` verfügbar ist. Weitere Informationen zum Bezug dieses Plugins finden Sie unter Aktivieren Sie die Verschlüsselung auf Spaltenebene Enterprise.

Mit Verschlüsselung auf Spaltenebene Enterprise können Sie Ihre eigenen Schlüssel für die Verschlüsselung verwenden. Administratoren haben die Wahl, ob von ServiceNow® bereitgestellte Schlüssel oder Ihre eigenen vom Kunden bereitgestellten Schlüssel (CSK) für die Verschlüsselung auf dem Now Platformverwendet werden.

Wichtig: Um die Option des vom Kunden bereitgestellten Schlüssels verwenden zu können, benötigen Sie einen eigenen kryptografischen Schlüssel.

Sobald Sie Ihren Schlüssel haben, können Sie ihn in Ihren Instanzen verwenden, indem Sie die folgenden Schritte ausführen.

1. Konfigurieren Sie Eigenschaften für vom Kunden bereitgestellte Schlüssel

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Es gibt drei Systemeigenschaften, die die Größe, den Füllalgorithmus und den Gültigkeitszeitraum des umschließenden RSA-Schlüsselpaars definieren. Überprüfen Sie diese Eigenschaften, und passen Sie ihre Werte an, wenn die Standardwerte nicht Ihren Anforderungen entsprechen.

2. Packen Sie Ihren vom Kunden bereitgestellten Schlüssel ein

   Verwenden Sie ein kryptografisches Tool wie OpenSSL, um den symmetrischen Schlüssel zur Verschlüsselung mit dem heruntergeladenen öffentlichen Schlüssel zu umschließen.

Konfigurieren Sie den von Ihrem Kunden bereitgestellten Schlüssel, und laden Sie ihn hoch

Laden Sie den verpackten, vom Kunden bereitgestellten Schlüssel hoch, und konfigurieren Sie das kryptografische Modul, um Ihren Schlüssel für die Verschlüsselung in Ihrer Instanz zu verwenden.

Konfigurieren Sie Eigenschaften für vom Kunden bereitgestellte Schlüssel

Wenn das Plugin Verschlüsselung auf Spaltenebene Enterprise aktiviert ist, können Sie Systemeigenschaften verwenden, um den Schlüsselabstand, die Größe des flüchtigen Schlüsselpaars und einen Schlüsselgültigkeitszeitraum Ihrer vom Kunden bereitgestellten Schlüssel zu definieren.

Verschlüsselung auf Spaltenebene Enterprise Mit der Schlüsselverwaltung können Sie den gesamten Schlüssellebenszyklus Ihrer Datenverschlüsselungsschlüssel verwalten. Optional können Sie in Ihrer Umgebung generierte Datenverschlüsselungsschlüssel sicher austauschen.

Mit der Plattformverschlüsselung mit Schlüsselverwaltung können Sie den gesamten Schlüssellebenszyklus Ihrer Datenverschlüsselungsschlüssel verwalten. Optional können Sie in Ihrer Umgebung generierte Datenverschlüsselungsschlüssel sicher austauschen.

Systemeigenschaften zum Definieren von Schlüsselpaarattributen

Wenn Sie Ihren eigenen Schlüssel bereitstellen, müssen Sie ihn mit dem öffentlichen RSA-Schlüssel umschließen. Drei Eigenschaften definieren die Größe, den Abstandsalgorithmus und den Gültigkeitszeitraum des umschließenden RSA-Schlüsselpaars:

- *glide.kmf.ephemeral_key.key_padding* Steuert das Schlüsselabstandsschema für den flüchtigen Schlüssel. Das Standardschema ist OAEP SHA256, aber auch SHA1 wird unterstützt.
- *glide.kmf.ephemeral_key.key_size* steuert die Schlüsselgröße des flüchtigen Schlüsselpaars. Der Standardwert ist 4096 Bit, es werden jedoch auch 2048 Bit unterstützt.
- *glide.kmf.ephemeral_key.key_validity_period* definiert den Zeitraum, für den das flüchtige Schlüsselpaar gültig ist. Der Standardwert beträgt zwei Stunden.

Nachdem der Datenverschlüsselungsschlüssel in die Instanz importiert wurde, schützt ein sicherer Packschlüssel neue Modulschlüssel in der Instanz. Der Wrapping-Schlüssel ist ein Instance Key Encryption Key (IKEK), der von einem Hardware-Sicherheitsmodul (HSM) in SafeNet KeySecure generiert wird. Einzelheiten zu den Schlüsseltypen finden Sie unter Schlüssel auf Instanzebene im Key Management Framework.

Fahren Sie mit Packen Sie Ihren vom Kunden bereitgestellten Schlüssel einfort.

Packen Sie Ihren vom Kunden bereitgestellten Schlüssel ein

Umschließen Sie den symmetrischen Schlüssel, der für die Verschlüsselung verwendet werden soll, mit dem heruntergeladenen öffentlichen Schlüssel.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Hinweis: Dieses Verfahren beschreibt Optionen, die mit dem KMF Basissystem verfügbar sind, und Optionen, die mit der Funktionalität Verschlüsselung auf Spaltenebene Enterprise verwendet werden sollen. Die Funktionalität Verschlüsselung auf Spaltenebene Enterprise ist nur verfügbar, wenn das Plugin *„com.glide.now.platform.encryption"* aktiv ist. Unter Aktivieren Sie die Verschlüsselung auf Spaltenebene Enterprise finden Sie weitere Informationen zum Abrufen von Verschlüsselung auf Spaltenebene Enterprise.

Einige der Schritte in diesem Dokument erfordern die Verwendung eines kryptografischen Tools, das auf Ihrem lokalen Gerät installiert ist. Die Beispiele in dieser Aufgabe verwenden das OpenSSL-Tool. Weitere Informationen zu diesem Tool finden Sie unter https://www.openssl.org . Wenn Sie andere kryptografische Tools wie LibreSSL oder GnuTLS verwenden, finden Sie ähnliche Schritte in der Dokumentation dieser Produkte.

- Ändern Sie optionale Eigenschaften, die die Größe, den Füllalgorithmus und den Gültigkeitszeitraum des Schlüssels steuern. Weitere Informationen finden Sie unter Konfigurieren Sie Eigenschaften für vom Kunden bereitgestellte Schlüssel.

- Sie benötigen Ihren symmetrischen Schlüssel (.BIN) zur Verschlüsselung.

  Wichtig: Der Schlüssel muss im Binärformat vorliegen. Wenn ein anderes Format verwendet wird, ist die Validierung eines `-Tokens fehlgeschlagen. Fügen Sie das unveränderte Token erneut an. Die Fehlermeldung` wird angezeigt.

- Sie benötigen ein kryptografisches Tool, um Ihren Schlüssel zu umschließen. In diesem Beispiel wird OpenSSL 1.1 verwendet.

Erforderliche Rolle: sn_kmf.cryptographic_manager oder sn_kmf.admin

Prozedur

1. Navigieren zu **Alle** > **Key Management Framework** > **Kryptografische Module** > **Alle**an.
2. Wählen Sie in der zugehörigen Liste Krypto-Spezifikationen das kryptografische Modul aus, das Sie für den vom Kunden bereitgestellten Schlüssel erstellt haben.
3. Sie werden zum Schritt „ **Schlüsselerstellung** " weitergeleitet.
4. Wenn Sie den Packschlüssel noch nicht heruntergeladen haben, klicken Sie auf den Link, um *token_publickey* herunterzuladen<id> ZIP -Datei, und speichern Sie sie am selben Speicherort wie Ihren Schlüssel.

   Hinweis: Benennen Sie den heruntergeladenen *token_publickey* nicht um<id> Datei.

5. Extrahieren Sie die Datei in Ihr lokales Netzwerk.
   Die ZIP-Datei enthält zwei Dateien, ein Importtoken und ein öffentliches Schlüsselzertifikat (`PEM` -Zertifikat). Umschließen Sie Ihren symmetrischen Schlüssel mit dem öffentlichen Schlüssel, um ihn zu verschlüsseln.
6. Kopieren Sie den Namen der Datei *token_publickey* in die Zwischenablage.
7. Verwenden Sie in einer Befehlszeile den Namen der kopierten *token_publickey*-Datei, um den Ordner der extrahierten Dateien als Platzhalter für den umschlossenen Schlüssel zu öffnen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Bearbeiten Sie dieses Skript, indem Sie die Beispiele durch die Namen Ihrer Krypto-Dateien ersetzen.

```
"downloads user.name$ cd token_publickey_<token>
openssl pkeyutl -encrypt -pubin -inkey publickey_<keyname>.PEM
-in <keyname.bin>
-out wrapped_key_material -pkeyopt rsa_padding_mode:oaep -pkeyopt
 rsa_oaep_md:sha<128 or 256> "
```

Überprüfen Sie die Schlüsselumbruchbefehle in der folgenden Tabelle, um weitere Informationen zu erhalten.

Schlüsselumbruchbefehle

Richtungen	Befehl	Beispiel
Öffnen Sie das Dateiverzeichnis, in das Sie das Packstoken heruntergeladen haben.	`cd`	`CD token_publickey123456789`
Fügen Sie den Namen des `publickey.PEM`-Zertifikats ein.	`openssl pkeyutl -encrypt -pubin -inkey`	`publickey_586798643ffff.PEM`
Fügen Sie den Namen Ihres Schlüssels hier ein.	`-in`	`mykey.bin`
Geben Sie den Befehl <-out> ein, und geben Sie an, ob der Schlüssel 128 Bit oder 256 Bit groß ist.	`-out wrapped_key_material -pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256`	N/V

9. Führen Sie den Befehl aus.
In einer Systemmeldung wird `token_publickey_ angezeigt.`<keynumber> . Der Schlüssel wird generiert, und dem Verzeichnis wird eine *`Wrapped_key_material`*-Datei hinzugefügt.
10. Laden Sie den umschlossenen Schlüssel hoch.

Nächste Maßnahme

Kehren Sie zu Konfigurieren Sie den von Ihrem Kunden bereitgestellten Schlüssel, und laden Sie ihn hoch zurück, um Ihren umschlossenen Schlüssel hochzuladen.

Konfigurieren Sie den von Ihrem Kunden bereitgestellten Schlüssel, und laden Sie ihn hoch

Sie können anstelle der vom System ServiceNow® generierten Schlüssel auch Ihren eigenen, vom Kunden bereitgestellten Schlüssel verwenden.

Vorbereitungen

Erforderliche Rolle: security_admin, sn_kmf.cryptographic_manager

Wenn Sie KEINE eigenen Schlüssel bereitstellen, müssen Sie dieses Verfahren nicht ausführen. Um ein kryptografisches Modul mit ServiceNow® -Schlüsseln zu erstellen, wechseln Sie zu Erstellen Sie ein kryptografisches Modul oder Erstellen Sie ein kryptografisches Modul für die Verschlüsselung auf Spaltenebene.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

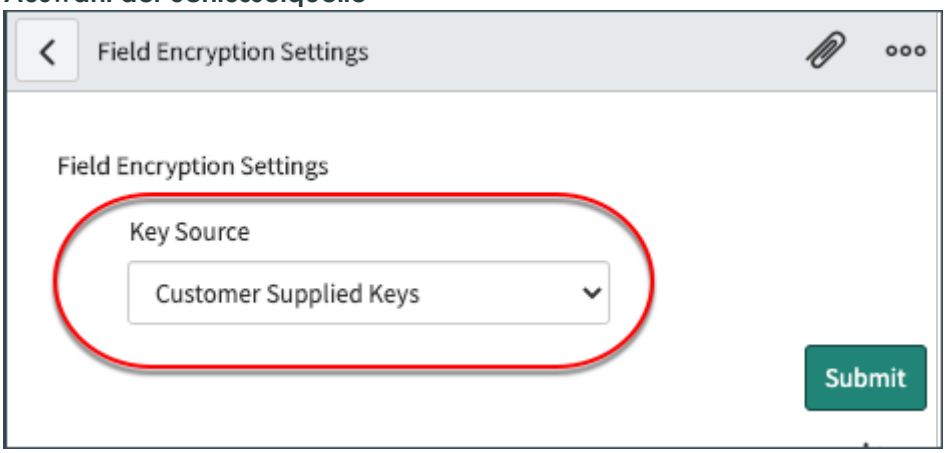
Hinweis: Dieses Verfahren gilt nur für die Funktionalität Verschlüsselung auf Spaltenebene Enterprise. Weitere Informationen finden Sie unter Aktivieren Sie die Verschlüsselung auf Spaltenebene Enterprise.

Wichtig: Sie können einen vom Kunden bereitgestellten Schlüssel nicht widerrufen.

Prozedur

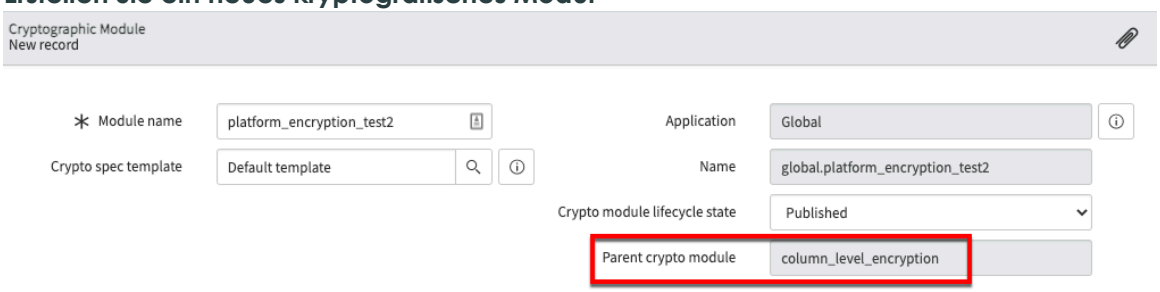
1. Navigieren zu **Alle** > **Systemsicherheit** > **Einstellungen für Feldverschlüsselung** und prüfen Sie, ob **Vom Kunden bereitgestellte Schlüssel** ausgewählt sind.

Auswahl der Schlüsselquelle



2. Wählen Sie **Absenden**.
3. Zurück zu **Systemsicherheit** > **Feldverschlüsselungsmodule** > > **Neu erstellen:**an.

Erstellen Sie ein neues kryptografisches Modul



4. Füllen Sie das Formular „Kryptografisches Modul“ wie folgt aus:

Felder des kryptografischen Moduls

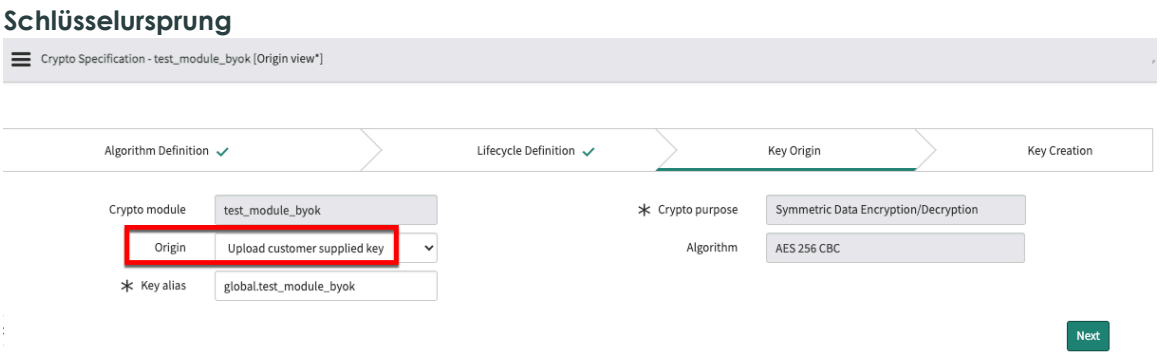
Feld	Beschreibung
Modulname	Geben Sie einen Namen für das Modul ein.
Krypto-Spezifikationsvorlage	Die standardmäßige kryptografische Vorlage ist ausgewählt.
Name	Wird automatisch basierend auf dem Modulnamen ausgefüllt und stellt dem Namen den Bereich voran, um sicherzustellen, welche Anwendung angewendet wird. In diesem Fall wird der globale Bereich angewendet.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Lebenszyklusstatus kryptografisches Modul	Auswahlvorgang **Veröffentlicht** um das Krypto-Modul zu aktivieren.
Übergeordnetes kryptografisches Modul	Das übergeordnete Modul **column_level_encryption** wird automatisch ausgewählt, wenn vom Kunden bereitgestellte Schlüssel und Verschlüsselungsmodule verwendet werden.

5. Wählen Sie **Absenden**.
6. Wählen Sie das neu erstellte kryptografische Modul aus der Tabelle aus.
   Wählen Sie in der zugehörigen Liste **„Krypto-Spezifikationen** " den automatisch generierten Schlüsselalias mit dem AES 256 CDB-Algorithmus aus.

   Das System füllt den Krypto-Zweck und den Algorithmus für CLE automatisch aus und springt zur Phase **Schlüsselursprung**.
7. Beachten Sie, dass **Vom Kunden bereitgestellten Schlüssel hochladendie** Quelle ist und der **Schlüsselalias** bereits ausgefüllt ist.



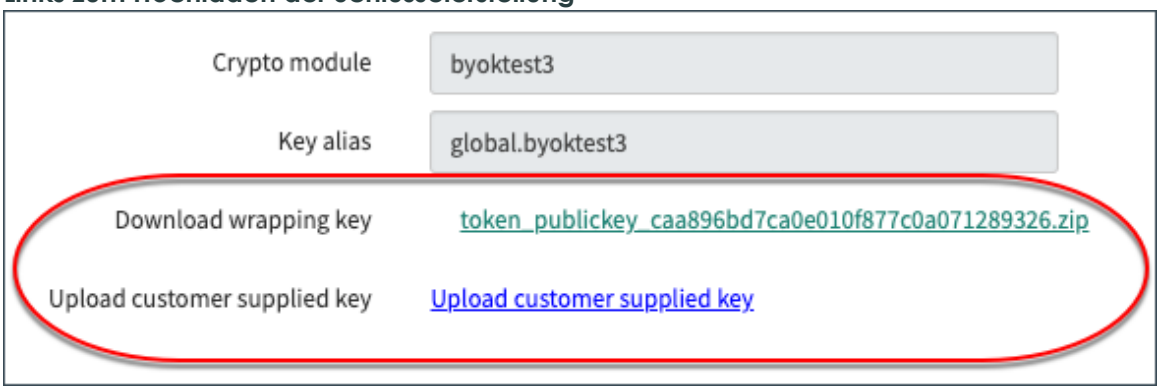
8. Wählen Sie **Weiter** aus, um zur Phase **Schlüsselerstellung** zu wechseln.

   Es gibt zwei Links:

   - **Beim Herunterladen des Wrapping-Schlüssels** wird der Schlüssel in einer ZIP-Datei heruntergeladen, die ein `Importtoken` und ein Zertifikat des öffentlichen Schlüssels (PEM-Datei) enthält. Verwenden Sie das Importtoken, um das erfolgreiche Key Wrapping gemäß der Sicherheitsspezifikation für die Instanz zu überprüfen. Verwenden Sie die `PEM` -Datei des Zertifikats des öffentlichen Schlüssels, um den von einem Kunden bereitgestellten Schlüssel sicher zu verpacken, bevor Sie ihn zusammen mit dem Token hochladen.
   - **Vom Kunden bereitgestellten Schlüssel hochladen** öffnet den Dateibrowser, um das Token und den verschlüsselten Schlüssel auszuwählen, den Sie umschlossen haben.

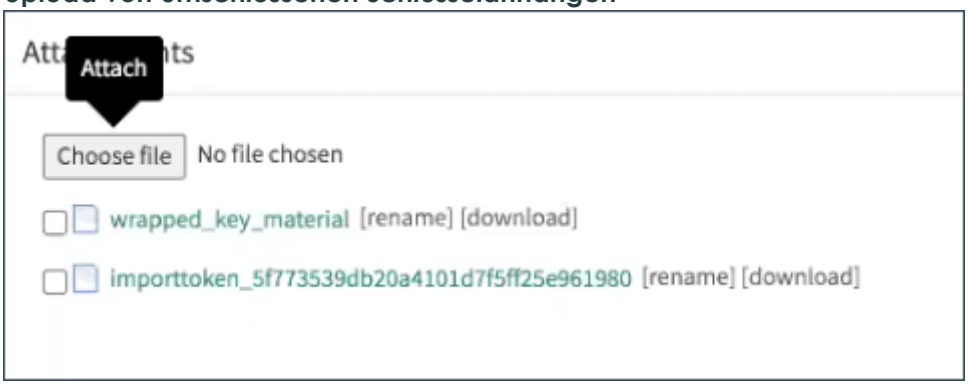
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Links zum Hochladen der Schlüsselerstellung



9. Wählen Sie **Umwickelten Schlüssel herunterladen**, um das Token zu speichern. Speichern Sie das Token am selben Zielspeicherort, an dem der Schlüssel in Ihrem System gespeichert ist. Benennen Sie das heruntergeladene Token nicht um.
10. Führen Sie den BYOK-Befehl in einem Terminal aus, um den Schlüssel zu umbrechen. Weitere Informationen finden Sie unter Packen Sie Ihren vom Kunden bereitgestellten Schlüssel ein.
11. Wählen Sie **Vom Kunden bereitgestellten Schlüssel hochladen aus**.
12. Wählen Sie **Durchsuchen**, um die beiden Dateien, den umschlossenen Schlüssel und die Tokendatei auszuwählen.
    Im Fenster „Anhänge“ werden die beiden Dateien angezeigt.

Upload von umschlossenen Schlüsselanhängen



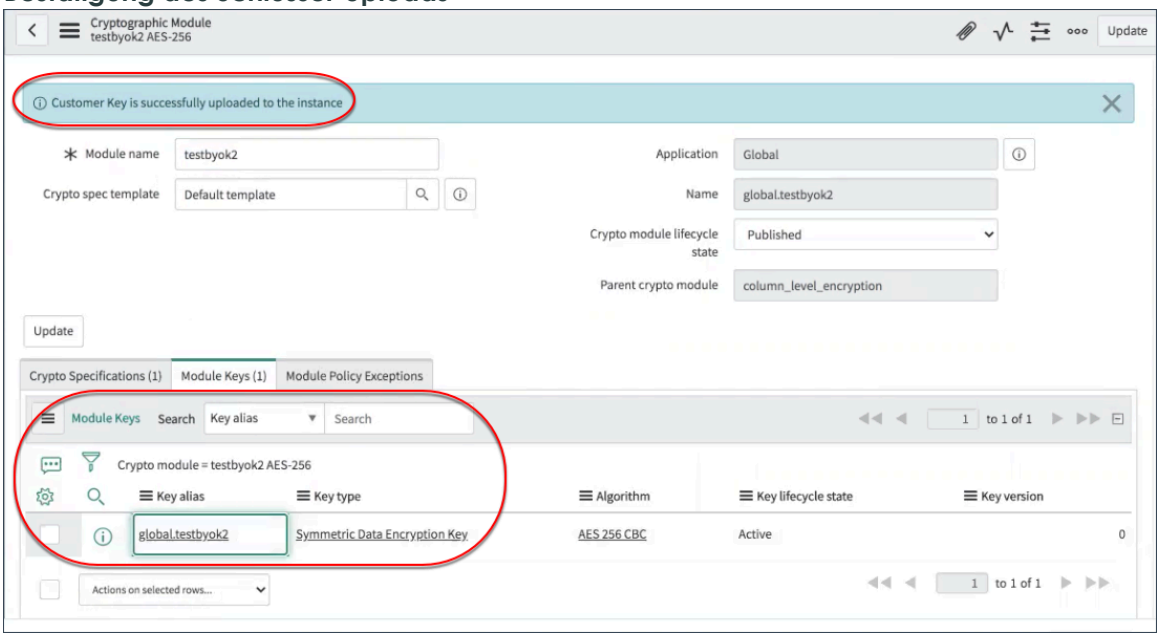
Wählen Sie die zu entfernende und bei Bedarf erneut hochzuladende Datei aus.

13. Wählen Sie **OK**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie kehren zum Bildschirm „Kryptografisches Modul“ zurück. Für einen erfolgreichen Upload des Kundenschlüssels wird eine Bestätigungsmeldung angezeigt. Der Schlüssel ist auch in der zugehörigen Liste „Modulschlüssel“ aufgeführt.

Bestätigung des Schlüssel-Uploads



Nächste Maßnahme

Nachdem Sie nun die Konfiguration Ihres kryptografischen Moduls mit dem vom Kunden bereitgestellten Schlüssel abgeschlossen haben, fahren Sie mit fort Erstellen Sie eine Modulzugriffsrichtlinie

Felder und Anhänge werden verschlüsselt

Nachdem Sie Ihre kryptografischen Module erstellt haben, erstellen Sie verschlüsselte Feldkonfigurationen und geben an, ob ein Feld in einer Tabelle oder Anhänge verschlüsselt werden sollen.

Informationen zum Verschlüsseln von Feldern

Hinweis: Verschlüsselte Felder werden nicht vom Design geprüft. Dieses Verhalten ist nicht konfigurierbar.

1. Geben Sie die Schlüsselquelle an: vom System generierte Schlüssel oder von Ihrem Kunden bereitgestellte Schlüssel (Bring Your Own Key) in **Systemsicherheit** > **Einstellungen für Feldverschlüsselung**an.
2. Nachdem Sie die Schlüsselquelle angegeben haben, erstellen Sie ein neues kryptografisches Modul, oder verwenden Sie ein vorhandenes kryptografisches Modul. Beginnen Sie mit Erstellen Sie ein kryptografisches Modul für Anweisungen.

Hinweis: Wenn Sie vom Kunden bereitgestellte Schlüssel verwenden, befolgen Sie die Anweisungen in Erstellen Sie ein kryptografisches Modul für die Verschlüsselung auf Spaltenebene und Konfigurieren Sie Eigenschaften für vom Kunden bereitgestellte Schlüssel.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Erstellen Sie eine verschlüsselte Feldkonfiguration, in der Sie die Tabelle angeben, für die die Verschlüsselung durchgeführt wird, und entweder die Spalte in der Tabelle oder die Anhänge in der zu verschlüsselnden Tabelle. Informationen zu den ersten Schritten finden Sie unter Legen Sie Konfigurationen für verschlüsselte Felder fest.

Hinweis: In Enterprise-Beispiele für Verschlüsselung auf Spaltenebene wird veranschaulicht, wie Felder und Anhänge mit vom Kunden bereitgestellten Schlüsseln verschlüsselt werden.

Legen Sie Konfigurationen für verschlüsselte Felder fest

Konfigurieren Sie, welche Tabellenspalten oder Anhänge das System mit einem vorkonfigurierten kryptografischen Modul verschlüsselt.

Vorbereitungen
Erforderliche Rolle: sn_kmf.cryptographic_manager und security_admin oder Erhöhung der Rolle zum Sicherheitsadministrator.

Warum und wann dieser Vorgang ausgeführt wird
Stellen Sie sicher, dass Sie sich im richtigen Anwendungsbereich befinden, damit Sie die Tabellen in diesem Bereich sehen können.

Nur Anwender, die Zugriff auf das in dieser Konfiguration verwendete kryptografische Modul haben, können die Daten in der verschlüsselten Tabellenspalte lesen oder auf den Anhang zugreifen.

- Wenn ein Benutzer über Schreibzugriff, aber nicht über Lesezugriff verfügt, wird das Feld im Bearbeitungsmodus angezeigt, und die eingegebenen Daten werden als Sternchen angezeigt.
- Wenn ein Benutzer über Lesezugriff, aber nicht über Schreibzugriff verfügt, zeigt das Feld die entschlüsselten Daten im schreibgeschützten Modus an.
- Wenn ein Benutzer über alle Zugriffsrechte verfügt, sind für das verschlüsselte Feld sowohl Lese- als auch Schreibfunktionen verfügbar.

Siehe Erstellen Sie ein kryptografisches Modul oder Erstellen Sie ein kryptografisches Modul für die Verschlüsselung auf Spaltenebene, um zu beginnen.

Wichtig:

Nach dem Verschlüsseln einer Spalte werden alle neuen Daten, die in die Spalte eingefügt werden, automatisch verschlüsselt. Daten, die in der Spalte vorhanden waren, bevor die Verschlüsselung aktiv war, werden jedoch nicht automatisch verschlüsselt.

Um Daten zu verschlüsseln, die vor der Verschlüsselung der Spalte vorhanden waren, müssen Sie einen separaten Massenverschlüsselungsauftrag ausführen. Weitere Informationen zur Massenverschlüsselung finden Sie unter Massenverschlüsselung oder -entschlüsselung ausführen.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Feldverschlüsselung** > **Verschlüsselungsfeld-Konfigurationen** > **Neu**an.
2. Wählen Sie **Neu**.
3. Füllen Sie das Formular aus.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Typ	**Spalte** zum Verschlüsseln einer Tabellenspalte oder Anhang zum Verschlüsseln aller **Anhänge** einer Tabelle. Folgende Arten von Daten werden verschlüsselt: ◦ Zeichenfolgentext (UTF-8 komplett) ◦ Anhänge ◦ Datum, Datum/Uhrzeit: **Hinweis:** Sie können Verschlüsselungsfeld-Konfigurationen zum Verschlüsseln der vorhandenen Datums- und Datums-/Uhrzeitfelder erstellen. Sie können eine neue Verschlüsselungskonfiguration nur einer übergeordneten Tabelle hinzufügen. Sie können einer untergeordneten Tabelle keine neue Verschlüsselungskonfiguration hinzufügen. ◦ URL ◦ Verschlüsselung auf Spaltenebene Enterprise unterstützt auch die folgenden Feldtypen: ▪ HTML ▪ Journal ▪ Übersetzt
Tabelle	Tabelle, deren Felder oder Anhänge verschlüsselt werden sollen.
Spalte	Spalte (Feld), die verschlüsselt werden soll, wenn Sie „ **Spalte** “ als Typ ausgewählt haben.
Aktiv	Auswählen, um die Konfiguration als aktiv zu markieren. Deaktivieren Sie die Option, wenn die Konfiguration noch nicht verwendet wird.
Crypto-Modul	Das kryptografische Modul, für das die verschlüsselte Feldkonfiguration gilt.
Methode	Wählen Sie **Einzelnes Modul** aus, um die Feldkonfiguration für ein Modul festzulegen. Wählen Sie **„Mehrere Module“** für einen rollenbasierten Zugriff aus, der sich über mehr als ein kryptografisches Modul erstreckt. Einzelnes Modul Verwenden Sie diese Option, um alle Anhänge mit einem einzelnen Modul zu verschlüsseln. Ihre Anwender müssen auf dieses Modul zugreifen, andernfalls können sie keine Anhänge hochladen. Mehrere Module Verwenden Sie diese Option, um Anwendern die Auswahl eines Moduls beim Hochladen von Anhängen zu ermöglichen. Benutzer mit Zugriff auf mindestens ein Modul können ein Modul

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	zur Verschlüsselung auswählen. Benutzer ohne Modulzugriff können unverschlüsselte Anhänge hochladen.
Algorithmus verschlüsselt und konservierend [schreibgeschützt]	Gibt an, ob das von Ihnen ausgewählte Kryptomodul bereits für die Unterstützung der nicht deterministische Verschlüsselung konfiguriert ist. Das heißt, wenn dieselben Daten mehrmals verschlüsselt werden, ist die Verschlüsselung jedes Mal anders.

4. Wählen Sie **Absenden**.

Skriptzugriff für kryptografische Module

Skripts können ausgeführt werden, um für einen kryptografischen Zweck auf eine kryptografische Modulrichtlinie zuzugreifen.

Für Key Management Frameworkkönnen Richtlinien auf Skripts basieren. Wenn eine Zugriffsrichtlinie für den Skriptzugriff ausgelöst wird, kann das Back-End-Skript die Modulrichtlinienaktionen aus dem Skript ausführen.

Kryptografische Module können einen oder mehrere Verschlüsselungszwecke unterstützen, z. B. asymmetrische Datenentschlüsselung und symmetrische Datenentschlüsselung. Jeder kryptografische Zweck erfordert die Generierung eines Verschlüsselungsschlüssels und einen definierten kryptografischen Zweck.

Beachten Sie bei der Ausführung einer Verschlüsselungsskriptanforderung Folgendes:

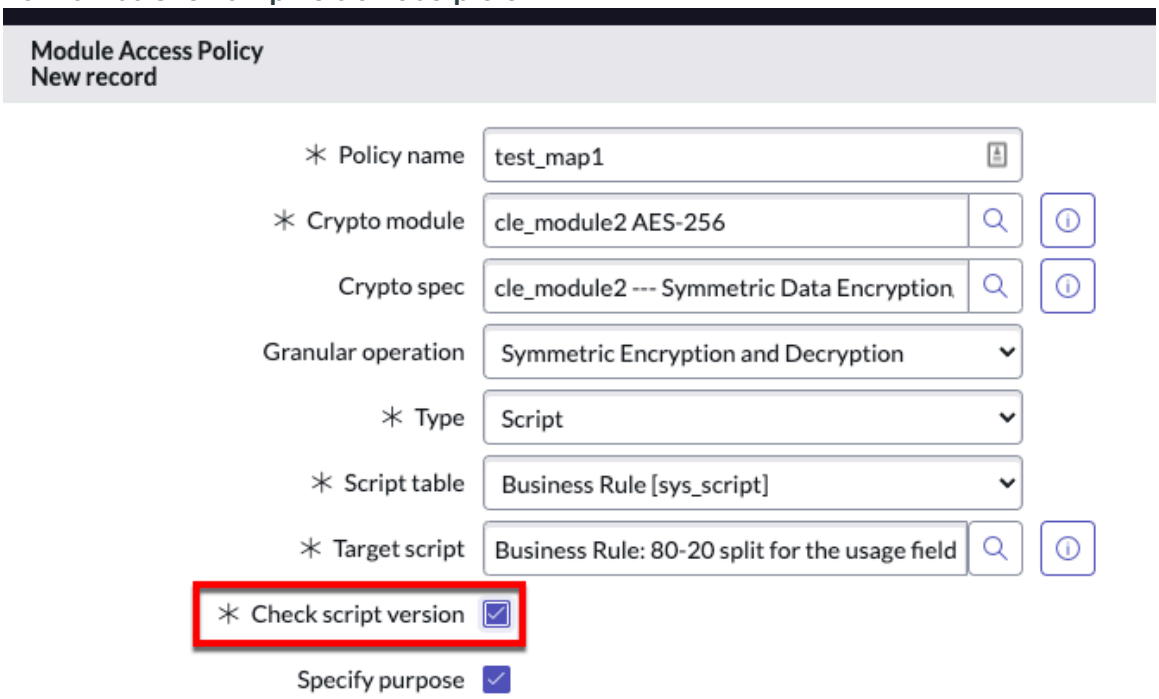
- Der referenzierte kryptografische Zweck muss im kryptografischen Modul definiert sein.
- Für das kryptografische Modul muss ein aktiver generierter Schlüssel vorhanden sein.
- Der Typ der Modulzugriffsrichtlinie muss auf **Skript**festgelegt sein.

Skriptversion überprüfen

Beim Erstellen einer Modulzugriffsrichtlinie, die auf den Skripttyp festgelegt ist, steht eine Option zum Validieren der Integrität der zugegriffenen Skriptversion zur Verfügung. Nur die zugewiesene Version des Skripts darf auf die Verschlüsselungsmodule zugreifen. Wenn in der Modulzugriffsrichtlinie das **Kontrollkästchen Skriptversion** überprüfen aktiviert ist, führt das System bei jeder Ausführung des Skripts einen Versionsvergleich durch. Wenn das Skript geändert wurde, wird der Benutzer benachrichtigt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kontrollkästchen Skriptversion überprüfen



Konfigurieren Sie den Skriptzugriff auf verschlüsselte Daten

Führen Sie ein Skript aus, um die kryptografische Modulrichtlinie für einen kryptografischen Zweck auszuführen. Spezifischer Lesezugriff (entschlüsseln/entpacken) oder Schreibzugriff (verschlüsseln, umbrechen) kann basierend auf der Granularität des Modulzugriffsrichtlinienvorgangs definiert werden.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_manager

Warum und wann dieser Vorgang ausgeführt wird

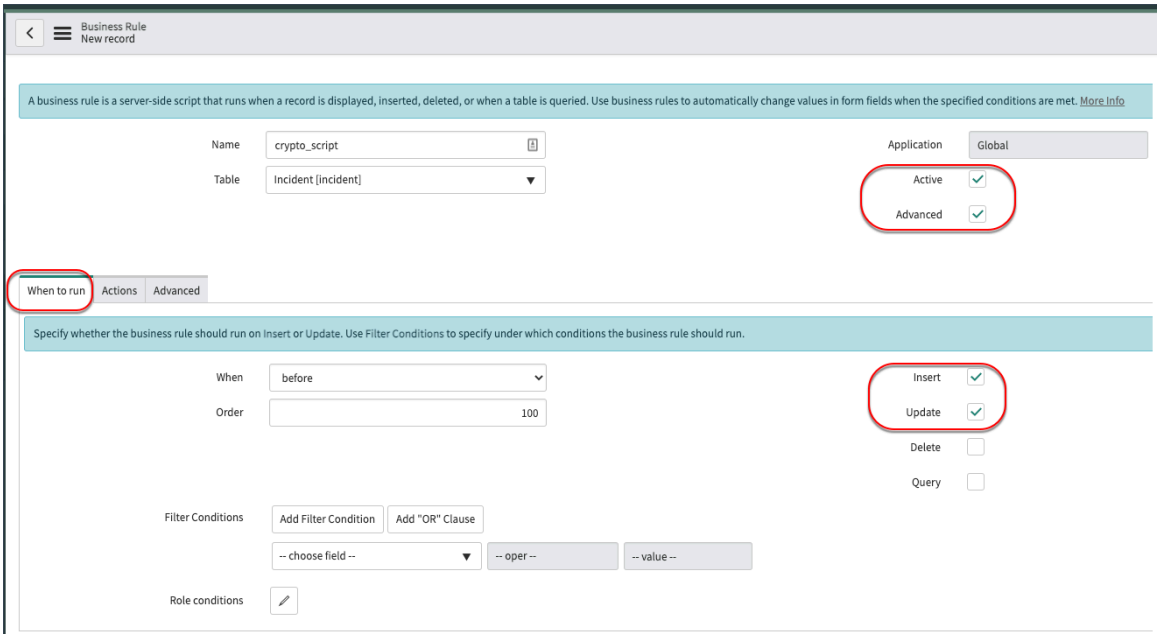
Anwendungsbeispiele sind Business-Regeln und Skripteinbindungen. In diesem Verfahren wird ein Skript für Geschäftsregeln verwendet.

Prozedur

1. Erstellen Sie ein kryptografisches Modul mit dem symmetrischen Datenverschlüsselungs-/-entschlüsselungsalgorithmus.
   Weitere Informationen finden Sie unter Erstellen Sie ein kryptografisches Modul. Der spezifische Zugriff auf die Daten oder Anhänge wird mit einer Modulzugriffsrichtlinie mit den folgenden Eigenschaften gesteuert:
   - Symmetrische Verschlüsselung: Das Skript kann Daten verschlüsseln, aber nicht entschlüsseln.
   - Symmetrische Entschlüsselung: Das Skript kann hochgeladene verschlüsselte Daten oder Anhänge entschlüsseln, aber keine Daten oder Anhänge verschlüsseln.
   - Symmetrische Verschlüsselung und Entschlüsselung: Das Skript kann Daten oder Anhänge sowohl verschlüsseln als auch entschlüsseln.
2. Navigieren zu **Systemdefinition** > **Business-Regeln**an.
3. Klicken Sie auf **Neu**.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



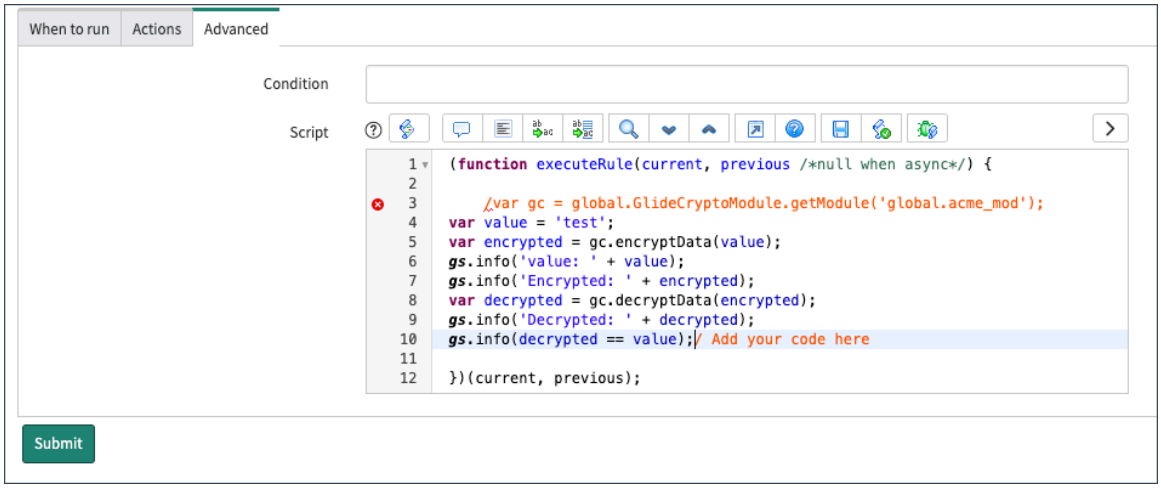
4. Füllen Sie das Formular auf der Registerkarte Zeitpunkt **für Ausführung aus**, und geben Sie das Skript auf der Registerkarte **Erweitert** ein:

Business Rule-Felder

Feld	Beschreibung
Name	Geben Sie einen Namen für die Business Rule ein.
Tabelle	Wählen Sie in der Dropdown-Liste **Incident [incident]**aus.
Anwendung	Standardmäßig ist**Global** ausgewählt.
Aktiv	Markieren Sie die Regel als **Aktiv**.
Erweitert	Aktivieren Sie die Checkbox, um erweiterte Optionen anzuzeigen.
Registerkarte „Ausführungszeitpunkt“	Aktivieren Sie auf der Registerkarte Zeitpunkt **für Ausführung** die Felder **Einfügen** und **Aktualisieren**.

Registerkarte „Erweitert“	Fügen Sie auf der Registerkarte **Erweitert** den folgenden Text in Zeile 3 ein:
	`//`
	`var gc = global.GlideCryptoModule.getModule('global.acme_mod');`
	`var value = 'test';`
	`var encrypted = gc.encryptData(value);`
	`gs.info('value: ' + value);`
	`gs.info('Encrypted: ' + encrypted);`
	`var decrypted = gc.decryptData(encrypted);`
	`gs.info('Decrypted: ' + decrypted);`
	`gs.info(decrypted == value);`
	Hinweis: Einzelheiten finden Sie in der Abbildung „Business-Regeln – Registerkarte „Erweitert““.

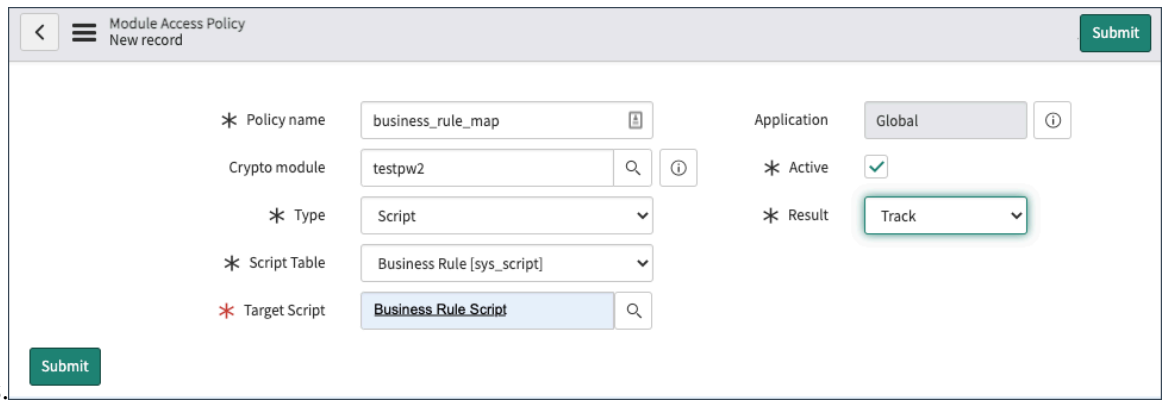
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Klicken Sie auf **Absenden**.
6. Navigieren zu **Schlüsselverwaltung** > **Modulzugriffsrichtlinien** > **Alle**.

> **Hinweis:** Weitere Informationen finden Sie unter Erstellen Sie eine Modulzugriffsrichtlinie.

7. Klicken Sie auf **Neu**.
8. Füllen Sie das Formular aus.



Felder „Modulzugriffsrichtlinien“

Feld	Beschreibung
Richtlinienname	Geben Sie einen Namen für die Richtlinie ein.
Crypto-Modul	Klicken Sie auf das Suchsymbol, um ein Modul mit dem symmetrischen Datenverschlüsselungs-/-entschlüsselungsalgorithmus auszuwählen.
Typ	Wählen Sie Skript aus, um den Zugriff nach **Skript** zu steuern.
Skripttabelle	Wählen Sie einen Wert aus der Drop-down-Liste der Skripttabelle aus. Wählen Sie für dieses Beispiel **Business-Regel [sys_script] aus**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zielskript	Wählen Sie das Skriptdokument für die Richtlinie aus. Wählen Sie den **Tabellennamen** und dann das zugehörige Dokument für die Richtlinie aus. Wählen Sie für dieses Beispiel die Geschäftsregel aus, die Sie in den vorherigen Schritten erstellt haben.
Aktiv	Wählen Sie diese Option aus, um die Richtlinie zu aktivieren.
Ergebnis	Um dem Skript Zugriff auf das Modul zu gewähren, wählen Sie **Nachverfolgen** im Feld **Ergebnis** aus.

9. Klicken Sie auf **Absenden**.
   Die Modulzugriffsrichtlinie für das Skript ist jetzt im System verfügbar.

Zeigen Sie abgelehnte Anforderungen zur Nutzung des kryptografischen Moduls an

Zeigen Sie kryptografische Module an, die Verschlüsselungsanforderungen von Skripts aufgrund nicht unterstützter Verschlüsselungsmechanismen abgelehnt haben.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_manager

Warum und wann dieser Vorgang ausgeführt wird

Kryptografische Module können einen oder mehrere Verschlüsselungszwecke unterstützen, z. B. asymmetrische Datenentschlüsselung und symmetrische Datenentschlüsselung. Auf verschlüsselte Daten kann nur basierend auf der Modulzugriffsrichtlinie zugegriffen werden. Wenn ein Skript versucht, ein kryptografisches Modul für einen nicht im Modul definierten Zweck zu verwenden, kann das Skript nicht auf die verschlüsselten Daten zugreifen.

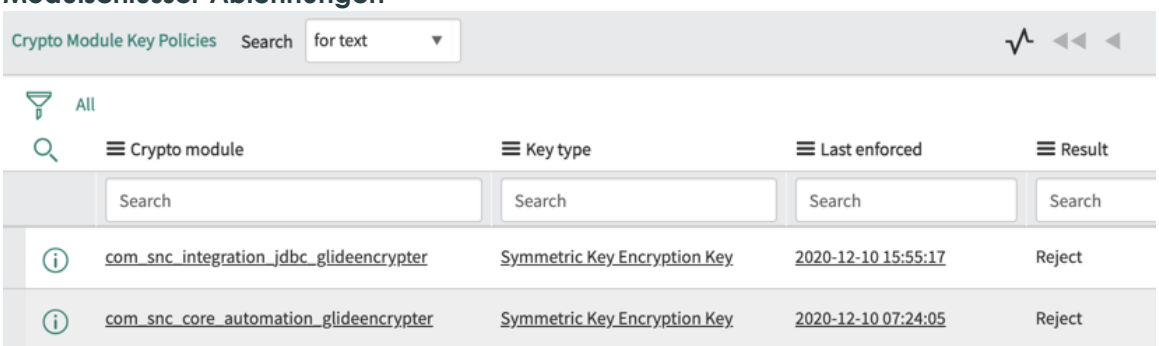
Im folgenden Beispiel wurde einem kryptografischen Modul ein kryptografischer Zweck zugewiesen, für den jedoch nie ein Schlüssel generiert wurde.

Prozedur

Navigieren zu **Alle** > **Schlüsselverwaltung** > **Modulschlüssel-Richtlinien** > **Modulschlüssel-Ablehnungen**an.

Eine Liste der kryptografischen Module, die Anforderungen abgelehnt haben, wird zusammen mit dem im entsprechenden Skript verwendeten Verschlüsselungsschlüssel angezeigt.

Modulschlüssel-Ablehnungen



© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn ein anderes Skript versucht, dasselbe kryptografische Modul mit demselben Schlüsseltyp zu verwenden, wird der Wert für **Letzte erzwungene** Updates geändert. Es wird keine weitere Zeile generiert.

In diesem Beispiel hat das erste Modul um 2020-02-10_15:55:17 eine Anforderung abgelehnt, da der Schlüssel von module1 gefährdet ist. Um 2020-02-10_07:24:05 hat das zweite Modul eine Anforderung abgelehnt, da der Schlüssel des zweiten Moduls angehalten ist.

Um Skripts bei der nächsten Ausführung die Berechtigung zur Verwendung des Verschlüsselungsmoduls zu erteilen, erstellen Sie eine Modulzugriffsrichtlinie für die Skriptverschlüsselung. Weitere Informationen finden Sie unter Konfigurieren Sie den Skriptzugriff auf verschlüsselte Daten.

Planen Sie Aufträge zur Massenverschlüsselung, -entschlüsselung und zur erneuten Schlüsselerstellung

Planen Sie Verschlüsselungs-, Entschlüsselungs- und Schlüsselerstellungsaufgaben so, dass sie zu einem Zeitpunkt ausgeführt werden, der für Ihre Instanz am besten geeignet ist.

Vorbereitungen

Verschlüsselungs-, Entschlüsselungs- und Neuschlüsselungsaufträge können zeit- und ressourcenintensiv sein. Planen Sie sie daher außerhalb der Spitzenzeiten ein. Stellen Sie außerdem sicher, dass der Benutzer, der die Aufgabe plant, über die entsprechenden Zugriffsrechte für jede Aufgabe verfügt.

Erforderliche Rolle: sn_kmf.cryptographic_manager

Warum und wann dieser Vorgang ausgeführt wird

Massenverschlüsselung und -entschlüsselung ist auch im Formular „Konfigurationen verschlüsselter Felder“ verfügbar. Siehe Massenverschlüsselung oder -entschlüsselung ausführen für Anweisungen.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Strenge Sicherheitseinstellungen** > **Security-Aufträge**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie das Zeitplanformular aus.

Feld	Beschreibung
Name	Name des Verschlüsselungs-, Entschlüsselungs- oder Neuschlüsselungsauftrags.
Typ	Auftragstyp: ◦ **Schlüsselmigrationskontext zu Modul:** Massenmigration von Verschlüsselungskontextschlüsseln zu Verschlüsselungsmodulen, einschließlich der Erstellung von Modulzugriffsrichtlinien-Datensätzen für Zugriffssteuerungen auf den Verschlüsselungsmodulen ◦ Datenmigrationskontext**zu Modul**: Migriert Daten, die mit Verschlüsselungskontexten verschlüsselt wurden, zu Verschlüsselungsmodulen ◦ Massenentschlüsselungsanhang:**Entschlüsselt**alle verschlüsselten Anhänge in Datensätzen für eine einzelne Tabelle, die Sie im Feld „ **Tabelle** “ definieren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	◦ **Massenverschlüsselungsanhang**: Verschlüsselt alle Anhänge in Datensätzen für eine einzelne Tabelle, die Sie im Feld „ **Tabelle** “ definieren. ◦ **Massenverschlüsselungsmodul**: Verschlüsselt einen bereits vorhandenen Wert in der definierten Spalte/dem definierten Feld, die/das in der Feldverschlüsselungskonfiguration verwendet wird ◦ **Massenentschlüsselungsmodul**: Entschlüsselt einen bereits vorhandenen Wert in der definierten Spalte/dem definierten Feld, der/das in der Feldverschlüsselungskonfiguration mit Einzelmodul verwendet wird. ◦ Massenentschlüsselung für mehrere**Module**: Entschlüsselt einen bereits vorhandenen Wert in der definierten Spalte/dem definierten Feld, der bzw. das in der Feldverschlüsselungskonfiguration mit mehreren Modulen verwendet wird. ◦ **Modul-Neuschlüsselung**: Verschlüsselt einen bereits vorhandenen Wert in der definierten Spalte/dem definierten Feld, der/das in der Feldverschlüsselungskonfiguration verwendet wird, mit dem aktuell aktiven Schlüssel für das Modul erneut. ◦ **Anhangskontext zu Modul**migrieren: Verschlüsselt alle bereits vorhandenen Anhänge in der Tabelle, die in der Feldverschlüsselungskonfiguration definiert sind. Jeder zuvor mit einem Kontext verschlüsselte Anhang wird mit dem Modul erneut verschlüsselt.
Status	Der anfängliche Job-Status ist Neu. Nachdem die Aufgabe wie geplant ausgeführt wurde, wird der Status entsprechend aktualisiert.
Zeitfensterstart	Startzeit für den Auftrag im 24-Stunden-Format.
Zeitfensterende	Endzeit für den Auftrag im 24-Stunden-Format.
Tabelle	Zu verschlüsselnde oder zu entschlüsselnde Tabelle.
Feld	Zu verschlüsselndes oder zu entschlüsselndes Feld.
Zusammenfassung	Informationen zum Auftragsstatus, wenn der Auftrag ausgeführt wird, abgeschlossen ist oder Fehler aufweist.

Hinweis: Aufgrund des System-Overheads sollten Sie Massenverschlüsselungs-, Entschlüsselungs- und Schlüsselerstellungsaufgaben so planen, dass sie außerhalb der Spitzenzeiten ausgeführt werden. Now Platform führt den Auftrag zwischen **Zeitfensterstart** und **Zeitfensterende aus**. Wenn der Auftrag in einem Verarbeitungsfenster nicht abgeschlossen wird, wird er im nächsten angegebenen Verarbeitungsfenster fortgesetzt, bis die gesamte Verarbeitung abgeschlossen ist.

4. Klicken Sie auf **Absenden**.
5. Nachdem Sie eine Aufgabe geplant haben, können Sie wie folgt vorgehen.
   - **Klicken** Sie auf Auftrag abbrechen, um einen laufenden Auftrag abzubrechen.
   - Klicken Sie auf **Start**, um einen Auftrag sofort zu starten.
   - Klicken Sie auf **Aktualisieren**, um alle Änderungen zu speichern, die Sie am Aufgabenzeitplan vorgenommen haben.
   - Klicken Sie auf **Löschen**, um die geplante Aufgabe zu löschen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Massenverschlüsselung oder -entschlüsselung ausführen

Sie können eine Massenverschlüsselung für Verschlüsselungskonfigurationen sowie eine Massenentschlüsselung ausführen, um zuvor verschlüsselte Werte zu entschlüsseln.

Vorbereitungen
Erforderliche Rolle: security_admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können auch geplante Aufgaben für die Massenverschlüsselung und -entschlüsselung erstellen. Siehe Planen Sie Aufträge zur Massenverschlüsselung, -entschlüsselung und zur erneuten Schlüsselerstellung für Anweisungen.

Massenverschlüsselung und -entschlüsselung sind nur verfügbar, wenn eine verschlüsselte Feldkonfiguration das einzelne kryptografische Modul verwendet. Die Massenentschlüsselung ist sowohl für die Einzel- als auch für die Mehrfachverschlüsselungsmethodeverfügbar.

Hinweis: Sie sollten die Massenverschlüsselung und -entschlüsselung nur außerhalb der Spitzenzeiten durchführen, da diese Vorgänge ressourcen- und zeitintensiv sind.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Feldverschlüsselung** > **Verschlüsselungsfeld-Konfigurationen**an.
2. Öffnen Sie die Konfiguration des verschlüsselten Felds für das Feld, das Sie massenweise verschlüsseln oder entschlüsseln möchten.
3. Wählen Sie unter „Zugehörige Links“ eine verfügbare Option aus.
   - **Planen Sie einen Massenentschlüsselungsauftrag**
   - **Planen Sie einen Massenverschlüsselungsauftrag**
4. Bestätigen Sie Ihre Auswahl im Dialogfeld.

Ergebnisse
Bei Ausführung einer Massenverschlüsselung werden alle Werte mit dem Verschlüsselungsmodul verschlüsselt, das im Konfigurationsdatensatz des verschlüsselten Felds definiert ist. Bei der Ausführung einer Massenentschlüsselung werden nur Felder entschlüsselt, die mit einem Verschlüsselungsmodul verschlüsselt sind, auf das Sie Zugriff haben.

Enterprise-Beispiele für Verschlüsselung auf Spaltenebene

Diese Beispiele führen Sie durch die Verschlüsselung von Feldern und Anhängen mit von Kunden bereitgestellten Schlüsseln.

Walkthrough zur Feldverschlüsselung

Diese Tour zeigt, wie Sie ein Feld in Ihrer -Instanz mithilfe von Verschlüsselung auf Spaltenebene Enterprise mit Key Management Framework (KMF) verschlüsseln. Außerdem erfahren Sie, wie Sie Ihren eigenen Schlüssel verwenden.

Vorbereitungen

Hinweis: Dieses Verfahren gilt nur für die Funktionalität Verschlüsselung auf Spaltenebene Enterprise. Unter Aktivieren Sie die Verschlüsselung auf Spaltenebene Enterprise finden Sie weitere Informationen zum Abrufen von Verschlüsselung auf Spaltenebene Enterprise.

Erforderliche Rolle: admin oder security_admin

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: security_admin ist eine privilegierte Rolle. Weitere Informationen zur Verwendung von privilegierten Rollen finden Sie unter Erhöhen auf eine privilegierte Rolle

Warum und wann dieser Vorgang ausgeführt wird

Diese Tour beginnt mit einer Instanz, in der Sie bereits Ihren persönlichen kryptografischen Schlüssel erstellt und hochgeladen haben. Sie könnten den Schlüssel ServiceNow verwenden, in diesem Beispiel wird jedoch ein vom Kunden bereitgestellter Schlüssel verwendet.

Nachdem der Schlüssel in einem kryptografischen Modul gespeichert wurde, können Sie mit der Konfiguration von Feldern in Ihrer Instanz beginnen, z. B. Gehalts- oder Sozialversicherungsnummern, auf die nur bestimmte Benutzer zugreifen können. Geben Sie in der Konfiguration des verschlüsselten Felds an, welche autorisierten Mitarbeiter auf vertrauliche Daten zugreifen können.

Diese Aufgabe demonstriert zwei Szenarien. In einem Beispiel wird das Feld **Kurzbeschreibung** in einem Incident für Benutzer verschlüsselt, die nicht berechtigt sind, die vertraulichen Daten anzuzeigen.

Anhänge können auch verschlüsselt werden und sind nur für Benutzer sichtbar, denen Zugriff gewährt wird, oder sie sind für alle Benutzer sichtbar, die nicht vom Anzeigen der Daten ausgeschlossen sind. Informationen zum Verschlüsseln eines Anhangs finden Sie unter Verschlüsselungstour des Anhangs.

Prozedur

1. Stellen Sie sicher, dass Verschlüsselung auf Spaltenebene Enterprise aktiviert ist.
2. Erstellen Sie ein kryptografisches Modul für column_level_encryption.
   Weitere Informationen finden Sie unter Erstellen Sie ein kryptografisches Modul für die Verschlüsselung auf Spaltenebene Erstellen Sie ein kryptografisches Modul.
3. Navigieren zu **Systemsicherheit** > **Verschlüsselungsfeld-Konfigurationen**an.
4. Klicken Sie auf **Neu**.
5. Füllen Sie die Felder des Formulars aus.

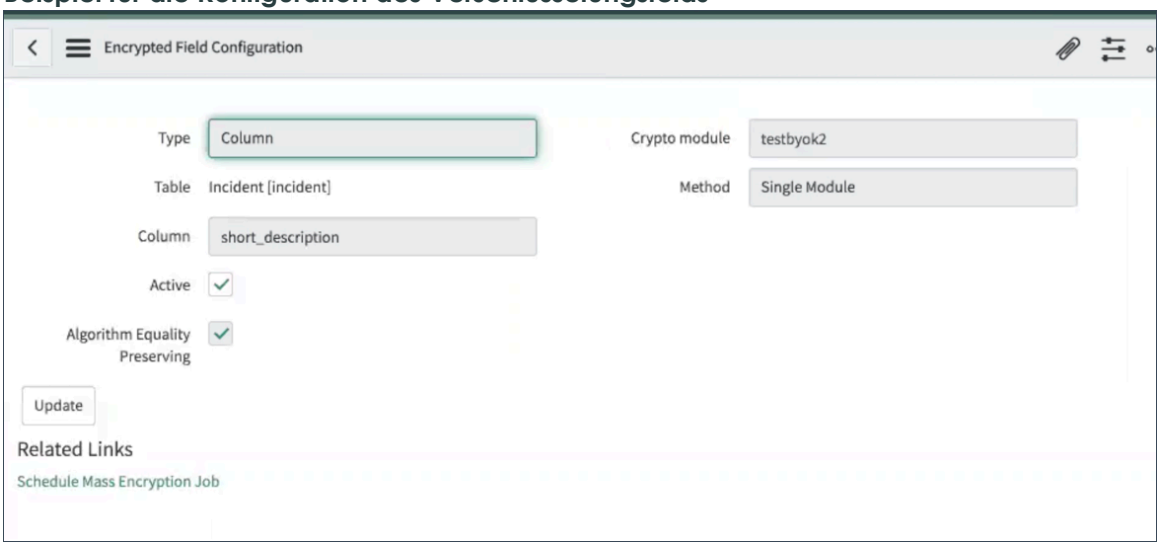
Konfigurationsformular für verschlüsselte Felder

Feld	Beschreibung
Typ	**Spalte** ist erforderlich, um Ihren persönlichen Schlüssel zu verwenden.
Tabelle	Tabelle, in der die vertraulichen Informationen gespeichert werden. Wählen Sie für dieses Beispiel **Incident [Incident]**aus.
Spalte	Spalte oder bestimmte Informationen, die das zu verschlüsselnde vertrauliche Datum darstellen. Wählen Sie für dieses Beispiel **short_description aus**.
Aktiv	Option zum Markieren von **„Aktiv“**, um die Feldkonfiguration zu verwenden.
Algorithmus-Gleichstellungserhaltung	Die Option ist automatisch ausgewählt.
Crypto-Modul	Modul, das Sie zur Verwendung mit dem persönlichen Schlüssel erstellt haben.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Methode	Die Option **Einzelnes Modul** wird verwendet, um die Richtlinien für ein Modul anzuwenden. **Mehrere Module** werden verwendet, um die Richtlinien auf mehrere Module anzuwenden.

Beispiel für die Konfiguration des Verschlüsselungsfelds



6. Klicken Sie auf **Absenden**.

   Richten Sie eine Modulzugriffsrichtlinie ein, um Zugriff auf das kryptografische Modul zuzuweisen. Weitere Informationen finden Sie unter Erstellen Sie eine Modulzugriffsrichtlinie.

7. Navigieren zu **Schlüsselverwaltung** > **Modulzugriffsrichtlinien** > > **Neu erstellen:** > **an.**
8. Füllen Sie die Felder des Formulars aus.

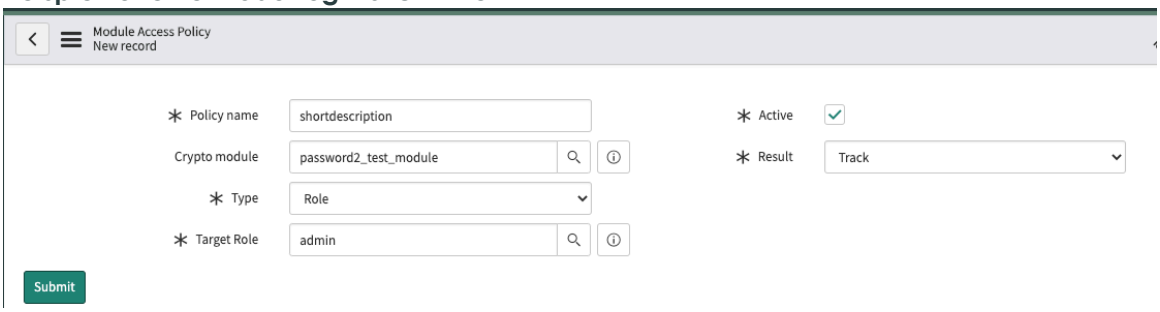
Formular „Modulzugriffsrichtlinie“

Feld	Beschreibung
Richtlinienname	Name für die Richtlinie, z. B. als `Kurzbeschreibung`.
Crypto-Modul	Crypto-Modul, das Sie zum Verschlüsseln Ihres Schlüssels erstellt haben.
Typ	Typ der Zugriffsbezeichnung für die Kryptorichtlinie. Verwenden Sie die **Rolle**, um den Zugriff auf das verschlüsselte Feld nur den Anwendern zu gewähren, denen die Rolle zugewiesen ist.
Zielrolle	Die Rolle, die Zugriff auf das verschlüsselte Feld hat. **Wählen**Sie in diesem Beispiel Administrator aus.
Aktiv	Option zum Aktivieren der Modulzugriffsrichtlinie.
Ergebnis	Die **Option**„Nachverfolgen“ aktiviert den Zugriff auf das Feld für die ausgewählte Rolle. (Um den Zugriff auf dieses Feld für die ausgewählte Rolle zu beschränken, wählen Sie **Ablehnen** oder**Striktes Ablehnen**.)

Automatische Übersetzung

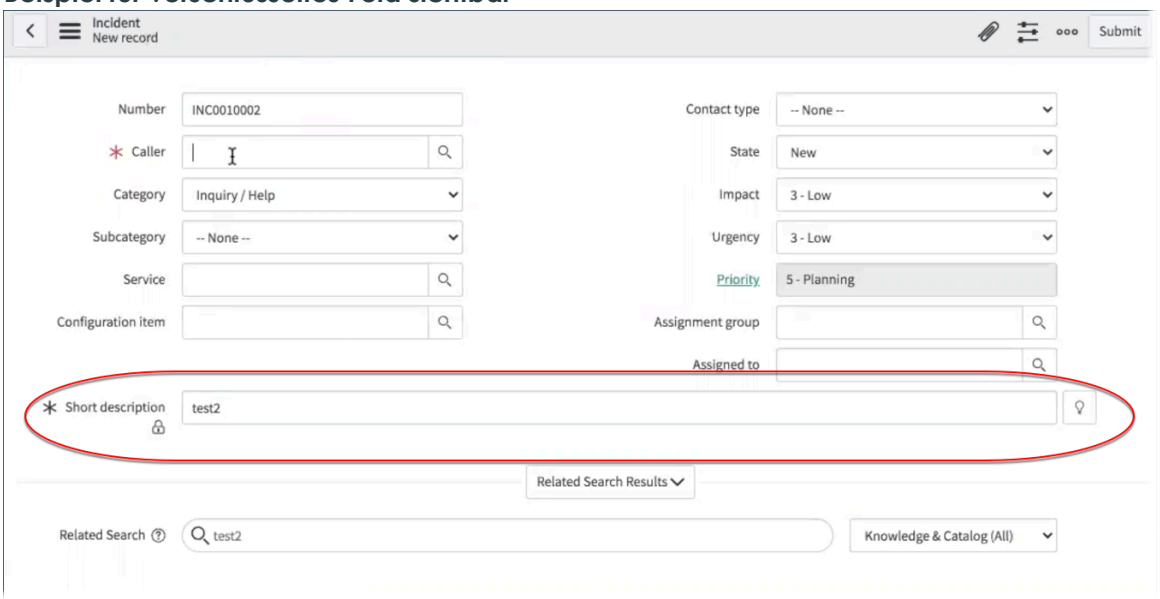
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für eine Modulzugriffsrichtlinie



9. Klicken Sie auf **Absenden**.
10. Navigieren Sie als Benutzer mit der Rolle sn_kmf.admin zu **Incident** > **Neu**an.

Beispiel für verschlüsseltes Feld sichtbar



Sie können jetzt das Feld Kurzbeschreibung basierend auf der Konfiguration der Modulzugriffsrichtlinie anzeigen.

Hinweis: Der Rolle sn_kmf.admin wurde Benutzerzugriff auf das verschlüsselte Feld Kurzbeschreibung gewährt, indem die **Modulzugriffsrichtlinie**auf Nachverfolgung festgelegt wurde. Beachten Sie das Sperrsymbol ( ) unter dem Feldnamen, das angibt, dass das Feld ein verschlüsseltes Feld ist.

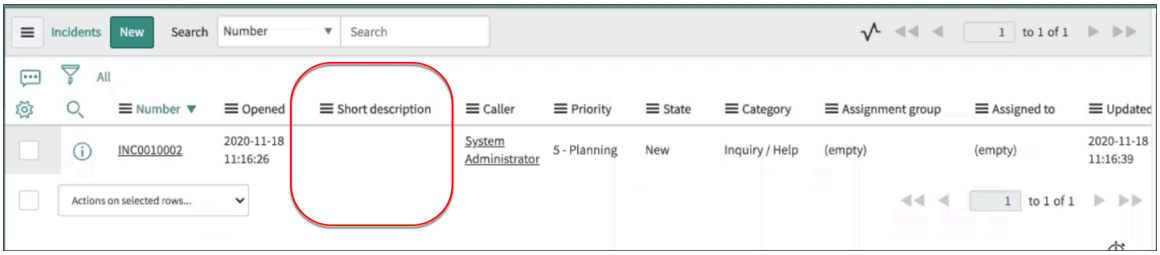
Sie können jetzt als Endanwender auf das **Incidents** -Modul zugreifen, um die Konfiguration des verschlüsselten Felds zu testen.

11. Melden Sie sich als Anwender an, damit Sie die verschlüsselten Daten im konfigurierten Feld nicht anzeigen können.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verschlüsselte Daten auf Feldebene



Wenn Sie auf die Incident-Nummer zugreifen, sind die Daten in der Kurzbeschreibung nicht sichtbar.

Ergebnisse

Sie haben Ihren symmetrischen Schlüssel erfolgreich verwendet, um den Zugriff auf ein bestimmtes Feld mithilfe von Verschlüsselung auf Spaltenebene Enterprisezu steuern.

Verschlüsselungstour des Anhangs

Diese Tour zeigt, wie Sie einen Anhang in Ihrer -Instanz mithilfe von Verschlüsselung auf Spaltenebene Enterprise mit Key Management Framework (KMF) verschlüsseln. Außerdem erfahren Sie, wie Sie Ihren eigenen Schlüssel verwenden.

Vorbereitungen

Hinweis: Dieses Verfahren gilt nur für die Funktionalität Verschlüsselung auf Spaltenebene Enterprise. Unter Aktivieren Sie die Verschlüsselung auf Spaltenebene Enterprise finden Sie weitere Informationen zum Abrufen von Verschlüsselung auf Spaltenebene Enterprise.

Erforderliche Rolle: KMF-Kryptografiemanager

Warum und wann dieser Vorgang ausgeführt wird

Diese Tour beginnt mit einer Instanz, in der Sie den vom Kunden bereitgestellten kryptografischen Schlüssel bereits erstellt und hochgeladen haben. Sie könnten den Schlüssel ServiceNow® verwenden, in diesem Beispiel wird jedoch ein vom Kunden bereitgestellter Schlüssel verwendet.

Laden Sie vertrauliche Anhänge in Ihre Instanz hoch, und beschränken Sie den Zugriff für bestimmte Anwender. Verwenden Sie die verschlüsselte Feldkonfiguration, um anzugeben, welche autorisierten Mitarbeiter auf vertrauliche Daten zugreifen können.

Wir zeigen Ihnen, wie Sie Anhänge so verschlüsseln, dass sie nur für Benutzer sichtbar sind, denen Zugriff gewährt wird, oder für alle Benutzer sichtbar sind, die nicht vom Anzeigen der Daten ausgeschlossen werden. In diesem Beispiel verhindern wir, dass eine bestimmte Rolle auf einen Anhang im **Incidents** -Modul zugreifen kann.

Hinweis: Obwohl Sie mehrere Module mit Spaltenverschlüsselung verwenden können, müssen für die Anhangsverschlüsselung einzelne Module verwendet werden.

Prozedur

1. Stellen Sie sicher, dass Verschlüsselung auf Spaltenebene Enterprise aktiviert ist.
2. Erstellen Sie ein kryptografisches Modul.
   Weitere Informationen finden Sie unter Erstellen Sie ein kryptografisches Modul für die Verschlüsselung auf Spaltenebene.
3. Navigieren zu **Systemsicherheit** > **Verschlüsselungsfeld-Konfigurationen**an.

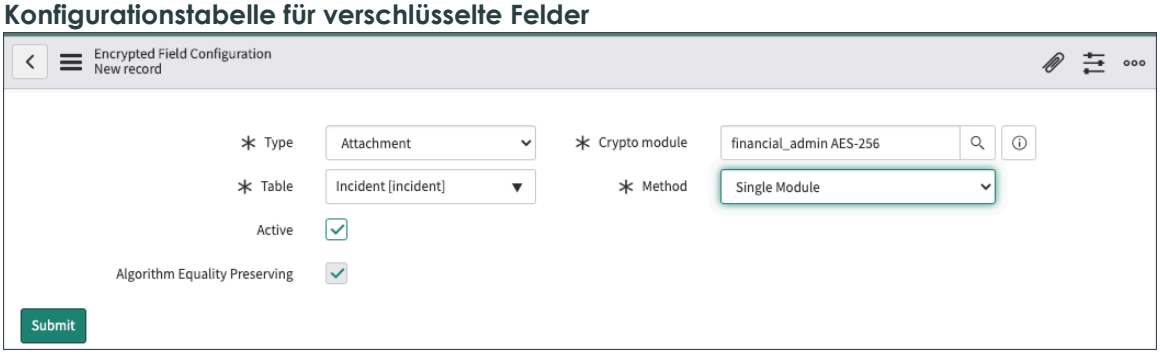
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Neu**.
5. Füllen Sie das Formular aus:

Konfigurationsfelder für verschlüsselte Felder

Feld	Beschreibung
Typ	Wählen Sie **Anhang** aus, um Ihren persönlichen Schlüssel zum Verschlüsseln eines Anhangs aus der ausgewählten **Tabelle** zu verwenden. Wählen Sie in diesem Beispiel **Incident**aus.
Tabelle	Wählen Sie die Tabelle aus, um auf die vertraulichen Informationen zuzugreifen. Wählen Sie für dieses Beispiel **Incident [Incident]**aus.
Aktiv	Markieren Sie „ **Aktiv** “, um die Feldkonfiguration verwenden zu können.
Algorithmus-Gleichstellungserhaltung	Wenn Sie die Verschlüsselung auf Spaltenebene auswählen, ist dieses Feld basierend auf der ausgewählten Tabelle sichtbar.
Crypto-Modul	Wählen Sie das von Ihnen erstellte Modul zur Verwendung mit dem persönlichen Schlüssel aus.
Methode	Die Option **Einzelnes Modul** wird verwendet, um die Richtlinien für ein Modul anzuwenden. **Mehrere Module** werden verwendet, um die Richtlinien auf mehrere Module anzuwenden.

Konfigurationstabelle für verschlüsselte Felder



6. Klicken Sie auf **Absenden**.

Richten Sie eine Modulzugriffsrichtlinie ein, um Zugriff auf das kryptografische Modul zuzuweisen. Weitere Informationen finden Sie unter Erstellen Sie eine Modulzugriffsrichtlinie.

7. Navigieren zu **Schlüsselverwaltung** > **Modulzugriffsrichtlinien** > **Alle**an.
8. Klicken Sie auf **Neu**.
9. Füllen Sie das Formular aus:

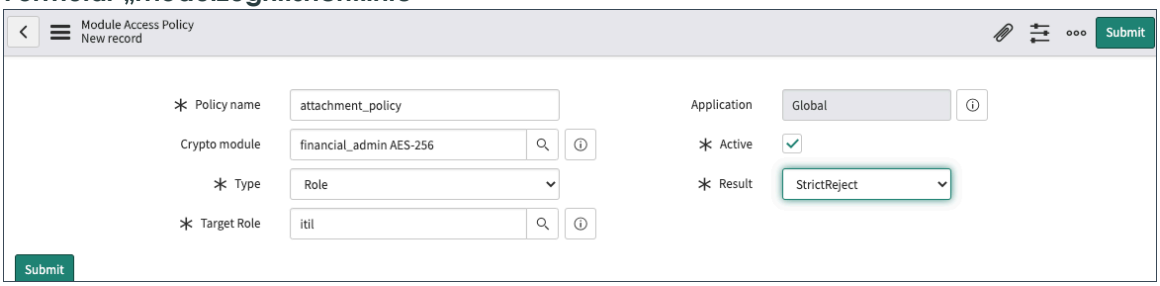
Felder für die Zugriffsrichtlinie für das Modul

Feld	Beschreibung
Richtlinienname	Geben Sie einen Namen für die Richtlinie ein, z. B. „Anhangrichtlinie“.
Crypto-Modul	Wählen Sie das Kryptomodul aus, das Sie zum Verschlüsseln Ihres Schlüssels erstellt haben.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

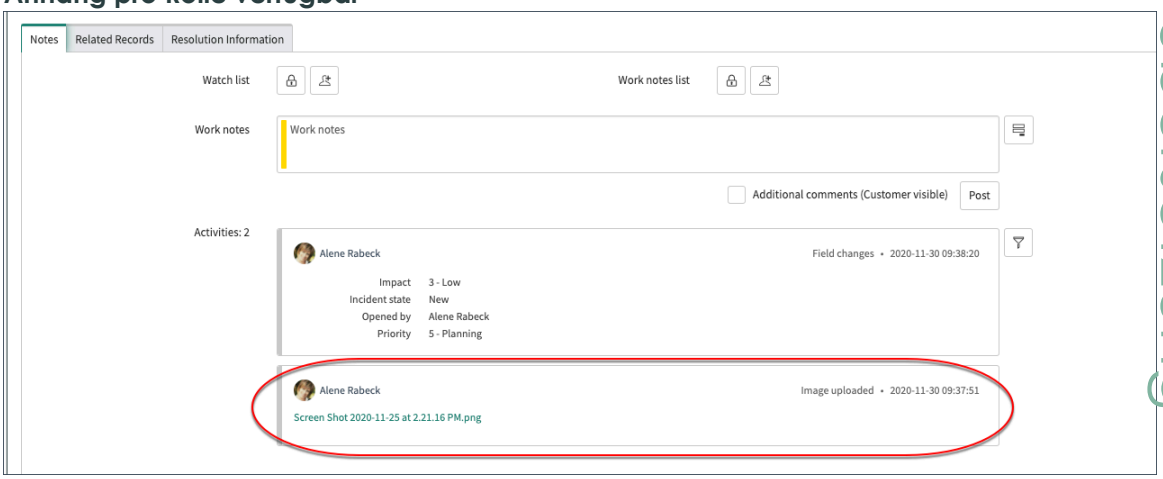
Feld	Beschreibung
Typ	Wählen Sie „ **Rolle“** aus, um den Zugriff auf das verschlüsselte Feld von Benutzern mit der zugewiesenen Rolle zu beschränken.
Zielrolle	Wählen Sie die Rolle aus, die keinen Zugriff auf das verschlüsselte Feld hat. Wählen Sie in diesem Beispiel **itil aus**.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um die Modulzugriffsrichtlinie verwenden zu können.
Ergebnis	Wählen Sie **Striktes Ablehnen** aus, um den Zugriff auf den Anhang über die ausgewählte Rolle zu steuern. (Um Zugriff für die ausgewählte Rolle zu gewähren, wählen Sie **Nachverfolgen**.)

Formular „Modulzugriffsrichtlinie“



10. Klicken Sie auf **Absenden**.
11. Navigieren Sie als Administrator oder als Person, die den Incident erstellt hat, zu **Incidents**, und fügen Sie **Aktivitäten** in der zugehörigen Liste **Notizen** einen Anhang hinzu.

Anhang pro Rolle verfügbar



12. Melden Sie sich als ein Anwender an, der den Zugriff auf den verschlüsselten Anhang eingeschränkt hat.
13. Öffnen Sie den Incident, und scrollen Sie zum Abschnitt **Aktivitäten:.**
    Der Link zum Öffnen des Anhangs ist für Anwender mit der eingeschränkten Rolle nicht zugänglich.
14. Sie haben jetzt Ihren vom Kunden bereitgestellten Schlüssel erfolgreich verwendet, um den Zugriff auf einen bestimmten Anhang mithilfe der Verschlüsselung auf Spaltenebene zu steuern.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Column Level Encryption Enterprise

Verschlüsselung auf Spaltenebene Enterprise (CLE) nutzt Key Management Framework (KMF), damit Sie die Verschlüsselung und Entschlüsselung von Feldern und Anhängen in Ihrer Instanz anpassen und verwalten können. Für die Verwendung von Verschlüsselung auf Spaltenebene Enterpriseist ein Abonnement erforderlich.

Wichtig: Dieses Thema behandelt die Enterprise-Version von Verschlüsselung auf Spaltenebene. Informationen zur Standardversion von CLE oder die Unterschiede zwischen den beiden Versionen finden Sie unter Verschlüsselung auf Spaltenebene erkunden.

Verschlüsselung auf Spaltenebene Enterprise wird mit Verschlüsselung auf Spaltenebene (CLE) benötigt und nutzt Key Management Framework und dessen vollständige Unterstützung für Schlüsselverwaltungsfunktionen. Verschlüsselung auf Spaltenebene Enterprise bietet Schlüsselschutz und Schlüssellebenszyklusverwaltung für die Feldverschlüsselung auf Anwendungsebene. Alle Schlüssel sind durch eine Key-Wrapping-Hierarchie geschützt, die letztendlich in FIPS 140-2-L3-Hardwaresicherheitsmodulen (HSM) basiert.

Verschlüsselung auf Spaltenebene Enterprise bietet Ihnen die Möglichkeit zu verwalten, wie unterstützte Felder gemäß den NIST 800-57- Praktiken verschlüsselt und entschlüsselt werden. Außerdem wird die neueste Version der Verschlüsselung auf Feldebene verwendet, einschließlich der Integration für ordnungsgemäßen Schlüsselschutz und ordnungsgemäße Verwaltung.

Verschlüsselung auf Spaltenebene Enterprise nutzt die Verschlüsselungsmodule KMF, um Ihnen mehr Kontrolle über die serverseitige Verschlüsselung zu geben. KMF stellt mithilfe von Schlüsselhierarchie und Umschlagverschlüsselung einen angemessenen Schutz für Datenverschlüsselungsschlüssel sicher. Ihre -Instanz verschlüsselt Daten über von Ihnen konfigurierte kryptografische Module. Sie können eine Zugriffsrichtlinie für jedes Modul erstellen und dann kryptografische Spezifikationen und Zugriffsrichtlinien konfigurieren sowie die Steuerung der Lebenszyklusverwaltung für Schlüssel steuern.

Verschlüsselung auf Spaltenebene Enterprise unterstützt Modulzugriffsrichtlinien basierend auf:

- Umfang
- Rolle
- Skript
- Ressourcenaustausch
- Systemanwender

Weitere Informationen finden Sie unter Erstellen Sie eine Modulzugriffsrichtlinie.

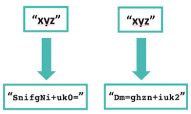
Hinweis: Ausführliche Informationen zu den unterstützten Funktionen der Verschlüsselung auf Spaltenebene und zum Upgraden und Abonnieren der Berechtigung [Verschlüsselung auf Spaltenebene Enterprise finden Sie unter Abonnementpaket für Verschlüsselung und Schlüsselverwaltung.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verschlüsselungsbegriffe

Benennung	Beschreibung
Schlüsselverwaltung 	Unterstützung für -Schlüsselverwaltung Grundlage für Verschlüsselung auf Spaltenebene Enterprise ist das Key Management Framework (KMF). Erwerben Sie die folgenden Fähigkeiten: • Schlüssel-Lebenszyklusmanagement. • Schlüsselrotation. Details siehe Schlüssel rotieren. • Schlüsselschutz und Schlüsselgenerierung mit FIPS 140-2-L3 Hardware Security Modules (HSMs). • Trennung von Rollen und Aufgaben. • Die sichere Übertragung von Datenverschlüsselungsschlüsseln zwischen Instanzen, z. B. Produktionsinstanzen und Instanzen außerhalb der Produktion. • Vom Kunden bereitgestellte Schlüssel (CSK) mit Schlüsselumschließung. • Nicht deterministische Verschlüsselung. • Massenverschlüsselung/-entschlüsselung. • Audit des Schlüsselzugriffs/der Schlüsselverwendung. Details siehe Key Management Framework.
Vom Kunden bereitgestellter Schlüssel 	Unterstützung für vom Kunden bereitgestellte Schlüssel Einer der größten Vorteile von Verschlüsselung auf Spaltenebene Enterprise besteht darin, dass Sie Ihre eigenen Schlüssel für die Verschlüsselung verwenden können. Administratoren haben die Wahl, ob von ServiceNow bereitgestellte Schlüssel oder Ihre eigenen vom Kunden bereitgestellten Schlüssel (CSK) für die Verschlüsselung auf dem Now Platform® verwendet werden. Sie können auch den Schlüssellebenszyklus verwalten und entscheiden, wann die Schlüssel widerrufen, rotiert und deaktiviert werden sollen. Nachdem Sie vom Kunden bereitgestellte Schlüssel aktiviert und ein kryptografisches Modul erstellt haben, laden Sie ein Token und einen öffentlichen flüchtigen Schlüssel herunter. Sie verwenden das Token und den öffentlichen Schlüssel, um Ihren Schlüssel zu umschließen und dann in die Instanz hochzuladen. Informationen zur Verwendung von vom Kunden bereitgestellten Schlüsseln finden Sie unter Konfigurieren Sie die Feldverschlüsselungseinstellungen, um den Schlüsseltyp auszuwählen und Verwendung von vom Kunden bereitgestellten Schlüsseln mit Verschlüsselung auf Spaltenebene Enterprise.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benennung	Beschreibung
Verschlüsselung auf Spaltenebene 	Unterstützung für Feldverschlüsselung und Anhangverschlüsselung Sowohl die Feldverschlüsselung als auch die Anhangsverschlüsselung verwenden kryptografische Module und Zugriffsrichtlinien über verschlüsselte Feldkonfigurationen. Das Formular „Konfiguration verschlüsselter Felder“ wird verwendet, um einen Verschlüsselungstyp der Spalten- oder Anhangsverschlüsselung auszuwählen. Weitere Informationen und unterstützte Feldtypen finden Sie unter Legen Sie Konfigurationen für verschlüsselte Felder fest.
Nicht deterministische Verschlüsselung 	Unterstützung für nicht deterministische Verschlüsselung Verschlüsselung auf Spaltenebene Enterprise unterstützt die nicht deterministische Verschlüsselung, um die Sicherheit zu erhöhen. Wenn das System dieselben Daten mehrmals verschlüsselt, sind die Geheimtexte jedes Mal anders. Die nicht deterministische Verschlüsselung ist mit der AES-Verschlüsselung mit CIpher Block Chaining (CBC) verfügbar. Sie können diese Funktion über die Option „Gleichstellungserhaltung“ in der Phase „Algorithmusdefinition“ der kryptografischen Spezifikation aktivieren. Erstellen Sie eine kryptografische Spezifikation für ein Kryptomodul, definieren Sie einen Algorithmus für die Verschlüsselung und generieren Sie den Schlüssel. Unter Erstellen Sie ein kryptografisches Modul erfahren Sie, wie Sie die für kryptografische Vorgänge verwendeten Mechanismen definieren und weitere Informationen zum Aktivieren der nicht deterministische Verschlüsselung erhalten.
Ressourcenaustausch 	Ressourcenaustausch Verschlüsselung auf Spaltenebene Enterprise verschlüsselt Instanz für Instanz auf sichere Weise mithilfe der kryptografischen APIs KMF, um Vertraulichkeit, Integrität, Authentifizierung und Nachweisbarkeit bereitzustellen. Ressourcenaustausch ist eine Funktion von KMF, mit der Sie auf sichere Weise Ressourcen zwischen Instanzen austauschen können. Details siehe Key Management Framework Resource Exchange.

Hinweis: Wenn Sie Verschlüsselung auf Spaltenebene Enterprisenicht aktivieren, können Sie weiterhin die Verschlüsselung auf Spaltenebene verwenden. Weitere Informationen finden Sie unter Verschlüsselung auf Spaltenebene erkunden.

Verschlüsselung auf Spaltenebene Enterprise unterstützt lokale Kunden. Domain Separation wird nicht unterstützt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterstützung für zusätzliche Module und Modulzugriffsrichtlinien

Die Standardversion von Verschlüsselung auf Spaltenebene ist auf fünf Module und Modulzugriffsrichtlinien (Module Access Policies, MAP) beschränkt. Verschlüsselung auf Spaltenebene Enterprise unterstützt eine größere Anzahl von Modulen und MAPs.

Unterstützte Feldinformationen

Die folgenden Feldtypen können verschlüsselt werden:

- Anhänge
- Datum
- Datum/Uhrzeit
- E-Mail
- HTML
- Journal
- Journaleingabe
- Journalliste
- Telefon
- Zeichenfolgentext
- Übersetztes Feld
- Übersetzte HTML
- Übersetzter Text
- URL

Anhangsverschlüsselung

Standardmäßige Anhangsverschlüsselung

Bei Kunden, die die Verschlüsselung auf Spaltenebene verwenden, werden Anhänge standardmäßig in Tabellen verschlüsselt, die über den aktiven EFC-Typ (Encrypted Field Configuration) *Attachment*verfügen.

Diese von der EFC-Konfiguration definierte Standardverschlüsselung bedeutet, dass Administratoren nicht manuell deklarieren müssen, dass ein Anhang beim Hochladen für diese Tabellen verschlüsselt werden soll.

Administratoren können Anwendern das Anhängen unverschlüsselter Dateien verbieten

Details finden Sie unter Verhindern, dass Anwender unverschlüsselte Dateien anhängen.

Standardverschlüsselung deaktivieren

Wenn Sie nicht möchten, dass Anhänge basierend auf der EFC-Konfiguration standardmäßig verschlüsselt werden, können Sie diese Option deaktivieren, indem Sie sich an den ServiceNow -Support wenden.

Um diese Funktion zu deaktivieren, erstellen Sie eine Supportanfrage beim Support ServiceNow, und fügen Sie die folgende Anweisung in einen Kommentar zum Falldatensatz ein:

```
„Ich [Kundenname] verstehe, dass ich ServiceNow bitte, eine
empfohlene Best Practice für die Sicherheit von Anhängen zu
deaktivieren, und dass [Kundenunternehmen] jedes zusätzliche
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Risiko im Zusammenhang mit der Konfiguration und Verwendung unverschlüsselter Anhänge in der Anwendung ServiceNow] übernimmt. “

API-Unterstützung

Verschlüsselung auf Spaltenebene Enterprise aktualisiert die APIs „ `setDisplayValue()` “ und „`setValue()`“, damit verschlüsselte Daten für verschlüsselte Felder eingefügt werden können. Außerdem können `getDisplayValue()` und `getValue()` Klartextwerte zurückgeben.

Das folgende Skript veranschaulicht diese API-Änderungen, wenn die Kurzbeschreibung des Incident verschlüsselt wird:

```
var gr = new GlideRecord('incident'); //creates a new incident
gr.setValue('short_description','test123'); //sets the value to test123
var sys_ID = gr.insert(); //inserts the record in the Incident table.
gs.info(gr.getValue('short_description')); //displays the unencrypted
 value
```

Wenn Sie `getValue()` zum Abrufen von verschlüsseltem Text verwenden, gibt das Skript keinen Geheimtext mehr zurück. Ihr Skript gibt den Nur-Text zurück und geht davon aus, dass der Benutzer Zugriff auf das kryptografische Modul hat. `getValue()` gibt den Geheimtext für Benutzer zurück, die keinen Zugriff auf das kryptografische Modul haben.

Cloud-Verschlüsselung mit Schlüsselverwaltung

ServiceNow® Cloud-Verschlüsselung bietet verschlüsselten Speicher für die Datenbank mithilfe von Blockverschlüsselung sowie erweiterte Schlüsselverwaltung. Cloud-Verschlüsselung ist mit dem Abonnementpaket der Plattformverschlüsselung ServiceNow®] verfügbar.

Cloud-Verschlüsselung bietet:

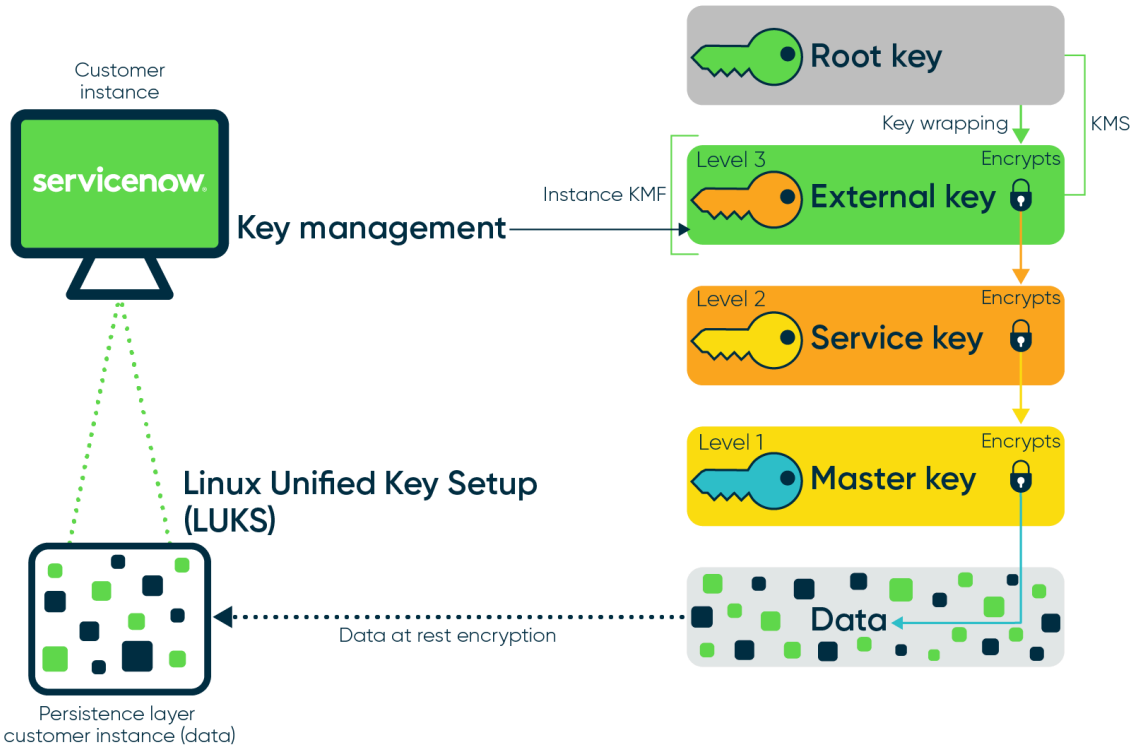
- Aufgabentrennung.
- Rotation von ServiceNow verwalteten Schlüsseln.
- Option Vom Kunden verwaltete Schlüssel.

> **Hinweis:** Erwägen Sie diese Option, wenn Sie in Ihrer Organisation Schlüsselmaterial verwenden müssen, das von Ihren eigenen kryptografischen Tools oder Bibliotheken, einem Unternehmensschlüsselverwaltungssystem oder einem Hardwaresicherheitsmodul (HSM) generiert wurde. Details siehe Schlüsselverwaltungsvorgänge.

Das folgende Diagramm zeigt die Funktionsweise von Cloud-Verschlüsselung.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übersicht über die Cloud-Verschlüsselung



Das Modul Cloud-Verschlüsselung Key Management besteht aus den folgenden Submodulen:

- Schlüsselverwaltungsvorgänge:
  - Greifen Sie auf die Liste der Schlüssel zu.
  - Führen Sie Schlüsselrotationsvorgänge durch.
  - Vom Kunden verwalteten Schlüssel zurückziehen.
- Transaktionen der Schlüsselverwaltung:

  Verweisen Sie auf alle Transaktionen, die für die verwendeten Schlüssel stattgefunden haben.

  Eigenen, vom Kunden verwalteten Schlüssel für die Verschlüsselung verwenden.

Unter bestimmten Umständen können Sie sich für eine Schlüsselrückzugsanforderung entscheiden, wenn Sie einen vom Kunden verwalteten Schlüssel verwenden. Dazu müssen Sie das optionale Add-on „Cloud Encryption-Zurückziehen und erneut bereitstellen“-SKU lizenzieren und dann die Aktivierung der Schlüsselrückzugsfunktion durch ein Mitglied des Kundenservice und Support -Teams anfordern.

Die Option Quorum Control-Richtlinieneinstellungen wird verfügbar, wenn die Widerrufsfunktion aktiviert ist. Andernfalls wird das Modul im Menü nicht angezeigt. Diese Funktion kann nur aktiviert werden, wenn vom Kunden verwaltete Schlüssel verwendet werden. Diese Richtlinie ermöglicht die Konfiguration von Einstellungen für das Quorum, wenn die Widerrufsfunktion aktiviert ist. Weitere Informationen zu dieser Funktion finden Sie unter Quorum-Steuerungsrichtlinie.

Cloud-Verschlüsselung unterstützt Produktionsinstanzen und Instanzen außerhalb der Produktion für MariaDB- und Berichterstatter-Datenbanken. Cloud Encryption wird in der ServiceNow Commercial Cloud, dem GCC-Pod 101 (Government Customer Cloud) und der ServiceNow Protected Platform – Australien (SPP-AU) unterstützt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

Lizenzierung und Aktivierung von Cloud-Verschlüsselung

Informationen zur Lizenzierung Cloud-Verschlüsselungfinden Sie unter Abonnementpaket für Verschlüsselung und Schlüsselverwaltung.

Für lizenzierte Kunden mit neuen Instanzen enthält die neue Instanzbereitstellung Cloud-Verschlüsselung.

Lizenzierte Kunden mit vorhandenen Instanzen zum Anfordern der Verschiebung einer Instanz nach Cloud-Verschlüsselungbefolgen die Anweisungen in KB1117369 . Sie müssen über die Rolle „Kundenadministrator“ oder „Partneradministrator“ verfügen, um das Servicekatalogelement zum Aktivieren der Cloud-Verschlüsselung in Ihrer Instanz anzufordern. Zum Aktivieren dieser Funktion ist ein einstündiges Wartungsfenster erforderlich.

Anwenderoberfläche für Cloud-Verschlüsselung

Wenn die Cloud-Verschlüsselung aktiviert ist, ist die Anwenderoberfläche (UI) der Cloud-Verschlüsselung für den Benutzer security_admin sichtbar, sofern dieser Benutzer über die Rolle sn_kmf.admin verfügt.

Um auf die Cloud Encryption-UI zuzugreifen, suchen Sie in der Navigationsleiste nach **Cloud-Verschlüsselungsschlüsselverwaltung**. Navigieren Sie zum Abschnitt „ **Schlüsselverwaltungsvorgänge** “, um Informationen über Verschlüsselungsschlüssel anzuzeigen, z. B. Details des aktiven Schlüssels und ob die Cloud-Verschlüsselung für die Instanz aktiviert ist.

Schlüsselverwaltungsvorgänge

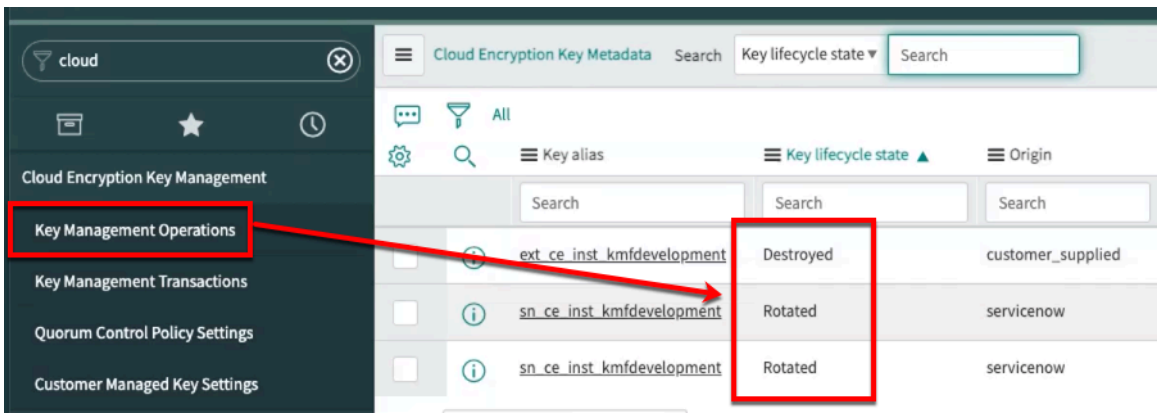
Das Submodul Key Management Operations bietet Zugriff zum Anzeigen und Verwalten aller mit ServiceNow Cloud-Verschlüsselungverwendeten Verschlüsselungsschlüssel.

Erste Schritte mit Cloud-Verschlüsselung

Schlüssel-Lebenszyklusstatus

Es ist zu jeder Zeit nur ein aktiver Schlüssel im System vorhanden. Wenn Sie einen Schlüssel auswählen, greifen Sie auf die Aktivität für den ausgewählten Schlüssel zu, z. B. darauf, welche Schlüssel rotiert oder zurückgezogen wurden, sowie auf den entsprechenden Zeitstempel.

Der Status des Schlüssel-Lebenszyklus wird entsprechend dem durchgeführten Schlüsselverwaltungsvorgang aktualisiert.



Weitere Informationen finden Sie unter Rotieren Sie einen von ServiceNow verwalteten Schlüssel oder Rotieren Sie einen vom Kunden verwalteten Schlüssel.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Die Schlüsselrotation kann bis zu 20 Minuten dauern.

Rotieren Sie einen von ServiceNow verwalteten Schlüssel

Aktiven Cloud-Verschlüsselung ServiceNow verwalteten Schlüssel rotieren.

Vorbereitungen

Erforderliche Rolle: sn_kmf.admin oder sn_kmf.cryptographic_manager

Wichtig: Wenn Sie vom Kunden verwaltete Schlüssel verwenden, finden Sie weitere Informationen unter Rotieren Sie einen vom Kunden verwalteten Schlüssel.

Prozedur

1. Navigieren zu **Alle** > **Cloud-Verschlüsselungsschlüssel-Verwaltung** > **Vorgänge der Schlüsselverwaltung**an.
   Die Liste der Schlüsselmetadaten Cloud-Verschlüsselung wird geladen. Alle in Ihrer Instanz verwendeten Schlüssel sind aufgelistet. Zu einem bestimmten Zeitpunkt kann nur ein Schlüssel aktiv sein.

   Beim erstmaligen Zugriff auf das Modul Cloud-Verschlüsselung sind Schlüsseleinträge verfügbar, nachdem eine erste Schlüsselrotation durchgeführt wurde. Ein verwalteter Schlüssel von ServiceNow ist der Standardwert im System.
2. Wählen Sie den aktiven Schlüssel aus der Tabelle aus.
   Die Tabelle „Schlüsseldefinition“ wird mit allgemeinen Informationen zu Ihrem von ServiceNow generierten Schlüssel angezeigt.
3. Wählen Sie die Schaltfläche **Schlüssel** rotieren aus.
   Es wird eine Benachrichtigung mit der Option angezeigt, die Schlüsselrotation fortzusetzen oder den Vorgang abzubrechen.
4. Wählen Sie „ **OK**“ aus, um den Schlüssel zu rotieren.
   Oben auf der Seite Schlüsseldefinition wird eine Bestätigungsmeldung angezeigt.
5. Kehren Sie zum Bildschirm „Schlüsselverwaltungsvorgänge“ zurück, um die Schlüsselmetadatentabelle Cloud-Verschlüsselung zu aktualisieren.
   Einträge werden für den aktuell aktiven Schlüssel und den Schlüssel aufgelistet, der generiert wird, um anstelle des aktuell aktiven Schlüssels zu rotieren. Informationen zu den verschiedenen verfügbaren Status finden Sie unter Schlüssellebenszyklusstatus des Key Management Framework.

   Der aktive Schlüssel wird mit einer Schlüsselversion von `0` aufgeführt, und der generierte Schlüssel hat eine Version von `1`.
6. Öffnen Sie den Eintrag für den ursprünglichen Schlüssel, um die Schlüsselverwaltungstransaktionen anzuzeigen.
   Weitere Informationen finden Sie unter Transaktionen der Schlüsselverwaltung.
   Der zuvor aktive Schlüssel, Version `0`, wurde auf den Schlüssel-Lebenszyklusstatus `Rotiert` aktualisiert, und der neue Schlüssel, Version `1`, lautet `Aktiv`.

Bereiten Sie Ihren vom Kunden verwalteten Schlüssel vor

Führen Sie diese Schritte aus, um den vom Kunden verwalteten Schlüssel für den Upload in Ihre Instanz vorzubereiten.

Vorbereitungen

Erforderliche Rolle: sn_kmf.admin oder sn_kmf.cryptographic_manager

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Für einen vom Kunden verwalteten Schlüssel können Sie eine beliebige kryptografische Bibliothek oder ein beliebiges HSM verwenden, um Ihren Schlüssel zu generieren. Dieser Schlüssel muss ein AES-256-Bit-Schlüssel sein und von einem Cloud Encryption-Wrapperzertifikat mit einem RSAES_OAEP_SHA_256-Verschlüsselungsschema umschlossen sein.

Hinweis:

Wenn Sie das kryptografische Tool OpenSSL zum Generieren Ihres Schlüssels verwenden, muss die OpenSSL-Version Version 1.1.1x oder höher sein.

Wenn Sie Ihren vom Kunden verwalteten Schlüssel mit Windowserstellen und umschließen, müssen Sie den umschlossenen Schlüssel über Anwendungen zur Unterstützung von Bash-Shells wie Git Bash generieren.

Prozedur

1. Generieren Sie einen zufälligen Wert, der als symmetrischer AES-256-Bit-Schlüssel mit OpenSSL verwendet wird.

   Wenn Sie openSSL verwenden, können Sie diesen Schlüssel beispielsweise mit dem Befehl „ `openssl rand 32` “ generieren.

   Aus Kompatibilitätsgründen muss Ihr symmetrischer Schlüssel die folgenden Attribute aufweisen:

Attribut	Wert
Schlüsseltyp	Auf dem AES-Algorithmus (Advanced Encryption Standard) basierender symmetrischer Schlüssel.
Schlüsselgröße	256 Bit (32 Byte)
Schlüsselumwickelte Anforderung	◦ RSA-Verschlüsselungsalgorithmus ◦ optimaler asymmetrischer Verschlüsselungsabstand (OAEP) ◦ SHA-256-Hash-Funktion (RSAES_OAEP_SHA_256) ◦ Mit Base64-Algorithmus codiert

2. Speichern Sie den Schlüssel in einer Datei.
   Beispielsweise generiert der openSSL-Befehl `openedsl rand 32 > Klartext_key.bin` einen 32-Byte-Schlüssel und speichert ihn in einer Datei mit dem Namen `Klartext_key.bin`.

   Wichtig: Speichern Sie diese Datei zur späteren Verwendung an einem sicheren Ort. Dieser Schlüssel wird mit dem öffentlichen Schlüssel für den Upload umschlossen.

3. Extrahieren Sie den öffentlichen Schlüssel aus der heruntergeladenen Wrapping-Zertifikatdatei Ihrer Instanz:

```
openssl x509 -pubkey -noout -in wrapping_cert.pem > public_key.pem
```

Hinweis: Informationen zum Herunterladen des Packzertifikats finden Sie unter.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Umschließen Sie den generierten Schlüssel mit dem öffentlichen Schlüssel, der mit dem Wrapping-Zertifikat heruntergeladen wurde, indem Sie den Algorithmus RSAES_OAEP_SHA_256 verwenden:

```
cat plaintext_key.bin | openssl pkeyutl -encrypt -inkey public_key.pem
 -pubin -pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256 |
 openssl base64 -A -out wrapped_key.txt
```

   Eine in diesem Befehl angegebene Datei enthält einen umschlossenen, vom Kunden verwalteten Schlüssel, der SN für den CMK-Prozess bereitgestellt werden kann.

Wechseln Sie zwischen ServiceNow und vom Kunden verwalteten Schlüsseln

Wechseln Sie zwischen einem vom Kunden verwalteten Schlüssel oder einem von ServiceNow verwalteten Schlüsseln zur Verwendung in ServiceNow Cloud-Verschlüsselung.

Standardmäßig ist Ihre Instanz für die Verwendung von ServiceNow verwalteten Schlüsseln konfiguriert, und die Generierung der Verschlüsselungsschlüssel ServiceNow ist aktiv. Administratoren können jedoch vom Kunden verwaltete Schlüssel verwenden. Sie können auch zu den von ServiceNow verwalteten Schlüsseln zurückkehren.

Rotieren Sie einen vom Kunden verwalteten Schlüssel

Rotieren Sie Ihren vom Kunden verwalteten Schlüssel zu Ihrer -Instanz, nachdem Sie Ihren vom Kunden verwalteten Schlüssel für Cloud-Verschlüsselungumschlossen haben.

Vorbereitungen

Erforderliche Rolle: sn_kmf.admin oder sn_kmf.cryptographic_manager

Prozedur

1. Navigieren zu **Alle** > **Cloud-Verschlüsselungsschlüssel-Verwaltung** > **Vorgänge der Schlüsselverwaltung**an.
   Die Liste der **Cloud-Verschlüsselungsschlüssel-Metadaten** wird geladen. Alle Schlüssel, die in Ihrer Instanz verwendet wurden, sind aufgelistet.
2. Öffnen Sie in der Liste **„Metadaten des Cloud-Verschlüsselungsschlüssels“** den Datensatz für Ihren aktiven Schlüssel.
   Wenn Sie mehrere Schlüssel haben, wählen Sie den Schlüssel mit dem **Schlüssellebenszyklusstatus**`Aktiv`aus. In Ihrer Instanz ist nur ein aktiver Schlüssel vorhanden.
3. Wählen Sie im Schlüsseldefinitionsdatensatz die Schaltfläche **Schlüssel** rotieren aus.
4. **Führen Sie im Fenster „Vom Kunden verwalteten Schlüssel** hochladen“ die aufgeführten Schritte aus.

   a. Wählen Sie **Wrapping-Zertifikat herunterladen aus**.
      Die *`Datei „public_certificate....zip`* "wird auf Ihren lokalen Computer heruntergeladen und zum Umschließen Ihres vom Kunden verwalteten Schlüssels verwendet.

      ⚠ **Warnung:** Vermeiden Sie potenzielle Probleme im Zusammenhang mit dem Zertifikat, indem Sie das Wrapping-Zertifikat jedes Mal herunterladen, wenn Sie zu einem vom Kunden verwalteten Schlüssel rotieren oder zu ihm wechseln.

   b. Wählen Sie **Durchsuchen**, um Ihren vom Kunden verwalteten Schlüssel hochzuladen. Suchen Sie dann Ihren verpackten Verschlüsselungsschlüssel, und wählen Sie ihn aus. Um eine andere Datei auszuwählen, wählen Sie die Datei aus, und wählen **Sie Entfernen**aus.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Schließen Sie das Fenster „Anhänge“.

d. Wählen Sie „ **OK“** aus, um Ihren Schlüssel hochzuladen.
Wenn der Schlüssel das richtige Format hat, wird eine Bestätigungsmeldung angezeigt, andernfalls wird eine Fehlermeldung angezeigt. Die Schlüsseldatei wird an den Schlüsseldefinitionsdatensatz angehängt.

In der Tabelle „Transaktionen der Schlüsselverwaltung“ werden die Schritte zum Herunterladen und Hochladen des Schlüssels aufgelistet. Weitere Informationen zu den Anforderungsschritten finden Sie unter Transaktionen der Schlüsselverwaltung.

5. Navigieren zu **Alle** > **Cloud-Verschlüsselungsschlüssel-Verwaltung** > **Vorgänge der Schlüsselverwaltung** , um die Liste der Schlüssel anzuzeigen.
In der Liste der Schlüssel sehen Sie einen neuen Datensatz für Ihren vom Kunden verwalteten Schlüssel. Dieser neue Schlüssel hat den **Ursprungswert** „ **customer_supplier“** und befindet sich im Status **„Aktiv** “. Ihr vorheriger Schlüssel befindet sich im Status „ **Rotiert“**.

Wechseln Sie zu einem vom Kunden verwalteten Schlüssel

Verwenden Sie Ihren vom Kunden verwalteten Schlüssel für ServiceNow Cloud-Verschlüsselung.

Vorbereitungen

Erforderliche Rolle: sn_kmf.admin oder sn_kmf.cryptographic_manager

Um zu einem vom Kunden verwalteten Schlüssel zu wechseln, benötigen Sie einen verpackten vom Kunden verwalteten Schlüssel, der im Rahmen dieser Schritte hochgeladen werden kann. Weitere Informationen zum Vorbereiten dieses Schlüssels für den Upload finden Sie unter Bereiten Sie Ihren vom Kunden verwalteten Schlüssel vor. Nachdem Sie Ihren Schlüssel hochgeladen haben, initiiert dieser Prozess eine Schlüsselrotation für Ihren neuen Schlüssel.

Prozedur

1. Navigieren zu **Alle** > **Cloud-Verschlüsselungsschlüssel-Verwaltung** > **Vorgänge der Schlüsselverwaltung**an.
2. Öffnen Sie in der Liste **„Metadaten des Cloud-Verschlüsselungsschlüssels“** den Datensatz für Ihren aktiven Schlüssel.
Wenn Sie mehrere Schlüssel haben, wählen Sie den Schlüssel mit dem **Schlüssellebenszyklusstatus**`Aktiv`aus. In Ihrer Instanz ist nur ein aktiver Schlüssel vorhanden.
3. Wählen Sie im Abschnitt „ **Zugehörige Links** “ des Formulars den Link **Zu vom Kunden verwalteten Schlüssel** wechseln.
4. Wählen Sie im Dialogfeld „Zu vom **Kunden verwalteten Schlüssel** wechseln“ die Schaltfläche **Verwalteten Schlüssel** hochladen.
5. Führen Sie im Dialogfeld „ **Vom Kunden verwalteten Schlüssel** hochladen“ die aufgeführten Schritte aus.

a. Wählen Sie **Wrapping-Zertifikat herunterladen aus**.

> ⚠ **Warnung:** Vermeiden Sie potenzielle Probleme im Zusammenhang mit dem Zertifikat, indem Sie das Wrapping-Zertifikat jedes Mal herunterladen, wenn Sie zu einem vom Kunden verwalteten Schlüssel rotieren oder zu ihm wechseln.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

b. Wählen Sie **Durchsuchen**und befolgen Sie die Eingabeaufforderungen, um Ihren Schlüssel auszuwählen und von Ihrem Gerät hochzuladen.

c. Wählen Sie **Zu vom Kunden verwalteten Schlüssel wechseln**.

Von der -Instanz wird eine Anforderung generiert, zu Ihrem vom Kunden verwalteten Schlüssel zu wechseln. Im aktuellen Formular können Sie sehen, dass der **Schlüssel-Lebenszyklusstatus** des ursprünglich aktiven Schlüssels in **Rotiert**geändert wurde.

6. Navigieren zu **Alle** > **Cloud-Verschlüsselungsschlüssel-Verwaltung** > **Vorgänge der Schlüsselverwaltung** , um die Liste der Schlüssel anzuzeigen.
In der Liste der Schlüssel sehen Sie einen neuen Datensatz für Ihren vom Kunden verwalteten Schlüssel. Dieser neue Schlüssel hat den **Ursprungswert** „ **customer_supplier“** und befindet sich im Status **„Aktiv** “.

Ergebnisse
Ihre Instanz von verwendet jetzt Ihren vom Kunden verwalteten Schlüssel für ServiceNow Cloud-Verschlüsselung.

Wichtig: Stellen Sie sicher, dass für Schlüsselverwaltungsvorgänge immer eine Kopie Ihres Verschlüsselungsschlüssels an einem sicheren Ort verfügbar ist. Ohne diesen Schlüssel ist Ihre Instanz möglicherweise nicht zugänglich.

Wechseln Sie zu einem von ServiceNow verwalteten Schlüssel

Wechseln Sie von einem vom Kunden verwalteten Schlüssel zurück zu einem verwalteten Schlüssel für ServiceNow Cloud-Verschlüsselung.

Vorbereitungen
Erforderliche Rolle: sn_kmf.admin oder sn_kmf.cryptographic_manager

Prozedur

1. Navigieren zu **Alle** > **Cloud-Verschlüsselungsschlüssel-Verwaltung** > **Vorgänge der Schlüsselverwaltung**an.
2. Öffnen Sie in der Liste **„Metadaten des Cloud-Verschlüsselungsschlüssels“** den Datensatz für Ihren aktiven Schlüssel.
Wenn Sie mehrere Schlüssel haben, wählen Sie den Schlüssel mit dem **Schlüssellebenszyklusstatus**`Aktiv`aus. In Ihrer Instanz ist nur ein aktiver Schlüssel vorhanden.
3. Wählen Sie im Abschnitt „ **Zugehörige Links** “ des Formulars den Link **Zu von ServiceNow verwaltetem Schlüssel** wechseln.
4. **Wählen Sie im Dialogfeld „Zu von ServiceNow verwaltetem Schlüssel** wechseln“ die Schaltfläche **Zu von ServiceNow verwaltetem Schlüssel** wechseln.
Von der -Instanz wird eine Anforderung für den Wechsel zu einem von ServiceNow verwalteten Schlüssel generiert. Im aktuellen Formular können Sie sehen, dass der **Schlüssel-Lebenszyklusstatus** des ursprünglich aktiven Schlüssels in **Rotiert**geändert wurde.
5. Navigieren zu **Alle** > **Cloud-Verschlüsselungsschlüssel-Verwaltung** > **Vorgänge der Schlüsselverwaltung** , um die Liste der Schlüssel anzuzeigen.
In der Liste der Schlüssel sehen Sie einen neuen Datensatz für einen von ServiceNow verwalteten Schlüssel. Dieser neue Schlüssel hat den **UrsprungswertServiceNow** und befindet sich im Status „ **Aktiv** “.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Planen Sie eine Schlüsselrotation

Legen Sie einen Zeitplan für die automatische Rotation Ihrer von ServiceNow verwalteten Schlüssel fest. Dieser Prozess zieht einen Verschlüsselungsschlüssel automatisch zurück und ersetzt den alten Schlüssel durch einen neu generierten kryptografischen Schlüssel. Wenn Sie einen vom Kunden verwalteten Schlüssel verwenden, kann dieser Zeitplan Sie daran erinnern, Ihre anwenderdefinierten Schlüssel manuell zu rotieren.

Vorbereitungen

Erforderliche Rolle: sn_kmf.admin

Prozedur

1. Navigieren zu **Alle** > **Cloud-Verschlüsselungsschlüssel-Verwaltung** > **Einstellungen für geplante Schlüsselrotation**an.
2. Aktivieren Sie das Kontrollkästchen **Geplante Schlüsselrotation aktivieren**.
3. Füllen Sie die verbleibenden Felder entsprechend Ihren Geschäftsanforderungen aus.

Einstellungen für geplante Schlüsselrotation

Feld	Beschreibung
Anzahl der Monate zwischen Schlüsselrotationen (maximal 60 Monate)	Anzahl der Monate zwischen Schlüsselrotationen. Dieser Wert ist standardmäßig `12` und darf maximal `60` Monate haben.
Wochentag für die Schlüsselrotation	Wochentag, an dem die Schlüsselrotation durchgeführt wird.
Uhrzeit für die Schlüsselrotation	Uhrzeit, zu der die Schlüsselrotation durchgeführt wird.
Datum und Uhrzeit der nächsten Schlüsselrotation	Datum und Uhrzeit der nächsten geplanten Schlüsselrotation. Dieser Wert kann nicht direkt bearbeitet werden und wird automatisch basierend auf Ihrer Auswahl berechnet.
Angabe, wie viele Tage vor der Schlüsselrotation die Erinnerung gesendet werden soll (maximal 15 Tage)	Anzahl der Tage vor dem Datum der Schlüsselrotation, in denen Ihre Instanz Benachrichtigungen sendet.
E-Mail-Benachrichtigungen werden an die folgende Liste genehmigter Sicherheitsadministratoren gesendet	Liste der Anwender, die Benachrichtigungen zur Schlüsselrotation erhalten. Der **Systemadministrator** ist standardmäßig in dieser Liste enthalten.

4. Wählen Sie **Absenden**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachdem Sie „Absenden“ ausgewählt haben, wird oben im Formular eine Benachrichtigung angezeigt. Die Benachrichtigungen bestätigen Ihre Schlüsselrotation und Ihren Benachrichtigungszeitplan.

⚠ Warnung:

Jede geplante Schlüsselrotation verfügt über eine eindeutige Signatur, die die Integrität eines Auftrags sicherstellt und nicht autorisierte Änderungen erkennt. Die Signatur für eine regelmäßige Aufgabe ist für jede Instanz eindeutig. Beim Klonen eines geplanten Schlüsselrotationsauftrags aus einer Quellinstanz A auf eine Zielinstanz B schlägt der geplante Auftrag in Instanz B die Signaturvalidierung fehl. In diesem Fall können Sie die Signatur neu erstellen, indem Sie das Kontrollkästchen **Geplante Schlüsselrotation** aktivieren deaktivieren und dann erneut aktivieren. Weitere Informationen zu diesem Problem finden Sie unter KB1247113 .

Ziehen Sie einen vom Kunden verwalteten Schlüssel zurück

Nachdem die Funktion zum Zurückziehen des vom Kunden verwalteten Schlüssels aktiviert wurde, ist auf der Seite „Key Management Operations“ ein Vorgang zum Zurückziehen verfügbar. Vorgänge zum Zurückziehen von Schlüsseln und Quorum-Genehmigungen können ebenfalls verwaltet werden.

Vorbereitungen

Erforderliche Rolle: sn_kmf.admin oder sn_kmf.cryptographic_manager

Dieser Abschnitt gilt nur, wenn Sie Cloud Encryption Zurückziehen und erneut bereitstellen, ein optionales Add-on für Cloud-Verschlüsselung, lizenziert haben.

Prozedur

1. Navigieren zu **Alle** > **Cloud-Verschlüsselungsschlüssel-Verwaltung** > > **Vorgänge der Schlüsselverwaltung**an.
2. Wählen Sie den aktiven vom Kunden verwalteten Schlüssel aus der Tabelle aus. Die Tabelle „Schlüsseldefinition“ wird mit allgemeinen Informationen zu Ihrem Kundenschlüssel angezeigt. Eine Schlüsselfunktion zum Zurückziehen ist jetzt verfügbar.
3. Wählen Sie den Zurücknahmeschlüssel aus, um den **Auszahlungsprozess** auszulösen.

⚠ Warnung:

Die Warnmeldung Schlüssel zurückziehen wird angezeigt. Das Zurückziehen des Schlüssels löst ein Herunterfahren Ihrer Instanz aus, bis ein Wiederherstellungsvorgang mit dem zurückgezogenen Schlüssel ausgeführt wird.

Gefahr: Sie können einen Wiederherstellungsvorgang nur mit demselben Schlüssel ausführen, der zurückgezogen wurde. Wenn Sie zu einem anderen Schlüssel rotieren möchten, müssen Sie den zurückgezogenen Schlüssel wiederherstellen.

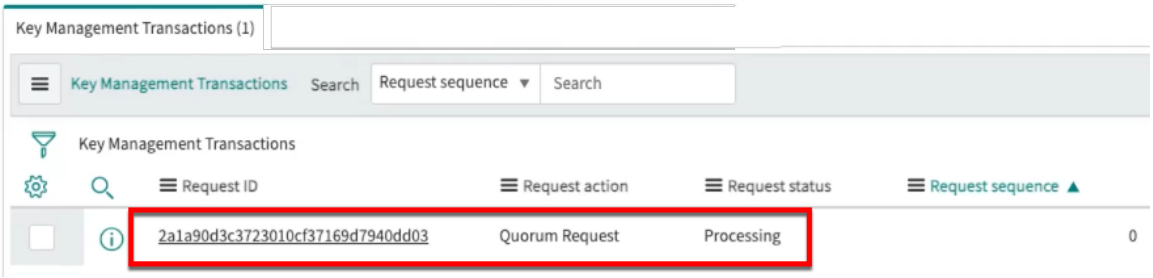
Wenn der zurückgezogene vom Kunden verwaltete Schlüssel nicht innerhalb des Zeitrahmens wiederhergestellt wird, für den ServiceNow Sicherungen aufbewahrt (Einzelheiten finden Sie in der SOP für Sicherung und Wiederherstellung [Standard Operating Procedure]), ist der Zugriff auf Ihre Instanzdatenbanksicherungen nicht mehr möglich. Auf diese Weise verlorene Sicherungsdaten können nicht wiederhergestellt werden.

4. Wählen Sie **OK**, um den Schlüssel zurückzuziehen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wählen Sie **Abbrechen** aus, wenn Sie Fragen an der Funktion zum Zurückziehen des Schlüssels haben.
Sie kehren zum Bildschirm Schlüsseldefinition zurück, und eine Bestätigungsmeldung wird angezeigt.

5. Aktualisieren Sie die Seite „Schlüsseldefinition“, um die ausstehende Auszahlungsanforderung anzuzeigen.



Wenn die Quorum Control-Richtlinie aktiviert wurde, muss der Genehmigungsworkflow erfolgreich abgeschlossen werden, um das Zurückziehen des Schlüssels abzuschließen. Details siehe Verwalten Sie die Quorum-Steuerung.

Stellt einen vom Kunden verwalteten Schlüssel erneut bereit

Nachdem ein Vorgang zum Zurückziehen eines Schlüssels abgeschlossen wurde, muss der vom Kunden verwaltete Schlüssel erneut in Ihrer Instanz bereitgestellt werden.

Vorbereitungen

Erforderliche Rolle: sn_kmf.admin oder sn_kmf.cryptographic_manager

Hinweis: Dieser Abschnitt gilt nur, wenn Sie eine Lizenz für Cloud-Verschlüsselung zurückziehen und erneut bereitstellen haben.

Prozedur

1. Wechseln Sie zu Now Support und navigieren Sie zu **Servicekatalog** > **Katalog** > **Instanzenverwaltung** > **Instanzwiederherstellung: Verwalteter Schlüssel erneut bereitstellen**an.
2. Klicken Sie auf **Anforderung**.
3. **Wählen** Sie im Fenster **Instanzwiederherstellung - Verwalteter Schlüssel erneut liefern** in der Dropdown-Liste Instanz auswählen Ihre Instanz aus.
4. Laden Sie das Wrapping-Zertifikat herunter, indem Sie auf den Text des **Wrapping** -Zertifikats klicken.

Warnung: Sie müssen jedes Mal, wenn Sie einen vom Kunden verwalteten Schlüssel rotieren oder hochladen, ein neues Packzertifikat herunterladen.

5. Bereiten Sie Ihren Schlüssel für den Upload vor.
Details zu diesem Vorgang finden Sie unter Bereiten Sie Ihren vom Kunden verwalteten Schlüssel vor.
6. Klicken Sie im Abschnitt „ **Schritt 4** “ auf **Durchsuchen und hochladen**, um Ihren umschlossenen Schlüssel von Ihrem lokalen Gerät hochzuladen.
Nachdem Ihr Schlüssel hochgeladen wurde, wird er unter **Unterhalb der Datei erfolgreich**hochgeladen angezeigt. Wenn Sie den Schlüssel erneut hochladen müssen, klicken Sie auf **Datei entfernen,** und laden Sie Ihren Schlüssel erneut hoch, wie in den vorherigen Schritten beschrieben.
7. Klicken Sie auf **Schlüssel rotieren**, um die erneute Bereitstellung abzuschließen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quorum-Steuerungsrichtlinie

Die Quorum-Steuerungsrichtlinie gibt die Mindestanzahl von Genehmigungen an, die aus der Gesamtzahl der ausgewählten Genehmiger erforderlich sind, um das Quorum für den vom Kunden verwalteten Schlüsselrückzug zu erreichen.

⚠ **Warnung:** Sie müssen einen rechtlichen Nachtrag unterzeichnen, um die Funktion zum Zurückziehen des Schlüssels zu aktivieren. Die Option „Quorum Control-Richtlinieneinstellungen“ wird verfügbar, wenn die Widerrufsfunktion aktiviert ist. Andernfalls wird das Modul im App-Menü nicht angezeigt. Nach dem Zurückziehen des Schlüssels ist Ihre Instanz nicht mehr verfügbar, bis der Verschlüsselungsschlüssel erneut bereitgestellt und wieder aktiviert wird.

Unter bestimmten Umständen möchten Sie möglicherweise eine Schlüsselrücknahme erstellen. Sie müssen die Funktion zum Zurückziehen des Schlüssels zuerst von Kundenservice und Supportanfordern.

Die Quorum-Steuerungsrichtlinie gibt die Mindestanzahl von Genehmigungen an, die aus der Gesamtzahl der ausgewählten Genehmiger erforderlich sind, um das Quorum für den vom Kunden verwalteten Schlüsselrückzug zu erreichen. Beispiel: Es gibt insgesamt fünf Genehmiger, aber nur vier Genehmigungen sind erforderlich, um das Quorum zu erreichen. Wenn vier Genehmigungen eingeholt wurden, wird die Auszahlungsanforderung verarbeitet und der Schlüssel zurückgezogen.

Immer wenn in einer für die Quorum-Genehmigung aktivierten Gruppe ein Zurücknahmevorgang ausgeführt wird, wird ein Workflow für die Quorum-Genehmigung ausgelöst. Eine E-Mail-Benachrichtigung wird an alle Benutzer gesendet, die eine Genehmigung erteilen können. Aufgaben werden auch in den Konten der Genehmiger generiert, die im Dashboard angezeigt werden, wenn sie sich bei ihrem Konto ServiceNow anmelden.

Die Benutzer können Genehmigungen über die Seite „Instanz“, „E-Mail“ oder „Schlüsselverwaltungsvorgänge“ erteilen. Der Vorgang zum Zurückziehen des Schlüssels wird blockiert, bis das Quorum erfüllt ist.

Sobald die Mindestanzahl von Genehmigern erreicht ist, wird das Quorum erreicht und das Zurückziehen des Schlüssels ausgelöst. Der Widerruf wird durchgeführt und protokolliert, einschließlich der Namen der Benutzer, die die Anforderung genehmigt haben.

Weitere Informationen zum Setup finden Sie unter Konfigurieren Sie Richtlinieneinstellungen für die Quorum-Steuerung.

Konfigurieren Sie Richtlinieneinstellungen für die Quorum-Steuerung

Führen Sie diese Schritte aus, um die Richtlinieneinstellungen für die Quorum-Steuerung zu konfigurieren.

Vorbereitungen

Erforderliche Rolle: sn_kmf.admin

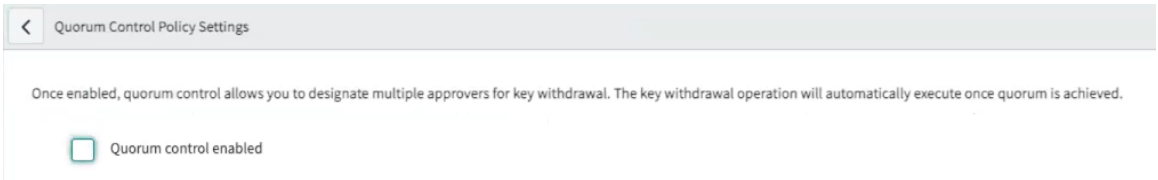
Warum und wann dieser Vorgang ausgeführt wird

⚠ **Warnung:** Sie müssen einen rechtlichen Nachtrag unterzeichnen, um die Funktion zum Zurückziehen des Schlüssels zu aktivieren. Die Option „Quorum Control-Richtlinieneinstellungen“ wird verfügbar, wenn die Widerrufsfunktion aktiviert ist. Andernfalls wird das Modul im App-Menü nicht angezeigt. Nach dem Zurückziehen des Schlüssels ist Ihre Instanz nicht mehr verfügbar, bis der Verschlüsselungsschlüssel wieder aktiv ist.

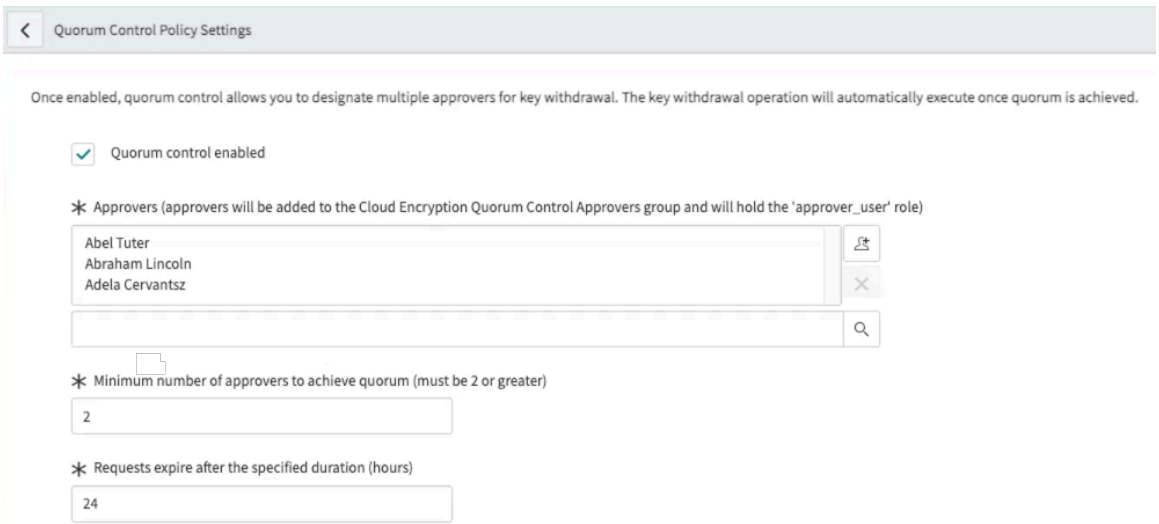
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Fordern Sie die Funktion zum Zurückziehen des Schlüssels von Kundenservice und Supportan.
2. Navigieren zu **Cloud-Verschlüsselungsschlüssel-Verwaltung** > **Einstellungen für Quorum Control-Richtlinie**an.
3. Aktivieren Sie das **Kontrollkästchen Quorum Control**



aktiviert.
Es werden zusätzliche Felder angezeigt, die zum Konfigurieren der Quorum-Steuerung erforderlich



sind.

4. Füllen Sie die Felder aus, um das Formular auszufüllen.

Feld	Beschreibung
Genehmiger	Bestimmen Sie die Mitglieder des Quorums aus der Liste der Benutzer. Wählen Sie das Sperrsymbol um das Anwenderverzeichnis zu öffnen. Die Anzahl der auswählbaren Genehmiger ist unbegrenzt.
Mindestanzahl von Genehmigern zum Erreichen des Quorums	Legen Sie die Mindestanzahl von Genehmigern fest, die zum Erreichen des Quorums erforderlich sind. Wenn beispielsweise neun Genehmiger ausgewählt sind, können mindestens fünf für das Quorum konfiguriert werden. Wenn fünf Genehmigungen im System eingegangen sind, wird das Quorum erreicht, und der Zurücknahmevorgang wird gestartet. **Hinweis:** Die Mindestanzahl der erforderlichen Genehmiger beträgt zwei.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Anforderungen laufen nach der angegebenen Dauer (Stunden) ab.	Legen Sie einen numerischen Wert in Stunden fest, der der maximalen Zeitzuteilung für die Mindestanzahl der einzuholenden Genehmigungen entspricht. Nach Ablauf des Zeitrahmens laufen auch die Quorum-Anforderungen ab. Eine neue Quorum-Anforderung ist erforderlich, um mit einer Widerrufsanforderung fortzufahren.

5. Klicken Sie auf **Absenden**.
   Eine Bestätigungsmeldung wird angezeigt.

Nächste Maßnahme
Die Auszahlungsaktionen sind in Schlüsselverwaltungsvorgängeverfügbar.

Verwalten Sie die Quorum-Steuerung

Nachdem der Workflow für einen Widerrufvorgang ausgelöst wurde, können Quorum-Aktionen auf der Seite „Schlüsselverwaltungsvorgänge“ verwaltet werden. Der Vorgang zum Zurückziehen des Schlüssels wird blockiert, bis das Quorum erfüllt ist.

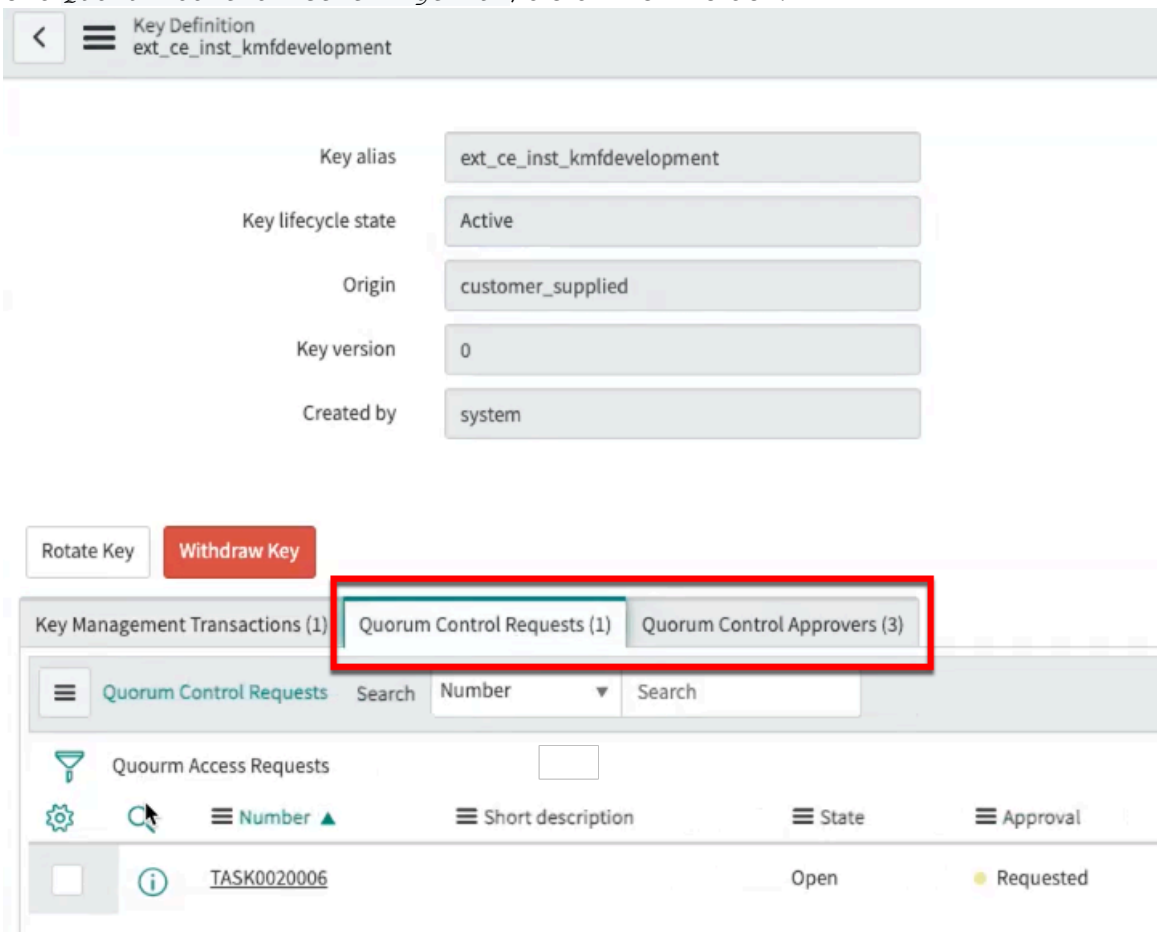
Vorbereitungen
Erforderliche Rolle: sn_kmf.admin oder sn_kmf.cryptographic_manager

Wenn das Quorum genehmigt oder abgelehnt wurde, erhält die anfordernde Person des Schlüsselrückzugs eine E-Mail mit der Nachricht, ob das Quorum erreicht oder abgelehnt wurde.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

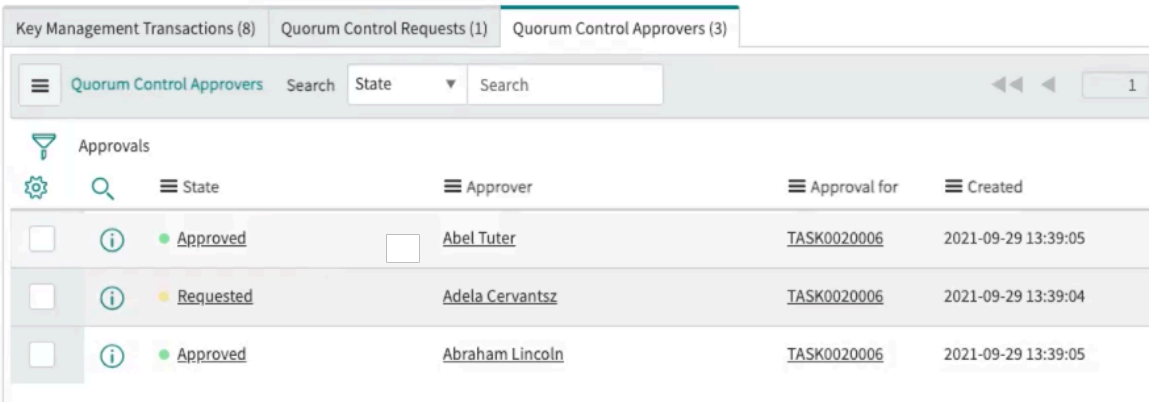
1. Führen Sie die Schritte zum Zurückziehen eines von einem Kunden verwalteten Schlüssels in Schlüsselverwaltungsvorgängeaus.
2. Zeigen Sie die Registerkarten *Quorum Control Anforderungen* und *Quorum Control Genehmiger an*, die aktiviert wurden.



3. Öffnen Sie die **Quorum Control-Anforderungen** Registerkarte zum Anzeigen der tatsächlich erstellten Anforderung.
   - Status:
     - Offen: Bei der Aktion zum Zurückziehen des Schlüssels steht die Erfüllung des Quorums aus.
     - Abgeschlossen: Das Quorum wurde erfüllt, und für diese bestimmte Quorum-Anforderung kann keine weitere Aktion durchgeführt werden.
   - Genehmigung:
     - Angefordert: Es wurden Genehmigungs-E-Mails gesendet, und der Workflow wurde ausgelöst, um das Quorum zu erreichen.
     - Genehmigt: Der Schlüssel wird zurückgezogen und die Instanz wird heruntergefahren.
     - Abgelehnt: Die Quorum-Anforderung wird abgebrochen, und mit dieser Anforderung wird keine weitere Aktion ausgeführt. Zum Zurückziehen des Schlüssels ist eine neue Auszahlungsanforderung erforderlich.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Öffnen Sie die Registerkarte Quorum Control-Genehmiger, um die Liste der Genehmiger und den Status der Genehmigungsanforderung anzuzeigen.



   Status:

   - Angefordert: Der Genehmiger hat die Genehmigungsanforderung noch nicht bearbeitet.
   - Genehmigt: Die Anforderung wurde entweder über die E-Mail oder über die Genehmigungsseite genehmigt.

5. Wählen Sie die Registerkarte **Transaktionen der Schlüsselverwaltung**, um den Fortschritt des Anforderungsschritts für das Zurückziehen des Schlüssels anzuzeigen.
   - Schritt 0 – Quorum-Anforderung: Die tatsächliche Quorum-Anforderung. Die Quorum-Anforderung muss abgeschlossen werden, um die Schritte zum Zurückziehen des Schlüssels auszulösen.
   - Schritt 1 – Schlüsselrücknahme: Der Schritt zum Zurückziehen des Schlüssels. Diese besteht aus den Schritten 2 bis 7.
   - Schritt 2 – Request_preparation: Erstellt eine auszulösende Anforderung sowie das Packen und die Rotation.
   - Schritt 3 – request_integrity_check: Validiert, dass die Anforderung berechtigt und sicher ist.
   - Schritt 4 – request_validation: Validiert, dass eine Anforderung in Bearbeitung ist. Es kann jeweils nur eine Rotationsanforderung verarbeitet werden.
   - Schritt 5 – hsm_key_delete: ruft KeySecure auf, um den aktiven Schlüssel zu löschen.
   - Schritt 6 – key_metadata_withraw: konvertiert den aktiven Lebenszyklusstatus der Schlüsselmetadaten in „zerstört“.
   - Schritt 7 – post_withraw: Tätigt einen Anruf, um die Instanz herunterzufahren.

Automatische Übersetzung

Genehmigen Sie eine Quorum Control-Anforderung, oder lehnen Sie sie ab

Genehmigen Sie eine Quorum Control-Anforderung in Schlüsselverwaltungstransaktionen, oder lehnen Sie sie ab.

Warum und wann dieser Vorgang ausgeführt wird

Wenn eine Quorum-Anforderung erstellt wurde, müssen die Mitglieder die Mindestanzahl von Genehmigungen einhalten. Nachdem der Workflow für einen Widerrufvorgang ausgelöst wurde, können Quorum-Aktionen mit verschiedenen Methoden verwaltet werden. Die Benutzer können Genehmigungen auf der Seite „Key Management Operations“, „Meine Genehmigungen“ in der Instanz oder direkt in der Anforderungs-E-Mail erteilen. Der Vorgang zum Zurückziehen des Schlüssels wird blockiert, bis das Quorum erfüllt ist.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieses Verfahren beschreibt, wie Sie eine Quorum-Anforderung über die Seite „Key Management Operations“ (Schlüsselverwaltungsvorgänge) genehmigen oder ablehnen.

Vorbereitungen
Erforderliche Rolle: sn_kmf.admin oder sn_kmf.cryptographic_manager

Prozedur

1. Navigieren zu **Alle** > **Cloud-Verschlüsselungsschlüssel-Verwaltung** > **Transaktionen der Schlüsselverwaltung** > **Quorum Control-Genehmiger**an.
2. Wählen Sie Ihren Anwendernamen aus der Tabelle aus.
3. Genehmigen Sie die Anforderung, oder lehnen Sie sie ab.

Genehmigen Sie eine Quorum-Anforderung, oder lehnen Sie sie ab

Wenn eine Quorum-Anforderung erstellt wurde, müssen die Mitglieder die Mindestanzahl von Genehmigungen einhalten. Nachdem der Workflow für einen Widerrufvorgang ausgelöst wurde, können Quorum-Aktionen mit verschiedenen Methoden verwaltet werden. Die Benutzer können Genehmigungen auf der Seite „Key Management Operations“, „ **Meine Genehmigungen** “ in der Instanz oder direkt in der Anforderungs-E-Mail erteilen. Der Vorgang zum Zurückziehen des Schlüssels wird blockiert, bis das Quorum erfüllt ist.

Vorbereitungen
Erforderliche Rolle: sn_kmf.admin oder sn_kmf.cryptographic_manager

Transaktionen der Schlüsselverwaltung

Das Submodul Key Management Transactions zeigt alle Transaktionen an, die für die Schlüssel in Ihrer Instanz ServiceNow stattgefunden haben.

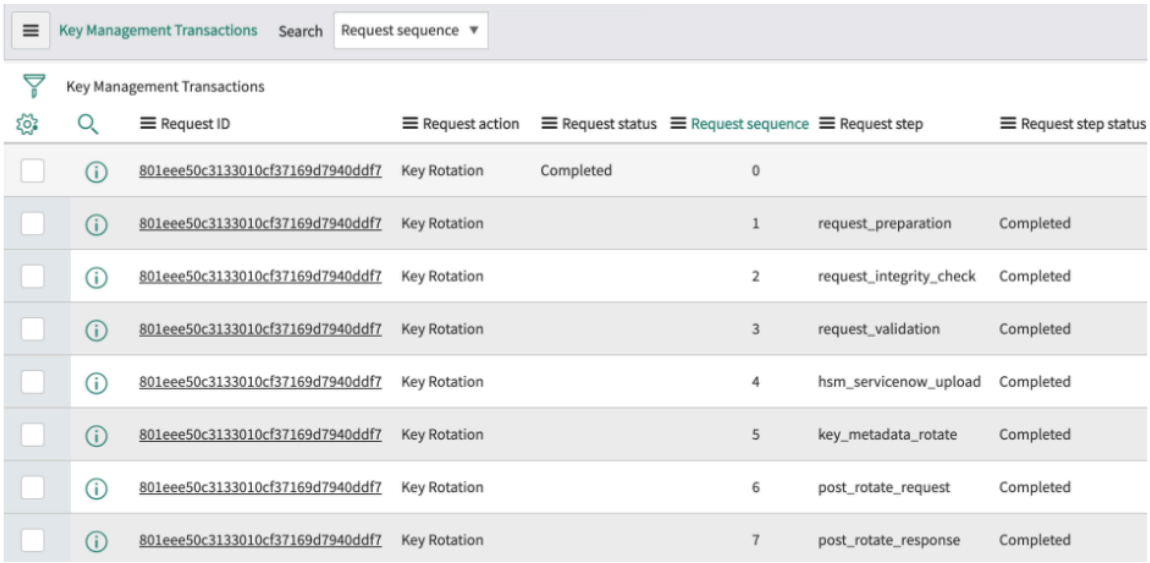
- Eine Schlüsseltransaktion ist wie folgt definiert:
  - besteht aus mehreren Anforderungsschritten.
  - Eine einzige *Anforderungs-ID* wird für alle Anforderungsschritte gemeinsam genutzt.
  - Der erste Schritt, Anforderungssequenz 0, einer Transaktion liefert den aktuellen Status der gesamten Transaktion.

    Wie in der Abbildung unten zu sehen ist, hat der erste Schritt 0 den Gesamtanforderungsstatus *Abgeschlossen*.
- Folgendes kann für die Transaktion durch den einzelnen Anforderungsschritt identifiziert werden:
  - Die Reihenfolge der einzelnen Schritte in einer Transaktion kann durch die Sequenznummer für den Schritt identifiziert werden.
  - Der Status jeder Transaktion ist über den Status des Anforderungsschritts sichtbar.
  - Wenn ein Schritt über den ersten Schritt hinaus fehlschlägt, erhält die gesamte Transaktion den Status Fehlgeschlagen. Wenn alle Schritte abgeschlossen sind, lautet der Transaktionsstatus ebenfalls „Abgeschlossen“.

Der folgende Bildschirm ist ein Beispiel für die Art von Informationen, die mit einer ServiceNow -Tastenrotation angezeigt werden.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die folgende Tabelle enthält die Feldinformationen, die auf der Seite „Transaktionen der Schlüsselverwaltung“ verfügbar sind.

Transaktionen der Schlüsselverwaltung

Feld	Beschreibung
Anforderungs-ID	Eindeutige, vom System generierte ID für die durchgeführte Aktion Alle Anforderungsschritte teilen eine Anforderungs-ID.
Anforderungsaktion	Zeigt die Aktion für die ausgeführte Tastenbetätigung an.
Anforderungsstatus	• Verarbeitung: Eine Anforderung wurde eingegeben, ist jedoch noch nicht abgeschlossen. • Abgeschlossen: Die Anforderung wurde erfolgreich abgeschlossen. • Fehlgeschlagen: Ein Problem ist aufgetreten, und der Prozess wurde nicht abgeschlossen. **Hinweis:** Wenden Sie sich an Kundenservice und Support, und geben Sie die Anforderungsnummer an, unter der der Fehler aufgetreten ist.
Schlüssel-Alias	Alphanumerischer Eintrag.
Schlüssel-Lebenszyklusstatus	Definitionen finden Sie unter Schlüssellebenszyklusstatus des Key Management Framework.
Quelle	• ServiceNow Schlüssel • Vom Kunden verwalteter Schlüssel
Schlüsselversion	Wenn ein Schlüssel rotiert, erhöht sich die Versionsnummer.
Anforderungssequenz	Zeigt die Reihenfolge an, in der eine Anforderung im System verarbeitet wird.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Transaktionen der Schlüsselverwaltung (Fortsetzung)

Feld	Beschreibung
Anforderungsschritt	Zeigt an, ob während der Schlüsselrotation ein Schritt im System verarbeitet wird. Anzahl und Inhalt der Schritte variieren je nach Art der durchgeführten Tastenbetätigung. **1.** request_preparation: Erstellt eine Anforderung zum Auslösen sowie für das Packen und die Rotation. **2.** request_integrity_check: Validiert, dass die Anforderung berechtigt und sicher ist. **3.** request_validation: Validiert, dass eine Anforderung in Bearbeitung ist. Es kann jeweils nur eine Rotationsanforderung verarbeitet werden. **4.** „attachment_process“: Extrahiert das verpackte Schlüsselmaterial aus dem Anhang. (Zusätzlicher Schritt beim Rotieren eines vom Kunden verwalteten Schlüssels.) **5.** hsm_<key type> _upload: Lädt das verpackte Schlüsselmaterial in das HSM KeySecure hoch. **6.** key_metadata_rotate: Generiert die neuen Schlüsselmetadaten. **7.** post_rotate_request: Sendet eine Anforderung zur Durchführung der Schlüsselrotation. **8.** post_rotate_response: Antwort zur Durchführung der Schlüsselrotation basierend auf der Anforderung der Kundeninstanz. **Hinweis:** Geben Sie den Anforderungsschritt für Kundenservice und Support an, um den Statusverlauf zu analysieren, falls ein Anforderungsschritt nicht abgeschlossen wird.
Anforderungsschritt-Status	• Abgeschlossen: Rotation ist erfolgreich. • Fehlgeschlagen: Die Rotation ist nicht erfolgreich. **Hinweis:** Geben Sie den Anforderungsschritt für Kundenservice und Support an, um den Statusverlauf zu analysieren, falls ein Anforderungsschritt nicht abgeschlossen wird.

Protokollierung für die Cloud-Verschlüsselung

Erfahren Sie mehr über Protokollierungsoptionen für Cloud-Verschlüsselung.

Protokollierungstabellen für die Cloud-Verschlüsselung

Verwenden Sie diese Tabellen, um Protokollierungsinformationen für Cloud Encryption-Transaktionen in Ihrer Instanz zu finden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Cloud-Verschlüsselungsmetadaten [dare_key_metadata]	Mit Metadaten zur Cloud-Verschlüsselung werden Metadaten für das Schlüssel-Lebenszyklusmanagement erfasst. In dieser Tabelle finden Sie wichtige Lebenszyklus-, Status- und Versionsinformationen. Diese Tabelle wird nach jeder Tastenbetätigung aktualisiert.
Transaktionen der Schlüsselverwaltung [dare_key_request]	„Transaktionen der Schlüsselverwaltung“ erfasst Transaktionsinformationen der Schlüsselverwaltung. In dieser Tabelle finden Sie Protokollierung für jeden Schritt einer Transaktion. Die Tabelle zeichnet alle Fehlerinformationen für eine Transaktion im Feld **Fehlermeldung** auf.
Sys-Audits [sys_audit]	Die Tabelle „Sys Audits“ erfasst Einfügungen und Aktualisierungen für alle geprüften Datensätze in Ihrer Instanz. In dieser Tabelle finden Sie Änderungen an Datensätzen in Ihrer Instanz, wann die Änderungen vorgenommen wurden und welches Benutzerkonto die Änderung initiiert hat.

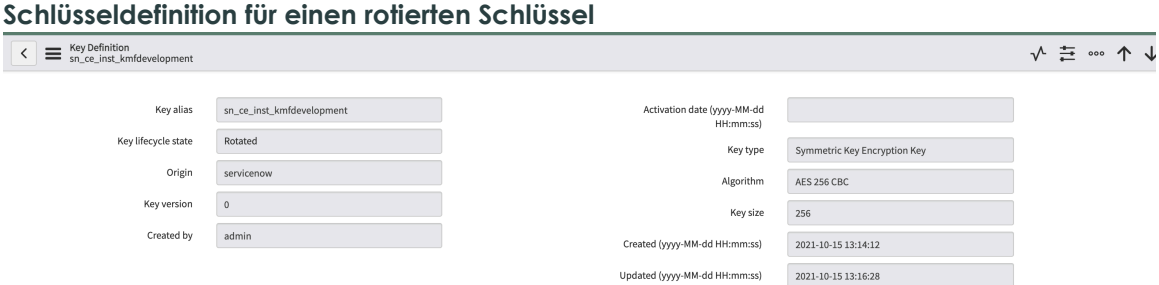
Überwachen Sie Schlüsselrotationsvorgänge

Verwenden Sie die Tabelle „Metadaten des Cloud-Verschlüsselungsschlüssels“ [dare_key_metadata], um Informationen zum Lebenszyklus Ihres Schlüssels zu erhalten. In dieser Tabelle finden Sie Informationen wie Herkunft, Aktivierungsdatum, Status und Version Ihrer Schlüssel.

Verwenden Sie die Tabelle „Transaktionen der Schlüsselverwaltung“ [dare_key_request], um Transaktionen von wichtigen Vorgängen zu überwachen. In dieser Tabelle finden Sie alle Anforderungen, die sich auf Ihre Schlüssel beziehen, einschließlich Status, Status und Schritt im Prozess, in dem sich die Anforderung befindet. Abgeschlossene Anforderungen werden in dieser Tabelle mit dem Status **Abgeschlossen** beibehalten.

Dieses Beispiel zeigt einen Schlüsselrotationsvorgang. Während dieses Vorgangs wird der alte Schlüssel-Lebenszyklusstatus von „Aktiv“ in „Rotiert“ und der Versionsstatus von „Aktiv“ in „Deaktiviert“ geändert.

Schlüsseldefinition für einen rotierten Schlüssel

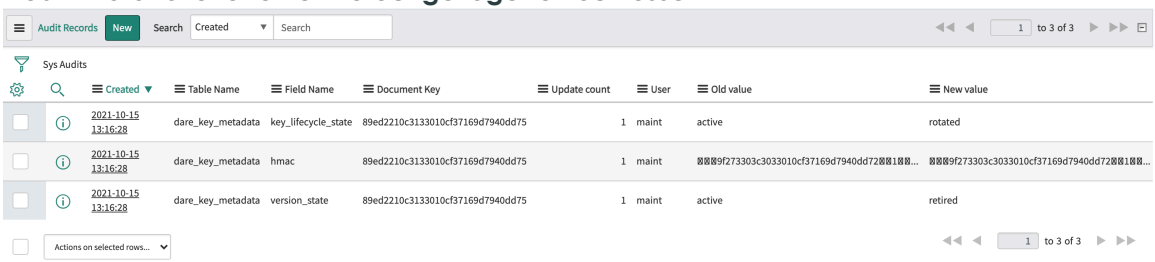


In der Tabelle „Sys Audits“ [sys_audit] können Administratoren sehen, welche Änderungen an Datensätzen in der Tabelle „Metadaten des Cloud-Verschlüsselungsschlüssels“ [dare_key_metadata] vorgenommen wurden. Administratoren

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

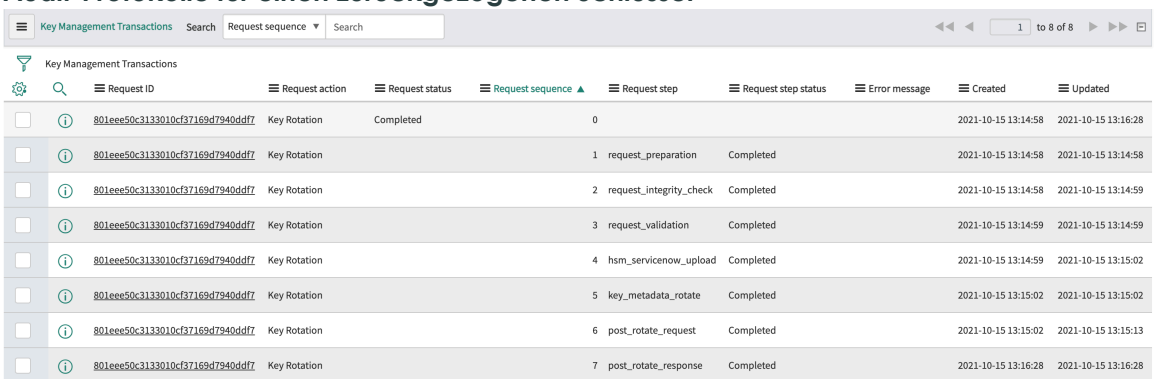
können sehen, welche Datensätze wann aktualisiert wurden. Die Protokolleinträge erfassen auch das Feld, das geändert wurde, und die alten und neuen Werte.

Audit-Protokolle für einen zurückgezogenen Schlüssel



Administratoren können die Datensätze in der Tabelle mit Metadaten des Cloud-Verschlüsselungsschlüssels [dare_key_metadata] anzeigen. In den Audit-Datensätzen unten wurde der Anforderungsstatus von „In Verarbeitung“ in „Abgeschlossen“ geändert.

Audit-Protokolle für einen zurückgezogenen Schlüssel

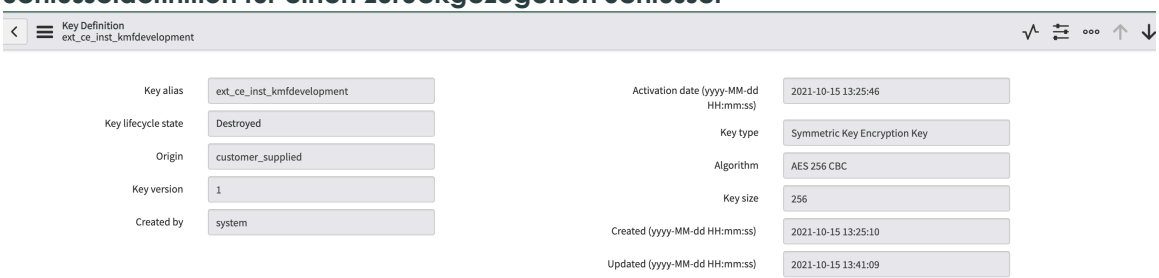


Protokollierung für Schlüsselrückzugsvorgänge

Protokollierungsinformationen zum Zurückziehen des Schlüssels werden in der Tabelle „Audits“ [sys_audit] gespeichert. Diese Protokollierungsinformationen enthalten Informationen darüber, wer das Zurückziehen des Schlüssels initiiert hat und wann es stattgefunden hat.

Dieses Beispiel zeigt einen Vorgang zum Zurückziehen eines Schlüssels. Während dieses Vorgangs wird der Schlüssel-Lebenszyklusstatus von „generiert“ über „aktiv“ bis „zerstört“ aktualisiert. Die Schlüsselversion wird von „unbekannt“ über „aktiv“ zu „deaktiviert“ aktualisiert.

Schlüsseldefinition für einen zurückgezogenen Schlüssel



In der Tabelle „Sys Audits“ [sys_audit] können Administratoren die Tabelle „Metadaten des Cloud-Verschlüsselungsschlüssels“ [dare_key_metadata] ändern.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Audit-Protokolle für einen zurückgezogenen Schlüssel

Audit Records | New | Search | Created | Search | 1 to 7 of 7

Sys Audits

Created	Table Name	Field Name	Document Key	Update count	User	Old value	New value
2021-10-15 13:41:09	dare_key_metadata	key_lifecycle_state	7960bad0c3133010cf37169d7940dd06	2	system	active	destroyed
2021-10-15 13:41:09	dare_key_metadata	hmac	7960bad0c3133010cf37169d7940dd06	2	system	▯▯▯9f273303c3033010cf37169d7940dd72▯▯1▯▯...	▯▯▯9f273303c3033010cf37169d7940dd7
2021-10-15 13:41:09	dare_key_metadata	version_state	7960bad0c3133010cf37169d7940dd06	2	system	active	retired
2021-10-15 13:25:46	dare_key_metadata	version_state	7960bad0c3133010cf37169d7940dd06	1	maint	unknown	active
2021-10-15 13:25:46	dare_key_metadata	key_lifecycle_state	7960bad0c3133010cf37169d7940dd06	1	maint	generated	active
2021-10-15 13:25:46	dare_key_metadata	activation_date	7960bad0c3133010cf37169d7940dd06	1	maint		2021-10-15 20:25:46
2021-10-15 13:25:46	dare_key_metadata	hmac	7960bad0c3133010cf37169d7940dd06	1	maint	▯▯▯9f273303c3033010cf37169d7940dd72▯▯1▯▯...	▯▯▯9f273303c3033010cf37169d7940dd7

Actions on selected rows... | 1 to 7 of 7

Manipulationserkennung

Verwenden Sie die Manipulationserkennung, um die Sicherheit zu verbessern, indem Sie nicht autorisierte Änderungen an Ihren Quorum-Steuerungseinstellungen erkennen.

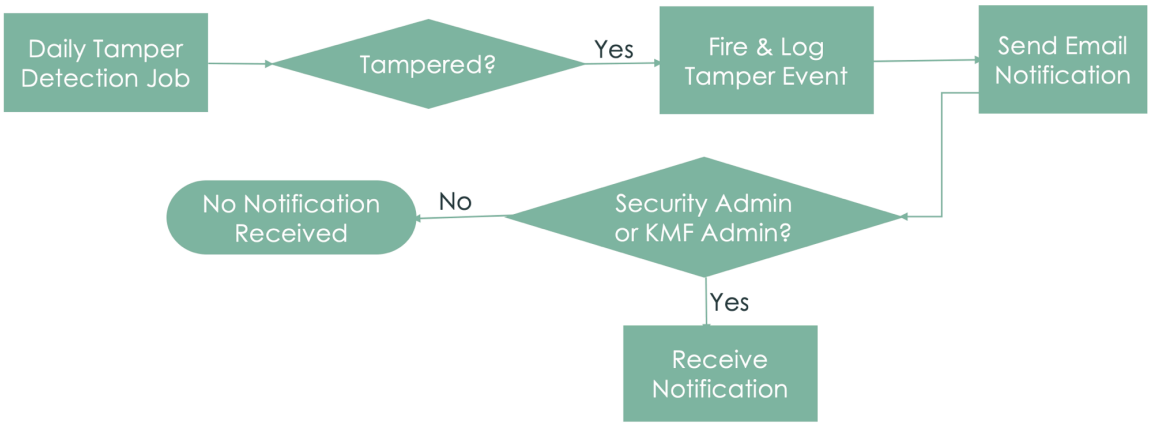
Manipulationserkennungsprozess

Wenn diese Option aktiviert ist, validiert die Manipulationserkennung Ihre Quorum-Steuerungseinstellungen, indem sie auf nicht autorisierte Änderungen (Manipulation) prüft. Die Manipulationserkennung verwendet einen hashbasierten Nachrichtenauthentifizierungscode (HMAC).

1. Wenn eine Einstellung geändert oder erstellt wird, erstellt Ihre -Instanz einen HMAC. Der HMAC basiert auf dem Wert des Einstellungsdatensatzes (dare_property).
2. Wenn Ihre -Instanz diese Einstellungen verwendet, validiert die Manipulationserkennung sie mithilfe des HMAC.
3. Wenn die Einstellung erfolgreich validiert wird, kann sie von der Plattform verwendet werden, andernfalls ist dies nicht möglich.

Die Manipulationserkennung wird täglich für Ihre Instanz von ausgeführt

Die Manipulationserkennung überprüft Ihre Einstellungen mithilfe einer täglichen geplanten Aufgabe auf Manipulationen und meldet Validierungsfehler in Ihren Knoten- und Sicherheitsprotokollen. Die Manipulationserkennung sendet bei Validierungsfehlern eine Benachrichtigung an Sicherheits- und KMF-Administratoren.

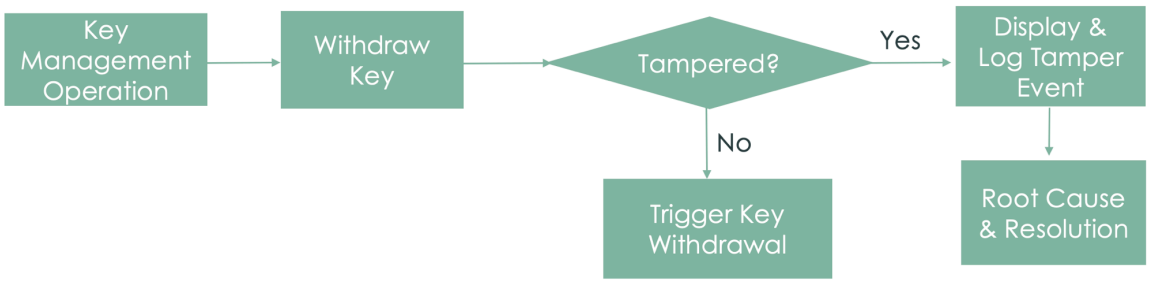


Die Manipulationserkennung wird ausgeführt, bevor ein Schlüsselrückzug ausgeführt wird

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Manipulationserkennung validiert auch Ihre Eigenschaften, wenn Sie einen Schlüsselrückzug anfordern. Wenn Ihre Einstellungen die Validierung nicht bestehen, wird der Schlüsselrückzug nicht ausgeführt. In diesem Fall müssen Sie alle Validierungsprobleme beheben, bevor das Zurückziehen des Schlüssels durchgeführt werden kann.



Identifizieren von Manipulationen

Die Manipulationserkennung aktualisiert Ihre Protokolle, wenn die Validierung fehlschlägt.

Wenn die Manipulationserkennung eine Ihrer Quorum-Steuerungseinstellungen nicht validieren kann, werden die folgenden Fehler in Ihren Knoten- und Sicherheitsprotokollen angezeigt. Der Protokolleintrag enthält die sys_id des Einstellungsdatensatzes (dare_property), dessen Validierung fehlgeschlagen ist.

```
2022-06-28 13:45:46 (582) Default-thread-5
 B6FAC1F6C3D01110CF37169D7940DD6E txid=231c4d72c310 SEVERE
 HMAC_VALIDATION_FAILED:The dare_property record with sys_id:
 776e3200c3210110900b169d7940dd76 failed HMAC validation

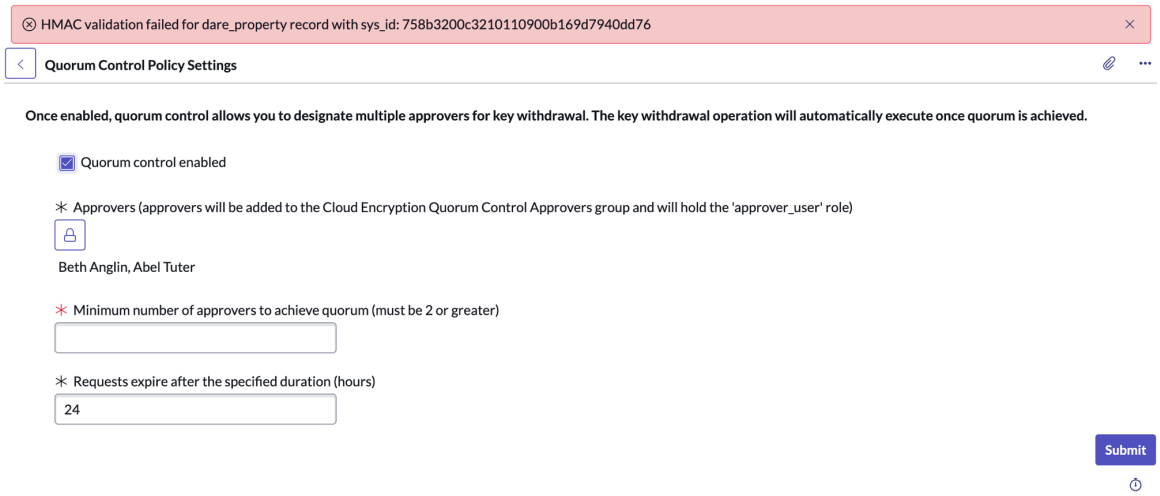
2022-06-28 13:47:35 (264) Default-thread-8
 B6FAC1F6C3D01110CF37169D7940DD6E txid=8e8cc972c310 SEVERE
 HMAC_VALIDATION_FAILED:The dare_property record with sys_id:
 758b3200c3210110900b169d7940dd76 failed HMAC validation
```

Bei der Protokollierung werden ähnliche Informationen wie in den folgenden Beispielen angezeigt, wenn die Validierung fehlschlägt. Erfolgreiche Validierungen werden nicht in den Protokollen angezeigt.

Die Manipulationserkennung zeigt auf der Einstellungsseite für das Quorum-Steuerelement eine Warnmeldung an

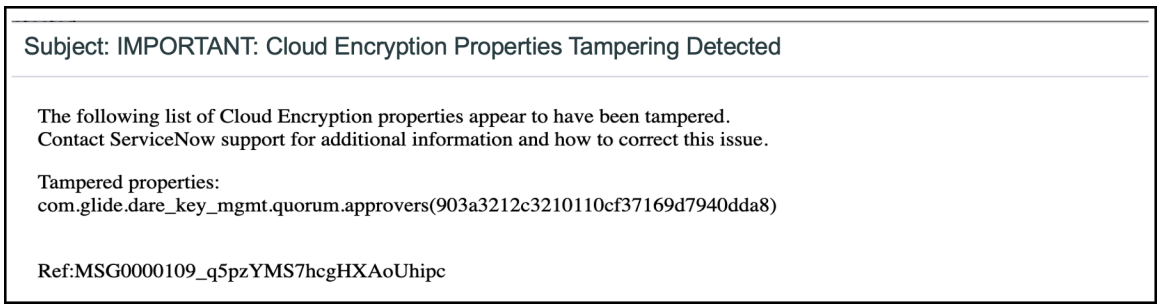
Wenn die Validierung einer Quorum Control-Einstellung fehlgeschlagen ist, wird auf der Seite mit den Einstellungen für die Quorum Control-Richtlinie in Ihrer Instanz eine Warnung angezeigt. Die Warnung enthält die sys_id des Einstellungsdatensatzes (dare_property), dessen Validierung fehlgeschlagen ist.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



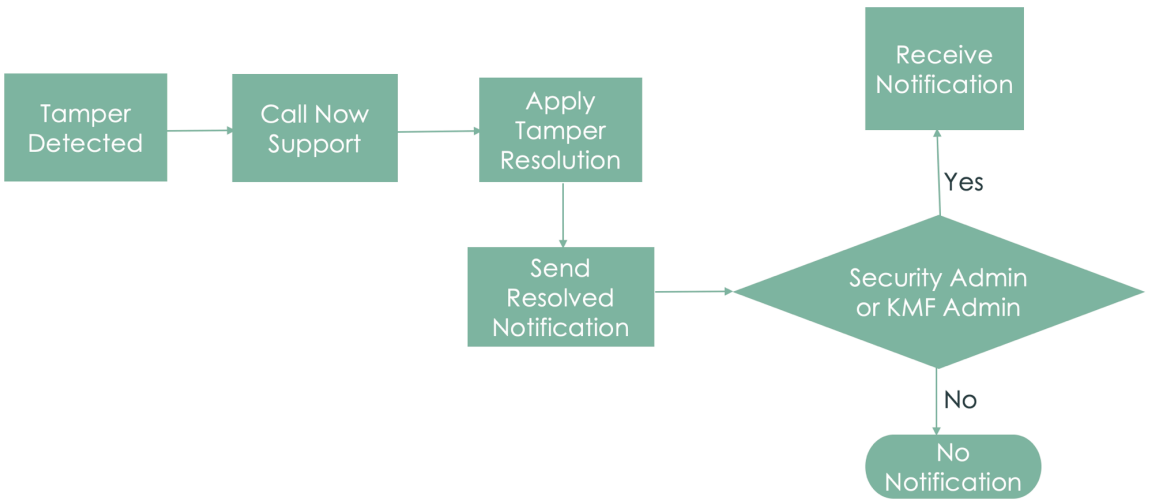
Die Manipulationserkennung sendet Benachrichtigungen an Benutzer mit den Rollen *Security Admin* und *KMF Admin*.

Wenn die Manipulationserkennung eine Ihrer Quorum-Steuerungseinstellungen nicht validieren kann, erhalten Ihre Sicherheitsadministratoren und KMF-Administratoren eine Benachrichtigung ähnlich dieser.



Manipulationsprobleme mit dem ServiceNow -Supportbeheben

Wichtig: Validierungsfehler bei der Manipulationserkennung können nur mit Unterstützung des ServiceNow -Supports behoben werden.

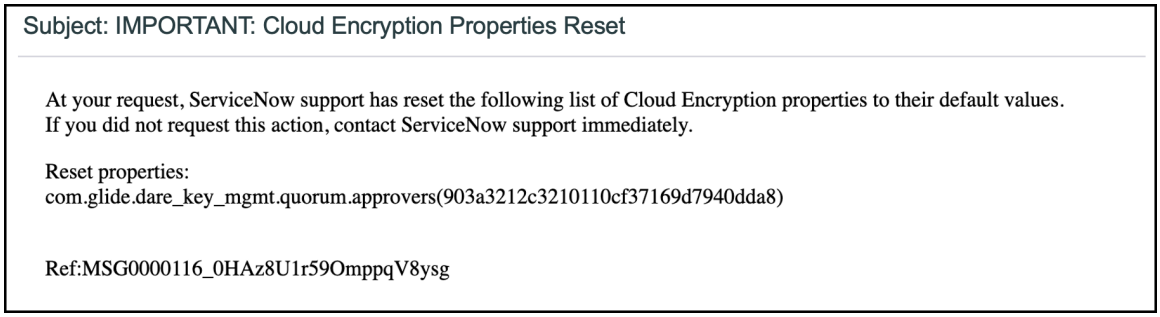


Wenn die Manipulationserkennung eine Ihrer Quorum-Steuerungseinstellungen nicht validieren kann, wenden Sie sich an den Support ServiceNow, um Unterstützung bei der Lösung des Problems zu erhalten. Nachdem ein Supportmitarbeiter den Validierungsfehler

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

behoben hat, erhalten Sicherheits- und KMF-Administratoren eine Benachrichtigung, dass das Problem gelöst wurde.


Subject: IMPORTANT: Cloud Encryption Properties Reset

At your request, ServiceNow support has reset the following list of Cloud Encryption properties to their default values.
If you did not request this action, contact ServiceNow support immediately.

Reset properties:
com.glide.dare_key_mgmt.quorum.approvers(903a3212c3210110cf37169d7940dda8)

Ref:MSG0000116_0HAz8U1r59OmppqV8ysg

Vollständige Datenträgerverschlüsselung

Die vollständige Festplattenverschlüsselung (FDE) wendet die Verschlüsselung nur auf das gesamte Speichersystem innerhalb des Datenbankservers an, da dies die einzige Komponente ist, die Kundendaten speichert. FDE schützt nur vor physischem Verlust oder Diebstahl von Speichergeräten. Wenn Server mit verschlüsselten Festplatten aktiv sind und Daten bereitstellen, bietet die Verschlüsselung keinen zusätzlichen Schutz.

Vollständige Datenträgerverschlüsselung

Die Festplattenverschlüsselung kann für stark regulierte Organisationen relevant sein, kann jedoch die Kosten für die Bereitstellung eines Kunden ServiceNow erheblich erhöhen. Maßnahmen, die von ServiceNow getroffen wurden, um den Verlust oder den Diebstahl von Speichergeräten zu minimieren, können ebenfalls ein Faktor bei der Auswahl sein.

Aus der Perspektive Now Platform fließen alle Daten in entschlüsselt.

Kommerzielle Umgebungen verwenden die vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE) mit FIPS 140-validierten Hardware- oder Speichergeräten, die zusammen mit einer dedizierten Hardwareoption ServiceNow gegen zusätzliche Kosten validiert werden. FDE bezieht sich auf die Hardware selbst und bietet daher eine Verschlüsselung im Ruhezustand für alle Daten, die in jeder Ihnen zugewiesenen Instanz gespeichert sind.

Weitere Informationen zur Auswahl von FDE und dedizierten Hardwareoptionen erhalten Sie von Ihrem ServiceNow -Vertreter.

Edge Encryption

ServiceNow® Edge Encryption ™ verschlüsselt vertrauliche Daten in Ihrem Unternehmen, bevor sie über das Internet an Ihre Instanz ServiceNow gesendet werden (während der Übermittlung verschlüsselt), wo die Verschlüsselung im Ruhezustand erhalten bleibt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Untersuchen



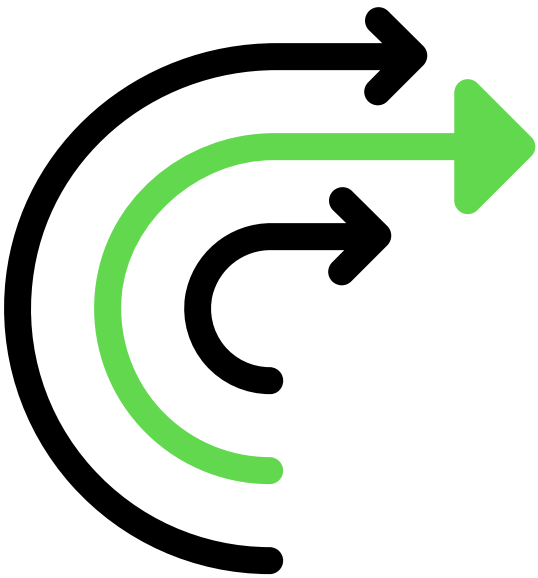
Lernen Sie die Funktionen und den Geschäftsnutzen von Edge Encryption kennen.

Planen



Erfahren Sie, wie Edge Encryption geplant wird.

Installieren



Installieren Sie Edge Encryption.

Upgrade von Edge Encryption

Upgrade-



Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erfahren, wie Edge Encryption aktualisiert wird.

Konfigurieren



Erfahren Sie, wie Sie Edge Encryption konfigurieren.

Edge Encryption erkunden

Edge Encryption ist ein Netzwerkverschlüsselungssystem in Ihrem Netzwerk, das vertrauliche Daten während der Übertragung zwischen Ihrem Rechenzentrum und der ServiceNow-Cloud verschlüsselt und entschlüsselt.

Edge Encryption – Beschreibung

Edge wird auch als „clientseitige“ Verschlüsselung bezeichnet und erfordert, dass der gesamte bidirektionale Benutzerdatenverkehr über Proxys geleitet wird, die in Ihrer Infrastruktur verwaltet werden. Sie haben die vollständige Kontrolle über Ihre Schlüsselverwaltung, da die Schlüssel innerhalb Ihres Proxys in Ihrer Infrastruktur gespeichert werden. Now Platform kann Ihren Geheimtext nicht entschlüsseln, um auf Ihre Schlüssel zuzugreifen.

Die Funktion Edge Encryption ist eine zusätzliche Kostenoption, mit der Sie die End-to-End-Verschlüsselung Ihrer Daten und die Schlüsselverwaltung steuern können. Edge Encryption verwendet eine Proxy-Anwendung, die von ServiceNow bereitgestellt und von Ihnen in Ihrem eigenen Netzwerk installiert wird. Diese Proxy-Anwendung tokenisiert angegebene Datenmuster oder verschlüsselt Zeichenfolgenfelder, Datumsfelder, Datums-/Uhrzeitfelder und Anhangsdaten, bevor sie von Ihrer Umgebung an Ihre Instanz gesendet werden. Die Proxy-Anwendung entschlüsselt dieselben Daten auch innerhalb Ihres eigenen Netzwerks und verwendet Schlüssel, die nur innerhalb Ihres eigenen Netzwerks gespeichert sind.

Die relevanten Verschlüsselungsschlüssel und die Konfiguration sind nur auf dem Edge-Proxy in Ihrem Netzwerk vorhanden und für ServiceNownicht sichtbar. Die Daten werden ab dem

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Moment verschlüsselt, in dem sie Ihre Umgebung verlassen, und werden erst beim Abrufen entschlüsselt. ServiceNow -Systeme oder -Mitarbeiter können zu keinem Zeitpunkt im Klartext auf die Daten zugreifen.

Edge Encryption – Benutzer

Nur ein Benutzer, der über einen Proxyserver in Ihrem Netzwerk bei der Instanz angemeldet ist, kann verschlüsselte Daten im Klartext anzeigen. Ebenso kann Edge Encryption nur von einem security_admin-Benutzer konfiguriert und verwaltet werden, der sich über einen Proxy-Server in Ihrem Netzwerk bei einer Instanz angemeldet hat.

Da sich der Proxyserver in Ihrem Netzwerk befindet, besitzen und verwalten Sie die Verschlüsselungsschlüssel, und sie werden nie an die -Instanz gesendet. Daher werden vertrauliche Daten von ServiceNow niemals im Klartext angezeigt.

Neben der Konfiguration des Edge-Proxy und der Verwaltung von Regeln sind Sie für die Erfüllung der üblichen Anforderungen für den Betrieb eines Servers in Ihrer Umgebung (einschließlich Hosting, Routing, Sicherung, DNS-Konfiguration usw.) verantwortlich, um Ihre Edge-Proxys zu aktivieren und zu unterstützen.

Verschlüsselung und Tokenisierung

Edge Encryption unterstützt sowohl die Verschlüsselung (durch Verschlüsselungskonfigurationen) als auch die Tokenisierung (durch Verschlüsselungsmuster) für den Schutz Ihrer vertraulichen Informationen.

Verschlüsselungskonfigurationen

Sie können einzelne Felder mit Verschlüsselungskonfigurationen verschlüsseln. Edge Encryption unterstützt AES mit 128-Bit- und 256-Bit-Verschlüsselungsschlüsseln. Edge Encryption unterstützt standardmäßige, gleichstellungserhaltende und ordnungserhaltende Verschlüsselungstypen.

Neben Anlagen können Sie folgende Feldtypen verschlüsseln:

- Datum
- E-Mail
- Datum/Uhrzeit
- HTML
- IP-Adresse
- Journal
- Journaleingabe
- Mehrzeiliger Text
- Einzeiliger Text
- Zeichenfolge
- URL

Hinweis:

Wenn dem Aktivitätsstrom ein Journal Feld hinzugefügt wird, das für die Verschlüsselung markiert ist, werden alle Benutzereingaben in das Feld im Aktivitätsstrom verschlüsselt.

Multi-Byte-Zeichen innerhalb der unterstützten Feldtypen können verschlüsselt werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

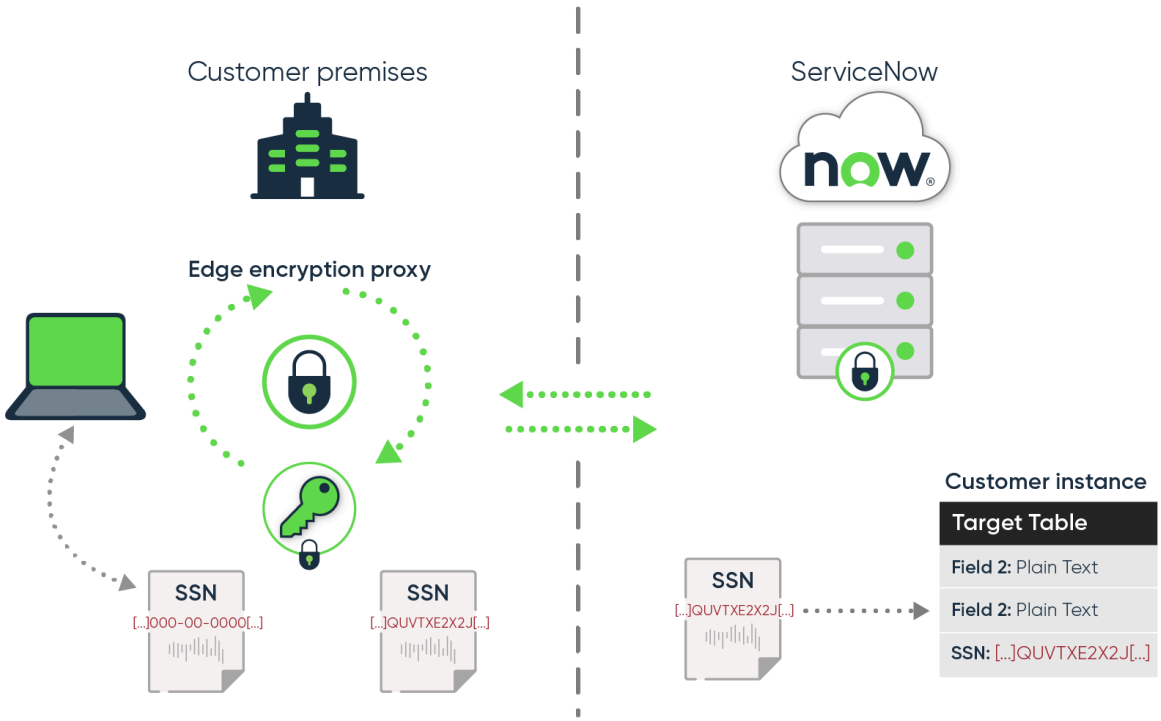
Sie können auch die folgenden Servicekatalog-Variablentypen verschlüsseln:

- Zeichenfolgentypen
- ◦ Einzeiliger Text
  ◦ Mehrzeiliger Text
  ◦ Breite einzeilige Textzeile
- Datum
- Datum/Uhrzeit
- URL
- E-Mail
- HTML
- IP-Adresse

Verschlüsselungsmuster

Sie können Verschlüsselungsmuster verwenden, um Zeichenketten zu tokenisieren, die regulären Mustern wie Sozialversicherungs- und Kreditkartennummern entsprechen. Verschlüsselungskonfigurationen sollten zwar die primäre Verschlüsselungsmethode sein, verwenden Sie jedoch Verschlüsselungsmuster als Ergänzung, um vertrauliche Informationen außerhalb verschlüsselter Felder zu schützen.

Hinweis: Der Edge Encryption Proxy-Server erfordert nur eine MySQL-Datenbank in Ihrem Netzwerk, wenn Sie ordnungserhaltende Verschlüsselungs- oder Verschlüsselungsmuster verwenden. Klartextwerte werden in der Proxy-Datenbank in Ihrem Netzwerk gespeichert. Aus diesem Grund ist es wichtig, dass Sie Ihre Proxy-Datenbank schützen und regelmäßig sichern. Empfehlungen finden Sie unter Komponenten der Edge Encryption.



© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Edge Encryption auf Now Platform

Edge Encryption fungiert als Gateway zwischen Ihrem Browser und Ihrer ServiceNow-Instanz. Der Datenverkehr Ihres Browsers wird durch das Gateway auf dem Weg zur ServiceNow-Instanz. Das Gateway wiederum ist so konfiguriert, dass ausgehende Daten, die zur Verschlüsselung markiert sind, verschlüsselt werden. Eingehender Datenverkehr wird über das Gateway entschlüsselt, und der Endbenutzer sieht im Browser Klartext. Der Vorteil dieser Implementierung in Bezug auf die Sicherheitskontrolle besteht darin, dass die Verschlüsselung und die Schlüsselverwaltung extern über ServiceNow erfolgen.

Vor- und Nachteile

Wie bei Verschlüsselung auf Spaltenebene Enterprise und der Verschlüsselung auf Spaltenebene führt auch Edge Encryption aufgrund der zusätzlichen Sicherheit zu einigen funktionalen Einschränkungen innerhalb einer Instanz. Der lokale Edge-Proxy bietet jedoch auch einige zusätzliche Funktionen in Bezug auf die Sortierung im Vergleich zur Verschlüsselung auf Spaltenebene.

Vorteile:

- Edge Encryption bietet vollständige Kontrolle darüber, wer Ihre Informationen sieht, und verhindert Datenschutzverletzungen.
- Informationen verbleiben auf Ihrem Proxy-Server und verlassen Ihr Netzwerk niemals unverschlüsselt.
- Informationen werden während der Übertragung verschlüsselt, bevor sie die Instanz ServiceNow überhaupt erreichen.
- Sie besitzen und verwalten alle Ihre eigenen Verschlüsselungsschlüssel. Niemand sonst, nicht einmal Mitarbeiter von ServiceNow, kann auf Ihre Schlüssel zugreifen.
- Sie können die Stärke des Verschlüsselungsalgorithmus auswählen: AES-128 oder AES-256.
- Edge Encryption bietet die Möglichkeit zum Verschlüsseln von Zeichenfolgen, Datums- und Datums-/Uhrzeit-Feldern, Anhängen, URLs und Journalen.
- Edge Encryption bietet Standardverschlüsselung, Gleichstellungserhaltung und Reihenfolgeerhaltung von Daten im Ruhezustand innerhalb der -Datenbank und -Instanz.
- Mit Verschlüsselungsregeln können Sie anwenderdefinierte Skripts schreiben, die dem Proxy-Server genau mitteilen, was verschlüsselt werden soll und wo die verschlüsselten Informationen in der Instanz abgelegt werden sollen. Diese Skripts sind nützlich, wenn die Datenstruktur nicht genau mit der Instanz ServiceNow übereinstimmt.
- Mit Verschlüsselungsmustern können Sie Informationen wie Passwörter tokenisieren.

Nachteile:

- Edge Encryption erfordert einen zusätzlichen Netzwerk-Hop durch das Edge-Proxy-Cluster und zusätzliche Verarbeitung, was den Datenverkehr verzögern kann. Die zusätzliche Verarbeitungsverzögerung der Anwendung Edge Encryption ist im Vergleich zum Netzwerk-Hop vernachlässigbar.
- Die Verwaltung eigener Verschlüsselungsschlüssel kann komplex und zeitaufwändig sein.
- Sie können maximal zwei Schlüssel verwalten, ohne die Flexibilität zu haben, verschiedene Schlüssel für verschiedene Teilmengen von Spalten/Daten oder für verschiedene Rollen usw. zu definieren
- Edge Encryption hat den Nebeneffekt, dass der Server oder die Plattform die Daten nicht entschlüsseln kann, um die entschlüsselten Daten zu bearbeiten. Daher können die Funktionen und die Datenverarbeitung auf Now Platform eingeschränkt sein, wenn Spalten mit Edge Encryption verschlüsselt werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Was Sie wissen müssen, bevor Sie beginnen

Da Verschlüsselung und Tokenisierung die Art Ihrer Daten ändern, kann Edge Encryption sich auf andere Instanzprozesse auswirken. Prüfen Sie vor der Nutzung von Edge Encryption sorgfältig die Auswirkungen auf Ihre Instanz.

Da der Proxy-Server in Ihrem Netzwerk installiert und verwaltet wird, erfordert Edge Encryption eine Netzwerkadministration und -verwaltung. Überprüfen Sie die Netzwerkanforderungen, um eine reibungslose Implementierung sicherzustellen.

Lesen Sie die folgenden Themen, um die Auswirkungen nachzuvollziehen, die Edge Encryption auf Ihre Instanz hat:

- Die Edge Encryption planen
- Edge Encryption – Systemanforderungen
- Umgebungsgröße Ihrer Edge Encryption anpassen
- Die Größe der Datenbank für die Ordnungserhaltung und Tokenisierung berechnen
- Edge Encryption – Einschränkungen
- Schlüsselverwaltung für Edge Encryption

Komponenten der Edge Encryption

Edge Encryption besteht aus dem Proxy-Server Edge Encryption, der auf einem Server in Ihrem Netzwerk ausgeführt wird, und dem Plugin Edge Encryption, das in Ihrer Instanz von ServiceNow installiert sein muss. Wenn Sie Verschlüsselungstypen oder Verschlüsselungsmuster mit Ordnungserhaltung verwenden, muss auch eine Proxy-Datenbank in Ihrem Netzwerk installiert sein.

Proxy-Anwendung

Bei der Verwendung des Proxy-Servers Edge EncryptionEdge Encryption können Sie mit dem Plugin [] angeben, welche Felder, Muster und Anhänge verschlüsselt werden sollen. Sie können auch Verschlüsselungsregeln zum Verschlüsseln bestimmter Anforderungen verwalten und Massenverschlüsselungsaufgaben planen.

Proxy-Server

Der Edge Encryption -Proxyserver verwendet Verschlüsselungsregeln, um zu identifizieren, was in einer HTTP-Anforderung ggf. verschlüsselt werden muss, und verschlüsselt es, bevor die Anforderung an die Instanz weitergeleitet wird. Zur Entschlüsselung sucht der Proxyserver Edge Encryption in den HTTP-Antworten nach verschlüsselten Daten und entschlüsselt sie, bevor die Antwort an den Client zurückgesendet wird. Damit diese Entschlüsselung erfolgt, müssen alle HTTP-Anforderungen und -Antworten über den Proxy-Server Edge Encryption geleitet werden. Zu diesen HTTP-Anforderungen gehören alle Anforderungen, die von einem Browser stammen, sowie alle SOAP- oder REST-Anforderungen.

Proxy-Datenbank

Wenn Sie ordnungserhaltende Verschlüsselungs- oder Verschlüsselungsmuster verwenden, verlassen sich Ihre Proxy-Server auf eine MySQL-Datenbank, die sich in Ihrem Netzwerk befindet. Alle Proxy-Server in Ihrem Netzwerk müssen dieselbe Datenbank verwenden.

Diese Tabellen sind in der Proxy-Datenbank enthalten.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Proxy-Datenbanktabellen

Name	Beschreibung
db_id	Eindeutige Datenbank-ID
edge_token_map	Verschlüsselungsmusterdaten
token_map	Ordnungserhaltende Verschlüsselungsdaten

Sichern Ihrer Proxy-Datenbank

Da Verschlüsselungsmuster von der Tokenisierung abhängen, werden Klartextwerte in Ihrer Proxy-Datenbank gespeichert. Wenn die Datenbank verloren geht, können Klartextwerte nicht wiederhergestellt werden. Es ist wichtig, dass Sie regelmäßige Sicherungen durchführen. Um Datenverlust zu vermeiden, sichern Sie Ihre Proxy-Datenbank gemäß ServiceNow Empfehlungen.

- Sichern Sie Ihre Datenbank alle 24 Stunden.
- Bewahren Sie die binären Protokolldateien der MySQL-Datenbank für mindestens zwei Tage auf. Nachdem eine Sicherung wiederhergestellt wurde, können Sie das binäre Protokoll verwenden, um die seit der letzten Sicherung verlorenen Daten wiederherzustellen.

Edge Encryption-Clients

Edge Encryption verwendet drei Clients, um die Instanz zu informieren, dass der Proxy ausgeführt wird, um Anforderungen zwischen dem Proxy und der Instanz zu synchronisieren und alle Endbenutzer-Anforderungen nach einer potenziellen Verschlüsselung an die Instanz weiterzuleiten.

Client	Beschreibung
Heartbeat/Keepalive-Client	Dafür verantwortlich, alle 5 Sekunden eine Anforderung an die ServiceNow-Instanz zu senden, um die Instanz wissen zu lassen, dass dieser Proxy betriebsbereit ist und ausgeführt wird. Die Anforderungen geben das Feld last_response_on in der Edge-Proxy-Tabelle vor und folglich auch den Proxy-Status. Falls bei Ihrem System Probleme beim Senden von Anforderungen auftreten, oder wenn die Anforderungen oder die Verarbeitung der Anforderungen verzögert wird, kann die Instanz den Proxy gegebenenfalls mit der Markierung „Keine Reaktion“ versehen, auch wenn die anderen Clients (einschließlich des Clients für den Benutzerdatenverkehr) einsatzbereit sind. Dieser Client steuert auch den Online-Status des Proxys in der Instanz. Die Eigenschaft *edgeencryption.proxy.keepalive.interval* steuert die Abfragehäufigkeit für diesen

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Client	Beschreibung
	Client. Der Standardwert beträgt 5 (Sekunden).
Abfrage-/Synchronisierungsclient	Verantwortlich für verschiedene Anforderungen, die vom Proxy zum Synchronisieren mit der Edge Encryption-Konfiguration (z. B. die zu verschlüsselnde Tabelle, Spalte oder Anlage sowie Schlüssel, Aufträge, Regeln und Tokenisierungsmuster) an die Instanz gesendet werden. Die Eigenschaft *edgeencryption.config.poll.interval* steuert die Abfragehäufigkeit für diesen Client. ⚠ **Warnung:** Ändern Sie diese Einstellung nicht. Eine Änderung der Standardeinstellung der Proxy-Abfragehäufigkeit führt möglicherweise dazu, dass die Synchronisierung verzögert wird, wenn die Edge Encryption-Einstellungen für die Instanz aktualisiert werden.
Standard-/Benutzerdatenverkehr-Client	Für alles andere verarbeitet dieser Client alle Endbenutzer-Anforderungen und leitet diese nach einer möglichen Verschlüsselung an die ServiceNow-Instanz weiter. Dieser Client verarbeitet auch Antworten von der Instanz und leitet sie nach einer möglichen Entschlüsselung an den Endbenutzer weiter.

Schlüsselverwaltung für Edge Encryption

Sie sind für die Bereitstellung und Verwaltung der von Edge Encryption verwendeten Verschlüsselungscodes verantwortlich.

Dieses Thema bezieht sich auf Schlüssel für das Produkt Edge Encryption. Wenn Sie Informationen zum Key Management Framework suchen, das mit der Verschlüsselung auf Spaltenebene verwendet werden kann, lesen Sie unter Key Management Frameworknach.

Wenn Sie Verschlüsselungscodes erhalten und erstellen, die die von Edge Encryption verwendeten Verschlüsselungsarten unterstützen, beachten Sie Folgendes:

- Soll AES 128-Bit oder AES 256-Bit verwendet werden? Sie müssen einen Standard-AES 128-Bit-Verschlüsselungsschlüssel definieren, auch wenn er nicht verwendet wird.
- Gibt an, ob Dateisystem, Java KeyStore oder Enterprise Key Management (EKM) verwendet werden soll.
- Wann müssen die Verschlüsselungsschlüssel rotiert werden?
- Wann und ob ein Massenverschlüsselungsauftrag verwendet wird, um Daten mit dem neuen Schlüssel erneut zu verschlüsseln.

Vor dem Entfernen eines Schlüssels aus den Proxy-Konfigurationsdateien und dem Schlüsselspeicher müssen unbedingt alle Daten in der Instanz entschlüsselt werden, die den

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schlüssel verwendet. Sie können dies tun, indem Sie einen neuen Verschlüsselungscode hinzufügen und einen Auftrag zur Massenrotation von Schlüsseln planen.

Schlüsselspeicher

Edge Encryption unterstützt die folgenden Arten der Schlüsselspeicherung.

Dateispeicher

Schlüssel werden in einer Datei in einem Dateisystem gespeichert, auf das der Edge Encryption Proxy Zugriff hat. In einer Datei gespeicherte Verschlüsselungsschlüssel werden nicht verschlüsselt. Der Schutz dieser Dateien liegt also in Ihrer Verantwortung.

Java KeyStore

Schlüssel werden im JCEKS KeyStore von Java gespeichert. Ein Java KeyStore ist durch ein Passwort geschützt. Daher ist es sicherer als das Speichern von Schlüsseln in einer Datei im Dateispeicher. Ein einzelner Java KeyStore kann mehrere Schlüssel speichern. Die Schlüssel werden durch einen Schlüsselalias identifiziert, wodurch die Verwaltung mehrerer Schlüssel vereinfacht wird.

Enterprise Key Management (EKM)

Schlüssel werden mit den Schlüsselverwaltungssystemen SafeNet KeySecure oder Unbound Technology gespeichert und abgerufen.

Der Edge Encryption Proxy wird mit der Java JCEKS KeyStore-Datei mit dem Namen `keystore.jceks` im Verzeichnis `Schlüsselspeicher` geliefert. Diese Schlüsselspeicherdatei enthält den öffentlichen Schlüssel ServiceNow, mit dem die von ServiceNow signierten Verschlüsselungsregeln überprüft werden.

Hinweis: Wenn Sie einen anderen Schlüsselspeicher als das Basissystem Java JCEKS KeyStore verwenden, müssen Sie den öffentlichen Schlüssel ServiceNow in Ihren Schlüsselspeicher importieren. Der Alias für den öffentlichen Schlüssel lautet *`servicenow`*.

Zusätzlich zu den Verschlüsselungsschlüsseln wird im Java JCEKS KeyStore das RSA-Schlüsselpaar zum digitalen Signieren der in der Instanz gespeicherten Verschlüsselungskonfigurations- und Verschlüsselungsregeln und das digitale Zertifikat gespeichert, das der Proxy Edge Encryption verwendet, um eine sichere Verbindung mit den Browsern und allen anderen Clients herzustellen.

SafeNet-Schlüsselversionsverwaltung für Edge Encryption

Verwenden Sie die SafeNet-Schlüsselversionsverwaltung, um das Wechseln der Schlüssel zu vereinfachen. Anstatt für jeden neuen Schlüssel einen Alias zu erstellen, behält die SafeNet-Schlüsselversionsverwaltung denselben Alias bei und erhöht die Version.

Sie müssen die Schlüssel-Versionsverwaltung in SafeNet einrichten, bevor Sie die SafeNet-Schlüssel-Versionsverwaltung auf dem Edge-Proxy-Server konfigurieren können.

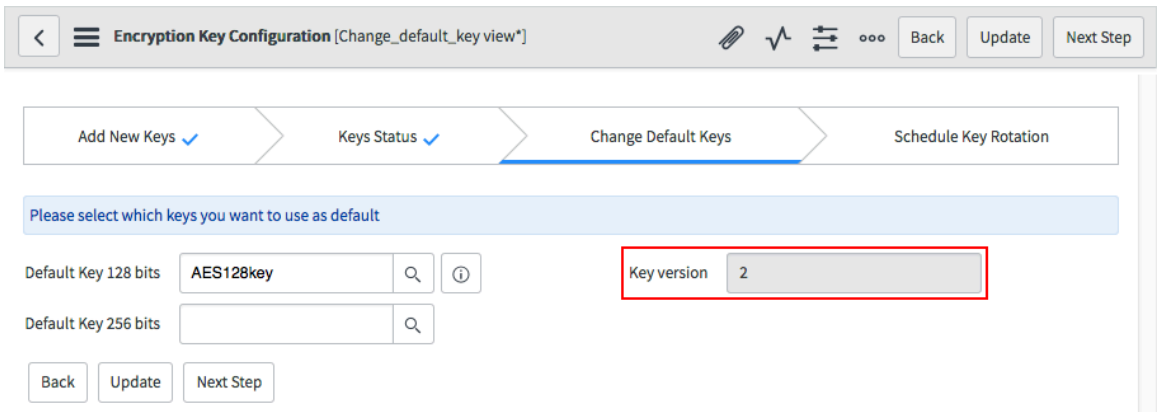
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Vor der Version London installierte Edge-Proxys unterstützen SafeNet-Schlüssel, jedoch keine Versionsverwaltung von SafeNet-Schlüsseln. Wenn Sie versehentlich einen versionierten Schlüssel auf einem Kingston-Proxy oder einem älteren Proxy verwenden, erkennt der London-Proxy oder der spätere Proxy beim Upgrade auf die Version London oder höher dieses Problem, und um möglichen Datenverlust zu vermeiden, startet der Proxy nicht.

Sie müssen zunächst einen Auftrag für eine Massenschlüsselrotation oder einen einzelnen Schlüsselrotationsauftrag planen, um den alten SafeNet versionierten Schlüssel durch einen nicht versionierten Schlüssel zu ersetzen, und dann bei Bedarf einen neuen SafeNet versionierten Schlüssel erstellen. Dieser neue versionierte Schlüssel kann sicher für den Proxy London oder höher verwendet werden, und Sie können den Proxy neu starten.

Konfiguration des Verschlüsselungsschlüssels

Bei Verwendung von mit SafeNet versionierten Schlüsseln enthält der Abschnitt „Ändern des Abschnitts Standardschlüssel im Formular zur Konfiguration des Verschlüsselungsschlüssels“ neue Felder für die **Schlüsselversion** der standardmäßigen 128-Bit- und 256-Bit-Schlüssel. Die Felder für die **Schlüsselversion** sind ausgegraut und können nicht bearbeitet werden.

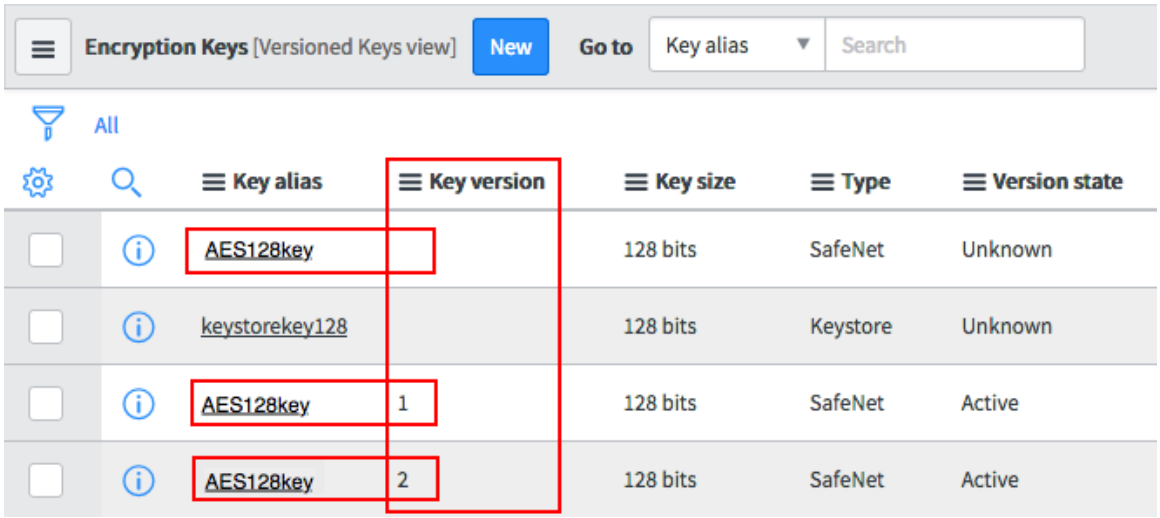


Hinweise zu Verfahren siehe Verschlüsselungsschlüssel für die Instanz konfigurieren.

Versionierte Schlüssel

Bei Verwendung von Schlüsseln mit SafeNet-Version, wenn Sie zu navigieren **Konfiguration der Edge Encryption** > **Konfiguration des Verschlüsselungsschlüssels** > **Alle Schlüssel**, Schlüssel mit Schlüsselversion enthalten die **Schlüsselversion**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Für die ersten Einträge, die Sie im Abschnitt „Standardschlüssel ändern“ des Formulars „Konfiguration der Verschlüsselungsschlüssel“ vornehmen, wird keine Versionsnummer angezeigt. Wenn der Proxy-Server einen Schlüssel von SafeNet anfordert, fügt das System eine neue Zeile für den Aliasnamen und die **Schlüsselversion** hinzu.

Im obigen Beispiel ist **AES128key** dreimal aufgeführt:

- Die erste Auflistung ohne angegebener **Schlüsselversion** ist der erste Eintrag.
- Die zweite Auflistung mit **1** in der Spalte **Schlüsselversion** ist die erste Version des von SafeNet zurückgegebenen Schlüssels.
- Die dritte Auflistung mit **2** in der Spalte **Schlüsselversion** ist die zweite Version des von SafeNet zurückgegebenen Schlüssels.
- Da andere Versionen des Schlüssels von SafeNet zurückgegeben werden, werden neue Zeilen hinzugefügt, um die jetzt verwendete **Schlüsselversion** aufzuzeichnen.

Verschlüsselungskonfigurationen und -muster

Mit Edge Encryption können Felder verschlüsselt und Zeichenketten tokenisiert werden.

Verschlüsselungskonfigurationen

Sie können einzelne Felder mit Verschlüsselungskonfigurationen verschlüsseln. Edge Encryption unterstützt AES mit 128-Bit-Verschlüsselungsschlüsseln. Wenn die Richtliniendateien der Java Cryptography Extension (JCE) für die Beschränkung der Gültigkeitsdauer installiert sind, unterstützt Edge Encryption AES-256-Bit-Verschlüsselungsschlüssel für jeden Verschlüsselungstyp. Edge Encryption unterstützt die folgenden Arten von Verschlüsselungskonfigurationen.

Standardverschlüsselung

Der verschlüsselte Wert eines Felds unterscheidet sich jedes Mal, wenn das Feld verschlüsselt wird, auch wenn der Feldwert gleich bleibt. Standardverschlüsselung ist die robusteste Form der Verschlüsselung. Felder, die Standardverschlüsselung verwenden, können nicht sortiert, gruppiert oder gefiltert werden.

Gleichstellungserhaltende Verschlüsselung

Der verschlüsselte Wert eines Felds ist derselbe, wenn der Feldwert derselbe bleibt. Unterstützt Gleichstellungsvergleiche und Gruppieren nach Operationen in einem Feld.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn für ein Feld, das bereits Daten enthält, die gleichstellungserhaltende Verschlüsselung ausgewählt wird, werden bei der Gruppierung nach Aktion für das Feld möglicherweise keine Felder mit demselben Wert gruppiert, wenn eines verschlüsselt ist und das andere nicht.

Ordnungserhaltende Verschlüsselung

Verwendet Token und Verschlüsselung, um Daten in Ihrer Proxy-Datenbank zu sichern. Unterstützt Gleichstellungsvergleiche, Gruppieren nach Operationen und die Möglichkeit der Datensortierung. Der ordnungserhaltende Verschlüsselungstyp wird nur unterstützt, wenn eine MySQL-Datenbank für den Edge Encryption Proxy-Server konfiguriert ist.

Hinweis: Wenn die ordnungserhaltende Verschlüsselung verwendet wird und die Proxy-Datenbank inaktiv ist, können Aktualisierungen an Feldern mit ordnungserhaltender Verschlüsselung vorgenommen werden. Die Sortierreihenfolge ist jedoch beim Versuch, Daten anhand dieser Felder zu sortieren, nicht korrekt. Gruppen funktionieren ebenfalls nicht wie erwartet. Wenn die Proxy-Datenbank wieder betriebsbereit ist, planen Sie einen Auftragstoken-Reparaturauftrag ein, um fehlende Token zu reparieren.

Verschlüsselungstypen

Die folgenden Verschlüsselungstypen sind gemäß abnehmender Sicherheitsqualität aufgeführt.

Verschlüsselungstyp	Beschreibung
Standard AES 256	Felder können nicht gefiltert, sortiert oder verglichen werden.
Standard AES 128	Felder können nicht gefiltert, sortiert oder verglichen werden.
Gleichstellungserhaltung von AES 256	Felder können mit Gleichstellungsvergleichen gefiltert werden.
Gleichstellungserhaltung von AES 128	Felder können mit Gleichstellungsvergleichen gefiltert werden.
Ordnungserhaltung von AES 256	Felder können sortiert und Gleichstellungsfilterung verwendet werden. Erfordert die Verwendung einer MySQL-Datenbank in Ihrem Netzwerk.
Ordnungserhaltung von AES 128	Felder können sortiert und Gleichstellungsfilterung verwendet werden. Erfordert die Verwendung einer MySQL-Datenbank in Ihrem Netzwerk.

Verschlüsselungsmuster

Sie können vertrauliche Daten in Zeichenfolgen mithilfe von Verschlüsselungsmustern schützen. Sobald ein Verschlüsselungsmuster gespeichert und aktiviert ist, identifiziert der Edge Encryption Proxy-Server Zeichenfolgen, die dem Muster in Anforderungen entsprechen. Nach der Suche wird die Klartextzeichenfolge in der Proxy-Datenbank gespeichert und in der Instanz durch ein Token ersetzt. Verwenden Sie Verschlüsselungsmuster, um Zeichenketten zu kennzeichnen, die regulären Mustern entsprechen, z. B. Sozialversicherungs- und Kreditkartennummern. Wir empfehlen, dass Verschlüsselungskonfigurationen die primäre Verschlüsselungsmethode sind. Verwenden Sie jedoch Verschlüsselungsmuster als Ergänzung, um vertrauliche Informationen zu finden und zu schützen, die außerhalb verschlüsselter Felder gefunden werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Der Edge Encryption Proxy-Server erfordert nur eine MySQL-Datenbank in Ihrem Netzwerk, wenn Sie ordnungserhaltende Verschlüsselungs- oder Verschlüsselungsmuster verwenden. Klartextwerte werden in der Proxy-Datenbank in Ihrem Netzwerk gespeichert. Aus diesem Grund ist es wichtig, dass Sie Ihre Proxy-Datenbank schützen und regelmäßig sichern. Empfehlungen finden Sie unter Komponenten der Edge Encryption.

Zugehörige Informationen

Felder mit Verschlüsselungskonfigurationen verschlüsseln

Zeichenketten mithilfe von Verschlüsselungsmustern tokenisieren

Mit Edge Encryption installiert

Edge Encryption installiert Tabellen zum Speichern verschlüsselungsbezogener Daten, Systemeigenschaften zum Konfigurieren des Standardverhaltens und die Rolle edge_encryption zur Verwaltung von Edge Encryption.

Mit Edge Encryption installierte Tabellen

Edge Encryption fügt die folgenden Tabellen hinzu.

Konfiguration der Edge Encryption [sys_encryption_configuration]

Enthält verschlüsselte Felder und Tabellen, für die Anhänge verschlüsselt werden.

Edge Encryption-Regel [sys_encryption_rule]

Enthält für jede Regel einen Datensatz. Eine Regel hat einen Namen, die Bedingung für deren Verwendung, ein Skript und ein Auftragsfeld.

Edge Encryption – Ungültiges Einfügungsprotokoll [sys_edge_encryption_invalid_insert_log]

Enthält Protokollnachrichten, die für Versuche erstellt wurden, unverschlüsselte Daten in einem verschlüsselten Feld zu speichern.

Edge Encryption-Proxy [sys_encryption_proxy]

Enthält Informationen zur Verschlüsselungs-Proxy-Anwendung.

Edge-Proxy-Verschlüsselungstyp [sys_proxy_encryption_type]

Wird zum Aktivieren und Deaktivieren von Verschlüsselungstypen im Verschlüsselungsformular verwendet.

Ausführung des Verschlüsselungsauftrags [sys_encryption_job_execution]

Unterstützt Aufträge zur Massenverschlüsselung.

Ausführungsblock für Verschlüsselungsauftrag [sys_encryption_job_execution_chunk]

Unterstützt Aufträge zur Massenverschlüsselung.

Geplanter Verschlüsselungsauftrag [sysauto_encryption_job]

Listet geplante Aufträge für die Verschlüsselung, Entschlüsselung, Schlüsselrotation, Auftragstokenreparatur und Datenbankwiederherstellung auf.

Konfiguration des Verschlüsselungsschlüssels [sys_encryption_key_configuration]

Listet die Standard-Verschlüsselungsschlüssel auf.

Verschlüsselungsschlüssel [sys_encryption_key]

Listet die verfügbaren Schlüssel und Schlüsselattribute auf.

Proxy-Verschlüsselungsschlüssel [sys_encryption_proxy_key]

Listet Proxy-Verschlüsselungsschlüssel auf.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit Edge Encryption installierte Eigenschaften

Edge Encryption fügt die folgenden Eigenschaften hinzu.

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

glide.edge.pattern.disallowed.chars

Eine Liste von Zeichen, die in Mustern nicht zulässig sind.

- **Typ**: eine Zeichenkette einer durch Komma getrennten Liste von Werten
- **Speicherort**: Tabelle „Systemeigenschaften“ [sys_properties]

glide.edge.pattern.min.size

Die minimal zulässige Mustergröße. Das Erlauben kleinerer Muster bedeutet, mehr Übereinstimmungen zu finden, was den Aufwand erhöht.

- **Typ**: Zahl
- **Standardwert**: 5
- **Speicherort**: Tabelle „Systemeigenschaften“ [sys_properties]

sn_edge_encryption.logging.destination

Wo Nachrichten protokolliert werden.

- **Typ**: Zeichenfolge
- **Standardwert**: Datei
- **Speicherort**: Tabelle „Systemeigenschaften“ [sys_properties]

sn_edge_encryption.logging.verbosity

Die zu verwendende Protokollierungsstufe.

- **Typ**: Zeichenfolge
- **Standardwert**: Info
- **Speicherort**: Tabelle „Systemeigenschaften“ [sys_properties]

sn_edge_encryption.encryption.proxy.buildtag

Die in Ihrer Instanz registrierte Proxy-Version.

- **Typ**: Zeichenfolge
- **Speicherort**: Tabelle „Systemeigenschaften“ [sys_properties]

sn_edge_encryption.cleartext.allowed

Bei „Wahr“ kann Klartext in einem verschlüsselten Feld gespeichert werden. Dies geschieht, wenn ein Benutzer auf die Instanz zugreift, ohne den Edge Encryption Proxy zu verwenden. Bei „Falsch“ verhindert das System, dass Klartext in einem verschlüsselten Feld gespeichert wird.

- **Typ**: Boolesch
- **Standardwert**: false
- **Speicherort**: Tabelle „Systemeigenschaften“ [sys_properties]

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Edge Encryption planen

Die erfolgreiche Implementierung von Edge Encryption erfordert Planung und Vorbereitung.

Beantworten Sie die folgenden Fragen bereits in der Planungsphase.

- Welche Felder sollen verschlüsselt werden?
- Welche Verschlüsselungstypen sollen verwendet werden?
- Wie viele Edge Encryption Proxys werden benötigt? Empfehlungen und Überlegungen finden Sie unter Umgebungsgröße Ihrer Edge Encryption anpassen.
- Wo befindet sich die MySQL-Datenbank, wenn ein ordnungserhaltender Verschlüsselungstyp oder ein Verschlüsselungsmuster verwendet werden soll?
- Welches Schlüsselmanagementsystem soll verwendet werden?

Systemadministratoren, Netzwerkadministratoren und Mitglieder des Sicherheitsteams haben unterschiedliche Aufgaben bei der Implementierung von Edge Encryption zu erfüllen.

- Systemadministratoren benötigen die Sicherheitsadministratorrolle. Der Systemadministrator muss:
  - Die Edge Encryption Proxy-Anwendung herunterladen.
  - Ein Edge Encryption Benutzerkonto für die Proxys einrichten, die zur Verbindung mit der Instanz verwendet werden sollen. Dem Benutzer muss die Rolle edge_encryption zugewiesen werden.
  - Die Verschlüsselungsschlüssel konfigurieren und die Standardschlüssel festlegen.
  - Edge Encryption auf der Instanz konfigurieren.
  - Verschlüsselungsaufträge planen.
  - Edge Encryption überwachen.
  - Verschlüsselungsregeln erstellen und bearbeiten.
- Ihr Netzwerkadministrator muss:
  - Die Edge Encryption Proxy-Anwendung installieren.
  - Die Netzwerkadressen für die Proxy-Server und die Proxy-Datenbank kennen, die zur Aufrechterhaltung der Verschlüsselungs- und Verschlüsselungsmuster verwendet wird.
  - Die Proxy-Datenbank installieren, die zur Aufrechterhaltung der Verschlüsselung und Verschlüsselungsmuster verwendet werden soll.
  - Die Proxy-Anwendung starten und stoppen.
  - Die Verschlüsselungsverwaltung durchführen.
  - Bestimmen, wie Benutzer zu Verschlüsselungs-Proxy-Anwendungen zugeordnet werden. Dies kann mit DNS-Einstellungen oder Routing-Regeln erfolgen und ist netzwerkspezifisch.
  - Mehrere Proxy-Server verwalten.
  - Load-Balancer-Pools und -Einstellungen konfigurieren.
- Ihr Sicherheitsadministrator muss die Verschlüsselungstypen festlegen, die jedem Feld zugewiesen werden sollen.

Edge Encryption – Systemanforderungen

Sie können die Edge Encryption-Proxy-Anwendung auf Servern oder virtuellen Computern ausführen, auf denen Microsoft Windows oder Linux ausgeführt wird. Damit eine optimale Leistung erzielt wird, stellen Sie sicher, dass Ihre Konfiguration diese Anforderungen erfüllt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Java-Anforderungen

Auf dem Hostcomputer, auf dem der Proxy-Server Edge Encryption installiert oder ausgeführt wird, muss eine unterstützte Version von Java installiert sein. Derzeit unterstützte Versionen sind Java 11.0.6 oder höher in der 11.x-Versionsserie

Hinweis: Java 8 wird ab dem Release Utah nicht mehr unterstützt. Aktualisieren Sie Ihre Umgebung mit dem Proxy Edge Encryption auf Java 11, bevor Sie versuchen, die Version Edge Encryption des Proxys [Utah zu installieren.

Hinweis: Java lässt Schlüssel mit unbegrenzter Stärke nicht automatisch zu. Sie müssen die Verwendung von AES 256-Bit-Verschlüsselung speziell aktivieren.

Unterstützung für OpenJDK

Now Platform unterstützt OpenJDK-Version 11.

Mindestkonfiguration für Proxy-Server

Ein Proxy-Server erfordert die folgende Mindestkonfiguration:

- Mindestens 4 GB Arbeitsspeicher pro Proxy-Server (für die meisten Bereitstellungen werden 6 GB empfohlen).

  Hinweis: Der Proxy-Server-Host muss mindestens 1 GB Arbeitsspeicher mehr aufweisen als der Proxy-Server. Der Proxy-Server-Host benötigt 1 GB zusätzlich für Betriebssystem-Services. Wenn Sie beispielsweise einen Proxy-Server zur Verwendung von 4 GB Arbeitsspeicher konfigurieren, müssen Sie mindestens 5 GB Arbeitsspeicher auf dem Proxy-Server-Host installieren.

  Da der Proxy-Server mindestens 4 GB Arbeitsspeicher benötigt, werden 32-Bit-JREs und 32-Bit-Betriebssysteme ab dem Release London nicht mehr unterstützt.

- CPU mit mindestens 3 GHz (4-Kern-CPU wird für eine optimale Leistung empfohlen).
- Mehrere einem Load Balancer nachgeschaltete Proxy-Server. Die Anzahl der benötigten Proxy-Server hängt von der Anzahl der Anwendungsknoten, der Anzahl der gleichzeitigen Benutzer und der Anzahl der für Failover-Zwecke benötigten Server ab. Weitere Informationen finden Sie unter Umgebungsgröße Ihrer Edge Encryption anpassen.
- Möglichkeit der Ausführung zusammen mit anderen Diensten, abhängig von der Serverauslastung und der Ressourcenverfügbarkeit.

Von Proxy-Servern unterstützte Systeme

Die folgenden Systeme werden unterstützt:

Unterstütztes System	Beschreibung
Windows Server 2012, 2012-R2, 2016 und 2019	• Virtuelle Maschinen oder physische Hardware • 64-Bit-Systeme

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterstütztes System	Beschreibung
Linux	• Virtuelle Maschinen oder physische Hardware • 64-Bit-Systeme Auf 64-Bit-Linux-Systemen muss die 32-Bit GNU C-Bibliothek (glibc) installiert werden. Der Installationsbefehl für CentOS lautet `yum install glibc.i686`.

Anforderungen an die Proxy-Server-Version

Halten Sie Ihre Edge Encryption -Proxy-Version mit Ihrer ServiceNow -Instanzversion synchron (gleicher Hauptrelease, z. B. Tokyo). Um Ausfallzeiten während des Upgradevorgangs zu vermeiden, ist der Edge Encryption -Proxy abwärts kompatibel. Es ist jedoch wichtig, so bald wie möglich ein Upgrade durchzuführen, um sicherzustellen, dass Benutzer Zugriff auf neue Funktionen und wichtige Fehlerbehebungen haben.

Verbindungsanforderungen des Proxy-Servers

Der Proxy-Server, auf dem die Edge Encryption-Anwendung ausgeführt wird, muss mit den Computern in Ihrem Netzwerk kommunizieren können. Stellen Sie sicher, dass der Proxy-Server über folgende Netzwerkprivilegien verfügt:

Netzwerkprivileg	Beschreibung
Firewallzugriff	Konfigurieren Sie alle Firewalls zwischen dem Proxy-Server und den Clientgeräten so, dass sie eine Verbindung zulassen. Wenn in Ihrem Netzwerk eine demilitarisierte Zone (DeMilitarized Zone, DMZ) verwendet wird, sodass Ihr lokales Netzwerk (LAN) um eine zusätzliche Sicherheitsebene erweitert wird, und Ihre Netzwerksicherheitsprotokolle den Portzugriff innerhalb des Netzwerks auf die DMZ beschränken, müssen Sie möglicherweise einen Proxy-Server auf einem Computer in der DMZ bereitstellen.
Netzwerkzugriff	Konfigurieren Sie jeden Client so, dass der Proxy-Server eine Verbindung mit ihm herstellen kann. Wenn Sie aufgrund der Netzwerksicherheit keine neuen Computer konfigurieren können, die eine Verbindung zu den Clients herstellen können, installieren Sie den Proxy-Server auf einem vorhandenen Computer mit Verbindungsberechtigungen.
Instanz-Zugriff	Stellen Sie sicher, dass der Proxy-Server über einen Netzwerkzugriff auf die Instanz verfügt. Stellen Sie sicher, dass Sie das vom Proxy-Server verwendete Netzwerk so konfigurieren, dass Datenverkehr über den TCP-Port 443 zugelassen wird.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Netzwerkprivileg	Beschreibung
Netzwerk-Konto	Installieren Sie den Proxy-Server mit dem Konto eines lokalen oder Domänenadministrators.

Anforderungen an das Datenbanksystem für die Ordnungserhaltung und die Tokenisierung

Für die ordnungserhaltende Verschlüsselung und das Verschlüsselungsmuster müssen Sie eine Oracle MySQL-Datenbank für den Edge Encryption-Proxy-Server konfigurieren. Bei einer ordnungserhaltenden Verschlüsselung kann ein beliebiger Vergleichsvorgang direkt auf verschlüsselte Daten angewendet werden, ohne dass die Daten erst entschlüsselt werden müssen. Mit Verschlüsselungsmustern können Sie Zeichenfolgenmuster durch Token ersetzen (sog. Tokenisierung), bevor sie an die Datenbank gesendet und darin gespeichert werden. Verwenden Sie aufgrund der Größe der MySQL-Datenbank einen dedizierten Proxy-Server, um die Datenbank für die ordnungserhaltende Verschlüsselung und die Tokenisierung auszuführen.

Die Mindestanforderungen für das Datenbanksystem umfassen:

MySQL-Datenbank	Anforderung
Version	MySQL-Datenbankversionen 5.7 und 8.0 **Hinweis:** Die MySQL-Versionen 5.5 und 5.6 werden nicht mehr getestet und haben das Ende des Supports erreicht.
BS	64-Bit-Systeme
CPU	CPU mit mindestens 2 GHz (4-Kern-CPU wird für eine optimale Leistung empfohlen)
RAM	16 GB
Datenträger	Storage Area Network (SAN) oder lokaler Speicher (RAID 10 empfohlen)
Größe	Bestimmt durch die Anzahl potenzieller Datensätze multipliziert mit der Datensatzgröße. Weitere Informationen finden Sie unter Die Größe der Datenbank für die Ordnungserhaltung und Tokenisierung berechnen.
Konfiguration	Cluster für hohe Verfügbarkeit. Wenn Sie nicht sicher sind, wie Sie Ihren MySQL-Server konfigurieren, wenden Sie sich an MySQL , um Informationen zur Konfiguration zu erhalten.

Umgebungsgröße Ihrer Edge Encryption anpassen

Die Auswahl der Anzahl von Proxy-Servern für Ihre Umgebung ist von hoher Bedeutung. Berücksichtigen Sie die Anzahl der Benutzer, die Redundanzanforderungen und die akzeptable Latenzzeit.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Redundanz

Verwalten Sie redundante Proxy-Server für den Fall eines Hardwarefehlers. Proxy-Server sollten einem Load Balancer nachgeschaltet sein, um einen funktionalen Pfad für alle Benutzer bereitzustellen, wenn ein Proxy-Server nicht erreichbar ist. Stellen Sie sicher, dass immer mindestens zwei Proxy-Server verfügbar sind.

Größe

Die Größe bezieht sich auf die Anzahl der Proxy-Server, die erforderlich sind, um zusätzliche Latenzzeiten zu vermeiden, die durch die Verschlüsselung von Daten entstehen. Je nach Verwendung möchten Sie möglicherweise die Latenzzeit reduzieren, indem Sie zusätzliche Proxy-Server hinzufügen. Wenn beispielsweise regelmäßige Massenverschlüsselungen ausgeführt werden, fügen Sie zur Handhabung der Last zusätzliche Proxy-Server hinzu oder führen Sie die Massenverschlüsselungen bei geringer Benutzerlast durch. Außerdem beeinflusst die Hardware, auf der der Proxy-Server ausgeführt wird, die Leistung und Latenz. Proxy-Server, die auf Hardware mit schnelleren CPUs, mehr CPUs und mehr RAM laufen, haben einen höheren Durchsatz als langsamere, begrenzte Systeme.

In den folgenden Richtlinien wird davon ausgegangen, dass der Proxy-Server mindestens die Mindesthardwareanforderungen erfüllt. So bestimmen Sie die Anzahl der Proxy-Server:

- Erwägen Sie, für jeweils zwei Anwendungsknoten in der Instanz einen Proxy-Server einzurichten.
- Richten Sie aus Gründen der Redundanz mindestens zwei Proxy-Server hinter einem Load Balancer ein.
- Fügen Sie für jeweils 500 gleichzeitige Benutzer einen zusätzlichen Proxy-Server hinzu.
- Fügen Sie je nach gewünschter Redundanz weitere Proxy-Server für das Failover hinzu.

Für eine Instanz mit 2.000 Benutzern sollten Sie beispielsweise mindestens fünf Proxy-Server einem Load Balancer nachgeschaltet sein. Diese Berechnung umfasst einen Proxy-Server für jeweils 500 Benutzer und einen zusätzlichen Proxy-Server für Failover. Bestimmen Sie im Voraus, wann Sie sich einem Schwellenwert von 500 Benutzern nähern, und platzieren Sie einen anderen Proxy-Server im Load-Balancer-Pool.

Load Balancers

Um Anforderungen zu verteilen und die Antwortzeit des Servers zu verbessern, verteilen Sie Proxy-Server in einem Load-Balancer-Pool. Konfigurieren Sie Load Balancer für die Verwendung nach der Methode der „wenigsten Verbindungen“. Diese Methode verbindet Anfragen mit dem Proxy-Server mit den wenigsten aktiven Verbindungen, wodurch die Überlastung eines einzelnen Proxys verhindert wird.

CPU-Auslastung

Da Datenverschlüsselung und Tokenisierung CPU-intensive Operationen erfordern, sind CPU-Spitzen während der Datenverschlüsselung normal und zu erwarten. Wenn die CPU-Auslastung mehrere Minuten lang über 80 % liegt, bedeutet dies wahrscheinlich, eine zu hohe Auslastung des Proxy-Servers. In diesem Fall erhöht sich die Latenz für den Zeitraum, in dem die CPU-Auslastung hoch ist. Wenn die Latenz bestehen bleibt, kann das Hinzufügen eines weiteren Proxy-Servers zur Verringerung der Latenz beitragen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Arbeitsspeicher

Der Proxy-Server muss über mindestens 4 GB RAM verfügen (empfohlen sind 6 GB). Legen Sie die anfänglichen und oberen Speichergrenzen des Proxy-Servers auf die empfohlenen Einstellungen fest.

Die Größe der Datenbank für die Ordnungserhaltung und Tokenisierung berechnen

Wenn Sie ordnungserhaltende Verschlüsselung oder Verschlüsselungsmuster verwenden, bestimmen Sie die Größe Ihrer MySQL-Datenbank, indem Sie die Anzahl der potenziellen Datensätze mit der Datensatzgröße multiplizieren.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Verwenden Sie eine dedizierte Maschine, um die Datenbank für die Ordnungserhaltung und die Tokenisierung auszuführen. Führen Sie die Datenbank nicht auf derselben Hardware wie der Proxy-Server aus.

Prozedur

1. Bestimmen Sie die potenzielle Anzahl von Datensätzen, die Felder enthalten können, die mit auftragserhaltender Verschlüsselung verschlüsselt sind.
   a. Multiplizieren Sie die Anzahl der Verschlüsselungskonfigurationen mithilfe der auftragserhaltenden Verschlüsselung mit der Anzahl der Datensätze, auf die jede Konfiguration angewendet wird.
   b. Um Wachstum zu ermöglichen, multiplizieren Sie das Ergebnis mit drei.
2. Multiplizieren Sie das Ergebnis aus Schritt 1 mit 1.536.
   1.536 ist die durchschnittliche Größe eines Datensatzes in Bytes.
3. Wenn Sie Verschlüsselungsmuster verwenden, führen Sie die Schritte 1 und 2 für Datensätze mit Token aus, und fügen Sie das Ergebnis zur Summe hinzu.

Ergebnisse
Der berechnete Wert ist die empfohlene Größe in Bytes für Ihre auftragserhaltende und tokenisierende Datenbank.

Edge Encryption – Einschränkungen

Edge Encryption wirkt sich auf Systemfunktionen aus. Bewerten Sie sorgfältig die Auswirkungen der Verschlüsselung eines Feldes.

Feldtypeinschränkungen

Sie können nur die folgenden Feldtypen verschlüsseln:

- Datum
- E-Mail
- Datum/Uhrzeit
- HTML
- IP-Adresse
- Journal

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Journaleingabe
- Mehrzeiliger Text
- Einzeiliger Text
- Zeichenfolge
- URL

Die folgenden Feldtypen können Sie nicht verschlüsseln:

- Auswahlfelder
- Virtuelle Felder
- Felder in Systemtabellen mit Ausnahme bestimmter Felder in sys_user
- Systemfelder in Tabellen
- Zahlenfelder oder Felder, die mit einem Schema für die automatische Nummerierung verbunden sind
- Alle anderen oben nicht aufgeführten Feldtypen

Zusätzliche Einschränkungen:

- Wenn ein Journalfeld verschlüsselt ist, ist die **Schaltfläche „** Veröffentlichen“ inaktiv, auch wenn mehrere Journalfelder vorhanden sind und nur eines dieser Felder verschlüsselt ist.
- Verschlüsselte Felder sind in den Filterfeldern **„Gehe zu“** und „Header“ nicht verfügbar.
- Bei der Verschlüsselung von Feldern, die als Index verwendet werden, können Sie nur die Verschlüsselungstypen für die Ordnungserhaltung und Gleichstellungserhaltung verwenden. Indizierte Felder können nicht mit dem Standardverschlüsselungstyp verschlüsselt werden.

Weitere Informationen finden Sie unter Feldtypen .

Einschränkungen für das Filtern und Suchen

Standardverschlüsselung

Wenn Sie ein Feld vom Typ Zeichenfolge, Datum, Datum/Uhrzeit oder URL mit einer Feldkonfiguration für eine Standardverschlüsselung als linken Operanden in einem Filter auswählen, sind keine Filteroptionen verfügbar.

Gleichstellungserhaltende Verschlüsselung

Wenn Sie ein Feld vom Typ Zeichenfolge, Datum, Datum/Uhrzeit oder URL mit einer Feldkonfiguration für die gleichstellungserhaltende Verschlüsselung als linken Operanden in einem Filter auswählen, sind folgende Operatoren verfügbar:

- **ist**
- **ist nicht**
- **ist leer**
- **ist nicht leer**

Ordnungserhaltende Verschlüsselung

Wenn Sie ein Zeichenfolgenfeld mit einer verschlüsselten Feldkonfiguration zur Beibehaltung der Reihenfolge als linken Operanden in einem Filter auswählen, sind neben **ist**, **ist nicht**, **ist leer**und **ist nicht leer**die folgenden Operatoren verfügbar:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **größer als**
- **weniger als**

Wenn Sie ein Feld vom Typ Datum oder Datum/Uhrzeit mit einer verschlüsselten Feldkonfiguration zur Beibehaltung der Reihenfolge als linken Operanden in einem Filter auswählen, sind neben **ist**, **ist nicht**, **ist leer**und **ist nicht leer**die folgenden Operatoren verfügbar:

- **nach**
- **vor**
- **nach oder am**
- **vor oder am**

Auswahl von Datum sowie von Datum/Uhrzeit

Verwenden Sie für Datumsfelder die Datumsauswahl, um das Datum anzugeben:



Verwenden Sie für Felder vom Typ „Datum/Uhrzeit“ die Datums- und Uhrzeitauswahl, um Datum und Uhrzeit anzugeben: Datums-



Listen-Bedingungsfilter

Die Optionen **Übereinstimmungen anzeigen** und **Herausfiltern** werden in Listen unterstützt. Nur genaue Übereinstimmungen werden zurückgegeben oder herausgefiltert.

Hinweis: Das Hinzufügen von verschlüsselten Feldern in Bedingungsfiltern wird in Skripts wie UI-Richtlinien und Business-Regeln unterstützt.

Konfigurationseinschränkungen

Einschränkungen und Verhalten von Verschlüsselungskonfigurationen:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Nachdem Sie der Konfigurationstabelle Edge Encryption ein Feld hinzugefügt haben, können Sie den Konfigurationsdatensatz nicht löschen. Wenn Sie ein Feld nicht mehr verschlüsseln möchten, deaktivieren Sie den Datensatz in der Edge Encryption-Konfigurationstabelle und planen Sie einen Verschlüsselungsauftrag zum Entschlüsseln der Daten.
- Wenn ein Feld in einer übergeordneten Tabelle für die Verschlüsselung markiert ist, wird das Feld auch in allen vererbten Tabellen verschlüsselt. Wenn beispielsweise das Feld **Kurzbeschreibung** in der Aufgabentabelle verschlüsselt ist, wird der Inhalt des Felds **Kurzbeschreibung** in der Incident-Tabelle verschlüsselt.
- Wenn ein von einer übergeordneten Tabelle geerbtes Feld als verschlüsselt markiert ist, kann das Feld in der übergeordneten Tabelle nicht verschlüsselt werden. Wenn beispielsweise die **Kurzbeschreibung** in der Incident-Tabelle als verschlüsselt markiert ist, kann die **Kurzbeschreibung** in der Aufgabentabelle nicht verschlüsselt werden. In diesem Beispiel können Sie die **Kurzbeschreibung** in der Problemtabelle verschlüsseln.
- Wenn ein Feld mit einer definierten Verschlüsselungskonfiguration in ein beliebiges Format exportiert wird, enthält die Ausgabe auch dann verschlüsselte Werte, wenn sie über den Proxy-Server exportiert werden.
- Sie können keine Daten in ein Feld importieren, für das eine Verschlüsselungskonfiguration definiert ist.
- Sie können geerbte Felder vom Typ „Datum“ und „Datum/Uhrzeit“ nicht verschlüsseln. Felder vom Typ „Datum“ oder „Datum/Uhrzeit“, die von einer übergeordneten Tabelle geerbt werden, werden nicht in der Dropdown-Liste „ **Spalte** “ aufgeführt, und Sie können für diese Felder keine Verschlüsselungskonfigurationen für Datum oder Datum/Uhrzeit erstellen.
- Sie können ein Feld vom Typ Zeichenfolge oder URL nur von einer übergeordneten Tabelle oder einer untergeordneten Tabelle verschlüsseln, nicht jedoch von beiden.

Instanzeinschränkungen

Auswirkungen der Verwendung von Edge Encryption auf die Instanz:

- Back-End-Logik kann keine verschlüsselten Daten verarbeiten. Wenn die Instanz verschlüsselte Daten enthält, werden Business-Regeln, Back-End-Skripts oder Back-End-Funktionen, die auf der Auswertung der Daten im verschlüsselten Feld beruhen, nicht ordnungsgemäß ausgeführt.

  Hinweis: Daten, die mit gleichstellungserhaltender oder ordnungserhaltender Verschlüsselung verschlüsselt sind, bestehen weiterhin Äquivalenzprüfungen, wenn sie mit einem identischen verschlüsselten Wert verglichen werden.

- Da die E-Mail-Verarbeitung von den E-Mail-Systemen direkt an die Instanz erfolgt und nicht über den Edge-Proxy geleitet werden kann, können Daten, die per E-Mail gesendet oder gesendet werden, vom Edge-Proxy nicht verschlüsselt oder entschlüsselt werden.
  - Daten und Anhänge in eingehenden E-Mails werden nicht verschlüsselt.
  - Daten und Anhänge in ausgehenden E-Mails bleiben verschlüsselt und können nicht entschlüsselt werden.
- Auf dem Server ausgeführte Skripts können keine verschlüsselten Daten ändern.
- Globale Suche wird nicht unterstützt. Da die globale Suche versucht, sowohl verschlüsselte als auch Klartextdaten zu durchsuchen, sind die Ergebnisse möglicherweise nicht wie erwartet.
- Verschlüsselte Daten können nicht kopiert und in einen Datensatz eingefügt werden, in dem das Feld nicht verschlüsselt ist.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Abhängig vom ausgewählten Verschlüsselungstyp wird die Benutzeroberflächenfunktionalität für die verschlüsselten Felder reduziert. Beispielsweise kann die Möglichkeit zum Vergleichen, Gruppieren, Sortieren und Suchen beeinträchtigt werden Generell gilt: Je stärker die gewählte Verschlüsselung, desto mehr Funktionalität wird eingeschränkt.
- Abgesehen von Java KeyStore, SafeNet und Unbound Technology wird keine Verwaltung von Software- oder Hardware-Verschlüsselungsschlüsseln von Drittanbietern unterstützt.
- Obwohl mehrere mit einer einzelnen Instanz verbundene Proxyserver unterstützt werden, ist die Verwaltung und Überwachung von Verschlüsselungs-Proxy-Clustern nicht verfügbar. Jeder Proxy muss separat verwaltet werden.
- Systemkonfigurationen wie Auslastung und Anzahl der verschlüsselten Felder können sich auf die Leistung der verschlüsselten Felder auswirken.
- Der Edge Encryption Proxy-Server kann nur eine Verbindung zu einer einzelnen Instanz herstellen.
- Wenn Ihre Instanz eine Oracle-Datenbank verwendet und das Zeichenfolgenfeld, das Sie für die Verschlüsselung markieren, länger als 2925 Zeichen ist, kann dieses Feld nicht sortiert werden, auch wenn die Verschlüsselung mit Reihenfolgeerhaltung ausgewählt ist.
- Wenn Ihre Instanz eine Oracle-Datenbank verwendet, ist Unicode AL32UTF8 der einzige unterstützte Zeichensatz.
- Verschlüsselte Daten können nicht in Berichten verwendet werden.
- Edge Encryption kann nicht mit Datenarchivierung verwendet werden.

Edge Encryption wird installiert

Sie können einen Edge Encryption Proxy manuell oder mithilfe des interaktiven Installers Edge Encryption installieren.

Java-Anforderungen

Auf dem Hostcomputer, auf dem der Proxy-Server Edge Encryption installiert oder ausgeführt wird, muss eine unterstützte Version von Java installiert sein. Derzeit unterstützte Versionen sind Java 11.0.6 oder höher in der 11.x-Versionsserie

Hinweis: Java 8 wird ab dem Release Utah nicht mehr unterstützt. Aktualisieren Sie Ihre Umgebung mit dem Proxy Edge Encryption auf Java 11, bevor Sie versuchen, die Version Edge Encryption des Proxys [Utah zu installieren.

Proxy-Server installieren

Das Installieren von Edge Encryption beinhaltet diese Schritte.

- Installieren Sie die Edge Encryption Proxy-Anwendung auf einem Server in Ihrem Netzwerk mithilfe des interaktiven oder des manuellen Installationsprogramms.
- Generieren Sie das RSA-Schlüsselpaar für die digitale Signatur von Verschlüsselungskonfigurationen und Verschlüsselungsregeln.
- Installieren Sie die Java Cryptography Extension (JCE), wenn Sie die AES 256-Verschlüsselung verwenden möchten.
- Wenn Sie eine sichere SSL-Verbindung verwenden, beziehen Sie ein Serverzertifikat und importieren Sie es in den Java KeyStore.
- Richten Sie Ihren Schlüsselspeicher und den Verschlüsselungsschlüssel ein.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn ordnungserhaltende Verschlüsselungstypen oder Verschlüsselungsmuster verwendet werden sollen, richten Sie eine MySQL-Datenbank auf einem Computer in Ihrem Netzwerk ein.
- Stellen Sie die gewünschten Eigenschaften ein. Eigenschaften befinden sich in der Konfigurationsdatei `edgeencryption.properties`.
- Legen Sie fest, dass ein Proxy-Server eine vertrauenswürdige Quelle ist, sodass Edge Encryption Anforderungen von diesem Proxy-Server verarbeiten kann.

Zugriff auf den Proxy-Server

Verweisen Sie nach Abschluss der Installation den Browser jedes Benutzers auf den Edge Encryption Proxy mit dem URL-Format: `<host>:<port>`. Werte werden durch die Host- und Port-Eigenschaften in der Datei `edgeencryption.properties` bestimmt.

Ein Beispiel mit folgenden Werten:

Eigenschaft	Beispielwert
edgeencryption.proxy.host	hostname.mycompany.com
edgeencryption.proxy.http.port	8081

Ein Client greift unter der folgenden Adresse auf den Proxy-Server zu: `http://hostname.mycompany.com:8081/`.

Hinweis: DNS-Einstellungen und Routing-Regeln können verwendet werden. Host- und Portwerte werden von Ihrem Netzwerkadministrator festgelegt.

Edge Encryption anfordern

Das Edge Encryption Plugin (com.glide.edgeencryption) ist als separates Abonnement erhältlich.

Vorbereitungen

Wenden Sie sich an Ihren ServiceNow-Kundenbetreuer, um ein Abonnement zu erwerben. Der Account Manager sorgt im Allgemeinen innerhalb weniger Tage für die Aktivierung des Plugins in der Produktionsinstanz bzw. untergeordneten Produktionsinstanz Ihrer Organisation.

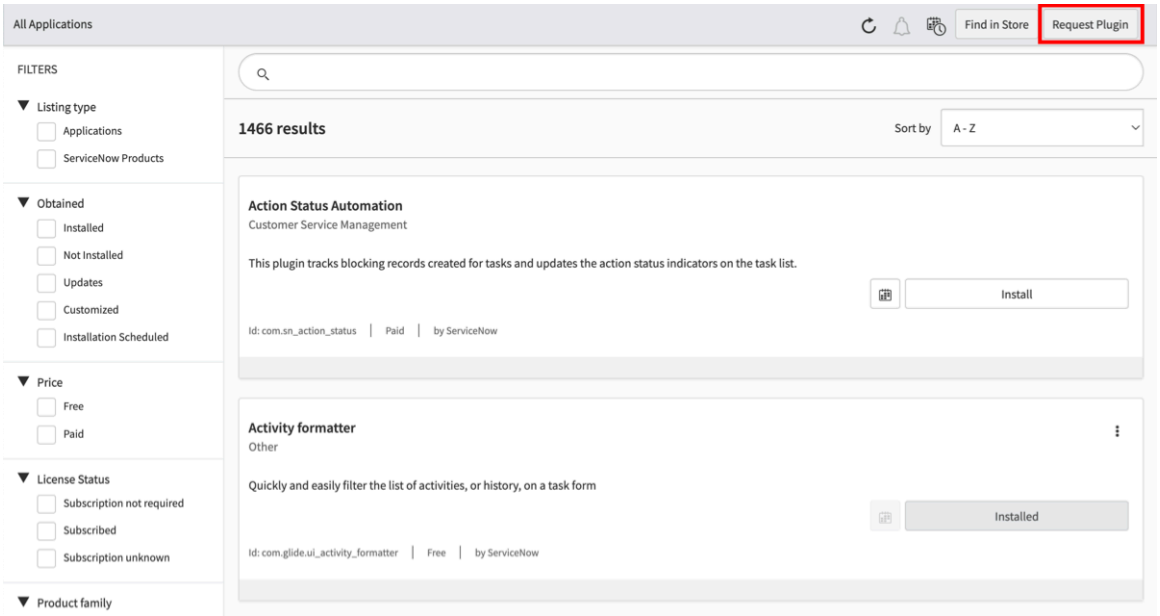
Wenn Sie keinen Account Manager haben, die Aktivierung nach dem Kauf verzögern oder das Produkt in einer Test- und Entwicklungsumgebung kostenlos testen möchten, führen Sie die folgenden Schritte aus.

Erforderliche Rolle: keine

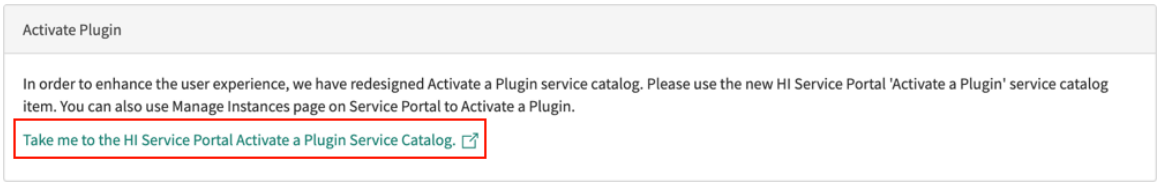
Prozedur

1. Navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Klicken Sie auf der Seite „Alle Anwendungen“ auf **Plugin anfordern**, um das Formular **Plugin aktivieren** auf Now Support zu öffnen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Wählen Sie unter Now Support den Link aus, um auf Now Support Serviceportal Servicekatalog zuzugreifen.



4. Wählen Sie Ihre Instanz aus.
5. Wählen Sie **Aktionen > Plugin aktivieren** aus.
6. Geben Sie im Formular **Plugin aktivieren** die folgenden Informationen an.

Formular „Plugin anfordern“

Feld	Beschreibung
What is your target instance (Ihre Zielinstanz)	Instanz, auf der das Plugin aktiviert werden soll.
Which plugin would you like to activate (Welches Plugin möchten Sie aktivieren?)	Name des zu aktivierenden Plugins **Hinweis:** Wenn das System das gewünschte Plugin nicht auflistet oder wenn Sie das Plugin auf einer OEM- oder lokalen Instanz aktivieren, aktivieren Sie das Kontrollkästchen **Plugin I'm looking for is not listed (Gesuchtes Plugin ist nicht aufgelistet)**, und geben Sie dann den Namen des Plugins ein.

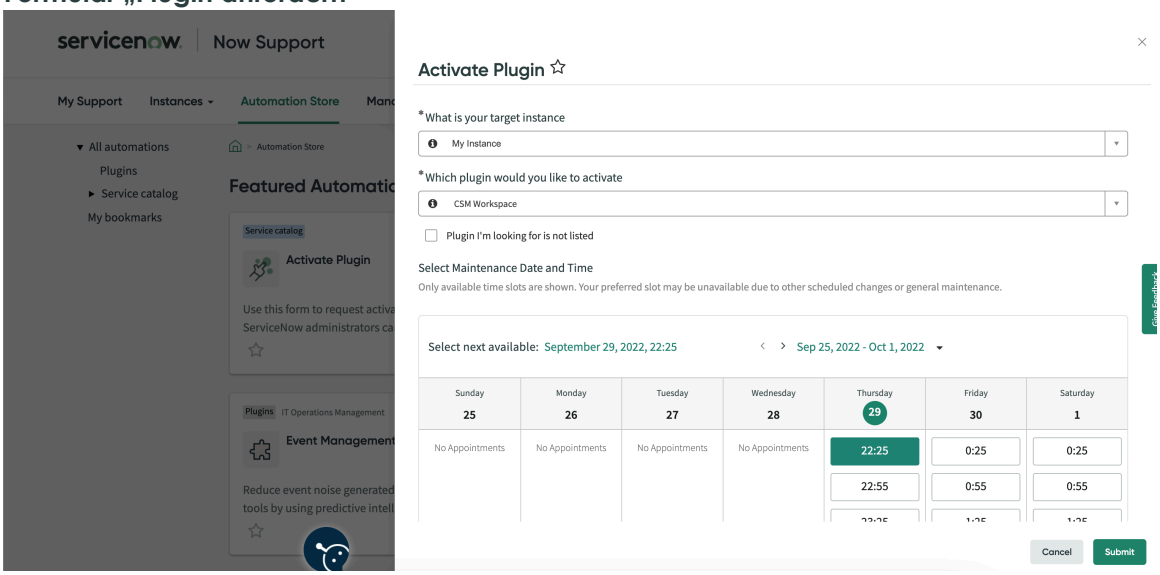
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Select Maintenance Date and Time (Datum und Uhrzeit der Wartung)	Datum und Uhrzeit zum Aktivieren des Plugins. **Hinweis:** Plugins werden in der pazifischen Zeitzone jeden Werktag in zwei Batches aktiviert, einmal am Morgen und einmal am Abend. Wenn das Plugin zu einem bestimmten Zeitpunkt aktiviert werden muss, geben Sie die Anforderung bei **Grund/ Kommentare** ein.

Example

Betrachten Sie beispielsweise das folgende Formular, um das Plugin „CSM Workspace“ in einer Instanz mit dem Namen „My Instance“ zu aktivieren.

Formular „Plugin anfordern“



7. Wählen Sie **Absenden**.
   Weitere Informationen zum Anfordern eines Plugins finden Sie im Artikel Plugin aus dem Servicekatalog anfordern [KB0751715] in der Now Support Knowledge Base.

Benutzerkonto für die Edge Encryption einrichten

Die Edge Encryption Proxys stellen als Benutzer eine Verbindung mit der Instanz her, um Informationen zur Verschlüsselungskonfiguration zu erhalten und zu aktualisieren. Erstellen Sie zu diesem Zweck ein Benutzerkonto, und weisen Sie dem Benutzer die Edge Encryption-Rolle zu.

Vorbereitungen

Das Edge Encryption Plugin muss installiert sein, bevor Sie die Rolle zuweisen können.

Erforderliche Rolle: admin

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Erstellen Sie auf Ihrer ServiceNow-Instanz ein Benutzerkonto, das von den Edge Encryption Proxy-Anwendung verwendet werden soll.
2. Weisen Sie dem Benutzer die edge_encryption-Rolle zu.

Proxy-Server für die Edge Encryption herunterladen

Laden Sie die Edge Encryption Proxy-Server-Anwendung aus Ihrer Instanz herunter, und kopieren Sie die Datei auf jeden Computer, auf dem der Edge Encryption Proxy-Server ausgeführt werden soll.

Vorbereitungen

Bevor Sie dieses Verfahren starten, muss das Edge Encryption Plugin auf Ihrer Instanz installiert und aktiviert sein.

Hinweis: Der Edge Encryption -Proxy wird offiziell nur von Oracle JRE unterstützt.

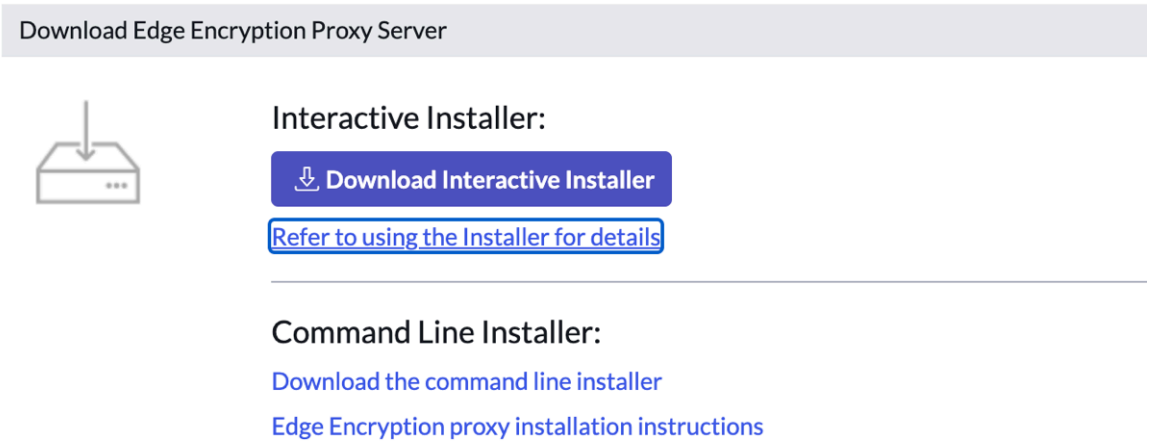
Erforderliche Rolle: security_admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Installation und Downloads** > **Downloads**an.
2. Um das interaktive Installationsprogramm zu verwenden, klicken Sie auf **Interaktives Installationsprogramm herunterladen**.

   Wenn Sie den Proxy-Server manuell installieren, wählen Sie die Betriebssystemversion für Ihren Proxy-Server aus.



Hinweis: Da der Proxy-Server mindestens 4 GB Arbeitsspeicher zum Ausführen benötigt, werden 32-Bit-JREs und 32-Bit-Betriebssysteme ab dem Release Washington DC nicht mehr unterstützt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Kopieren Sie das Installationsprogramm auf jeden Computer, auf dem der Edge Encryption Proxy-Server ausgeführt werden soll.

   Hinweis: Wenn Sie den Proxy-Server Edge Encryption manuell installieren, kopieren Sie die ZIP-Datei auf alle Computer, auf denen der Proxy-Server Edge Encryption ausgeführt werden soll.

Nächste Maßnahme

Nach dem Herunterladen des Edge Encryption Installationsprogramms, Den Proxy-Server für die Edge Encryption mithilfe des interaktiven Installationsprogramms installieren. Bei manueller Installation, Den Proxy-Server für die Edge Encryption mithilfe des Befehlszeilen-Installationsprogramms installieren.

Den Proxy-Server für die Edge Encryption mithilfe des interaktiven Installationsprogramms installieren

Installieren Sie den Edge Encryption Proxy-Server auf einem Windows- oder Linux-Computer mit dem interaktiven Installationsprogramm.

Vorbereitungen

Hinweis: SafeNet KeySecure-Keystore-Dateien werden vom Edge Encryption Installationsprogramm nicht unterstützt. So verwenden Sie einen SafeNet KeySecure-Keystore: Den Proxy-Server für die Edge Encryption mithilfe des Befehlszeilen-Installationsprogramms installieren.

Das Edge Encryption Plugin muss in Ihrer Instanz installiert und aktiviert sein, bevor Sie dieses Verfahren starten. Stellen Sie sicher, dass Java Version 11.0.6 oder höher auf dem Computer installiert ist, auf dem das Installationsprogramm Edge Encryption ausgeführt wird.

Erforderliche Rolle:

- security_admin auf Ihrer ServiceNow Instanz
- Lokaler oder Domänenadministrator auf einem Windows-Host
- Service-Benutzer mit vollem Dateisystemzugriff auf einem Linux-Host

Warum und wann dieser Vorgang ausgeführt wird

Nach der Installation eines neuen Proxy-Servers können Sie das Installationsprogramm erneut zur Durchführung von Tests ausführen, um Probleme bei der Installation zu erkennen oder die aktuellen Einstellungen zu ändern. Folgende Optionen stehen zur Verfügung:

- **Neu installieren**: Installieren Sie einen neuen Proxy-Server.
- **Installation überprüfen**: Führen Sie Tests durch, um Probleme bei einer früheren Installation zu erkennen und zu beheben.
- **Vorhandene neu installieren**: Führen Sie Tests durch, um Probleme in einer früheren Installation zu erkennen und zu beheben und vorhandene Einstellungen anzuzeigen oder zu ändern.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn Sie den Proxy-Server auf einem Linux-Computer an einem privilegierten Port (Port 80 oder 443) installieren, müssen Sie das Installationsprogramm als Root-Benutzer mit vollem Dateisystemzugriff ausführen. Um den Dateisystemzugriff nach der Installation des Proxy-Servers einzuschränken, können Sie die SetUID-Funktion im Proxy-Installationsprogramm verwenden. Um diese Funktion zu aktivieren, starten Sie das Installationsprogramm als „Root“ oder „Sudo Root“. Wenn Sie vom Installationsprogramm dazu aufgefordert werden, geben Sie den Benutzernamen und die Benutzergruppe eines nicht privilegierten Benutzers an. Der Proxy-Server wird mit den Dateisystemberechtigungen des angegebenen Benutzers installiert. Sie können diesen Schritt überspringen, um die Standardinstallation mit Root-Berechtigungen fortzusetzen.

Prozedur

Verwenden Sie das Installationsprogramm, um mehrere Proxys für Ihre Instanz auf mehreren Computern zu installieren. Stellen Sie dabei sicher, dass die folgenden Kriterien zutreffen:

- Alle Proxys müssen über dieselben Verschlüsselungsschlüssel und das gleiche RSA-Schlüsselpaar verfügen, mit dem Verschlüsselungskonfigurationen und -regeln digital signiert werden.
- Der Verschlüsselungsschlüssel muss der in der Instanz konfigurierte Standardschlüssel sein.
- Wenn eine Proxy-Datenbank als Teil der Installation eingerichtet wird, müssen alle Proxys dieselbe Proxy-Datenbank verwenden.

  Möglicherweise benötigen Sie eine Proxy-Datenbank für die gleichstellungserhaltende Verschlüsselung, die ordnungserhaltende Verschlüsselung oder Tokenisierung. Wenn keine dieser Funktionen verwendet wird, benötigen Sie keine Proxy-Datenbank.

Nächste Maßnahme

Informationen zur Verwendung von NVDA, einer Sprachausgabe für Assistive Technology zum Lesen von bedienungsfreundlichen Java-Anwendungen für Tastaturbenutzer, finden Sie unter 64-Bit-Host für Windows konfigurieren, um 32-Bit-NVDA mit Java-Anwendungen zu verwenden .

Legen Sie nach der Installation des Proxyservers Edge Encryptiondas anfängliche Arbeitsspeicherlimit des Proxy-Servers und das obere Arbeitsspeicherlimit des Proxy-Servers fest.

Den Edge Encryption Proxy-Server (interaktives Installationsprogramm) installieren

Installieren Sie den Edge Encryption Proxy auf einem Windows- oder Linux-Computer.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Den Proxy-Server für die Edge Encryption herunterladen.
2. Öffnen Sie das Edge Encryption Proxy-Installationsprogramm.

   Hinweis: Bei der Installation auf einem Windows-Computer müssen Sie das Installationsprogramm als Administrator ausführen.

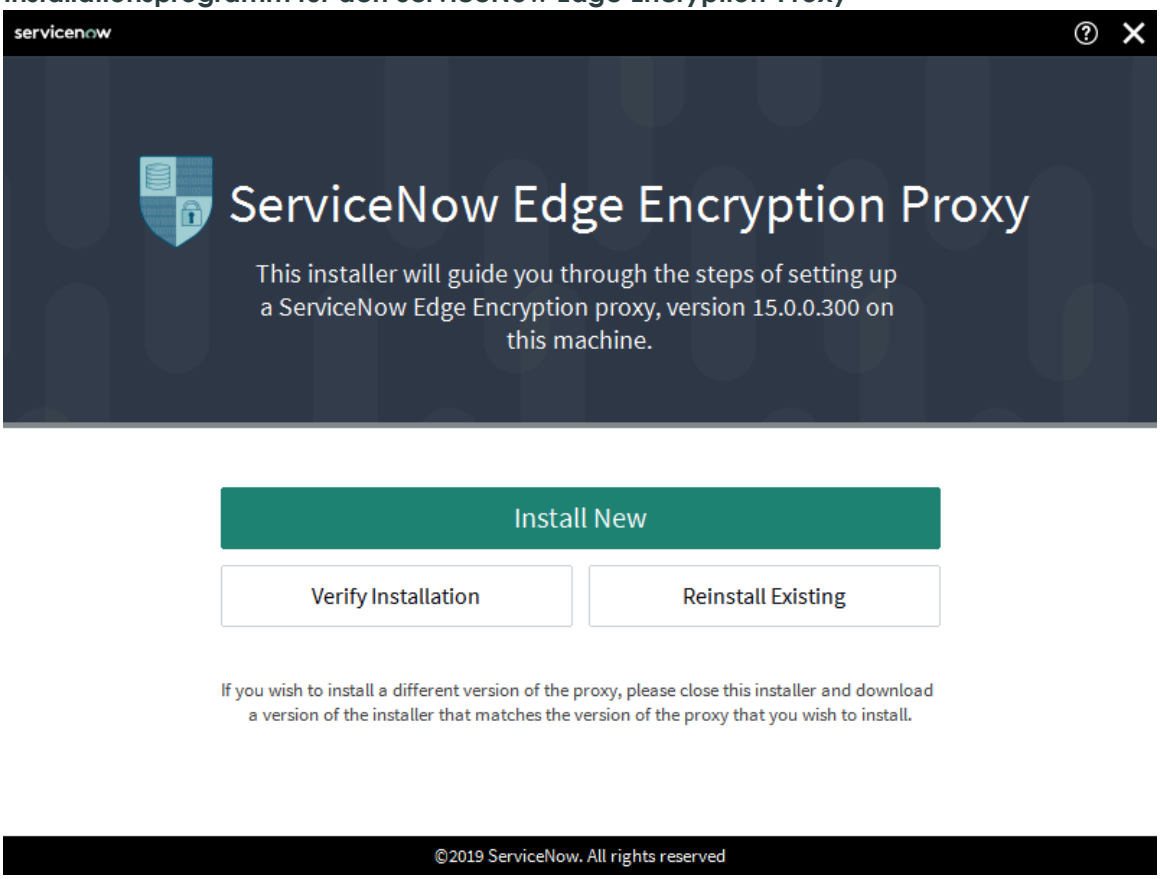
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Um das Installationsprogramm als Administrator auf einem Windows-Computer auszuführen, klicken Sie mit der rechten Maustaste auf die Eingabeaufforderung, und wählen Sie **Als Administrator ausführen**.

b. Navigieren Sie in der Befehlszeile zu dem Verzeichnis, in dem sich die heruntergeladene JAR-Datei befindet.

c. Führen Sie den folgenden Befehl aus: `java -jar <Dateiname>.jar`.

Installationsprogramm für den ServiceNow Edge Encryption-Proxy



3. Um einen neuen Proxy-Server zu installieren, wählen Sie **Neu installieren**.
Wenn bereits ein Proxy installiert ist, können Sie das Installationsprogramm folgendermaßen ausführen:

- **Installation überprüfen**: Führen Sie Tests durch, um Probleme bei einer früheren Installation zu erkennen und zu beheben.
- **Vorhandene neu installieren**: Führen Sie Tests durch, um Probleme in einer früheren Installation zu erkennen und zu beheben und vorhandene Einstellungen anzuzeigen oder zu ändern.

4. Konfigurieren Sie **Installationsort** und **ServiceNow-Zielinstanz**.

a. Klicken Sie **Durchsuchen**, um einen Installationsort zu wählen, oder geben Sie manuell einen Installationspfad ein.

b. Geben Sie die URL der ServiceNow Zielinstanz ein.
Geben Sie das Protokoll und die Portnummer an.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Example
`https://example.servicenow.com:443`

c. Geben Sie den Benutzernamen und das Passwort für einen Benutzer mit der Rolle „edge_encryption“ auf der ServiceNow Zielinstanz ein.

5. Klicken Sie auf **Weiter**.
6. Konfigurieren Sie die **Verbindungseinstellungen** und **Proxy-Einstellungen**.

Einstellung	Beschreibung
Proxy-Host	Vollständig qualifizierter Domänenname des Computers, auf dem Sie den Proxy-Server installieren. **Hinweis:** Klicken Sie auf **FQDN erkennen**, um nach dem vollständig qualifizierten Domänennamen des Computers suchen und das Feld **Proxy-Host** automatisch auszufüllen. Zusammen mit dem Port definiert diese Eigenschaft die URL, die der Client für den Zugriff auf den Proxy-Server verwendet.
HTTP-Port	Port auf dem Proxy für die HTTP-Kommunikation.
HTTPS-Port	Port auf dem Proxy für die HTTPS-Kommunikation.
Proxy-Name	Proxy- und Service-Name. Der Proxy-Name muss eindeutig sein.
Proxy-Abrufintervall	Abrufintervall in Sekunden. Bei der Standardeinstellung dauert es 5 Sekunden, bis Änderungen der Verschlüsselungskonfiguration den Proxy-Server erreichen. Größere Werte führen dazu, dass die Instanz länger braucht, um Online-Proxys zu erkennen. **Hinweis:** Das Ändern der Standardeinstellung des Proxy-Abrufintervalls kann zu Erkennungsverzögerungen führen, wenn ein Proxy online geschaltet wird.
Proxy-Keep-Alive-Ping-Intervall	Zeit in Sekunden zwischen den vom Proxy an die Instanz ausgegebenen Pings. Pings werden regelmäßig ausgegeben, um die Verbindung zwischen dem Proxy und der Instanz zu überprüfen. Der Standardwert ist 10. Der Mindestwert ist 5.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Klicken Sie auf **Installieren**.
   Der Edge Encryption Proxy-Server installiert. Die Installation kann einige Minuten in Anspruch nehmen.

CyberArk-Eigenschaftsschutz konfigurieren

Konfigurieren Sie optional den CyberArk-Eigenschaftsschutz für das sichere Speichern der Edge Encryption-Passwörter in einem zentralen und sicheren digitalen Tresor.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Sie müssen CyberArk AIM (Application Identity Management) erwerben und konfigurieren, bevor Sie CyberArk-Verbindungsparameter und geschützte Anmeldeinformationen für einen Proxy-Server konfigurieren können. Im Rahmen der Installation des AIM-Clients wird die Datei `JavaPasswordSDK.jar` im Installationsverzeichnis des AIM-Clients installiert. Der CyberArk-Tresor wird auf einem unabhängigen gehärteten Server installiert, und die AIM-Clients ermöglichen einen sicheren Zugriff auf diesen Server.

Hinweis: Sie müssen den CyberArk AIM-Client auf jedem Host-Computer installieren, auf dem ein Edge-Proxy installiert ist.

Im Edge-Installationsprogramm müssen Sie den Speicherort der Datei `JavaPasswordSDK.jar` angeben, um die CyberArk-Verbindung zum Edge-Proxy einzurichten. Sie müssen auch andere Werte eingeben, die Sie während der Installation des AIM-Clients definiert haben.

Das Einrichten des CyberArk-Passwortspeichers ist optional. Wenn Sie den CyberArk-Passwortspeicher nicht einrichten möchten, klicken Sie auf den CyberArk-Bildschirmen auf **Überspringen**.

Prozedur

1. Auf der CyberArk Connection-Seite des Edge Encryption-Installationsprogramms geben Sie die CyberArk-Verbindungsparameter ein.

CyberArk-Verbindungsparameter

Einstellung	Beschreibung
Pfad zu PasswordSDK.jar	Der Pfad zur Datei `JavaPasswordSDK.jar`, die während der CyberArk-Konfiguration auf dem Windows-Hostcomputer installiert wurde.
App-ID	Die bei der CyberArk-Konfiguration eingegebene **App-ID**.
Safe-Name	Der bei der CyberArk-Konfiguration eingegebene **Safe-Name**.

2. Klicken Sie auf **Weiter**.
3. Geben Sie auf der Seite „CyberArk-geschützte Anmeldeinformationen“ des Installationsprogramms die Anmeldeinformationen ein, die von CyberArk geschützt werden sollen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Um einen einzigen Anmeldeinformationsnamen für alle geschützten Passwörter zu verwenden, wählen Sie die Checkbox **Einen Anmeldeinformationsnamen für alle Anmeldeinformationen anwenden**, geben Sie den Anmeldeinformationsnamen ein, und klicken Sie auf **Übernehmen**.
- Geben Sie den Anmeldeinformationsnamen für eines oder mehrere der folgenden Felder ein. Anmeldeinformationsnamen sind die Benutzernamen, die während der CyberArk-Konfiguration für die SSH-Schlüssel eingegeben wurden.

CyberArk-geschützte Anmeldeinformationen

Einstellung	Beschreibung
Edge Encryption-Benutzer	Der CyberArk-Anmeldeinformationsname für einen Edge Encryption-Benutzer.
Schlüsselspeicher des Signaturschlüssels	Der CyberArk-Anmeldeinformationsname für den Schlüsselspeicher des Signaturschlüssels.
HTTPS Cert-Schlüsselspeicher	Der CyberArk-Anmeldeinformationsname für den Schlüsselspeicher der HTTP-Zertifizierung.
Schlüsselspeicher des Verschlüsselungsschlüssels	Der CyberArk-Anmeldeinformationsname für den Schlüsselspeicher des Verschlüsselungsschlüssels.
Datenbank	Der CyberArk-Anmeldeiinformationsname für den Datenbankschlüsselspeicher.
SafeNet HTTPS Cert-Schlüsselspeicher	Der CyberArk-Anmeldeinformationsname für den Schlüsselspeicher der SafeNet HTTP-Zertifizierung.
SafeNet-Server	Der CyberArk-Anmeldeinformationsname für den SafeNet-Server.
Forward Proxy	Der CyberArk-Anmeldeinformationsname für den Forward Proxy.

4. Klicken Sie auf **Weiter**.

Den Signaturschlüssel konfigurieren

Konfigurieren Sie den Signaturschlüssel nach der Installation des Proxy-Servers über das Edge Encryption Proxy-Installationsprogramm.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Der Signaturschlüssel kennzeichnet Änderungen an Konfigurationen und Eigenschaften, die vom Proxy-Server vorgenommen werden. Der Signaturschlüssel muss ein asymmetrisches RSA-Schlüsselpaar in einem JCEKS KeyStore sein.

Hinweis: Bei der Installation mehrerer Proxys muss jeder Proxy denselben Signaturschlüssel verwenden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wählen Sie auf der Seite „Signaturschlüssel“ des Edge Encryption Installationsprogramms den Schlüsselspeicher auf dem Host-Computer aus, um den Signaturschlüssel zu speichern.
   - **Einen neuen Java KeyStore erstellen**: Geben Sie Verzeichnisspeicherort, Name und Passwort für den neuen Keystore ein.
   - **Vorhandenen Keystore verwenden**: Geben Sie den Speicherort und das Passwort der Keystore-Datei ein.
2. Klicken Sie auf **Weiter**.
3. Wählen Sie einen Signaturschlüssel aus oder erstellen Sie ihn.
   - **Neuer Schlüssel**: Erstellen Sie einen Signaturschlüssel für diesen Proxy.
   - **Vorhandenen Schlüssel verwenden**: Verwenden Sie ein RSA-Schlüsselpaar aus dem ausgewählten Schlüsselspeicher.
   - **Vorhandenen Schlüssel importieren**: Importieren Sie ein RSA-Schlüsselpaar aus einem anderen Schlüsselspeicher. Navigieren Sie zur Keystore-Datei, geben Sie das Passwort für den Keystore ein und wählen Sie den Schlüsselalias aus. Geben Sie einen neuen Alias für den Schlüssel an.
4. Klicken Sie auf **Weiter**.

Das HTTPS-Zertifikat konfigurieren

Um Clients die Verbindung zum Edge Encryption Proxy-Server über eine sichere SSL-Verbindung zu ermöglichen, importieren Sie das HTTPS-Zertifikat in den Proxy-Server.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Der Edge Encryption Proxy stellt das HTTPS-Zertifikat für Clients bereit, die versuchen, eine Verbindung herzustellen.

Prozedur

1. Wählen Sie auf der Seite „HTTPS-Zertifikat“ des Edge Encryption Installationsprogramms den Schlüsselspeicher zum Speichern des Zertifikats aus.
   - **Einen neuen Java KeyStore erstellen**: Geben Sie Verzeichnisspeicherort, Name und Passwort für den neuen Keystore ein.
   - **Vorhandenen Keystore verwenden**: Geben Sie den Speicherort und das Passwort der Keystore-Datei ein.
2. Klicken Sie auf **Weiter**.
3. Wählen Sie ein Zertifikat aus oder importieren Sie es.
   Der Schlüsselalias ist der angegebene Alias für das Zertifikat.
   - **Vorhandenes Zertifikat verwenden**: Verwenden Sie ein vorhandenes Zertifikat im ausgewählten Schlüsselspeicher.
   - **Aus Datei oder KeyStore importieren**: Importieren Sie ein Zertifikat aus einem anderen Schlüsselspeicher oder einer CER-Datei. Navigieren Sie zum Keystore oder zur .CER-Datei, geben Sie das Passwort ein und wählen Sie den Alias aus. Sie müssen einen neuen Alias für das Zertifikat angeben.
4. Klicken Sie auf **Weiter**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Den AES 128-Bit-Verschlüsselungsschlüssel konfigurieren

Nachdem Sie das HTTPS-Zertifikat über das Edge Encryption-Proxy-Installationsprogramm konfiguriert haben, konfigurieren Sie den AES 128-Bit-Verschlüsselungsschlüssel zum Verschlüsseln Ihrer Daten.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Der Verschlüsselungsschlüssel ist entweder eine reine Textdatei im `/Schlüssel`-Verzeichnis oder ein geheimer Schlüssel in einem Schlüsselspeicher. Wenn Sie einen Keystore für Ihre AES 128-Bit- und AES 256-Bit-Verschlüsselungsschlüssel verwenden, müssen beide denselben Keystore verwenden.

Wenn Sie ein SSL-Zertifikat auf einem Edge-Proxy-Server aktualisieren, finden Sie weitere Informationen unter SSL-Zertifikat aktualisieren .

Prozedur

1. Wählen Sie den Ort des Verschlüsselungsschlüssels.

Option	Beschreibung
Dateispeicher	Verwenden Sie eine Datei zum Speichern eines einzelnen Verschlüsselungsschlüssels. Sie können eine vorhandene Datei im `/Schlüssel`-Verzeichnis verwenden oder eine neue Datei erstellen. Um eine neue Datei zu erstellen, geben Sie einen Alias ein und klicken Sie auf **Generieren**. Es wird eine Datei mit einem Verschlüsselungsschlüssel erstellt. **Hinweis:** Diese Auswahl steht für den Speicherort sowie für den Verschlüsselungsschlüssel. Wenn Sie **Dateispeicher**auswählen, klicken Sie auf **Weiter**, und fahren Sie mit Schritt 5fort.
Neuen Java KeyStore erstellen	Erstellen Sie einen Schlüsselspeicher zum Speichern des Verschlüsselungsschlüssels.
Java KeyStore-Datei	Speichern Sie den Verschlüsselungsschlüssel in einer vorhandenen Java KeyStore-Datei.

2. Klicken Sie auf **Next (Weiter)**.
3. Wählen oder erstellen Sie den Verschlüsselungsschlüssel.

Option	Beschreibung
Neuer Schlüssel	Erstellen Sie einen Verschlüsselungsschlüssel und einen Alias.

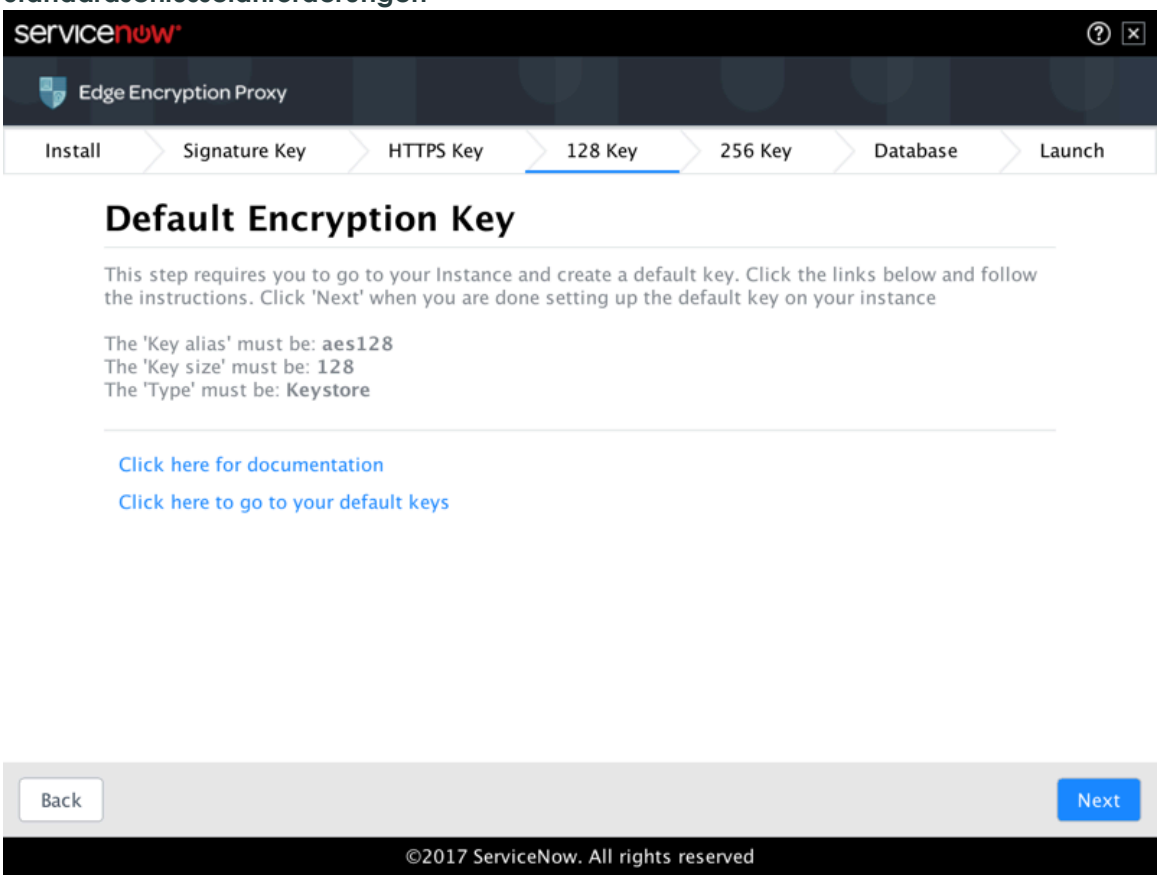
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	Hinweis: Gemäß den Java KeyStore-Anforderungen müssen Sie Kleinbuchstaben und Zahlen für den Aliasnamen (Schlüsselnamen, Schlüsselalias) verwenden. Weitere Informationen zum Keytool-Dienstprogramm finden Sie in der Java SE-Dokumentation .
Vorhandenen Schlüssel verwenden	Verwenden Sie einen vorhandenen Verschlüsselungsschlüssel im ausgewählten Schlüsselspeicher.
Vorhandenen Schlüssel importieren	Importieren Sie einen Verschlüsselungsschlüssel aus einem anderen Schlüsselspeicher.

4. Klicken Sie auf **Next (Weiter)**.
5. Konfigurieren Sie den Schlüssel in der Instanz gemäß den in Ihrem Installationsprogramm definierten Anforderungen.
   Um den Schlüssel in der Instanz zu konfigurieren, navigieren Sie zur Instanz und definieren Sie einen Standardschlüssel. Weitere Informationen finden Sie unter Verschlüsselungsschlüssel für die Instanz konfigurieren. Stellen Sie sicher, dass Schlüsselalias, Größe und Typ den im Installationsprogramm definierten Anforderungen entsprechen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardschlüsselanforderungen



6. Wenn der Schlüssel in der Instanz konfiguriert ist, kehren Sie zum Installationsprogramm zurück und klicken Sie auf **Nächster**.

Den AES 256-Bit-Verschlüsselungsschlüssel konfigurieren

Nachdem Sie den AES 128-Bit-Schlüssel über das Edge-Proxy-Installationsprogramm konfiguriert haben, können Sie optional einen AES 256-Bit-Verschlüsselungsschlüssel zum Verschlüsseln Ihrer Daten konfigurieren.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Der Verschlüsselungsschlüssel ist entweder eine reine Textdatei im `/Schlüssel`-Verzeichnis oder ein geheimer Schlüssel in einem Schlüsselspeicher. Wenn Sie einen Schlüsselspeicher für Ihre AES 128-Bit- und AES 256-Bit-Verschlüsselungsschlüssel verwenden, muss für beide Schlüssel derselbe Schlüsselspeicher verwendet werden. Wenn Sie keinen AES-256-Bit-Verschlüsselungsschlüssel konfigurieren möchten, wählen Sie **Überspringen**, um mit der Installation des Proxy-Servers fortzufahren.

Wenn Sie ein SSL-Zertifikat auf einem Edge-Proxy-Server aktualisieren, finden Sie weitere Informationen unter SSL-Zertifikat aktualisieren .

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wählen Sie den Ort des Verschlüsselungsschlüssels.

Option	Beschreibung
Dateispeicher	Verwenden Sie eine Datei zum Speichern eines einzelnen Verschlüsselungsschlüssels. Sie können eine vorhandene Datei im `/Schlüssel`-Verzeichnis verwenden oder eine neue Datei erstellen. Um eine neue Datei zu erstellen, geben Sie einen Alias ein, und wählen **Sie Generieren**aus. Es wird eine Datei mit einem Verschlüsselungsschlüssel erstellt. **Hinweis:** Diese Auswahl steht für den Speicherort sowie für den Verschlüsselungsschlüssel. Wenn Sie **Dateispeicher**auswählen, wählen Sie **Weiter**, und fahren Sie mit Schritt 5fort.
Neuen Java KeyStore erstellen	Erstellen Sie einen Schlüsselspeicher zum Speichern des Verschlüsselungsschlüssels.
Java KeyStore-Datei	Speichern Sie den Verschlüsselungsschlüssel in einer vorhandenen Java KeyStore-Datei.

2. Wählen Sie **Weiter**.
3. Wählen oder erstellen Sie den Verschlüsselungsschlüssel.

Option	Beschreibung
Neuer Schlüssel	Erstellen Sie einen Verschlüsselungsschlüssel und einen Alias. **Hinweis:** Sie müssen Kleinbuchstaben und Ziffern für den Aliasnamen (Schlüsselname, Schlüsselalias) gemäß den Java KeyStore-Anforderungen verwenden. Weitere Informationen zum Keytool-Dienstprogramm finden Sie in der Java SE-Dokumentation .
Vorhandenen Schlüssel verwenden	Verwenden Sie einen vorhandenen Verschlüsselungsschlüssel im ausgewählten Schlüsselspeicher.
Vorhandenen Schlüssel importieren	Importieren Sie einen Verschlüsselungsschlüssel aus einem anderen Schlüsselspeicher.

4. Wählen Sie **Weiter**.
5. Wahlweise: Wenn Sie die AES-256-Bit-Verschlüsselung verwenden möchten, lesen Sie unter Den AES 256-Bit-Verschlüsselungsschlüssel konfigurierennach.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Um die AES-256-Bit-Verschlüsselung zu verwenden, müssen Sie auch den AES-256-Bit-Standardverschlüsselungsschlüssel in der Instanz konfigurieren.

   Navigieren Sie dazu zur Instanz von und definieren Sie einen Standardschlüssel. Weitere Informationen finden Sie unter Verschlüsselungsschlüssel für die Instanz konfigurieren. Stellen Sie sicher, dass Schlüsselalias, Größe und Typ den im Installationsprogramm definierten Anforderungen entsprechen.

7. Nachdem der Schlüssel in der Instanz konfiguriert wurde, kehren Sie zum Installationsprogramm zurück, und wählen Sie **Weiter**aus.

Aktualisieren Sie das SSL-Zertifikat

Wenn Sie ein SSL-Zertifikat auf einem Edge-Proxy-Server aktualisieren, müssen Sie das alte löschen.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn Sie das SSL-Zertifikat auf dem Edge-Proxyserver aktualisieren, müssen Sie auch das alte Zertifikat löschen. Andernfalls wird das alte Zertifikat (in Form eines Alias in der KeyStore-Datei) weiterhin verwendet, auch wenn der Edge-Proxyserver für die Verwendung des neuen Zertifikats konfiguriert ist.

Prozedur

1. Listen Sie auf dem Edge-Proxy-Server die Einträge im Java KeyStore auf:

```
keytool -list -keystore keystore.jceks -storetype jceks -storepass
 MY_SUPER_PASSWORD
```

2. Altes SSL-Zertifikat entfernen:

```
keytool -delete -alias MY_OLD_ALIAS -keystore keystore.jceks -storetype
 jceks -storepass MY_SUPER_PASSWORD
```

3. Fügen Sie das neue SSL-Zertifikat dem Java KeyStore hinzu.

Die Proxy-Datenbank für die Edge Encryption konfigurieren

Bei Verwendung von ordnungserhaltenden Verschlüsselungstypen oder Verschlüsselungsmustern können Sie optional die Edge Encryption-Proxy-Datenbankeigenschaften konfigurieren.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Für die Verwendung von bestandserhaltenden Verschlüsselungstypen oder Verschlüsselungsmustern ist eine in Ihrem Netzwerk ausgeführte MySQL-Datenbank erforderlich. Diese Aufgabe verbindet den Proxy mit der Datenbank, die Datenbank wird jedoch nicht installiert oder konfiguriert.

Hinweis: Wenn Sie mehrere Proxy-Server verwenden, müssen alle Proxy-Server dieselbe Proxy-Datenbank verwenden. Die im Installationsprogramm eingegebenen Werte müssen für alle Proxy-Server gleich sein.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Bestätigen oder ändern Sie die Datenbank-URL. Dies ist der Speicherort der Proxy-Datenbank.
2. Geben Sie im Feld **Name** den Namen der Proxy-Datenbank ein.
   Der Standardwert ist *edgeencryption*.
3. Geben Sie den Benutzernamen und das Passwort für den Zugriff auf die Proxy-Datenbank ein.
4. Klicken Sie auf **Weiter**.

Den Proxy-Server der Edge Encryption starten

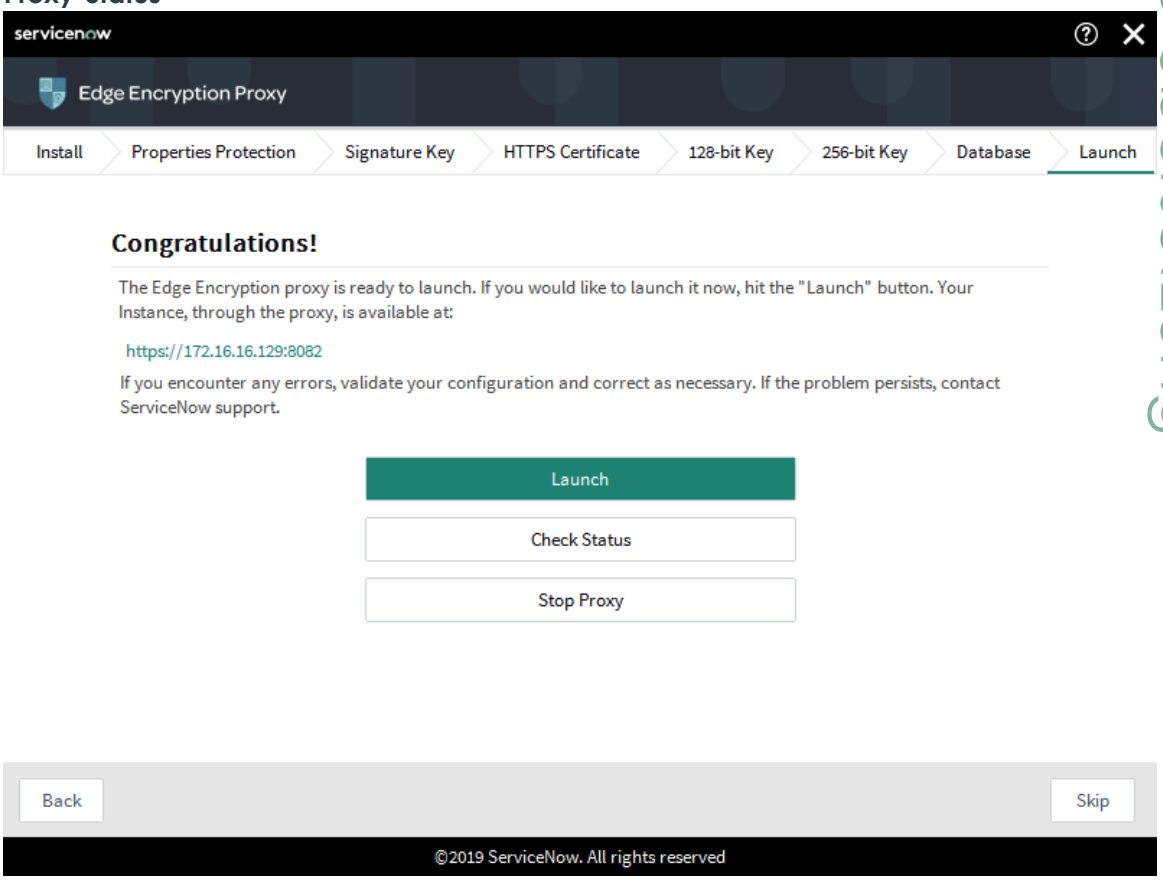
Nach dem Installieren und Konfigurieren eines Edge Encryption Proxys kann der Proxy aus dem Installationsprogramm gestartet werden.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Nachdem Sie die Schlüssel für die Instanz konfiguriert und die Proxy-Datenbank konfiguriert haben, kehren Sie zum Proxy-Installationsprogramm Edge Encryption zurück, und klicken Sie auf **Starten**.
2. Sie können bei Erkennen eines Problems oder zur Statusprüfung Ihres Proxy-Servers auf **Status prüfen**, um zu überprüfen, ob der Proxy ausgeführt wird.
   Eine Meldung zeigt den Proxy-Status an.

Proxy-Status



© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Nach erfolgreicher Installation des Edge Encryption Proxy-Servers, Die anfängliche Speichergrenze des Proxy-Servers und die obere Grenze des Speicherbereichs festlegen.

Überprüfen Sie die Installation des Proxy-Servers für die Edge Encryption, und führen Sie eine Fehlerbehebung durch.

Nach dem Installieren des Edge Encryption Proxy können Sie die Installation überprüfen, um Probleme zu lokalisieren oder den Proxy zu starten und zu stoppen.

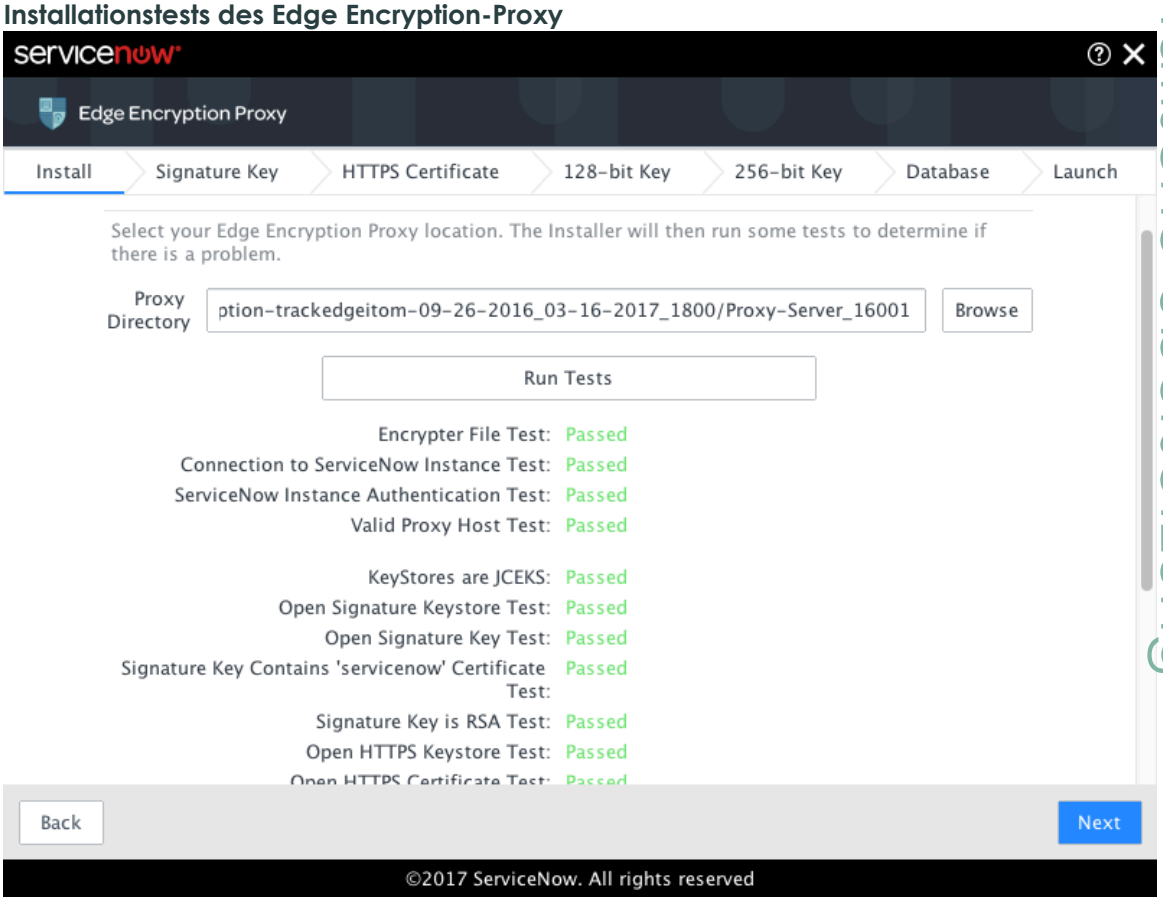
Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Öffnen Sie das Edge Encryption Proxy-Installationsprogramm.
2. Wählen Sie **Installation überprüfen**.
3. Klicken Sie auf **Proxy-Verzeichnis** und wählen Sie das Proxy-Verzeichnis.
4. Klicken Sie auf **Tests ausführen**.
   Testergebnisse werden angezeigt.

Installationstests des Edge Encryption-Proxy



5. Klicken Sie auf **Weiter**.
   Wenn ein Problem auftritt, können Sie das Installationsprogramm durchlaufen, um die Konfiguration zu korrigieren. Wenn keine Probleme auftreten, springt der Installer zur Seite **Starten**. Sie können den Proxy-Status überprüfen, den Proxy stoppen oder den Proxy aus der **Starten**-Seite starten.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Den Proxy-Server für die Edge Encryption mithilfe des Befehlszeilen-Installationsprogramms installieren

Installieren Sie manuell mehrere Edge Encryption Proxy-Server in Ihrem Netzwerk.

Vorbereitungen

Erforderliche Rollen: security_admin auf Ihrer ServiceNow-Instanz und lokaler Administrator auf dem Host-Computer.

Wenn ordnungserhaltende Verschlüsselungstypen oder Verschlüsselungsmuster verwendet werden sollen, richten Sie eine MySQL-Datenbank auf einem Computer in Ihrem Netzwerk ein, sofern noch nicht vorhanden.

Hinweis: Bei Verwendung der Unbound Technology-Verschlüsselungsschlüssel mit Edge Encryption installieren Sie den Proxy-Server mithilfe des Befehlszeileninstallationsprogramms auf dem Unbound-Client-Computer. Der Edge Encryption Proxy-Server muss auf dem gleichen Computer wie der Unbound Technology -Client ausgeführt werden.

Warum und wann dieser Vorgang ausgeführt wird

Richten Sie zuerst einen einzelnen Edge Encryption Proxy-Server ein. Nachdem Ihr erster Proxy-Server erfolgreich ausgeführt wurde, fügen Sie weitere Proxy-Server für eine Instanz hinzu, um eine optimale Umgebung zu gewährleisten. Siehe Umgebungsgröße Ihrer Edge Encryption anpassen, um die Anzahl zusätzlich erforderlicher Proxy-Server zu bestimmen.

Den Proxy-Server für die Edge Encryption installieren (Befehlszeilen-Installationsprogramm)

Installieren Sie einen Edge Encryption Proxy auf einem 64-Bit-Windows- oder Linux-Computer.

Vorbereitungen

Erforderliche Rolle: admin

Zum Ausführen des Installationsprogramms ist Java Version 11.0.6 oder höher in der 11.x-Versionsserie erforderlich.

Warum und wann dieser Vorgang ausgeführt wird

Installieren Sie den Edge Encryption Proxy-Server auf einem Computer in Ihrem Netzwerk mit dem entsprechenden Befehl für Ihren Zielcomputer. Bei der Installation des Edge Encryption Proxy-Servers auf einem Windows-Computer muss der Proxy-Server zusätzlich als Windows-Service installiert werden.

Wenn Sie den Proxy-Server der Edge Encryption aktualisieren, sichert das System den alten Proxy im Verzeichnis `backup.dist-upgrade-<timestamp>` unter dem aktuellen Installationsverzeichnis. Das Sicherungsverzeichnis wird während des Upgrade-Vorgangs erstellt und speichert die alten Proxy-Informationen.

Wenn Sie ein Upgrade über die Befehlszeile ausführen, kann eine dist-upgrade.log in dem Verzeichnis erstellt werden, in dem der Befehl ausgeführt wird. Das dist-upgrade.log enthält Protokolle für den Upgrade-Vorgang.

Bei einem fehlgeschlagenen Upgrade erstellt das System ein Verzeichnis `failed-backup.dist-upgrade-<timestamp>`. Zusätzlich kann `logs/wrapper.log` im ursprünglichen Proxy-Verzeichnis auch Fehlerinformationen enthalten.

Prozedur

1. Erstellen Sie das Installationsverzeichnis.
2. Laden Sie die Edge Encryption Proxy-Archivdatei in das Installationsverzeichnis herunter.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Öffnen Sie das Terminal und wechseln Sie in das Installationsverzeichnis.

   Hinweis: Bei der Installation auf einem Windows-Computer müssen Sie die Windows-Eingabeaufforderung mit Administratorrechten starten.

4. Führen Sie diesen Befehl für den Zielcomputer aus und ändern Sie die Variablen entsprechend Ihrer Konfiguration: `java -jar edgeencryption-<version>-all.jar -m install -n <ProxyName> --instancehost <host> -p <InstancePort> --protocol https`

Option	Variable	Beschreibung
Keine	Version	Versionsnummer des Edge Encryption Proxy, der zur Ausführung der aktuellen Operation verwendet wird.
-m	Modus	Die Operation oder der Modus, in dem ausgeführt werden soll (Installation oder Dist-Upgrade).
-n	ProxyName	Der Name der Verschlüsselungs-Proxy-Instanz. Verwenden Sie einen eindeutigen `ProxyName`, um bestimmte Proxy-Instanzen identifizieren zu können.
--instancehost	host	Der Hostname Ihrer ServiceNow-Instanz (z. B. `mycompany.service-now.com`).
-p	InstancePort	Der Port Ihrer Instanz. Bei Protokoll https ist der Port normalerweise 443.
--protocol	protocol	Das für den Zugriff auf Ihre ServiceNow-Instanz verwendete Protokoll (in der Regel https).

   Hinweis: Kopieren Sie keine Befehle aus dem Browser. Gelegentlich führen Kopier- / Einfügevorgänge dazu, dass unerwartete Zeichen auf dem Zielcomputer eingefügt werden und der Befehl falsch ausgeführt wird. Es ist am besten, den Befehl von Hand anhand der Dokumentation als Referenz einzugeben.

   Um den Hilfebildschirm anzuzeigen, führen Sie diesen Befehl ohne Argumente aus: `java -jar edgeencryption-<version>-all.jar`

5. Beim Installieren auf einem Windows-Computer installieren Sie den Edge Encryption Proxy als Windows-Dienst.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wahlweise: Ändern Sie den Namen des Service, indem Sie die Datei `conf/wrapper.conf` auf dem neuen Proxy öffnen und die Eigenschaften in der folgenden Tabelle festlegen.

Eigenschaft	Beschreibung
wrapper.ntservice.name	Eindeutiger Name des Edge Encryption Proxy-Service.
wrapper.ntservice.displayname	Anzeigename des Edge Encryption Proxy-Service.
wrapper.ntservice.description (optional)	Beschreibung des Proxy-Server.

Bei Nichtausführung dieses Schrittes wird der Edge Encryption Proxy-Service unter dem Namen **Edge Encryption** installiert.

b. Speichern und schließen Sie die Datei.

c. Öffnen Sie die Windows-Eingabeaufforderung und `cd` zu `ServerName_port/bin`.

d. Führen Sie `edgeencryption.bat installieren` aus.

Ergebnisse
Das Verzeichnis `ProxyName_port` wird im aktuellen Verzeichnis erstellt. Die Datei `edgeencryption.properties` wird mit den Host-, Port- und Protokollwerten über die Befehlszeile aktualisiert.

Das RSA-Schlüsselpaar für die digitale Signatur erstellen und konfigurieren

Erstellen Sie ein RSA-Schlüsselpaar, mit dem der Proxy-Server die digitale Signatur zum Signieren von Änderungen an den Verschlüsselungseigenschaften und der Konfiguration erstellen kann.

Vorbereitungen
Erforderliche Rolle: admin

Um die digitale Signatur zu erstellen und zu validieren, muss ein RSA-Schlüsselpaar generiert und im JCEKS Java KeyStore gespeichert werden, und jeder Proxy muss für die Verwendung dieses Schlüsselpaares konfiguriert sein. Generieren Sie ein Verschlüsselungsschlüsselpaar mit dem Befehl keytool.

Um das Dienstprogramm keytool mit einem auf SElinux installierten Proxy (CentOS) verwenden zu können, müssen Sie das Laden gemeinsam genutzter Bibliotheken aus dem Proxy-Java-Installationsverzeichnis aktivieren. Führen Sie dazu den folgenden Befehl als Root aus.

```
chcon -R -t texrel_shlib_t proxy_install_dir/java/jre /lib
```

Sie müssen die Java 1.8-Version des Keytool-Dienstprogramms verwenden. Eine Kopie des Dienstprogramms finden Sie unter `<proxy install dir>java/jre/bin/keytool`.

Prozedur

1. Wechseln Sie in das KeyStore-Verzeichnis im Proxy-Download-Verzeichnis.

2. Ändern Sie das Standardpasswort.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Standardpasswort lautet *changeme*.

```
keytool -keystore keystore.jceks -storetype jceks -storepasswd -new
 <newpassword>
```

3. Erstellen Sie ein Verschlüsselungsschlüsselpaar.

   Hinweis: Geben Sie kein Passwort für den Schlüssel ein, wenn das keytool-Dienstprogramm zur Eingabe auffordert.

   Geben Sie diesen Befehl in einer einzigen Zeile ein.

```
keytool -genkeypair -alias <key alias> -keyalg rsa -keystore
 keystore.jceks
-storetype jceks -storepass <keystore password> -keysize 2048
```

4. Aktualisieren Sie die Eigenschaftsdatei des Verschlüsselungsproxys (`edgeencryption.properties`).

   a. Wechseln Sie in das Verzeichnis `<installation directory>/conf/`.

   b. Öffnen Sie die Datei `edgeencryption.properties`.

   c. Geben Sie die Eigenschaften für die Digitale Signatur ein.

      Diese Eigenschaften müssen für alle Proxys gleich sein.

5. Speichern und schließen Sie die Datei `edgeencryption.properties`.

Das Zertifikat für eine sichere SSL-Verbindung importieren und konfigurieren

Um eine sichere SSL-Verbindung zu verwenden, importieren Sie ein Serverzertifikat und fügen es zum Java KeyStore hinzu.

Vorbereitungen

Erforderliche Rolle: admin

Sie müssen das Serverzertifikat und den entsprechenden privaten Schlüssel abrufen, bevor Sie sie zum Java KeyStore hinzufügen.

Prozedur

1. Generieren Sie mit dem Befehl `openedsl` eine Zertifikatsignaturanforderung (Certificate Signing Request, CSR).

```
openssl req -newkey rsa:2048 -keyout PRIVATEKEY.key -out MYCSR.csr
```

2. Senden Sie Ihre CSR (im Beispiel oben MYCSR.csr) an die Zertifizierungsstelle, damit sie signiert wird.
3. Erstellen Sie mit dem Befehl `openedsl` einen P12-Schlüsselspeicher für den Import.

```
openssl pkcs12 -export -in MYSIGNEDCERT.pem -inkey PRIVATEKEY.key -name
 shared > MY_SERVER.p12
```

4. Speichern Sie Ihr Zertifikat und Ihren privaten Schlüssel in einer JCEKS-Datei.

```
keytool -importkeystore -destkeystore keystore.jceks -deststoretype
 jceks -srckeystore MY_SERVER.p12 -srcstoretype pkcs12 -alias MYALIAS
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Alias, im Beispiel als `MYALIAS` dargestellt, kann ein beliebiger Wert sein. Sie verwenden diesen Alias in der Eigenschaft „ `edgeencryption.proxy.https.cert.alias` “ in der Datei „`edgeencryption.properties` “ im<installation directory> `/conf/-Ordner`.

5. Beenden Sie den Edge-Proxy, und starten Sie ihn neu.

> **Hinweis:** Bei einem Neustart ist der Proxy-Server für kurze Zeit offline. Die Zeitdauer wird von Ihrer Umgebung bestimmt und wie lange es dauert, den Proxy-Dienst zu stoppen und erneut zu starten.

Schlüsselspeicher und Verschlüsselungsschlüssel einrichten

Richten Sie den vom Edge Encryption Proxy Server verwendeten Schlüsselspeicher und die Verschlüsselungsschlüssel ein.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Bestimmen Sie sorgfältig den geeigneten Keystore-Typ entsprechend den Anforderungen Ihres Unternehmens.

Unterstützter Keystore	Beschreibung
Dateispeicher	Die Schlüssel werden in einer Datei in einem Dateisystem gespeichert, auf das der Edge Encryption Proxy-Server zugreift. In einer Datei gespeicherte Verschlüsselungsschlüssel werden nicht verschlüsselt. Der Schutz dieser Dateien liegt daher in Ihrer Verantwortung.
Java KeyStore	Ein Java KeyStore: ◦ Speichert Schlüssel in einem Java JCEKS KeyStore. ◦ Ist passwortgeschützt und sicherer als das Speichern von Schlüsseln in einer Datei im Dateisystem. ◦ Kann mehrere Schlüssel speichern. Ein Schlüsselalias repräsentiert jeden Schlüssel, was die Verwaltung mehrerer Schlüssel erleichtert. Der Edge Encryption Proxy wird mit der Java JCEKS KeyStore-Datei mit dem Namen `keystore.jceks` im Verzeichnis `Schlüsselspeicher` geliefert. Diese Schlüsselspeicherdatei enthält den öffentlichen Schlüssel ServiceNow, mit dem die von ServiceNow signierten Verschlüsselungsregeln überprüft werden.
Enterprise Key Management (EKM)	**SafeNet KeySecure** Schlüssel werden mit der Schlüsselverwaltung von SafeNet KeySecure gespeichert und abgerufen. Sie müssen eine Lizenz von Gemalto erwerben, die Bibliotheken herunterladen und den SafeNet KeySecure-Schlüsselspeicher auf einem Host-Computer in Ihrem Netzwerk installieren, bevor Sie den Schlüsselspeicher auf dem Edge Encryption Proxy-Server konfigurieren. **Unbound Technology**

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterstützter Keystore	Beschreibung
	Der base64-verschlüsselte Wrapped-Verschlüsselungsschlüssel wird als Textdatei auf dem Edge Encryption Proxy-Server gespeichert. Die Implementierung der Unbound Technology (zuvor Dyadic Security) behält die Kontrolle über den Wrapping-Schlüssel. Der Edge Encryption Proxy-Server muss auf dem gleichen Computer wie der Unbound-Technology-Client ausgeführt werden.

Hinweis: Wenn Sie einen anderen Schlüsselspeicher als das Basissystem Java JCEKS KeyStore verwenden, müssen Sie den öffentlichen Schlüssel ServiceNow in Ihren Schlüsselspeicher importieren. Der Alias für den öffentlichen Schlüssel lautet *servicenow*.

2. Richten Sie den Schlüsselspeicher und die Verschlüsselungsschlüssel in Ihrem lokalen Netzwerk ein.

Einen Java KeyStore-Schlüsselspeicher einrichten

Sie können einen Java KeyStore-Schlüsselspeicher zum Speichern von Verschlüsselungsschlüsseln verwenden.

Vorbereitungen
Erforderliche Rolle: admin

Sie müssen die Java 1.8-Version des Keytool-Dienstprogramms verwenden. Eine Kopie des Dienstprogramms finden Sie unter `<proxy install dir>/java/jre/bin/keytool`.

Warum und wann dieser Vorgang ausgeführt wird
Der Edge Encryption Proxy wird mit der Java JCEKS KeyStore-Datei mit dem Namen `keystore.jceks` im Verzeichnis `Schlüsselspeicher` geliefert. Diese Schlüsselspeicherdatei enthält den öffentlichen Schlüssel ServiceNow, mit dem die von ServiceNow signierten Verschlüsselungsregeln überprüft werden.

Prozedur

1. Richten Sie die Keystore-Eigenschaften ein.
   a. Wechseln Sie in das Verzeichnis `<installation directory>/conf/`.
   b. Öffnen Sie die Datei `edgeencryption.properties`.
   c. Geben Sie die Eigenschaften für den Java KeyStore ein.
2. Speichern und schließen Sie die Datei `edgeencryption.properties`.

Nächste Maßnahme
Nach dem Einrichten des Java KeyStore, Verschlüsselungsschlüssel mit dem Java KeyStore-Keytool erstellen.

Verschlüsselungsschlüssel mit dem Java KeyStore-Keytool erstellen

Sie können das mit der Verschlüsselungsproxy-Distribution mitgelieferte Keytool verwenden, um AES 128-Bit- und AES 256-Bit-Verschlüsselungsschlüssel zu erstellen.

Vorbereitungen
Erforderliche Rolle: admin

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie müssen die Java 1.8-Version des Keytool-Dienstprogramms verwenden. Eine Kopie des Dienstprogramms finden Sie unter `<proxy install dir>/java/jre/bin/keytool`.

Weitere Informationen zum Keytool-Dienstprogramm finden Sie in der Java SE-Dokumentation .

Warum und wann dieser Vorgang ausgeführt wird

Hinweis: Der Java KeyStore erfordert, dass der Aliasname (Schlüsselname, Schlüsselalias) Kleinbuchstaben und Zahlen verwendet.

Prozedur

1. Wechseln Sie in das Verzeichnis `<installation directory>/keystore/`.
2. Führen Sie einen der folgenden Befehle aus, um den Verschlüsselungsschlüssel zu erstellen.

Hinweis: Wenn Sie diese Befehle aus einem anderen Verzeichnis als dem Keystore-Verzeichnis ausführen möchten, d. h. Sie haben den vorherigen Schritt übersprungen, müssen Sie die Option *-keystore* ändern, um den Pfad von Ihrem aktuellen Verzeichnis zum Keystore-Verzeichnis aufzunehmen. Wenn Sie sich beispielsweise im Verzeichnis `<installation directory>\bin` befinden, lautet die Option `-keystore ../keystore/keystore.jceks`.

Option	Bezeichnung
AES 128	`keytool -genseckey -alias 128bitkey -keyalg aes -keysize 128 -keystore keystore.jceks -storetype jceks`
AES 256	`keytool -genseckey -alias 256bitkey -keyalg aes -keysize 256 -keystore keystore.jceks -storetype jceks`

Der Alias wird in der Instanz hinzugefügt, wenn Sie Standardschlüssel zuweisen.

Hinweis: Das Schlüsselpasswort muss mit dem Schlüsselspeicher-Passwort identisch sein.

Einen SafeNet KeySecure-Schlüsselspeicher einrichten

Wenn Sie einen SafeNet-Schlüsselspeicher verwenden, kopieren Sie einen Satz Bibliotheken in das Proxy-Distributionsverzeichnis.

Vorbereitungen

Erforderliche Rolle: admin

Sie müssen den SafeNet-Schlüsselspeicher installieren und einrichten, bevor Sie diesen Schritt ausführen. Sichern Sie sich eine Lizenz bei Thales , um die Bibliotheken herunterzuladen.

Hinweis: Für IngrianNAE Version 8.12 müssen Sie auch die Datei `commons-collections.jar` herunterladen

Warum und wann dieser Vorgang ausgeführt wird

Hinweis: Unter Linux verwenden Dateipfade einen Schrägstrich (/).

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wechseln Sie in das Verzeichnis `<installation directory>/conf/` directory, und öffnen Sie die Datei `edgeencryption.properties`.
2. Geben Sie die Eigenschaften für den SafeNet-Schlüsselspeicher ein.

Hinweis: Sie können den SafeNet-Schlüsselspeicher mit mit Anwendername/Passwort-Authentifizierung oder Client-Zertifikatauthentifizierung konfigurieren, aber nicht mit einer Kombination aus beidem.

Example

Ein Beispiel für einen SafeNet-Schlüsselspeicher mit Authentifizierung mit Benutzername und Passwort.

```
edgeencryption.nae.retries = 3
edgeencryption.nae.enabled = true
edgeencryption.nae.server = url
edgeencryption.nae.port = 9000
edgeencryption.nae.protocol = ssl
edgeencryption.nae.keystore.path = keystore/safenet_truststore
edgeencryption.nae.keystore.password = password
edgeencryption.nae.user = safenet_user
edgeencryption.nae.password = safenet_password
```

Example

Ein Beispiel für einen SafeNet-Schlüsselspeicher mit Client-Zertifikatsauthentifizierung. Durch diese Authentifizierungsmethode ist das Speichern von Benutzername und Passwort des SafeNet-Servers in der Eigenschaftendatei nicht erforderlich.

```
edgeencryption.nae.retries = 3
edgeencryption.nae.enabled = true
edgeencryption.nae.server = url
edgeencryption.nae.port = 9000
edgeencryption.nae.protocol = ssl
edgeencryption.nae.keystore.path = keystore/safenet_clientcert
edgeencryption.nae.keystore.password = password
edgeencryption.nae.client.certificate = cert_name
```

3. Hinzufügen oder Erstellen eines Schlüssels im SafeNet-Schlüsselspeicher.
   Der Schlüsselname (Alias) wird in der Instanz hinzugefügt, wenn Sie Standardschlüssel zuweisen.
4. Speichern und schließen Sie die Datei `edgeencryption.properties`.

Upgrade von Kingston oder niedriger auf London oder höher durchführen

Wenn Sie einen SafeNet-NAE-Server für die Schlüsselspeicherung mit Edge verwenden, müssen Sie vor dem Upgrade des Proxys von Kingston oder niedriger auf London oder höher die JAR-Dateien der Gemalto SafeNet-Client-ProtectApp kopieren und neue Eigenschaften hinzufügen.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Hinweis: Unter Linux verwenden Dateipfade einen Schrägstrich (/).

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Kopieren Sie die folgenden Dateien aus<installation directory> `/lib` für `/nae-Verzeichnis`:

   - `commons-sammlungen<version> .jar`
   - `ingrianlog4j-api-<version>.jar`
   - `ingrianlog4j-core-<version>.jar`
   - `ingrianNAE-<version>.jar`

2. Aktualisieren Sie in der aktuellen Version (nicht aktualisiert) des Proxys<installation directory> `/conf/edgeencryption.properties` durch Hinzufügen der folgenden beiden Eigenschaften:

   - *`edgeencryption.ekm.provider.classname`* = `com.snc.edgeencryption.encryption.CloudEdgeNaeKeyProvider`
   - *`edgeencryption.thirdparty.vendor.library.path`* =<directory path to the directory where you copied the jar files in step 1>

     Hinweis: *`edgeencryption.thirdparty.vendor.library.path`* für Java 11.

3. Speichern Sie die Änderungen.
4. Fahren Sie mit dem Upgrade auf London oder höher fort.

Unbound Technology-Schlüssel einrichten

Verwenden Sie ungebundene Technologieschlüssel (zuvor dyadische Sicherheit) mit Edge Encryption, indem Sie den base64-codierten umschlossenen Verschlüsselungsschlüssel als Textdatei auf dem Proxy-Server Edge Encryption] speichern und den Alias für den Wrapping-Schlüssel bereitstellen. Die Implementierung von Unbound Technology behält die Kontrolle über den Wrapping-Schlüssel.

Vorbereitungen

Erforderliche Rolle: security_admin

Identifizieren Sie in Ihrer Unbound Technology-Implementierung sowohl den Wrapping-Schlüssel als auch den Wrapped-Schlüssel. Verwenden Sie den RSA/ECB/OAEPWITHSHA-256ANDMGF1PADDING-Algorithmus für Umbruch und Auffüllung. Exportieren Sie den Wrapped-Schlüssel im base64-codierten Textformat. Speichern Sie die Datei mit dem Schlüsselalias als Namen ohne Dateierweiterung.

Hinweis: Bei Verwendung der Unbound Technology-Verschlüsselungsschlüssel mit Edge Encryption installieren Sie den Proxy-Server mithilfe des Befehlszeileninstallationsprogramms auf dem Unbound-Client-Computer. Der Edge Encryption Proxy-Server muss auf dem gleichen Computer wie der Unbound Technology -Client ausgeführt werden.

Prozedur

1. Fügen Sie den Wrapped-Verschlüsselungsschlüssel im base64-codierten Textformat zum Verzeichnis `<proxy-installation-directory>/keys` hinzu.
   Der Name der Datei muss der Schlüsselalias ohne Dateierweiterung sein.
2. Aktualisieren Sie die Datei `edgeencryption.properties`.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wechseln Sie in das Verzeichnis `<proxy-installation-directory>/conf`.

b. Öffnen Sie die Datei `edgeencryption.properties`.

c. Geben Sie die Dateispeichereigenschaften ein, und legen Sie den Wert *`edgeencryption.keyfile.directory`* auf `Schlüssel`fest.

   Diese Eigenschaft weist den Proxy-Server an, nach dem Verschlüsselungsschlüssel im Verzeichnis `<Java-home-directory>/keys` zu suchen.

   Weitere Informationen zu Edge Encryption Eigenschaften, siehe Eigenschaften des Proxy-Servers für die Edge Encryption.

d. Entfernen Sie das Kommentarzeichen für die Eigenschaften für die Konfiguration des dyadischen Anbieters, und legen Sie den Wert *`edgeencryption.ekm.provider.rsa.wrapping.key.alias`* auf den umschließenden Schlüsselalias in Ihrer ungebundenen Implementierung fest.

e. Speichern und schließen Sie die Datei.

Nächste Maßnahme
Fügen Sie der Instanz den Aliasnamen der Verschlüsselung hinzu. Der Alias des Verschlüsselungsschlüssels ist der Dateiname des Wrapped-Verschlüsselungsschlüssels, der zum Verzeichnis `<proxy-installation-directory>/keys` hinzugefügt wurde. Wenn zum Beispiel die Datei im Verzeichnis `myunboundkey` heißt, fügen Sie diesen Namen zum Feld **Schlüsselalias** hinzu. Weitere Informationen finden Sie unter Verschlüsselungsschlüssel für die Instanz konfigurieren.

Einen in einer Datei gespeicherten Verschlüsselungsschlüssel erstellen

Sie können eine einfache Textdatei als Schlüsselspeicher verwenden. Jede Datei enthält einen einzelnen Verschlüsselungsschlüssel.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Dieser Schritt erstellt sowohl den Schlüsselspeicher als auch den Verschlüsselungsschlüssel.

Hinweis: Der Name der Schlüsseldatei muss mit dem in der Tabelle der Verschlüsselungsschlüssel der Instanz angegebenen Schlüsselalias übereinstimmen. Weitere Informationen finden Sie unter Verschlüsselungsschlüssel für die Instanz konfigurieren.

Prozedur
1. Erstellen Sie eine Datei im Ordner `/keys` des Installationsverzeichnisses des Proxy-Servers.
2. Fügen Sie den Verschlüsselungsschlüssel zur Datei hinzu.

Option	Bezeichnung
AES 128	Platzieren Sie den Verschlüsselungsschlüssel (genau 16 Byte) in der Datei.
AES 256	Platzieren Sie den Verschlüsselungsschlüssel (genau 32 Byte) in der Datei.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Aktualisieren Sie die Datei `edgeencryption.properties`.
   a. Wechseln Sie in das Verzeichnis `<installation directory>/conf/`.
   b. Öffnen Sie die Datei `edgeencryption.properties`.
   c. Geben Sie die Eigenschaften für den Dateispeicher ein.
   d. Speichern und schließen Sie die Datei.

Verschlüsselungsschlüssel für die Instanz konfigurieren

Edge Encryption bietet die Tools zum Verwalten von Verschlüsselungsschlüsseln, ohne den Proxy offline zu schalten.

Vorbereitungen

Erforderliche Rolle: security_admin

Vor dem Einrichten neuer Verschlüsselungsschlüssel für die Instanz:

1. Erstellen Sie den Verschlüsselungsschlüssel.
2. Stellen Sie den neuen Schlüssel allen Verschlüsselungsproxys zur Verfügung. Kopieren Sie entweder die Datei oder die Java KeyStore-Datei auf jeden Proxy, oder stellen Sie sicher, dass jeder Proxy Zugriff auf das Java KeyStore- oder Enterprise Key Management(EKM)-Gerät hat.

Warum und wann dieser Vorgang ausgeführt wird

Schlüssel-Aliasse müssen eindeutig sein. Jeder Schlüsselalias muss auf jedem Proxy die gleiche Schlüsselgröße und den gleichen Typ haben, oder der Schlüssel kann nicht als Standard zugewiesen werden.

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Konfiguration des Verschlüsselungsschlüssels** > **Schlüssel einrichten**an.
2. Führen Sie im Abschnitt „Neue Schlüssel hinzufügen“ des Formulars die folgenden Schritte aus, um einen neuen Schlüssel hinzuzufügen.

   > **Wichtig:** Bei Verwendung von mit SafeNet versionierten Schlüsseln wird eine zusätzliche Spalte für die **Schlüsselversion** angezeigt. Die **Schlüsselversion** kann nicht bearbeitet werden. Klicken Sie auf den Link **Aktuelle Schlüsselversionen** abrufen unter „Zugehörige Links“, um die aktuelle Version jedes Schlüssels vom Edge-Proxy abzurufen.

   Zeilen in der Liste mit einem **X** in der linken Spalte können gelöscht werden. Schlüssel, die als Standard verwendet wurden oder den **Status Verfügbar** haben, können nicht gelöscht werden.

   a. Doppelklicken Sie in die Zeile **Neue Zeile einfügen.**.

   b. Geben Sie im Bearbeitungsfeld einen Namen für den Schlüssel ein, und klicken Sie dann auf das Häkchen.

      Schlüsselaliasnamen bestehen aus Kleinbuchstaben und Zahlen. Großbuchstaben werden beim Klicken auf **Aktualisieren** in Kleinbuchstaben geändert. Schlüssel-Aliasse müssen eindeutig sein.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn Sie Unbound Technology-Schlüssel verwenden, fügen Sie den Alias für den Verschlüsselungsschlüssel hinzu. Der Alias des Verschlüsselungsschlüssels ist der Dateiname des Wrapped-Verschlüsselungsschlüssels, der zum Verzeichnis `<proxy-installation-directory>/keys` hinzugefügt wurde. Wenn zum Beispiel die Datei im Verzeichnis `myunboundkey` heißt, fügen Sie diesen Namen zum Feld **Schlüsselalias** hinzu.

c. Doppelklicken Sie in derselben Zeile auf die Spalte **Schlüsselgröße**.

d. Wählen Sie im Auswahlfeld eine Schlüsselgröße, entweder **128 Bit** oder **256 Bits** aus und klicken Sie dann auf das Häkchen.

e. Doppelklicken Sie in derselben Zeile auf die Spalte **Typ**.

f. Wählen Sie im Auswahlfeld einen Schlüsseltyp, entweder **Datei**, **Keystore**, **SafeNet** oder **Unbound** aus und klicken Sie dann auf das Häkchen.

g. Wenn Sie mit dem Hinzufügen der Schlüssel fertig sind, klicken Sie auf **Nächster Schritt**. Sie müssen für jeden Schlüssel einen Aliasnamen, eine Schlüsselgröße und einen Schlüsseltyp angeben, bevor Sie fortfahren.

3. Überprüfen Sie im Abschnitt „Schlüsselstatus“ des Formulars die Option **Status** des Schlüssels und stellen Sie sicher, dass **Verfügbar** eingestellt ist.
4. Wenn der Schlüssel **Verfügbar** ist, klicken Sie auf **Nächster Schritt**.
   Dies kann einige Minuten dauern.

   Hinweis: Bei Verwendung von mit SafeNet versionierten Schlüsseln wird eine zusätzliche Spalte für die **Schlüsselversion** angezeigt. Die **Schlüsselversion** kann nicht bearbeitet werden.

   Die Instanz verfolgt den Status jedes für jeden Proxy verfügbaren Verschlüsselungsschlüssels. Wenn ein Schlüssel für alle Proxys verfügbar ist, ändert sich dessen Status zu **Verfügbar**. Wenn sich der Status nach einigen Minuten nicht ändert, überprüfen Sie, ob der Schlüssel für alle Proxys verfügbar ist. Wenn der Zustand **Nicht verfügbar** bestehen bleibt, hat einer oder haben mehrere Proxys den Schlüssel nicht.

Zustände der Verschlüsselungsschlüssel

Status	Beschreibung
Verfügbar	Alle Online-Proxys haben den Schlüssel.
Nicht verfügbar	Dies ist ein neuer Schlüssel, und die Proxys haben den Schlüssel noch nicht geladen, oder mindestens ein Proxy konnte den Schlüssel nicht laden.

5. Führen Sie im Abschnitt „Standardschlüssel ändern“ des Formulars einen der folgenden Schritte aus:
   - Geben Sie den Schlüsselalias ein.
   - Klicken Sie auf das Lupensymbol und wählen Sie einen Alias aus.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Bei Verwendung von mit SafeNet versionierten Schlüsseln wird ein zusätzliches Feld für die **Schlüsselversion** angezeigt. Die **Schlüsselversion** ist ausgegraut und kann nicht bearbeitet werden. Wählen Sie nur die neueste Schlüsselversion aus. Wenn Sie eine frühere Version wählen, wird die folgende Meldung angezeigt, wenn Sie auf **Aktualisieren** oder **Nächster Schritt**klicken.

```
One of the default keys chosen is not the latest version available
 for the key. Please use the latest version.
```

Wenn die Standardschlüssel nicht die neuesten Versionen der SafeNet-Schlüssel sind, wird unter „Zugehörige Links“ der Link **Standardschlüssel auf die neueste Version** aktualisieren angezeigt. Klicken Sie auf den Link, um die Standardschlüssel zu aktualisieren und die neueste Version zu verwenden.

6. Planen Sie im Abschnitt „Schlüsselrotation planen“ des Formulars einen Massenschlüssel-Rotationsauftrag oder einen Einzelschlüssel-Rotationsauftrag, um vorhandene Daten mit dem neuen Verschlüsselungsschlüssel zu verschlüsseln.

   Wenn Sie keinen Massenschlüssel-Rotationsauftrag oder Einzelschlüssel-Rotationsauftrag ausführen, bleiben vorhandene Daten mit dem alten Schlüssel verschlüsselt, bis auf die Daten erneut zugegriffen wird.

Konfigurieren zusätzlicher Eigenschaften in der Edge Encryption-Eigenschaftendatei

Nach dem Installieren des Edge Encryption Proxy-Server in Ihrem Netzwerk und Einrichten des Schlüsselspeichers und der Schlüssel konfigurieren Sie die zusätzlichen Edge Encryption-Eigenschaften.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Öffnen Sie die Datei `<installation directory>/conf/edgeencryption.properties`, und konfigurieren Sie die folgenden Edge Encryption Proxy-Server-Eigenschaften:
   - Zieleigenschaften (Instanz)
   - Benutzer-Account-Eigenschaften
   - Proxy-Eigenschaften
   - Konfigurieren Sie bei Verwendung von ordnungserhaltenden Verschlüsselungstypen oder Verschlüsselungsmustern die Proxy-Datenbankeigenschaften.
   - Klartext und statische IV-Eigenschaften
2. Speichern und schließen Sie die Datei.

Einen Web-Proxy konfigurieren

Wenn Ihr Netzwerk einen Web-Proxy verwendet, können Sie den Edge Encryption Proxy für die Verwendung für den Web-Proxy einrichten.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn Ihr Netzwerk keinen Web-Proxy verwendet, belassen Sie die Web-Proxy-Eigenschaften in der Konfigurationsdatei auskommentiert.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Edge Encryption Proxy-Server unterstützt die HTTP-Verbindung mit dem Web-Proxy und die Basisauthentifizierung.

Prozedur

1. Wechseln Sie in das Verzeichnis `<installation directory>/conf/`.
2. Öffnen Sie die Datei `edgeencryption.properties`.
3. Konfigurieren Sie die Web-Proxy-Eigenschaften.
4. Speichern und schließen Sie die Datei `edgeencryption.properties`.
5. Wenn der Web-Proxy ein kundenspezifisches Serverzertifikat verwendet, fügen Sie dieses Zertifikat zur JVM hinzu, die vom Edge Encryption Proxy-Server verwendet wird, um eine Vertrauensstellung zwischen dem Web-Proxy und dem Edge Encryption Proxy-Server zu erstellen.
   a. Verwenden Sie den Befehl `cd`, um zu zu navigieren<Java home directory> `/jre/lib/security/cacerts`
   b. Führen Sie den Befehl aus: `keytool -keystore cacerts -importcert -alias <chooseAlias> -file <certificateFile>`

Die anfängliche Speichergrenze des Proxy-Servers und die obere Grenze des Speicherbereichs festlegen

Legen Sie das anfängliche und das obere Speichergrenze fest, um festzulegen, wie viel Speicher der Proxy-Server verbrauchen kann. Legen Sie diese Grenzwerte fest, um Leistungsprobleme in Ihrer Edge Encryption Implementierung zu vermeiden.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Legen Sie als Richtlinie sowohl die anfängliche Speichergrenze als auch die obere Speichergrenze auf denselben Wert fest. Weisen Sie dem Betriebssystem auf einem beliebigen Computer 2 GB des physischen Speichers zu. Weisen Sie dann den Rest des physischen Speichers dem Heap zu, indem Sie die Eigenschaften für die anfängliche Speichergrenze und die obere Speichergrenze verwenden. Weisen Sie beispielsweise auf einem Computer mit 8 GB Arbeitsspeicher dem Betriebssystem 2 GB zu, und weisen Sie die verbleibenden 6 GB (6144 MB) dem anfänglichen und dem oberen Speicher zu.

Wichtig: Wenn der Edge Encryption Proxy-Server ausgeführt wird, müssen Sie den Proxy-Server nach der Aktualisierung dieser Eigenschaften anhalten und neu starten.

Prozedur

1. Öffnen Sie in Ihrem Proxy-Server-Verzeichnis `<install dir>/conf/wrapper.conf`.
2. Fügen Sie am Ende der Datei die folgende Zeile hinzu, um die anfängliche Speichergrenze festzulegen:

```
wrapper.java.additional.<number>=-Xms<min_memory_in_MB>m
```

   Legen Sie `<number>` auf die nächst verfügbare `<number>` in Reihenfolge der Eigenschaften von `wrapper.java.additional.<number>` fest, die in der Datei `wrapper.conf` definiert sind.

Example
Beispielsweise verfügen Sie über die folgende Liste von Eigenschaften `wrapper.java.additional.<number>`:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
wrapper.java.additional.1=
wrapper.java.additional.2=
```

Die höchste `<number>` in der obigen Liste ist **2**. Wenn Sie die Zeile `wrapper.java.additional.<number>=-Xms<min_memory_in_MB>m` hinzufügen, setzen Sie `<number>` auf **3**, die nächst verfügbare Zahl.

Wichtig: Lassen Sie keine Lücken in der Nummerierungsfolge.

Setzen Sie `<min_memory_in_MB>` auf die Anzahl der verbleibenden Megabytes des Arbeitsspeichers, nachdem dem Betriebssystem 2 GB Arbeitsspeicher zugewiesen wurde.

3. Legen Sie die obere Speichergrenze fest.
   Da im Basissystem keine Obergrenze für den Arbeitsspeicher festgelegt ist, kann der Proxy-Server den gesamten verfügbaren Arbeitsspeicher verwenden. Wenn auf dem Server andere Dienste ausgeführt werden, können Sie die obere Speichergrenze festlegen.

   Fügen Sie am Ende der Datei die folgende Zeile hinzu:

   `wrapper.java.additional.<number>=-Xmx<max_memory_in_MB>m`

   Legen Sie `<number>` auf die nächst verfügbare `<number>` in Reihenfolge der Eigenschaften von `wrapper.java.additional.<number>` fest, die in der Datei `wrapper.conf` definiert sind.

   Example
   Beispielsweise verfügen Sie über die folgende Liste von Eigenschaften `wrapper.java.additional.<number>`:

   ```
   wrapper.java.additional.1=
   wrapper.java.additional.2=
   ```

   Die höchste `<number>` in der obigen Liste ist **2**. Wenn Sie die Zeile `wrapper.java.additional.<number>=-Xmx<max_memory_in_MB>m` hinzufügen, setzen Sie `<number>` auf **3**, die nächst verfügbare Zahl.

   Hinweis: Lassen Sie keine Lücken in der Nummerierungsfolge.

   Setzen Sie `<max_memory_in_MB>` auf die Anzahl der verbleibenden Megabytes des Arbeitsspeichers, nachdem dem Betriebssystem 2 GB Arbeitsspeicher zugewiesen wurde.

4. Speichern und schließen Sie die Datei.

Example: Beispiel: Festlegen der anfänglichen und oberen Speichergrenzen des Proxy-Servers

```
wrapper.java.additional.1 = -Djava.io.tmpdir=../tmp
wrapper.java.additional.2 = -Dcloudedge.home.dist=..
# must ensure UTF8 encoding when running on Windows
wrapper.java.additional.3 = -Dfile.encoding=UTF8
# additional properties for heap settings
wrapper.java.additional.4 = -Xms6144m
wrapper.java.additional.5 = -Xmx6144m
```

Nächste Maßnahme

Edge Encryption Proxy starten.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Edge Encryption Proxy starten

Nach dem Installieren und Konfigurieren eines Edge Encryption Proxys kann der Proxy aus der Befehlszeile gestartet werden.

Vorbereitungen

Erforderliche Rolle: admin

Überprüfen Sie vor dem Starten des Verschlüsselungs-Proxys folgende Punkte:

- Das Plugin Edge Encryption ist in der Instanz aktiviert.
- Die Datei `edgeencryption.properties` wurde auf diesem Rechner konfiguriert.
- Bei Verwenden eines ordnungserhaltenden Verschlüsselungstyps oder Verschlüsselungsmusters wird die Proxy-Datenbank ausgeführt.

Hinweis: Beim erstmaligen Einrichten der Datei `edgeencryption.properties` oder Ändern der Eigenschaften können Sie bei Bedarf die Eigenschaft für die Passwortverschlüsselung nicht festlegen. Nachdem Sie überprüft haben, dass alles funktioniert, können Sie die Passwortverschlüsselungseigenschaft festlegen, den Proxy herunterfahren und den Proxy erneut starten.

Prozedur

1. Führen Sie den Proxy-Server aus.

Option	Bezeichnung
Auf einem Linux-Rechner	**a.** `CD` zu `ServerName_port` **b.** Ausführen von `./startup.sh`
Auf einem Windows-Rechner	Führen Sie die folgenden Schritte aus der Befehlszeile als Administrator aus: **a.** `CD` zu `ServerName_port/bin` **b.** Ausführen von `edgeencryption.bat starten`

2. Überprüfen Sie das Protokoll auf dem Proxy-Server, um sicherzustellen, dass der Proxy ausgeführt wird.

Passwörter in der Eigenschaftendatei verschleiern

Verschleiern Sie Passwörter in der Datei „ `edgeencryption.properties` “, um die Eigenschaftendatei freigeben zu können, ohne dass Klartextpasswörter offengelegt werden.

Vorbereitungen

Erforderliche Rolle: admin

Stellen Sie sicher, dass der Edge Encryption Proxy-Server eingerichtet ist und erfolgreich ausgeführt wird, bevor Sie diese Eigenschaft festlegen. Bevor Sie diese Eigenschaft festlegen, Den Edge Encryption Proxy stoppen.

Warum und wann dieser Vorgang ausgeführt wird

Das Festlegen dieser Eigenschaft kann das Debuggen von Verbindungs- und Zugriffsproblemen beim ersten Start schwierig machen. Legen Sie diese Eigenschaft nur in Produktionsumgebungen fest, nachdem der Proxy erfolgreich eingerichtet und getestet wurde.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wechseln Sie in das Verzeichnis `<installation directory>/conf/`.
2. Erstellen Sie im Verzeichnis `conf` eine Textdatei, die eine komplexe Zeichenfolge oder einen Satz enthält, die als Passphrase verwendet werden kann, die der Proxy zum Verschleiern der Passwörter in der Datei `edgeencryption.properties` verwendet.
   Diese Passphrase sollte eine zufällige und komplexe Phrase sein, die sich nicht auf die Passwörter selbst bezieht.
3. Öffnen Sie die Datei `edgeencryption.properties`.
4. Legen Sie die Passwort-Verschlüsselungseigenschaft fest.
5. Speichern und schließen Sie die Datei `edgeencryption.properties`.

Nächste Maßnahme

Nachdem Sie diese Eigenschaft festgelegt haben, können Sie Edge Encryption Proxy starten.

Einen zusätzlichen Proxy manuell hinzufügen

Nachdem der erste Edge Encryption richtig konfiguriert und getestet wurde, können Sie zusätzliche Proxys auf einem Linux- oder Windows-Computer einrichten. Das Installieren mehrerer Proxys auf demselben Computer wird nicht empfohlen.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Fügen Sie zusätzliche Proxy-Server auf zusätzlichen Computern hinzu, um eine optimale Umgebung sicherzustellen. Siehe Umgebungsgröße Ihrer Edge Encryption anpassen, um die Anzahl zusätzlich erforderlicher Proxys zu bestimmen.

Hinweis: Stellen Sie sicher, dass alle Proxys die gleichen Verschlüsselungsschlüssel und dasselbe RSA-Schlüsselpaar haben, das zum digitalen Signieren von Konfigurations- und Verschlüsselungsregeln für die Verschlüsselung verwendet wird. Wenn eine Proxy-Datenbank als Teil der Installation eingerichtet wurde, müssen alle Proxys dieselbe Proxy-Datenbank verwenden.

Prozedur

1. Installieren Sie den Proxy mit dem entsprechenden Befehl.
   Weitere Informationen finden Sie unter Den Edge Encryption Proxy-Server (interaktives Installationsprogramm) installieren.
2. Kopieren Sie alle Verschlüsselungsschlüssel und die Datei `edgeencryption.properties` vom ersten Proxy zum neuen Proxy.
   Verschlüsselungsschlüssel befinden sich möglicherweise im Proxy-Schlüsselspeicher im Verzeichnis `/Keys` oder in einem SafeNet KeySecure-Schlüsselspeicher.
3. Öffnen Sie die Datei `edgeencryption.properties` auf dem neuen Proxy.
4. Ändern Sie die folgenden Eigenschaften:

Eigenschaft	Beschreibung
edgeencryption.proxy.name	Eindeutiger Name des Proxy-Servers
edgeencryption.proxy.host	Der Servername, die IP-Adresse oder der vollständig qualifizierte Domänenname des

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	Computers, auf dem der Proxy ausgeführt wird.
edgeencryption.proxy.http.port	Port auf dem Proxy für die HTTP-Kommunikation. Muss für alle Prozesse auf der Maschine eindeutig sein.
edgeencryption.proxy.https.port	Port auf dem Proxy für die HTTPS-Kommunikation. Muss für alle Prozesse auf der Maschine eindeutig sein.

5. Wenn Sie den Proxy-Server auf einem Windows-Computer installieren, müssen Sie den Namen des Service ändern. indem Sie die Datei `conf/wrapper.conf` auf dem neuen Proxy öffnen und die in der folgenden Tabelle aufgeführten Eigenschaften hinzufügen.

   Hinweis: Sie müssen diesen Schritt ausführen, bevor Sie den Proxy-Server starten.

Eigenschaft	Beschreibung
wrapper.ntservice.name	Eindeutiger Name des Edge Encryption Proxy-Service.
wrapper.ntservice.displayname	Anzeigename des Edge Encryption Proxy-Service.
wrapper.ntservice.description (optional)	Beschreibung des Proxy-Servers.

6. Speichern und schließen Sie die Datei.
7. Starten Sie den Proxy mit dem entsprechenden Befehl.
   Weitere Informationen finden Sie unter Edge Encryption Proxy starten.

Einen Edge Encryption Proxy-Server authentifizieren

Legen Sie fest, dass ein Proxy-Server eine vertrauenswürdige Quelle ist, sodass Edge Encryption Anforderungen von diesem Proxy-Server verarbeiten kann.

Vorbereitungen

Wenn ein Proxy-Server nicht authentifiziert ist, enthält das Protokoll der Konsole folgende Meldung:

```
WARN This Edge Encryption proxy has not yet been authenticated by the
 instance.
Please navigate to the matching Proxy record on your ServiceNow instance
 and authenticate it.
```

Wenn Sie versuchen, auf den Proxy zuzugreifen, wird die folgende Meldung angezeigt: `Diese Website ist nicht erreichbar`.

Damit der Proxy während des Upgrade-Vorgangs betriebsbereit bleibt, wird die Authentifizierung erst erforderlich, wenn das Proxy-Update erfolgreich war.

Erforderliche Rolle: admin

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Proxys**an.
2. Wählen Sie den Proxy aus, und klicken Sie auf **Authentifizieren**.

Ergebnisse

Der Proxy wechselt von **Nicht authentifiziert** zu **Ausstehend** zu **Authentifiziert**. Wenn Sie die Authentifizierung starten, ändert sich der Status von **Nicht** authentifiziert in **Ausstehend**. Wenn die Authentifizierung abgeschlossen ist, ändert sich der Status von **Ausstehend** in **Authentifiziert**, Sie können auf den Proxy zugreifen und Edge Encryption kann Anforderungen vom Proxy akzeptieren.

Hinweis: Wenn Sie den Proxy anhalten und neu starten, bleibt der Proxy **authentifiziert** und wird erfolgreich neu gestartet.

Den Edge Encryption Proxy stoppen

Sie können einen Edge Encryption Proxy aus der Befehlszeile stoppen.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Den Proxy-Server stoppen.

Option	Bezeichnung
Auf einem Linux-Rechner	Ausführen von `./shutdown.sh`
Auf einem Windows-Rechner	Ausführen von `edgeencryption.bat stoppen` Um den Windows-Dienst zu entfernen, führen Sie `edgeencryption.bat entfernen` aus.

2. Überprüfen Sie das Protokoll auf dem Proxy-Server, um zu überprüfen, ob der Proxy angehalten wurde.

Den Edge Encryption Proxy unter Linux deinstallieren

Sie können den Edge Encryption Proxy deinstallieren. Wenn Sie den Proxy aktualisieren, ist es nicht notwendig, die aktuelle Version herunterzufahren und zu deinstallieren.

Vorbereitungen

Erforderliche Rolle: admin

Sie müssen Zugriff auf den Computer haben, auf dem der Edge Encryption Proxy ausgeführt wird.

Warum und wann dieser Vorgang ausgeführt wird

Stellen Sie vor dem Herunterfahren des Edge Encryption Proxy sicher, dass keine Benutzer über den Proxy mit der Instanz verbunden sind.

Der unter Linux ausgeführte Verschlüsselungs-Proxy arbeitet als einzelner Prozess. Sie können diesen Prozess beenden, um Aufgaben wie das erneute Bereitstellen des

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verschlüsselungsproxys auf einem anderen Host-Computer, das Aktualisieren der Proxyversion, das Aktualisieren der Java-Version oder das Ändern des eindeutigen Namens des Verschlüsselungsproxys bei der Bereitstellung des Verschlüsselungsproxys auf mehreren Proxy-Servern zu erledigen.

Prozedur

1. Sie können die Datei `edgeencryption.properties` speichern, bevor Sie das Verteilerverzeichnis löschen.
2. Führen Sie das Shell-Skript `shutdown.sh` aus.
3. Überprüfen Sie das Protokoll auf dem Proxy-Server, um sicherzustellen, dass der Proxy-Server heruntergefahren ist.
4. Löschen Sie die Dateien im Verteilerordner.

Den Edge Encryption Proxy unter Windows deinstallieren

Sie können den Edge Encryption Proxy deinstallieren. Wenn Sie den Proxy aktualisieren, ist es nicht notwendig, die aktuelle Version herunterzufahren und zu deinstallieren.

Vorbereitungen

Erforderliche Rolle: admin

Sie müssen Zugriff auf den Computer haben, auf dem der Edge Encryption Proxy ausgeführt wird.

Stellen Sie vor dem Herunterfahren des Edge Encryption Proxy sicher, dass keine Benutzer über den Proxy mit der Instanz verbunden sind.

Prozedur

1. Sie können die Datei `edgeencryption.properties` speichern, bevor Sie das Verteilerverzeichnis löschen.
2. Ausführen von `edgeencryption.bat stoppen`
3. Ausführen `edgeencryption.bat entfernen`
4. Überprüfen Sie das Protokoll auf dem Proxy-Server, um zu überprüfen, ob der Proxy-Server heruntergefahren ist.
5. Löschen Sie die Dateien im Verteilerordner.

SSO für mehrere Anbieter mit Edge Encryption einrichten

Richten Sie SSO für mehrere Anbieter ein, um die Anmeldung über die Edge Encryption Proxy-Server-URL oder Instanz-URL zu ermöglichen. Wenn Sie Single Sign-on (SSO) für mehrere Provider mit aktiviertem Edge Encryption implementieren, müssen sich einige Benutzer möglicherweise über den Proxy-Server Edge Encryption bei Ihrer Instanz anmelden, andere Benutzer möglicherweise nicht.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Aktivieren Sie das Plugin für die Installation des Single Sign-On-Installationsprogramms für mehrere Anbieter (com.snc.integration.sso.multi.installer).
- Aktivieren Sie das Plugin Edge Encryption (com.glide.edgeencryption) und stellen Sie sicher, dass ein oder mehrere Proxy-Server in Ihrem Netzwerk eingerichtet sind.
- Bestimmen Sie die URL für den Edge Encryption Proxy-Server, über den sich Benutzer mit SSO mehrerer Anbieter anmelden. Zum Ermitteln der URL eines Edge Encryption Proxy-Servers, siehe Edge Encryption wird installiert.

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Der Anwender, der sich anmeldet, muss die entsprechende URL verwenden, um sich anzumelden, und zwar entweder mit Edge-Proxy oder ohne Edge-Proxy.

- Wenn alle Benutzer über den Edge Encryption Proxy-Server geleitet werden, richten Sie Ihren Anbieter-Identifizierungsdatensatz ein und definieren Sie die Proxy-Server-URL in den Feldern **ServiceNow Homepage**, **Entitäts-ID/Aussteller** und **URI der Zielgruppe**.
- Um einige Benutzer über den Proxy-Server und einige Benutzer an die Instanz weiterzuleiten, erstellen Sie zwei Anbieter-Identifizierungsdatensätze. Beide Datensätze verwenden den gleichen Wert im Feld **URL des Identitätsanbieters**. Einer der Datensätze wird jedoch über den Proxy-Server geleitet, während der andere zur Instanz führt.
  - Anmeldung über Instanzname: `https://` <instance name> .service-now.com/ login_with_sso.do?glide_sso_id= <sys_id des IdP-Datensatzes für Nicht-Edge-Proxy
  - Melden Sie sich über den Edge-Proxy an: `https://` <edge hostname> :<port> / login_with_sso.do?glide_sso_id= <sys_id des IdP-Datensatzes für den Edge-Proxy

Prozedur

1. Aktivieren Sie die Duplizierung von Identitätsanbieter-URLs in Identitätsanbieter-Datensätzen.
   Eine eindeutige Einschränkung verhindert die Duplizierung der Identitätsanbieter-URL in zwei verschiedenen Identitätsanbieter-Datensätzen. Sie können die Duplizierung der URL des Identitätsanbieters in mehreren IdP-Datensätzen aktivieren, indem Sie ein Feld auf „false“ setzen.
   a. Navigieren zu **Systemdefinition** > **Lexikon**an.
   b. Öffnen Sie Identitätsanbietertabelle [saml2_update1_properties] den Definitionsdatensatz für das Feld **idp**.
   c. Konfigurieren Sie das Formular, um das Feld **Eindeutig** hinzuzufügen.
   d. Stellen Sie sicher, dass der Wert im Feld **Eindeutig** auf **Falsch** gesetzt ist.
2. Navigieren zu **Mehrfachanbieter-SSO** > **Identity Provider**an.
3. Erstellen Sie zwei Identitätsanbieter-Datensätze für denselben Identitätsanbieter: einen mit der Instanz-URL und einen mit der Edge Encryption Proxy-Server-URL.
   Informationen zum Erstellen eines Identitätsanbieter-Datensatzes finden Sie unter Externen Identitätsanbieter erstellen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Füllen Sie für die Edge Encryption Proxy-Server-URL das Formular mit diesen Werten aus.

Feld	Wert
URL des Identitätsanbieters	Importiert aus den IdP-Metadaten.
ServiceNow Homepage	Die URL für Ihre Proxy-Server-Startseite. Zum Beispiel: `https://<proxy hostname>:<port>/navpage.do`
Entitäts-ID/Aussteller	`https://<proxy hostname>:<port>`
Zielgruppen-URI	`https://<proxy hostname>:<port>`

b. Klicken Sie auf **Absenden**.

c. Füllen Sie für die Instanz-URL das Formular mit diesen Werten aus.

Feld	Wert
URL des Identitätsanbieters	Importiert aus den IdP-Metadaten.
ServiceNow Homepage	`https://<instance>.service-now.com/navpage.do`
Entitäts-ID/Aussteller	`https://<instance>.service-now.com/navpage.do`
Zielgruppen-URI	`https://<instance>.service-now.com/navpage.do`

d. Klicken Sie auf **Absenden**.

4. Wahlweise: Wenn Sie mehrere Identitätsanbieter verwenden, ändern Sie den MultiSSO-Installations-Exit.

a. Navigieren zu **Systemdefinition** > **Installationsausgänge**an.
Das System zeigt die aktuelle Liste der Installations-Exits an.

b. Öffnen Sie **MultiSSO** Installations-Exit.

c. Lokalisieren Sie die folgende Anweisung im Feld **Skript**.

```
var samlResponseTxt = request.getParameter("SAMLResponse");
if (!GlideSession.get().isLoggedIn() &&
 GlideStringUtil.notNil(samlResponseTxt)) {
    var idpRecord = this.getIdPRecord(request);
    if (idpRecord) {
        SSO_Helper.debug("IdP found based on SAML response: " +
 idpRecord.getUniqueValue());
        return new SSO_Helper(idpRecord.getUniqueValue(), false, null,
 true);
    }
}
```

d. Ersetzen Sie die Anweisung durch den folgenden Code.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
var samlResponseTxt = request.getParameter("SAMLResponse");
if (!GlideSession.get().isLoggedIn() &&
 GlideStringUtil.notNil(samlResponseTxt)) {
   /* // You have two profiles that use the same IdP entity id it
 cannot use
   // the IdP issuer / entity id from the response otherwise it may
 result in the
   // wrong IdP profile. IdP initiated login will not work
   var idpRecord = this.getIdPRecord(request);
   if (idpRecord) {
      SSO_Helper.debug("IdP found based on SAML response: " +
 idpRecord.getUniqueValue());
      return new SSO_Helper(idpRecord.getUniqueValue(), false, null,
 true);
      }*/
   return new SSO_Helper(null, true);
   }
```

Hinweis: Die durch IdP initiierte Anmeldung funktioniert in dieser Konfiguration nicht.

e. Klicken Sie auf **Aktualisieren**.

5. Wahlweise: Wenn Sie mehr als ein Unternehmen verwenden, konfigurieren Sie Anwender für SSO mit mehreren Anbietern, und aktualisieren Sie sys_id des Identitätsanbieter-Datensatzes abhängig vom Anwender.

(Optional) Weitere Informationen finden Sie unter Benutzer für Mehrfachanbieter-SSO konfigurieren.

- Um einen Benutzer für die Anmeldung über den Edge Encryption Proxy-Server zu konfigurieren, verwenden Sie die sys_id des Identitätsanbieter-Datensatzes, der die Edge Encryption Proxy-Server-URL verwendet.
- Um einen Benutzer für die Anmeldung an der Instanz zu konfigurieren, verwenden Sie die sys_id des Identitätsanbieter-Datensatzes, der die Instanz-URL verwendet.

Login-URLs

URL	Login-Ziel
`https://<proxy hostname>:<port>/login_with_sso.do?glide_sso_id=<sys_id of the IdP record for the proxy server URL>`	Meldet sich über den Proxy-Server an.
`https://<instance name>.service-now.com/login_with_sso.do?glide_sso_id=<sys_id of IdP record for the instance URL>`	Meldet sich über die Instanz an.

Eigenschaften des Edge Encryption Proxy-Servers

Die Konfigurationsdatei `edgeencryption.properties` im Ordner `<installation directory>/conf/` enthält Eigenschaften zum Konfigurieren Ihrer Umgebung.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie müssen den Proxy-Server neu starten, nachdem Sie Änderungen an den Eigenschaften des Proxy-Servers vorgenommen haben.

Klartext und statische IV-Eigenschaften

edgeencryption.customer.assigned.known.cleartext	Klartext, damit die Instanz überprüfen kann, ob alle Proxys die gleichen Schlüssel verwenden. Beim Start verschlüsselt der Proxy den Klartext und sendet den verschlüsselten Text an die Instanz. Die Instanz kennt weder den Klartext, noch werden an die Instanz Schlüssel gesendet. Diese Eigenschaft muss für alle Proxys gleich sein.
edgeencryption.encrypter.static.iv	Statischer IV (Initialisierungsvektor), der in der gleichstellungserhaltenden und ordnungserhaltenden Verschlüsselung verwendet wird. Diese Eigenschaft muss für alle Proxys identisch sein und genau 16 Byte (16 ASCII-Zeichen) sein.

Eigenschaften der digitalen Signatur

edgeencryption.proxy.signature.keystore.path	Pfad und Name der Java KeyStore-Datei.
edgeencryption.proxy.signature.keystore.password	Passwort. Das Standardpasswort lautet <changeme>. Ändern Sie das Passwort nach der Installation des Java KeyStore.
edgeencryption.proxy.signature.keystore.keyalias	Das als Alias angegebene Argument -alias, wenn das RSA-Schlüsselpaar generiert wird.

Dateispeichereigenschaft

edgeencryption.keyfile.directory	Das Verzeichnis gibt an, wo Schlüsseldateien gespeichert werden. Wenn Sie den Java KeyStore oder einen SafeNet KeySecure-Schlüsselspeicher verwenden, lassen Sie diese Eigenschaft auskommentiert. Beispiel: `edgeencryption.keyfile.directory=keys` Wenn Sie Schlüssel für Unbound Technology verwenden, deaktivieren Sie diese Eigenschaft und setzen Sie den Wert auf das Schlüsselverzeichnis.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Allgemeine Konfigurationseigenschaften

edgeencryption.config.poll.interval	Abrufintervall in Sekunden. Die Standardeinstellung bedeutet, dass es 5 Sekunden dauert, bis der Proxy von Änderungen der Verschlüsselungskonfiguration erfährt. Größere Werte führen dazu, dass die Instanz länger braucht, um einen Offline-Proxy zu erkennen. ⚠ **Warnung:** Diese Eigenschaft nicht ändern. Das Ändern der Standardeinstellung des Proxy-Abrufintervalls kann zu Erkennungsverzögerungen führen, wenn ein Proxy online geschaltet wird.
edgeencryption.rules.dir	Ordner, in dem die Verschlüsselungsregeln auf dem Proxy gespeichert sind.
edgeencryption.encryption.order_preserving.cache.enable	Die Einstellung bestimmt, ob Caching zur Unterstützung von ordnungserhaltenden Verschlüsselungstypen verwendet wird.
edgeencryption.encryption.order_preserving.cache.size	Maximale Cache-Größe, in Bytes.
edgeencryption.jobs.concurrency	Maximale Anzahl von Massenverschlüsselungsaufträgen, die gleichzeitig auf diesem Proxy ausgeführt werden können.
edgeencryption.jobs.requests_per_second	Anzahl der HTTP-Auftragsanforderungen pro Sekunde, die von diesem Proxy an die Instanz gesendet werden können.
edgeencryption.attachments.request.timeout.seconds	Zeitüberschreitung für das Hochladen von Anhängen in Sekunden.
edgeencryption.request.buffer.size	Größe einer Verschlüsselungsanforderung. Wenn eine Verschlüsselungsanforderung größer als diese Größe ist, wird der Überschuss auf der Festplatte gespeichert. ⚠ **Warnung:** Diese Eigenschaft nicht ändern.
edgeencryption.httpclient.request.buffer.size	Größe der Client-Anforderung. Wenn die Client-Anforderung größer als diese Größe ist, wird der Überschuss auf der Festplatte gespeichert. ⚠ **Warnung:** Diese Eigenschaft nicht ändern.
„edgeencryption.httpclient.header.size“	Größe des Anforderungs-/Antwort-Headers.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

	• Mindestwert: 8.000 • Höchstwert: 32.000 ⚠ **Warnung:** Diese Eigenschaft nicht ändern.
edgeencryption.proxy.idle.timeout	Zeit in Sekunden, nach der eine Transaktion abläuft. Standardwert: 300 (Sekunden)
edgeencryption.proxy.keepalive.interval	Zeit in Sekunden zwischen den vom Proxy an die Instanz ausgegebenen Pings. Pings werden regelmäßig ausgegeben, um die Verbindung zwischen dem Proxy und der Instanz zu überprüfen. • Standardwert: 10 (Sekunden) • Mindestwert: 5 (Sekunden)
edgeencryption.register.retry.count	Maximale Anzahl von Pings, die der Proxy an die Instanz sendet, um die Registrierung zu versuchen. Standardwert: 0 (keine Begrenzung)
edgeencryption.tokenization.exclusion.list	Verschlüsselungsmuster können in diesen Feldern gefundene Zeichenfolgen nicht tokenisieren.

Java KeyStore-Eigenschaften

edgeencryption.keystore.path	Pfad zum Java KeyStore. Wenn Sie einen Dateispeicher oder einen SafeNet KeySecure-Schlüsselspeicher verwenden, lassen Sie diese Eigenschaft auskommentiert. Beispiel: `edgeencryption.keystore.path = keystore/keystore.jceks`
edgeencryption.keystore.password	Passwort, das der Proxy für die Verbindung zum Java KeyStore verwendet. Wenn Sie einen Dateispeicher oder einen SafeNet KeySecure-Schlüsselspeicher verwenden, lassen Sie diese Eigenschaft auskommentiert.

Protokollierungseigenschaften

Die Protokollierungseigenschaften befinden sich in der Datei lo4gj2.properties im<installation directory> `/conf/-Verzeichnis`. Diese Eigenschaften werden nur zur Problembehandlung oder auf Anweisung des Supports für ServiceNow geändert. Einzelheiten hierzu finden Sie unter So erhöhen Sie die Debug-Protokollierung für den Edge Encryption-Proxy .

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

NAE-Geräteschlüsselspeicher-Eigenschaften

edgeencryption.nae.retries	Anzahl der Wiederholungsversuche.
edgeencryption.nae.enabled	Die Einstellung zeigt an, ob ein NAE-Gerät verfügbar ist.
edgeencryption.nae.server	Name des NAE-Servers
edgeencryption.nae.port	Vom NAE-Server verwendeter Port.
edgeencryption.nae.protocol	Vom NAE-Server verwendetes Protokoll.
edgeencryption.nae.keystore.path	Pfad zum Keystore auf dem NAE-Server.
edgeencryption.nae.keystore.password	NAE-Schlüsselspeicherpasswort.
edgeencryption.nae.username	Benutzername, der zur Authentifizierung beim NAE-Gerät verwendet werden soll.
edgeencryption.nae.password	Passwort zur Authentifizierung beim NAE-Gerät.
edgeencryption.nae.client.certificate	Das Zertifikat, das sich im Keystore des NAE-Servers befindet. Legen Sie diese Eigenschaft für die Authentifizierung mithilfe eines Zertifikats anstelle von Benutzername und Passwort fest.

Passworteigenschaft

edgeencryption.encrypter.properties.password	Name der Datei im Ordner `conf`, der eine Zeichenfolge enthält, die innerhalb eines sicheren Prozesses zum Verschleiern von Passwörtern in der Datei `edgeencryption.properties` verwendet wird. **Hinweis:** Name der Datei im Ordner `conf`, der eine Zeichenfolge enthält, die innerhalb eines sicheren Prozesses zum Verschleiern von Passwörtern in der Datei `edgeencryption.properties` verwendet wird.

Proxy-Eigenschaften

edgeencryption.proxy.host	Servername, IP-Adresse oder vollständig qualifizierter Domänenname des Computers, auf dem der Proxy ausgeführt wird. Zusammen mit dem Port definiert diese Eigenschaft die URL, die der Client für den Zugriff auf den Proxy-Server verwendet.
edgeencryption.proxy.name	Proxy-Name Muss für jeden Proxy eindeutig sein.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

edgeencryption.proxy.http.port	Port auf dem Proxy für die HTTP-Kommunikation.
edgeencryption.proxy.https.port	Port auf dem Proxy für die HTTPS-Kommunikation.

Eigenschaft für gesperrte Proxy-Konfiguration

edgeencryption.proxy.locked	Bei „Wahr“ akzeptiert der Proxy keine Konfigurationsänderungen der Verschlüsselung oder Änderungen der Verschlüsselungsregel von der Instanz. Legen Sie diese Eigenschaft für die Produktionsinstanz fest, nachdem alle Verschlüsselungskonfigurationen und Regeln abgeschlossen sind.

Proxy-Datenbankeigenschaften

edgeencryption.db.url	Proxy-Datenbankspeicherort Muss für alle Verschlüsselungs-Proxys identisch sein, die eine Verbindung mit derselben Instanz herstellen.
edgeencryption.db.user	Benutzername für den Zugriff auf die Proxy-Datenbank. Muss für alle Verschlüsselungs-Proxys identisch sein, die eine Verbindung mit derselben Instanz herstellen.
edgeencryption.db.password	Passwort für den Zugriff auf die Proxy-Datenbank. Muss für alle Verschlüsselungs-Proxys identisch sein, die eine Verbindung mit derselben Instanz herstellen.
edgeencryption.db.name	Proxy-Datenbankname. Muss für alle Verschlüsselungs-Proxys identisch sein, die eine Verbindung mit derselben Instanz herstellen. Der Standardwert für diese Eigenschaft ist `„edgeencryption“`.
edgeencryption.db.bootstrap.file	Bootstrap-Datei für die Proxy-Datenbank. Die Datei ist relativ zum Verzeichnis `sql/`. Muss für alle Verschlüsselungs-Proxys identisch sein, die eine Verbindung mit derselben Instanz herstellen. ⚠ **Warnung:** Unter normalen Umständen sollte dieser Parameter nicht geändert werden.

Proxy-Server-Performance-Eigenschaften

Proxy-Server-Performance-Eigenschaften sind standardmäßig nicht in der Konfigurationsdatei vorhanden. Um die Standardwerte zu ändern, müssen Sie die Eigenschaften hinzufügen und

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

den Proxy-Server neu starten. Weitere Informationen finden Sie unter Diagnose und Leistung der Edge Encryption.

edgeencryption.stat.collection.enabled	Aktiviert die Erfassung von Statistiken, die vom Edge Encryption Proxy-Server-Performance-Dashboard verwendet werden. Standardwert: true Fügen Sie diese Eigenschaft hinzu, und setzen Sie den Wert auf „false“, um die Sammlung von Statistiken zu deaktivieren, die vom Edge Encryption Proxy-Server-Performance-Dashboard verwendet werden.
edgeencryption.stat.collection.interval	Intervallzeit in Sekunden, in der der Edge Encryption Proxy-Server Statistiken erfasst. Der Wert darf nicht unter 30 Sekunden liegen. Standardwert: 30 (Sekunden)

SSL-Zertifikateigenschaften

Starten Sie Ihren Proxy neu, wenn Sie den Wert einer SSL-Zertifikateigenschaft ändern. Das System verwendet beim Start das HTTPS-Schlüsselpaar zum Herstellen der Proxy-Server-Verbindung sowie zum Bestimmen, wie der Proxy Client-Anforderungen beantwortet.

edgeencryption.proxy.https.cert.alias	Alias des Zertifikats, das vom Proxy-Server für die Verbindung von Clients bereitgestellt wird.
edgeencryption.proxy.https.keystore.path	Pfad zum Schlüsselspeicher, der das HTTPS-Zertifikat enthält.
edgeencryption.proxy.https.keystore.password	Passwort für den Schlüsselspeicher, der das HTTPS-Zertifikat enthält.

Zieleigenschaften (Instanz)

edgeencryption.target.host	Hostname für die Instanz. Muss für alle Verschlüsselungs-Proxys identisch sein, die eine Verbindung mit derselben Instanz herstellen. Diese Eigenschaft wird festgelegt, wenn der Proxy installiert wird. Zum Beispiel `instancename.servicenow.com`
edgeencryption.target.port	Instanzport. Muss für alle Verschlüsselungs-Proxys identisch sein, die eine Verbindung mit derselben Instanz herstellen. Diese Eigenschaft wird festgelegt, wenn der Proxy installiert wird.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

edgeencryption.target.protocol	Instanzprotokoll. Muss für alle Verschlüsselungs-Proxys identisch sein, die eine Verbindung mit derselben Instanz herstellen. Diese Eigenschaft wird festgelegt, wenn der Proxy installiert wird. Verfügbare Optionen: • http • https

Eigenschaften für nicht Unbound Technology-Anbieter

edgeencryption.ekm.provider.classname	Interner Klassenname für die Implementierung. ⚠ **Warnung:** Diese Eigenschaft nicht ändern.
edgeencryption.thirdparty.vendor.library.path	Pfad zur Unbound API-JAR-Datei auf dem Unbound-Client-Computer.
edgeencryption.ekm.provider.rsa.wrapping.keyalias	Wrapping-Schlüsselalias in der Implementierung der Unbound Technology. Muss für alle Proxys gleich sein.

Benutzer-Account-Eigenschaften

edgeencryption.target.username	Benutzername, mit dem sich der Proxy bei der Instanz anmeldet. Der Benutzer muss über die Rolle „edge_encryption“ verfügen. Weitere Informationen finden Sie unter Benutzerkonto für die Edge Encryption einrichten.
edgeencryption.target.password	Passwort, mit dem sich der Proxy bei der Instanz anmeldet.

Web-Proxy-Eigenschaften

edgeencryption.webproxy.host	Webproxy-Name oder IP-Adresse
edgeencryption.webproxy.port	Port auf dem Web-Proxy.
edgeencryption.webproxy.user	Benutzername, der zum Herstellen einer Verbindung zum Web-Proxy verwendet wird. Wenn Ihr Web-Proxy keine Authentifizierung verwendet, lassen Sie diese Eigenschaft auskommentiert.
edgeencryption.webproxy.password	Passwort für die Verbindung zum Web-Proxy. Wenn Ihr Web-Proxy keine Authentifizierung verwendet, lassen Sie diese Eigenschaft auskommentiert.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Veraltete Proxy-Verschlüsselungseigenschaften

edgeencryption.encrypter.default.key128

Gibt den Namen des aktuellen AES 128-Schlüssels an. Ein AES 128-Schlüssel muss verfügbar sein, auch wenn er nicht verwendet wird. Muss für alle Proxys gleich sein.

Führen Sie die Wartung dieser Schlüssel in der Instanz durch.

edgeencryption.encrypter.default.key256

Gibt den Namen des aktuellen AES 256-Schlüssels an. Muss für alle Proxys gleich sein.

Führen Sie die Wartung dieser Schlüssel in der Instanz durch.

edgeencryption.encrypter.key

Gibt den Schlüsselnamen für jeden Schlüssel an und wird verwendet, um die Standardschlüssel anzugeben. Dies ist der Schlüsselalias, der in die Metadaten integriert ist, die in jedem verschlüsselten Element enthalten sind und daher in der Instanz gespeichert werden. Der Schlüsselname muss aus Kleinbuchstaben bestehen.

edgeencryption.encrypter.type

Gibt den Typ des Verschlüsselungs-Schlüsselspeichersystems an.

edgeencryption.encrypter.file

Gibt den Pfad und den Dateinamen der dem Schlüssel zugeordneten Textdatei an.

edgeencryption.encrypter.password

Gibt das Passwort für den Zugriff auf den Schlüsselspeicher an.

CyberArk-Integration mit dem Edge-Proxy-Server

Verwenden Sie CyberArk, um Passwörter in einem zentralen und sicheren digitalen Tresor zu speichern, um Passwörter zu sichern, die zuvor im Klartext gespeichert und durch Dateizugriff gesichert wurden oder zuvor über eine zweite Datei verschlüsselt wurden.

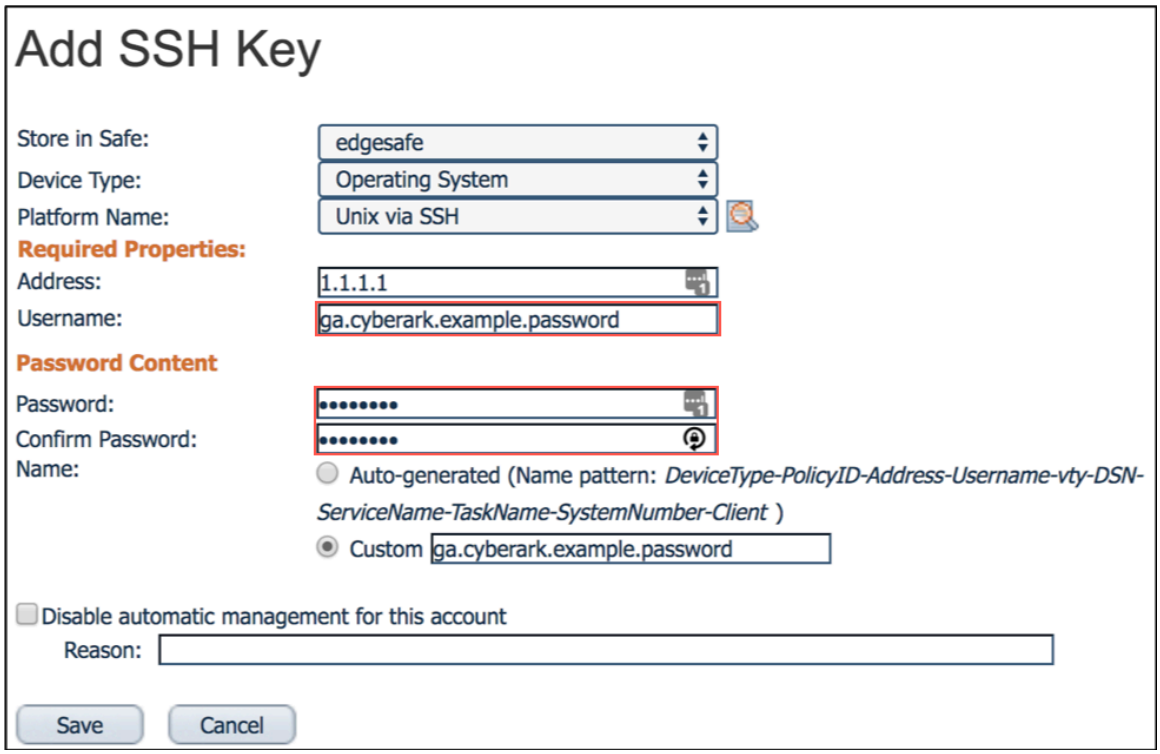
CyberArk AIM (Application Identity Management) verhindert unautorisierten Zugriff, indem hartcodierte und sichtbare Passwörter entfernt werden. AIM speichert Passwörter in einem digitalen Tresor auf einem unabhängigen gehärteten Server, wobei die Passwörter als digitale Anmeldeinformationen dargestellt werden. Die AIM-Clients (die Edge-Proxy-Server) verwenden die digitalen Anmeldeinformationen von CyberArk und greifen auf den unabhängigen Server zu, um die gesicherten Passwörter abzurufen. Auf den Edge-Proxy-Servern oder in der Instanz werden keine Passwörter gespeichert.

CyberArk-Anmeldeinformationen für digitale Tresore

Sie müssen CyberArk erwerben und konfigurieren, bevor Sie die CyberArk-Integration mit dem Edge-Proxy-Server einrichten können.

Legen Sie zum Hinzufügen eines Berechtigungsnachweises für CyberArk (der vom Edge-Proxy gelesen wird) den **Plattformnamen** der Anmeldeinformation auf **Unix über SSH** fest und stellen Sie sicher, dass Sie entweder einen **benutzerorientierten** Anmeldeinformations**namen** generieren oder den **Automatisch generierten** Ausweis**namen** notieren. Wenn Sie den Edge-Proxy für die Verwendung dieser Anmeldeinformation konfigurieren, stimmt der Proxy-Server mit dem **Namen** dieser Anmeldeinformation zur Einstellung im Proxy überein.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



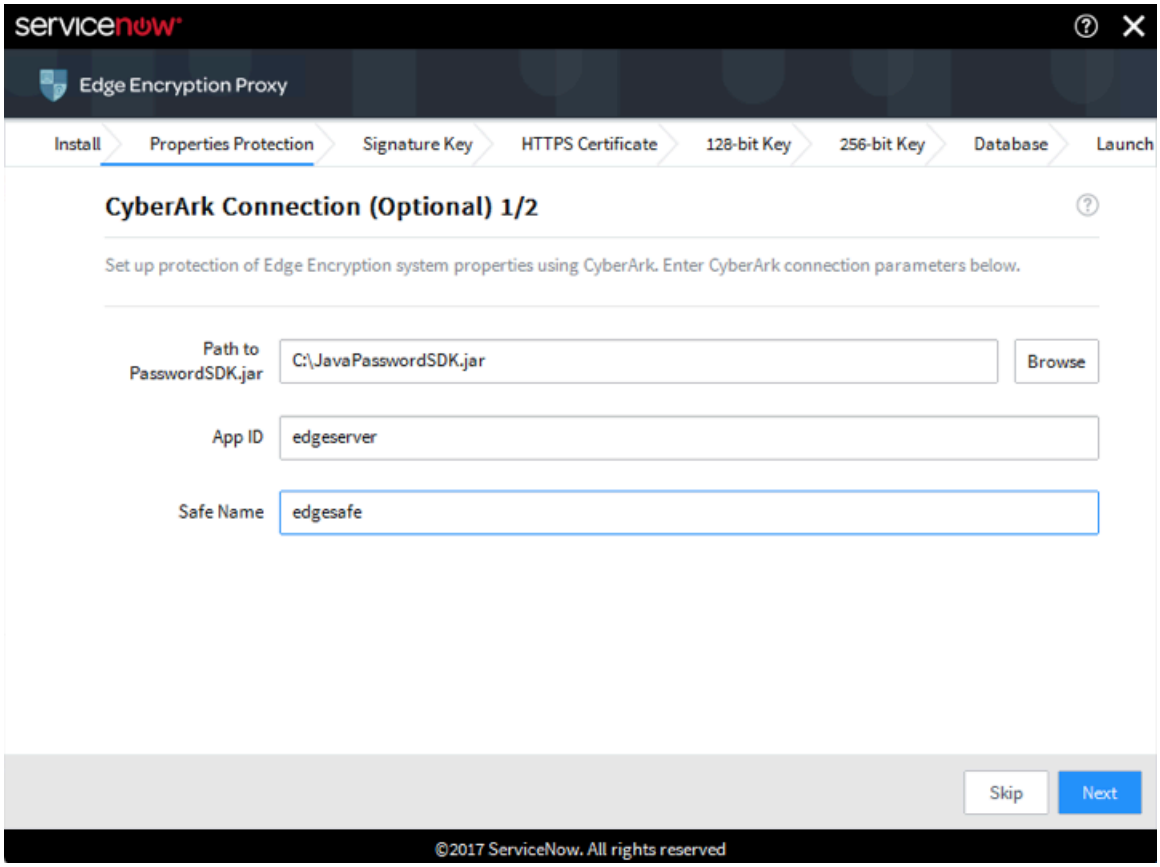
Jeder Anmeldeinformationseintrag enthält ein **Passwort**, das gespeichert wird, sowie einen **Namen** für die Anmeldeinformation, der von einer Anwendung für den Zugriff auf dieses Passwort verwendet wird.

Hinweis: CyberArk-Anmeldeinformationen sind keine Verschlüsselungsschlüssel.

Hinzufügen von CyberArk während der Installation eines Edge-Proxys

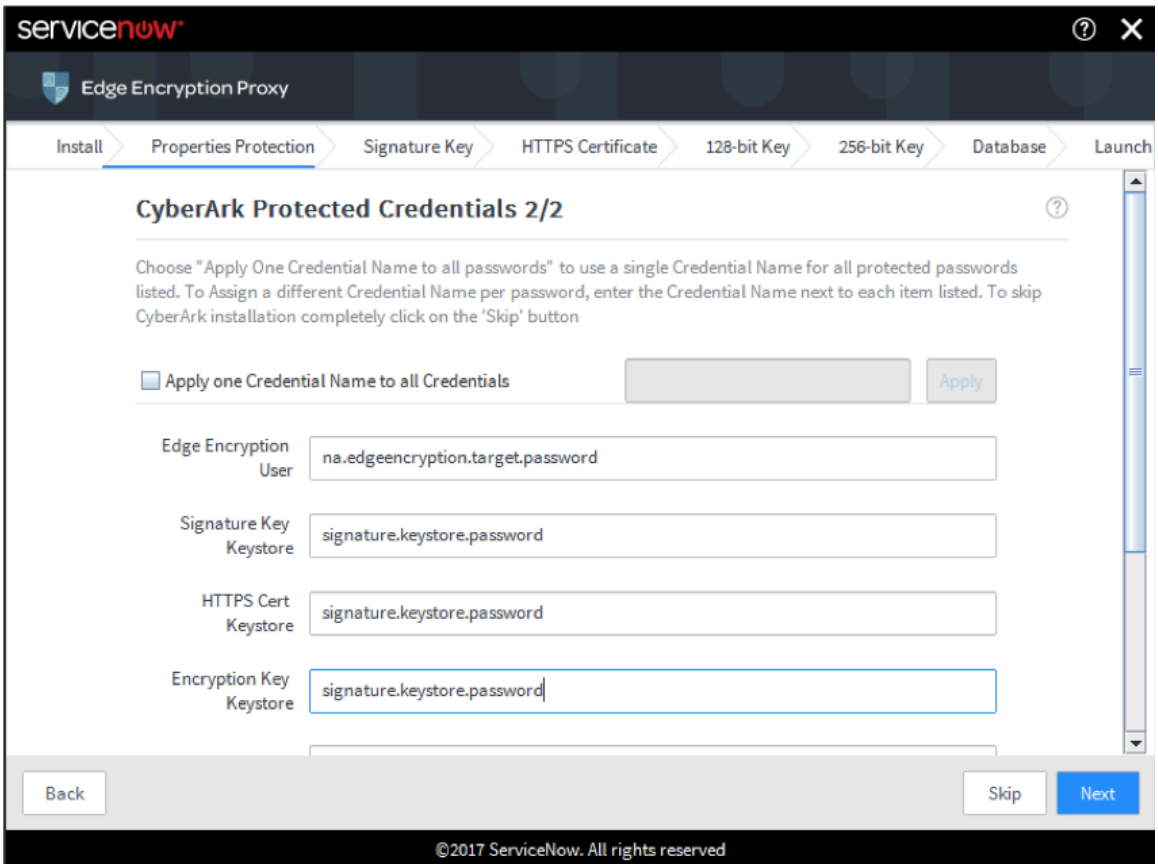
Das Proxy-Installationsprogramm enthält eine neue Konfigurationsseite für eine CyberArk-Integration. Diese Seite ist optional, wenn Sie CyberArk bei der Installation Ihres Proxy mit dem Proxy-Installationsprogramm nicht einschließen möchten. Sie können die CyberArk-Integration auch manuell in der Konfigurationsdatei einrichten und konfigurieren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Das Proxy-Installationsprogramm enthält auch eine neue Seite für CyberArk-geschützte Anmeldeinformationen. Auf dieser Seite können verschiedene Eigenschaften mit einem oder mehreren Namen für die Anmeldeinformationen konfiguriert werden. Diese Seite ist optional, wenn Sie CyberArk bei der Installation Ihres Proxy mit dem Proxy-Installationsprogramm nicht einschließen möchten.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



CyberArk-Passwortschutz

Jedes Passwortfeld im Edge-Proxy-Installationsprogramm, für das eine CyberArk-Anmeldeinformation im CyberArk-Tresor konfiguriert und auf der Seite mit den geschützten Anmeldeinformationen von CyberArk des Installationsprogramms angegeben ist, ist grau und enthält die Nachricht `Von CyberArk geschützt`.

Einen Load Balancer mit dem Edge-Proxy-Server verwenden

Sie können einen Load Balancer verwenden, um die Last auf den Proxy-Servern in Ihrem Edge Encryption Proxy-Setup auszugleichen. Wenn der Load Balancer und die Proxy-Server unterschiedliche Ports verwenden, geben Sie den Hostnamen und den HTTPS-Port des Load Balancer an, damit Benutzer die Antworten in ihrem Browser anzeigen können.

Wichtig: Alle Produktionsumgebungen sollten aus Gründen der Redundanz mindestens zwei Edge Encryption Proxy-Server enthalten.

Edge-Anforderungsverarbeitung ohne Load Balancer

Wenn Sie keinen Load Balancer verwenden, wird eine Anforderung wie im Folgenden beschrieben verarbeitet.

1. Der Benutzer gibt eine Anforderung von einem Browser aus.
2. Der Browser sendet die Anforderung an den Edge-Proxy-Server.
3. Der Proxy-Server sendet die Anforderung an die ServiceNow-Instanz.
4. Die ServiceNow-Instanz gibt die Antwort an den Proxy-Server zurück.
5. Der Proxy-Server fügt in der Antwortkopfzeile seine eigene Portnummer hinzu, bevor er die Antwort an den Browser des Benutzers zurücksendet.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Anforderung wurde erfolgreich abgeschlossen, da der Benutzer die Antwort des Proxy-Servers unter der in der Antwortkopfzeile angegebenen Anschlussnummer anzeigen kann.

Edge-Anforderungsverarbeitung mit einem Load Balancer

Wenn Sie jedoch einen Load Balancer verwenden, kommuniziert der Browser des Benutzers direkt mit dem Load Balancer, nicht mit dem Proxy-Server. Eine Anforderung wird wie im Folgenden beschrieben verarbeitet.

Hinweis: Das folgende Beispiel verwendet `1025` als Portnummer des Proxy-Servers.

1. Der Benutzer gibt eine Anforderung von einem Browser aus.
2. Der Browser sendet die Anforderung an eine virtuelle IP (VIP) des Load Balancers, die auch als virtueller Server bezeichnet wird.
3. Der VIP ist so konfiguriert, dass er auf den Proxy-Server verweist (z. B. `10.2.200.148:1025`). Somit leitet der Load Balancer die Anforderung an den Proxy-Server weiter.
4. Der Proxy-Server sendet die Anforderung an die ServiceNow-Instanz.
5. Die ServiceNow-Instanz gibt die Antwort an den Proxy-Server zurück.
6. Der Proxy-Server schreibt die Location-Kopfzeile in der Antwort mit Werten um, die in den Eigenschaften von `risk-servicenow.dev.echonet:1025` konfiguriert sind.
   - **Host**: `edgencryption.proxy.host`
   - **HTTP-Port**: `edgeencryption.proxy.http.port`
   - **HTTPS-Port**: `edgeencryption.proxy.https.port`
7. Der Proxy-Server leitet die Antwort an den Load Balancer weiter, wobei die Location-Kopfzeile auf den Port des Proxy-Servers verweist.

Das Ergebnis hängt davon ab, ob Load Balancer und Proxy-Server denselben Port verwenden.

- Wenn Load Balancer und Proxy-Server denselben Port verwenden, ist die Anforderung erfolgreich, da der Benutzer die Antwort vom selben Port empfängt, der in der Antwort-Kopfzeile angegeben ist.
- Wenn Load Balancer und Proxy-Server unterschiedliche Ports verwenden, schlägt die Anforderung fehl, da der Browser des Benutzers nur mit dem Load Balancer kommuniziert, die Antwort sich jedoch auf dem Proxy-Server befindet.

Lösung

Sie können das Problem beheben, indem Sie einfach den Load Balancer und alle Edge-Proxy-Server am selben Port verwenden. Dies ist jedoch keine ideale Lösung. Eine bessere Lösung besteht darin, das System wissen zu lassen, welchen Port der Load Balancer verwendet.

Die folgenden Eigenschaften ermöglichen es, dass der Edge-Proxy-Server Antwortnachrichten an den Load Balancer weiterleiten kann, wenn Proxy-Server und Load Balancer unterschiedliche Ports verwenden.

- *`edgeencryption.proxy.rewrite.location.host`* gibt den Hostnamen an, der für den Zugriff auf ServiceNow über den Load Balancer verwendet wird.
- *`edgeencryption.proxy.rewrite.location.https.port`* gibt den HTTPS-Port an, der für den Zugriff auf ServiceNow über den Load Balancer verwendet wird.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Den Load Balancer konfigurieren

Wenn der Load Balancer und die Proxy-Server unterschiedliche Ports verwenden, geben Sie den Hostnamen und den HTTPS-Port des Load Balancer an, damit Benutzer die Antworten in ihrem Browser anzeigen können.

Vorbereitungen

Erforderliche Rollen:

- Lokaler oder Domänenadministrator auf einem Windows-Host
- Service-Benutzer mit vollem Dateisystemzugriff auf einem Linux-Host

Prozedur

1. Melden Sie sich als Administrator, Domänenadministrator oder Service-Benutzer beim Proxy-Server-Host an.
2. Navigieren Sie zum Installationsverzeichnis für den Edge-Proxy und wählen Sie `conf/edgeencryption.properties`.
3. Setzen Sie die folgenden Eigenschaften:

Eigenschaft	Beschreibung
edgeencryption.proxy.rewrite.location.host	Wenn Ihre Edge-Konfiguration einen Load Balancer enthält, um die Last zwischen Proxy-Servern auszugleichen, werden die Antworten auf den Load Balancer neu geschrieben, so dass Anfragen abgeschlossen werden können. ◦ Wenn im Proxy-Setup ein Load Balancer vorhanden ist, geben Sie den Hostnamen an, mit dem Sie über den Load Balancer auf ServiceNow zugreifen. ◦ Optional: Wenn im Proxy-Setup kein Lastenausgleichsmodul vorhanden ist, können Sie diesen Wert auf den vom Proxy-Server verwendeten Hostnamen festlegen.
edgeencryption.proxy.rewrite.location.https.port	Wenn Ihre Edge-Konfiguration einen Load Balancer zum Ausgleich der Last zwischen Proxy-Servern enthält, geben Sie den HTTPS-Port an, über den auf ServiceNow über den Load Balancer zugegriffen wird. ◦ Wenn in der Konfiguration ein Load Balancer vorhanden ist, geben Sie den HTTPS-Port an, über den der Zugriff auf ServiceNow über den Load Balancer erfolgt. ◦ Optional: Wenn in der Konfiguration kein Lastenausgleichsmodul vorhanden ist,

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	können Sie diesen Wert auf den vom Proxy-Server verwendeten HTTPS-Port festlegen.

4. Speichern Sie die Datei.

Ergebnisse
Anforderungen können abgeschlossen werden, da Benutzer jetzt Antworten in ihrem Browser anzeigen können.

Upgrade von Edge Encryption

Sowohl Instanz-Upgrades als auch Proxy-Server-Upgrades erfordern in einer Edge Encryption-Umgebung eine besondere Berücksichtigung.

Instanz-Upgrades

Instanz-Upgrades in einer Edge-Encryption-Umgebung erfordern Vorsicht, um sicherzustellen, dass die Edge-Steuerelemente nach dem Instanz-Upgrade ordnungsgemäß funktionieren.

Während eines Instanz-Upgrades sollten Sie Folgendes nicht hinzufügen, bearbeiten oder löschen:

- Edge Encryption-Konfigurationen
- Edge Encryption-Regeln
- Edge Encryption-Tokenisierungsmuster
- Geplante Aufträge für die Edge Encryption
- Edge Encryption-Schlüsselkonfigurationen
- Geplante Upgrades für die Edge Encryption
- IP-Konfigurationen für Edge Encryption auf Deny-Liste

Ein geplanter Auftrag, der während des Instanz-Upgrades ausgeführt wird, wird nicht abgeschlossen. Um den unterbrochenen Auftrag abzuschließen, führen Sie den Auftrag nach dem Instanz-Upgrade erneut aus. Wenn Sie den Auftrag neu einplanen, geht die Verarbeitung, die vor dem Instanz-Upgrade stattgefunden hat, nicht verloren, und der Auftrag verarbeitet weiterhin nur die Daten, die noch nicht verarbeitet wurden.

Proxy-Server-Upgrades

Planen Sie ein Proxy-Upgrade, damit die Instanz den Edge Encryption Proxy-Server aktualisieren oder den Proxy-Server jederzeit manuell aktualisieren kann.

⚠ **Warnung:** Bei einem Upgrade unter Windows können Probleme mit Dateisperren auftreten, und das Upgrade schlägt möglicherweise fehl. Für ein erfolgreiches Upgrade dürfen im Installationsverzeichnis keine Dateien geöffnet sein. Außerdem darf im Installationsverzeichnis keine Shell vorhanden sein. Insbesondere wenn Sie den Proxy über die Befehlszeile starten (über `bin\edgeencryption.bat install/start`), während Sie sich im Installationsverzeichnis befinden, sollten Sie diese Shell schließen oder sie anschließend aus dem Installationsverzeichnis verschieben. Keine Dateien im Installationsverzeichnis dürfen mit einem Editor oder einer anderen Anwendung geöffnet werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bibliotheken von Drittparteien

Bibliotheken von Drittparteien, z. B. Gemalto, gehen bei Upgrades von Instanzen und Proxy-Servern verloren, wenn sie sich im selben Verzeichnis befinden. Um den Verlust von Drittparteibibliotheken während Upgrades zu verhindern, können Sie wie folgt vorgehen:

1. Fügen Sie die folgende Eigenschaft manuell zu „edgeencryption.properties“ hinzu:

   ```
   „edgeencryption.ekm.provider.classname“ =
   com.snc.edgeencryption.encryption.CloudEdgeNaeKeyProvider
   ```

2. Fügen Sie die Standorteigenschaft der Lieferantenbibliothek *edgeencryption.thirdparty.vendor.library.path* hinzu, und legen Sie sie auf `/path/to/jars`fest.

   Beispiel:

   ```
   „edgeencryption. thirdparty.vendor.library.path“ = /app/servicenow/libs
   ```

3. Kopieren Sie die SafeNet-JARs in diesen Pfad.

Nachdem Sie die Drittparteibibliotheken außerhalb der Edge Encryption -Installation installiert haben, gehen sie bei Upgrades nicht mehr verloren.

Geplante Upgrades

Wichtig: Aktualisieren Sie bei Upgrades der ServiceNow -Instanz auch die Version Ihres Proxy-Servers, um sie an die Version Ihrer -Instanz anzupassen und das Risiko von Kompatibilitätsproblemen zu verringern.

Planen Sie ein Upgrade, damit die Instanz den Proxy-Server zum geplanten Zeitpunkt aktualisieren kann. Diese Funktionalität ist nach dem Upgrade standardmäßig verfügbar. Ein geplantes Upgrade umfasst folgende Events:

1. Der Proxy-Server überprüft bei der Instanz, ob eine neue Version für das Upgrade verfügbar ist. Neue Versionen werden im Allgemeinen verfügbar, wenn die Instanz aktualisiert wird.
2. Der Administrator erhält beim Anmelden eine Benachrichtigung, wenn eine neue Version des Proxy-Servers verfügbar ist.
3. Der Administrator kann für jeden Proxy-Server Ein Upgrade des Edge Encryption Proxy-Servers planen.

   Hinweis: Nur Benutzer mit der Rolle „security_admin“ können einen Upgrade-Zeitplan über den Proxy-Server erstellen.

4. Sobald das Upgrade geplant ist, wird der Proxy-Server automatisch zum geplanten Zeitpunkt aktualisiert. Während des Upgrades ist der Proxy-Server nur für kurze Zeit offline.

   Hinweis: Da der Proxy-Server während des Upgrades neu startet, ist er für kurze Zeit offline. Die Zeitdauer wird von Ihrer Umgebung bestimmt und wie lange es dauert, den Proxy-Dienst zu stoppen und erneut zu starten.

5. Während des geplanten Upgrades wird ein neues Proxy-Verzeichnis erstellt und Ihre Konfigurationsdateien werden in das neue Verzeichnis kopiert. Neue Eigenschaften werden in Ihre vorhandene Eigenschaftendatei geschrieben. Die folgenden Dateien oder Verzeichnisse in Ihrem alten Proxy-Verzeichnis werden in das neue Proxy-Verzeichnis kopiert.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Das Verzeichnis `/conf`
- Das Verzeichnis `/keys`
- Das Verzeichnis `/keystore`
- Die Datei `java/jre/lib/security/cacerts`

Dadurch bleiben Ihre Schlüssel, Schlüsselspeicher, Einstellungen und Zertifikate erhalten.

Hinweis: Nur die oben genannten Dateien werden in das neue Proxy-Verzeichnis kopiert. Andere angepasste Dateien im Proxy-Server-Verzeichnis werden während eines geplanten Upgrades nicht beibehalten. Die Upgrade-Protokolldatei befindet sich im ursprünglichen Proxy-Verzeichnis im folgenden Ordner: `<original-proxy-directory>/tmp/upgrade-wrapper/bin`.

Voraussetzungen für geplante Upgrades

Stellen Sie vor dem Planen eines Upgrades für einen Edge Encryption Proxy Folgendes sicher:

1. Die Umgebungsvariable *JAVA_HOME* verweist auf eine Java-Installation auf dem Computer, der sich außerhalb der Verzeichnisstruktur des Edge Encryption Proxys befindet.
2. Die Umgebungsvariable *JAVA_HOME* verweist auf eine Java-Installation mit Version 1.8_u144 oder höher.
3. Der Parameter *-Djava.io.tmpdir* in der Datei wrapper.conf des Edge Encryption Proxy zeigt auf ein Verzeichnis außerhalb der Verzeichnisstruktur des Edge Encryption Proxys. Der Proxy verfügt über Lese-/Schreib-/Ausführungsberechtigungen für das Verzeichnis. Optional können Sie den Parameter vollständig auskommentieren, sodass Java seinen Standard-TMP-Speicherort verwendet.

Manuelle Upgrades

Anstatt einen Aktualisierungszeitplan zu erstellen, können Sie jeden Proxy-Server über die Befehlszeile manuell aktualisieren. Siehe Einen unter Linux laufenden Edge Encryption Proxy-Server manuell aktualisieren oder Einen unter Windows laufenden Edge Encryption Proxy-Server manuell aktualisieren.

Proxy-Build-Status

Sie können leicht feststellen, ob ein Proxy-Server veraltet ist, indem Sie zu navigieren **Konfiguration der Edge Encryption** > **Proxys** > **Alle**an. Der Status Ihres Proxy-Builds wird in der Spalte **Proxy Build** mit den folgenden Farben dargestellt:

Grün

Ihr Proxy-Server ist auf dem neuesten Stand.

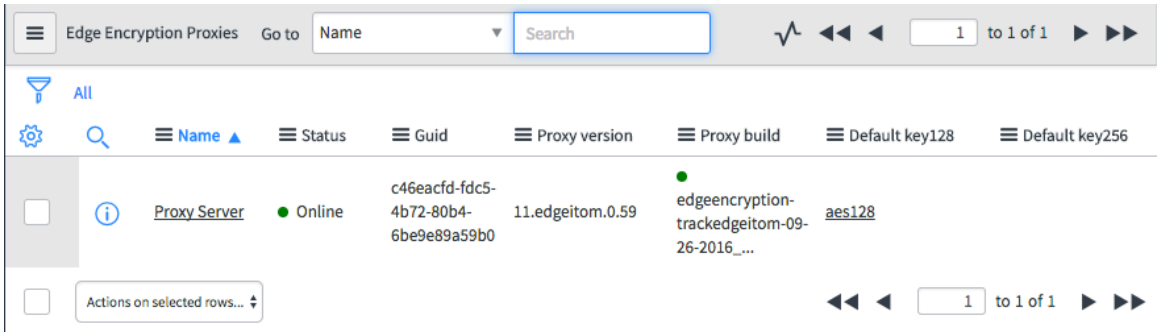
Gelb

Ihr Proxy-Server ist veraltet und ein Upgrade ist erforderlich.

Orange

Upgrade fehlgeschlagen. Ihr Proxy-Server wird auf die alte Version zurückgesetzt, um sicherzustellen, dass keine Ausfallzeiten auftreten.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Problembehandlung bei einem fehlgeschlagenen geplanten Proxy-Upgrade

Wenn ein geplantes Proxy-Upgrade fehlschlägt, wird der Proxy-Server auf die Version zurückgesetzt, von der Sie ein Upgrade durchführen. Alle Originaldaten, Schlüssel und Konfigurationsdateien bleiben erhalten. Dieser Vorgang kann mehrere Minuten dauern. Kontaktieren Sie Kundenservice und Support, um ein erfolgreiches Upgrade sicherzustellen.

Um den Grund für den Fehler zu ermitteln, können Sie **Fehlergrund** im Upgrade-Zeitplan überprüfen. Darüber hinaus wird das Installationsverzeichnis für das fehlgeschlagene Upgrade beibehalten, sodass Protokolldateien für die Problembehandlung verfügbar sind.

Hinweis: Überprüfen Sie vor dem Löschen zusätzlicher Proxy-Verzeichnisse immer, welches Verzeichnis aktuell ist, indem Sie die Protokolldateien überprüfen. Wenn die Protokolldateien eine aktuelle Aktivität aufweisen, ist der Proxy möglicherweise mit Ihrer Instanz verbunden.

Wenn ein geplantes Proxy-Upgrade wiederholt fehlschlägt, können Sie Ihren Proxy-Server manuell aktualisieren. Weitere Informationen finden Sie unter Einen unter Linux laufenden Edge Encryption Proxy-Server manuell aktualisieren und Einen unter Windows laufenden Edge Encryption Proxy-Server manuell aktualisieren.

Java-Mindestanforderungen

Auf dem Hostcomputer, auf dem der Proxy-Server Edge Encryption installiert oder ausgeführt wird, muss eine unterstützte Version von Java installiert sein. Derzeit unterstützte Versionen sind Java 11.0.6 oder höher in der 11.x-Versionsserie

Hinweis: Java 8 wird ab dem Release Utah nicht mehr unterstützt. Aktualisieren Sie Ihre Umgebung mit dem Proxy Edge Encryption auf Java 11, bevor Sie versuchen, die Version Edge Encryption des Proxys [Utah zu installieren.

Wenn Sie die AES 256-Bit-Verschlüsselung mit Java 8 Update 141 (8u141) oder niedriger verwenden, müssen Sie die Java Cryptography Extension (JCE) Jurisdiction Policy Files installieren, indem Sie sie in das Java-Stammverzeichnis des Systems des jeweiligen Edge Encryption Proxy-Server-Host kopieren. Fügen Sie diese Dateien dem Ordner `<Java-home-directory>/jre/lib/security` hinzu, bevor Sie ein geplantes oder manuelles Upgrade durchführen. Informationen zur Installation der Richtliniendateien für die AES-256-Bit-Verschlüsselung finden Sie unter Den AES 256-Bit-Verschlüsselungsschlüssel konfigurieren.

Umgebungen mit gemischten Proxy-Versionen

Obwohl eine Umgebung, in der alte Versionen des Proxy-Servers mit aktuellen Versionen des Proxy-Servers ausgeführt werden, nicht empfehlenswert ist, wird sie unterstützt, wenn sich alle Proxy-Server in der gleichen Versionsfamilie wie Ihre Instanz befinden. Wenn Sie beispielsweise eine Instanz im Xanadu Release haben, unterstützt Ihre Umgebung Proxy-Server von jedem Xanadu Patch oder Hotfix. Es gelten jedoch die folgenden Einschränkungen.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn ein Proxy-Server Funktionen unterstützt, die ein anderer Proxy nicht unterstützt, tritt ein inkonsistentes Verhalten auf, je nachdem, welcher Proxy-Server verwendet wird.
- Wenn ein Proxy-Server nicht mehr aktuell ist, enthält er möglicherweise keine aktuellen Sicherheitsverbesserungen.

Wenn ein Proxy-Server aus einer früheren Version mit einer neueren Version der Instanz registriert wird, erhalten Sie regelmäßig Benachrichtigungen, dass der Proxy-Server nicht mehr aktuell ist. Um eine optimale und sichere Umgebung zu gewährleisten, empfiehlt ServiceNow, den Proxy-Server stets auf die neueste Version der von Ihrer Instanz unterstützten Software zu aktualisieren.

Ein Upgrade für den Edge Encryption Proxy-Server planen

Erstellen Sie einen Upgrade-Zeitplan, damit die Instanz einen veralteten Proxy-Server aktualisieren kann.

Vorbereitungen

Um ein Upgrade zu planen, müssen Sie über den Proxy-Server bei Ihrer Instanz angemeldet sein.
Wenn Sie die AES 256-Bit-Verschlüsselung mit Java 8 Update 141 (8u141) oder niedriger verwenden, müssen Sie die Java Cryptography Extension (JCE) Jurisdiction Policy Files installieren, indem Sie sie in das Java-Stammverzeichnis des Systems des jeweiligen Edge Encryption Proxy-Server-Host kopieren. Fügen Sie diese Dateien dem Ordner `<Java-home-directory>/jre/lib/security` hinzu, bevor Sie ein geplantes oder manuelles Upgrade durchführen. Informationen zur Installation der Richtliniendateien für die AES-256-Bit-Verschlüsselung finden Sie unter Den AES 256-Bit-Verschlüsselungsschlüssel konfigurieren.

Erforderliche Rolle: security_admin

Warum und wann dieser Vorgang ausgeführt wird

Sobald das Upgrade geplant ist, wird der Proxy-Server automatisch zum geplanten Zeitpunkt aktualisiert. Während des Upgrades ist der Proxy-Server nur für kurze Zeit offline.

Hinweis: Da der Proxy-Server während des Upgrades neu startet, ist er für kurze Zeit offline. Die Zeitdauer wird von Ihrer Umgebung bestimmt und wie lange es dauert, den Proxy-Dienst zu stoppen und erneut zu starten.

Während des geplanten Upgrades wird ein neues Proxy-Verzeichnis erstellt und Ihre Konfigurationsdateien werden in das neue Verzeichnis kopiert. Neue Eigenschaften werden in Ihre vorhandene Eigenschaftendatei geschrieben. Die folgenden Dateien oder Verzeichnisse in Ihrem alten Proxy-Verzeichnis werden in das neue Proxy-Verzeichnis kopiert.

- Das Verzeichnis `/conf`
- Das Verzeichnis `/keys`
- Das Verzeichnis `/keystore`
- Die Datei `java/jre/lib/security/cacerts`

Dadurch bleiben Ihre Schlüssel, Schlüsselspeicher, Einstellungen und Zertifikate erhalten.

Hinweis: Nur die oben genannten Dateien werden in das neue Proxy-Verzeichnis kopiert. Andere angepasste Dateien im Proxy-Server-Verzeichnis werden während eines geplanten Upgrades nicht beibehalten. Die Upgrade-Protokolldatei befindet sich im ursprünglichen Proxy-Verzeichnis im folgenden Ordner: `<original-proxy-directory>/tmp/upgrade-wrapper/bin`.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn mehrere Proxy-Server nicht mehr aktuell sind, muss für jeden Proxy-Server ein Upgrade individuell geplant werden.

Hinweis: Vermeiden Sie das Hosten mehrerer Proxy-Server auf demselben Computer. Wenn Ihre Umgebung diese Konfiguration enthält, sollten Sie jedoch nicht gleichzeitig Upgrades für mehrere Proxys auf demselben Computer planen.

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Proxys** > **Upgrade-Zeitpläne**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie das Formular aus.

Formular für den Zeitplan für die Aktualisierung des Edge Encryption Proxy

Feld	Beschreibung
Proxy-Server	Proxy-Server wird aktualisiert.
Zielversion	Version, auf die Sie Ihren Proxy-Server aktualisieren. Dieser Wert ist schreibgeschützt und auf die aktuellste für Ihre Instanz verfügbare Proxy-Version festgelegt.
Geplante Startzeit	Datum und Uhrzeit, zu der das Upgrade gestartet werden soll.
Aktiv	Gibt an, ob das geplante Upgrade aktiv ist. Wenn dieses Feld nicht ausgewählt ist, wird das Upgrade nicht zum geplanten Datum und zur geplanten Uhrzeit ausgeführt.
Status	Der Upgrade-Status. Dieser Wert ist schreibgeschützt. Mögliche Status sind: ◦ Ausstehend ◦ Wird ausgeführt ◦ Abgeschlossen ◦ Fehlgeschlagen

4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Die typische Zeit für ein Upgrade beträgt weniger als 15 Minuten. Nachdem ein Upgrade ausgeführt wurde, können Sie die Upgrade-Details überprüfen, um mehr darüber zu erfahren. Wenn Ihr Upgrade fehlgeschlagen ist, überprüfen Sie **Fehlergrund**, um die nächsten Schritte festzulegen.

Upgrade-Details

Feld	Beschreibung
Ab Version	Die Version, von der der Server aktualisiert wurde.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Upgrade-Details (Fortsetzung)

Feld	Beschreibung
Zur Version	Die Version, auf die der Server aktualisiert wurde.
Tatsächliche Startzeit	Zeit, zu der das Upgrade begann.
Endzeit	Uhrzeit, zu der das Upgrade beendet wurde.
Fehlergrund	Grund für das Fehlschlagen des Upgrades.

Einen unter Linux laufenden Edge Encryption Proxy-Server manuell aktualisieren

Einen Proxy aktualisieren, der unter Linux ausgeführt wird.

Vorbereitungen

Wenn Sie die AES 256-Bit-Verschlüsselung mit Java 8 Update 141 (8u141) oder niedriger verwenden, müssen Sie die Java Cryptography Extension (JCE) Jurisdiction Policy Files installieren, indem Sie sie in das Java-Stammverzeichnis des Systems des jeweiligen Edge Encryption Proxy-Server-Host kopieren. Fügen Sie diese Dateien dem Ordner `<Java-home-directory>/jre/lib/security` hinzu, bevor Sie ein geplantes oder manuelles Upgrade durchführen. Informationen zur Installation der Richtliniendateien für die AES-256-Bit-Verschlüsselung finden Sie unter Den AES 256-Bit-Verschlüsselungsschlüssel konfigurieren.

Erforderliche Rolle: security_admin oder lokaler Administrator auf dem Hostcomputer

Prozedur

1. Laden Sie die Edge Encryption Proxy-Update-Archivdatei in das Installationsverzeichnis herunter.
   a. Navigieren zu **Konfiguration der Edge Encryption** > **Installation und Downloads** > **Downloads**
   b. Wählen Sie den Link **Befehlszeilen-Installationsprogramm herunterladen**.
   c. Wählen Sie zu Beginn des Downloads Ihr Installationsverzeichnis als Download-Speicherort aus.
2. Wechseln Sie in das Installationsverzeichnis.
3. Führen Sie den folgenden Befehl aus:

```
java -jar edgeencryption-dist-<version>-linux-x86-64.jar -m dist-upgrade
-c <proxy directory>
```

Option	Beschreibung
Proxy-Verzeichnis	Das Verzeichnis im Installationsverzeichnis, in dem der Proxy ursprünglich installiert wurde. Dieses Verzeichnis wird von der Installation erstellt.

Wenn Sie den Hilfebildschirm anzeigen möchten, führen Sie diesen Befehl ohne Argumente aus: `java -jar edgeencryption-dist-<version>-linux-x86-64.jar`

Es wird ein neues Proxy-Verzeichnis mit einem aktuellen Zeitstempel erstellt. Eine Sicherung des alten Proxy-Verzeichnisses wird als „backup.dist-upgrade_timestamp“ im neuen Proxy-Installationsverzeichnis verwaltet. Der alte Proxy wird heruntergefahren und der neue Proxy

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

gestartet. Alle offenen Verbindungen/Transaktionen auf dem alten Proxy-Server werden beendet.

4. Überprüfen Sie das Proxy-Protokoll im neuen Verzeichnis und in der Instanz, um sicherzustellen, dass der neue Proxy ausgeführt wird.

Einen unter Windows laufenden Edge Encryption Proxy-Server manuell aktualisieren

Einen Proxy aktualisieren, der unter Windows ausgeführt wird.

Vorbereitungen

Wenn Sie die AES 256-Bit-Verschlüsselung mit Java 8 Update 141 (8u141) oder niedriger verwenden, müssen Sie die Java Cryptography Extension (JCE) Jurisdiction Policy Files installieren, indem Sie sie in das Java-Stammverzeichnis des Systems des jeweiligen Edge Encryption Proxy-Server-Host kopieren. Fügen Sie diese Dateien dem Ordner `<Java-home-directory>/jre/lib/security` hinzu, bevor Sie ein geplantes oder manuelles Upgrade durchführen. Informationen zur Installation der Richtliniendateien für die AES-256-Bit-Verschlüsselung finden Sie unter Den AES 256-Bit-Verschlüsselungsschlüssel konfigurieren.

Erforderliche Rolle: security_admin oder lokaler Administrator auf dem Hostcomputer

Prozedur

1. Laden Sie die Edge Encryption Proxy-Update-Archivdatei in das Installationsverzeichnis herunter.
   a. Navigieren zu **Konfiguration der Edge Encryption** > **Installation und Downloads** > **Downloads**
   b. Wählen Sie den Link **Befehlszeilen-Installationsprogramm herunterladen**.
   c. Wählen Sie zu Beginn des Downloads Ihr Installationsverzeichnis als Download-Speicherort aus.
2. Starten Sie das Windows-CMD-Terminalprogramm mit Administratorrechten.
3. Wechseln Sie in das Installationsverzeichnis.
4. Führen Sie den folgenden Befehl aus:

```
Java -Jar-Edge-Verschlüsselung-Verteilung-<version> -all.jar -m dist-upgrade -c<proxy directory>
```

Option	Beschreibung
Proxy-Verzeichnis	Das Verzeichnis im Installationsverzeichnis, in dem der Proxy ursprünglich installiert wurde. Dieses Verzeichnis wird von der Installation erstellt.

Wenn Sie den Hilfebildschirm anzeigen möchten, führen Sie den folgenden Befehl ohne Argumente aus: `Java -Jar Edge-Verschlüsselung-Dist-`<version> -all.jar

Es wird ein neues Proxy-Verzeichnis mit einem aktuellen Zeitstempel erstellt. Eine Sicherung des alten Proxy-Verzeichnisses wird als „backup.dist-upgrade_timestamp“ im neuen Proxy-Installationsverzeichnis verwaltet. Der alte Proxy wird heruntergefahren und der neue Proxy gestartet. Alle offenen Verbindungen/Transaktionen auf dem alten Proxy-Server werden beendet.

5. Überprüfen Sie das Proxy-Protokoll im neuen Verzeichnis und in der Instanz, um zu überprüfen, ob der Proxy aktualisiert wurde und ausgeführt wird.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein Upgrade des Edge Encryption Proxy-Servers rückgängig machen

Wenn ein Proxy-Upgrade nicht erfolgreich ist, können Sie zur vorherigen Version zurückkehren.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn ein Upgrade bei Verwendung der geplanten Upgrade-Funktion in der Version Xanadu fehlschlägt, wird der Proxy-Server automatisch auf die alte Version zurückgesetzt. Der alte Proxy-Server wird unverändert in einem Sicherungsverzeichnis gespeichert.

Wenn Sie ein manuelles Upgrade rückgängig machen möchten, können Sie diese Schritte ausführen.

Prozedur

1. Fahren Sie den Proxy herunter.
2. Löschen Sie das neue Proxy-Verzeichnis.
3. Benennen Sie das Sicherungsverzeichnis in den Proxy-Namen um.
   Das Sicherungsverzeichnis befindet sich im Proxy-Installationsverzeichnis mit dem Namen `<proxy name>_backup`
4. Starten Sie den Proxy.
5. Überprüfen Sie das Proxy-Protokoll und die Instanz, um sicherzustellen, dass der Proxy online ist.

Konfigurieren von Edge Encryption

Nachdem der Edge Encryption Proxy-Server installiert ist und ausgeführt wird, verwalten Sie Edge Encryption über den Proxy-Server.

Sie müssen alle Schritte unter Edge Encryption wird installiert ausführen, bevor Sie Verschlüsselungskonfigurationen und Verschlüsselungsmuster auf der Instanz erstellen.

Hinweis: Um auf die Konfiguration von Edge Encryption zugreifen zu können, müssen Sie sich über den Proxy-Server anmelden und zur Rolle security_admin wechseln.

Rotation von Verschlüsselungsschlüsseln

Führen Sie die Rotation von Verschlüsselungsschlüsseln aus der Instanz aus. Fügen Sie einen neuen Schlüssel hinzu, ändern Sie die Standardschlüsselzuordnung, und planen Sie dann einen Massenschlüssel-Rotationsauftrag oder eine Einzelschlüsselrotation.

Bevor Sie einen Verschlüsselungsschlüssel als Standardschlüssel festlegen, stellen Sie den Schlüssel für jeden Proxy zur Verfügung. Dadurch wird sichergestellt, dass die Proxys den Schlüssel zur Verschlüsselung von Daten haben, wenn der Schlüssel als Standardschlüssel zugewiesen wird. Alle Proxys müssen Zugriff auf einen Schlüssel haben, bevor dieser Schlüssel als Standardschlüssel zugewiesen werden kann.

Warnung: Bevor Sie einen Schlüssel aus dem Proxy löschen, müssen Sie einen Massenschlüssel-Rotationsauftrag einrichten und ausführen, um sicherzustellen, dass keine Daten in der Instanz den Schlüssel verwenden. Wenn noch Daten mit diesem Schlüssel verschlüsselt sind, können Sie die Informationen nicht mehr entschlüsseln, nachdem der Schlüssel gelöscht wurde.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Edge-Filterung und Sortierverhalten

Stellen Sie jedes Mal, wenn Sie Standardschlüssel ändern, sicher, dass Sie eine Schlüsselrotation (Massen- oder Einzelschlüsselrotation) durchführen. Andernfalls erhalten Sie unter Umständen unerwartete Ergebnisse beim Sortieren und Filtern von Datensätzen. Stellen Sie sich zum Beispiel das folgende Szenario vor:

1. Sie erstellen mit einem einzigen Verschlüsselungsschlüssel verschlüsselte Datensätze.
2. Sie erstellen einen neuen Schlüssel und legen diesen als Standard fest.
3. Sie erstellen mit dem neuen Verschlüsselungsschlüssel einen neuen Satz verschlüsselter Datensätze.

Wenn Sie nach einem beliebigen verschlüsselten Feld filtern, während eine Verbindung über den Edge-Proxy hergestellt ist, werden möglicherweise nicht alle Datensätze richtig herausgefiltert, oder es werden gegebenenfalls Datensätze unerwarteterweise angezeigt. Der Filter funktioniert nur für Datensätze, die mit dem aktuellen Standardschlüssel verschlüsselt sind. Die Datensätze, die mit dem vorherigen Standardschlüssel verschlüsselt wurden, werden weiterhin in der Listenansicht angezeigt.

Wenn Sie nach einem beliebigen verschlüsselten Feld sortieren, während eine Verbindung über den Edge-Proxy hergestellt ist, werden zwei Gruppen von Datensätzen mit demselben visuell lesbaren Text im verschlüsselten Feld angezeigt.

Einen Einzelschlüssel-Rotationsauftrag planen

Planen Sie einen Auftrag, um Daten zu finden, die mit einem bestimmten Schlüsselalias verschlüsselt sind, und verschlüsseln Sie die Daten dann erneut mit dem aktuellen Standardverschlüsselungsschlüssel. Die Daten werden entschlüsselt, bevor sie mit dem Standardschlüssel erneut verschlüsselt werden.

Vorbereitungen

Erforderliche Rolle: security_admin
Aktualisieren Sie vor dem Planen dieses Auftrags den Standardschlüssel in **Konfiguration der Edge Encryption** > **Konfiguration des Verschlüsselungsschlüssels** > **Standardschlüssel festlegen**an.

Prozedur

1. Navigieren zu **Konfiguration der Edge Encryption** > **Reserviert** > **Einzelschlüsselrotation planen**an.
2. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Wert
Name	Geben Sie einen beschreibenden Namen ein.
Auftragsart	Wählen Sie **Einzelschlüsselrotation**.
Schlüssel	Geben Sie den Schlüssel ein, der stillgelegt werden soll. Stellen Sie sicher, dass dieser Schlüssel nicht mehr der Standardschlüssel in ist **Konfiguration der Edge Encryption** > **Konfiguration des Verschlüsselungsschlüssels** > **Standardschlüssel festlegen**an.
Anzahl der Datensätze schätzen	Geschätzte Gesamtzahl der zu verarbeitenden Datensätze. Nicht verfügbar, wenn eine Einzelschlüsselrotation ausgeführt wird.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
Historische Datensätze verarbeiten	Wählen Sie diese Option aus, um historische Datensätze in der Audit-Tabelle zu verarbeiten, wenn das Feld geprüft wird. Wenn Sie historische Datensätze für ein Feld in der Audit-Tabelle verschlüsseln, werden sowohl neue als auch alte Werte verschlüsselt. Dieses Feld ist schreibgeschützt und aktiv. Weitere Informationen zu geprüften Feldern finden Sie unter Auditing.
Schätzen Sie die maximale Anzahl der Audit-Datensätze	Geschätzte maximale Anzahl der Audit-Datensätze, die verarbeitet werden sollen. Nicht verfügbar, wenn eine Einzelschlüsselrotation ausgeführt wird.
Aktiv	Deaktivieren Sie dieses Kontrollkästchen, wenn Sie diesen Auftrag deaktivieren möchten.
Ausführen	Wählen Sie den Zeitraum zwischen den Auftragsausführungen.
Wird gestartet	Geben Sie das Datum und die Uhrzeit ein, zu der der Auftrag zum ersten Mal ausgeführt werden soll.

3. Klicken Sie auf das Menüsymbol in der Formular-Kopfzeile und wählen Sie **Speichern**. **Anzahl der Datensätze schätzen** wird bei der Verarbeitung geprüfter Felder nicht unterstützt.

Einen Massenschlüssel-Rotationsauftrag planen

Planen Sie einen Auftrag, um nach mit einem vorherigen Schlüssel verschlüsselten Daten zu suchen, und verschlüsseln Sie die Daten anschließend erneut mit den aktuellen Standard-Verschlüsselungsschlüsseln. Die Daten werden entschlüsselt, bevor sie mit dem aktuellen Standardschlüssel erneut verschlüsselt werden.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Reserviert** > **Schlüsselmassenrotation planen**an.
2. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Wert
Name	Geben Sie einen beschreibenden Namen ein.
Auftragsart	Wählen Sie **Massenschlüsselrotation**.
Schätzen Sie die Anzahl der Datensätze	Geschätzte Gesamtzahl der zu verarbeitenden Datensätze. Nicht verfügbar, wenn eine Massenrotation ausgeführt wird.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
Historische Datensätze verarbeiten	Wählen Sie diese Option aus, um historische Datensätze in der Audit-Tabelle zu verarbeiten, wenn das Feld geprüft wird. Wenn Sie historische Datensätze für ein Feld in der Audit-Tabelle verschlüsseln, werden sowohl neue als auch alte Werte verschlüsselt. Dieses Feld ist schreibgeschützt und aktiv. Weitere Informationen zu geprüften Feldern finden Sie unter Auditing.
Schätzen Sie die maximale Anzahl der Audit-Datensätze	Geschätzte maximale Anzahl der Audit-Datensätze, die verarbeitet werden sollen. Nicht verfügbar, wenn eine Massenrotation ausgeführt wird.
Aktiv	Deaktivieren Sie dieses Kontrollkästchen, um diesen Auftrag zu deaktivieren.
Ausführen	Wählen Sie den Zeitraum zwischen den Auftragsausführungen.
Wird gestartet	Geben Sie das Datum und die Uhrzeit ein, zu der der Auftrag zum ersten Mal ausgeführt werden soll.

3. Klicken Sie auf das Menüsymbol in der Formular-Kopfzeile und wählen Sie **Speichern**. **Anzahl der Datensätze schätzen** wird bei der Verarbeitung geprüfter Felder nicht unterstützt.

Einen Rotationsauftrag für einen Anhangsschlüssel planen

Planen Sie einen Auftrag, um mit einem bestimmten Schlüsselalias verschlüsselte Anhänge zu finden, und verschlüsseln Sie die Anhänge dann erneut mit dem aktuellen Standardverschlüsselungsschlüssel. Der Anhang wird entschlüsselt, bevor er mit dem Standardschlüssel erneut verschlüsselt wird.

Vorbereitungen
Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Reserviert** > **Anhangsschlüsselrotation planen**an.
2. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Wert
Name	Geben Sie einen beschreibenden Namen ein.
Auftragsart	Wählen Sie **Anhangsschlüsselrotation**.
Aktiv	Deaktivieren Sie das Häkchen, wenn Sie diesen Auftrag deaktivieren möchten.
Tabelle	Wählen Sie eine Tabelle.
Ausführen	Wählen Sie den Zeitraum zwischen den Auftragsausführungen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
Wird gestartet	Geben Sie das Datum und die Uhrzeit ein, zu der der Auftrag zum ersten Mal ausgeführt werden soll.

3. Klicken Sie auf das Menüsymbol in der Formular-Kopfzeile und wählen Sie **Speichern**.
4. Um eine geschätzte Anzahl von Datensätzen anzuzeigen, die aktualisiert werden sollen, klicken Sie auf **Geschätzte Datensatzanzahl**.
5. Um den Auftrag sofort auszuführen, klicken Sie auf **Jetzt ausführen**.

Felder mit Verschlüsselungskonfigurationen verschlüsseln

Verschlüsseln Sie Felder, indem Sie Verschlüsselungskonfigurationen erstellen.

Um Edge Encryption zu konfigurieren, müssen Sie über den Proxy mit der Instanz verbunden sein. Testen Sie alle Änderungen in einer Instanz außerhalb der Produktion, bevor Sie sie auf die Produktionsinstanz anwenden.

Verschlüsselungsschlüssel definieren

Nachdem ein oder mehrere Proxys eingerichtet und ein Standardverschlüsselungsschlüssel konfiguriert wurde, überprüft die Instanz, ob die Schlüssel für alle Proxys verfügbar sind. Sie können einen Verschlüsselungsschlüssel nicht zum Standardschlüssel machen, es sei denn, alle Proxys verfügen über den Schlüssel. Nachdem ein Standardschlüssel definiert wurde, können Sie Verschlüsselungskonfigurationen erstellen.

Zu verschlüsselnde Felder und Anlagen zuweisen

Die Zuweisung von zu verschlüsselnden Feldern und Anhängen bedeutet, dem Feld oder der Anlage einen Verschlüsselungstyp zuzuordnen. Bevor Sie ein Feld als verschlüsselt markieren, bewerten Sie diese Vorfälle.

- Bestimmen Sie, welche Systemfunktionen betroffen sein könnten.
- Überprüfen Sie alle Skripts auf die Verwendung des Felds.
- Nehmen Sie die gewünschten Änderungen an der Feldgröße vor. Nachdem ein Feld für die Verschlüsselung konfiguriert wurde, kann die Feldgröße nicht mehr geändert werden.

Durch Markieren eines zu verschlüsselnden Felds wird die Feldgröße zum Speichern der verschlüsselten Daten erweitert. Das Erweitern der Feldgröße kann je nach Anzahl der Datensätze in der Tabelle lange dauern.

API-Unterstützung

Die Verschlüsselung auf Spaltenebene aktualisiert die APIs `„setDisplayValue()“` und `„setValue()“`, damit verschlüsselte Daten für verschlüsselte Felder eingefügt werden können. Außerdem können `getDisplayValue()` und `getValue()` Klartextwerte zurückgeben.

Das folgende Skript veranschaulicht diese API-Änderungen, wenn die Kurzbeschreibung des Incident verschlüsselt wird:

```
var gr = new GlideRecord('incident'); //creates a new incident
gr.setValue('short_description','test123'); //sets the value to test123
var sys_ID = gr.insert(); //inserts the record in the Incident table.
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
gs.info(gr.getValue('short_description')); //displays the unencrypted
 value
```

Wenn Sie `getValue()` zum Abrufen von verschlüsseltem Text verwenden, gibt das Skript keinen Geheimtext mehr zurück. Ihr Skript gibt den Nur-Text zurück und geht davon aus, dass der Benutzer Zugriff auf das kryptografische Modul hat. `getValue()` gibt den Geheimtext zurück, wenn der Anwender keinen Zugriff auf das kryptografische Modul hat.

Erstellen Sie eine Feldverschlüsselungskonfiguration

Wählen Sie die zu verschlüsselnden Felder aus und geben Sie den Verschlüsselungstyp an.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Verschlüsselungskonfigurationen** > **Neu erstellen:**an.
2. Füllen Sie das Formular aus.

Feld	Beschreibung
Tabelle	Die Tabelle, die das zu verschlüsselnde Feld enthält.
Typ	Ob eine Tabellenspalte oder Anhänge für die Tabelle verschlüsselt werden sollen. Wählen Sie **Spalte**.
Spalte	Das zu verschlüsselnde Feld. Wird nur angezeigt, wenn der **Typ** auf **Spalte**festgelegt ist. Nur Felder vom Typ Zeichenfolge, Datum, Datum/Uhrzeit, Journal, Journaleingabe und URL werden unterstützt. ◦ **Felder vom Typ Zeichenfolge und URL**: Sie können eine Verschlüsselungskonfiguration einer übergeordneten Tabelle oder einer untergeordneten Tabelle hinzufügen. ◦ **Felder vom Typ Datum und Datum/Uhrzeit**: Sie können eine Verschlüsselungskonfiguration nur einer übergeordneten Tabelle hinzufügen. Sie können eine neue Verschlüsselungskonfiguration nicht einer untergeordneten Tabelle hinzufügen. **Hinweis:** Je nach Anzahl der Datensätze, die von den Datum- und Datum/Uhrzeit-Feldern, die Sie verschlüsseln, betroffen sind, kann es einige Minuten dauern, die Verschlüsselungskonfiguration zu erstellen. Stellen Sie sicher, dass Sie die Verschlüsselungskonfiguration für die Felder vom Typ Datum und Datum/Uhrzeit erstellen, wenn das Transaktionsvolumen in der Instanz gering ist.
Verschlüsselungstyp	Der zu verwendende Verschlüsselungstyp.

Hinweis: Eine bestimmte Tabellen- und Feldkombination kann jeweils nur eine aktive Konfiguration haben.

3. Klicken Sie auf **Absenden**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Nachdem Sie den Verschlüsselungskonfigurationsdatensatz hinzugefügt haben, können Sie einen Verschlüsselungsauftrag erstellen, um vorhandene Daten zu verschlüsseln. Wenn Sie keinen Verschlüsselungsauftrag ausführen, werden die vorhandenen Daten bei der nächsten Änderung der Daten von Edge verschlüsselt. Details finden Sie unter Einen Verschlüsselungsauftrag planen.

Erstellen Sie eine Konfiguration für die variable Verschlüsselung

Wählen Sie die zu verschlüsselnden Servicekatalogvariablen aus, und geben Sie den Verschlüsselungstyp an.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Konfiguration der Variablenverschlüsselung**an.
2. Klicken Sie in der Liste **Konfigurationen der Edge Encryption-Variablen** auf **Neu**.
3. Füllen Sie das Formular aus.

Feld	Beschreibung
Variable	Die zu verschlüsselnde Variable.
Verschlüsselungstyp	Der zu verwendende Verschlüsselungstyp.

4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Nachdem Sie den Verschlüsselungskonfigurationsdatensatz hinzugefügt haben, können Sie einen Verschlüsselungsauftrag erstellen, um vorhandene Daten zu verschlüsseln. Wenn Sie keinen Verschlüsselungsauftrag ausführen, werden die vorhandenen Daten bei der nächsten Änderung der Daten von Edge verschlüsselt. Details finden Sie unter Einen Verschlüsselungsauftrag planen.

Eine Verschlüsselungskonfiguration deaktivieren

Nachdem Sie ein Feld oder die Anhänge einer Tabelle für die Verschlüsselung konfiguriert haben, können Sie die Verschlüsselung beenden, indem Sie die Verschlüsselungskonfiguration deaktivieren. Nach dem Deaktivieren der Verschlüsselung können Sie einen Entschlüsselungsauftrag für Felder oder einen Entschlüsselungsauftrag für Anhänge ausführen, um die verschlüsselten Daten aus der Instanz zu entfernen.

Vorbereitungen

Erforderliche Rolle: security_admin

Warum und wann dieser Vorgang ausgeführt wird

⚠ **Warnung:** Durch das Deaktivieren einer Verschlüsselungskonfiguration wird der Verschlüsselungsdatensatz nicht gelöscht, und der Verschlüsselungstyp kann nicht geändert werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Konfiguration der Edge Encryption** > **Konfigurationen der Edge Encryption** > **Alle**an.
   Die Liste **Edge Encryption-Konfigurationen** wird angezeigt.
2. Klicken Sie auf die zu deaktivierende Verschlüsselungskonfiguration.
   Das Formular **Edge Encryption-Konfiguration** wird angezeigt.
3. Klicken Sie auf das Feld **Aktiv**.
   Das Feld **Aktiv** ist leer.
4. Klicken Sie auf **Aktualisieren**.
   Die Liste **Edge Encryption-Konfigurationen** wird angezeigt.

Nächste Maßnahme

Sie können einen Entschlüsselungs- oder Anlagenentschlüsselungsauftrag ausführen, um Daten in der Instanz zu entschlüsseln. Wenn Sie keinen Auftrag ausführen, werden die verschlüsselten Daten bei der nächsten Änderung entschlüsselt.

Einen Verschlüsselungsauftrag planen

Sie können einen Auftrag zum Auffinden und Verschlüsseln aller unverschlüsselten Daten in einem bestimmten Feld mit dem für das Feld konfigurierten Standardverschlüsselungsschlüssel planen. Wenn Sie nach dem Konfigurieren eines Felds für die Verschlüsselung keinen Verschlüsselungsauftrag erstellen, werden nur neue Werte verschlüsselt.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Konfiguration der Edge Encryption** > **Verschlüsselungskonfigurationen** > **Alle** um einen Auftrag für ein Feld oder zu erstellen **Konfiguration der Edge Encryption** > **Konfiguration der Variablenverschlüsselung** um einen Auftrag für eine Variable zu erstellen.
2. Klicken Sie auf das Feld, für das Sie einen Verschlüsselungsauftrag planen möchten.
3. Klicken Sie unter **Zugehörige Links** auf **Massenverschlüsselungsauftrag planen**.

   Das Formular **Geplanter Verschlüsselungsauftrag** wird mit allen Feldern angezeigt. Am unteren Rand des Formulars werden Datensätze für alle vorherigen Auftragsausführungen angezeigt.
4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Wert
Name	Geben Sie einen beschreibenden Namen ein.
Aktiv	Deaktivieren Sie dieses Kontrollkästchen, wenn Sie diesen Auftrag deaktivieren möchten.
Auftragsart	Wählen Sie **Verschlüsselung**.
Tabelle	Wählen Sie eine Tabelle.
Spalte	Wählen Sie eine Spalte.
Geschätzte Anzahl der Datensätze	Geschätzte Gesamtzahl der zu verarbeitenden Datensätze. Wird nach Auswahl von **Geschätzte Anzahl der Datensätze** ausgefüllt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
Historische Datensätze verarbeiten	Wählen Sie diese Option aus, um historische Datensätze in der Audit-Tabelle zu verarbeiten, wenn das Feld geprüft wird. Wenn Sie historische Datensätze für ein Feld in der Audit-Tabelle verschlüsseln, werden sowohl neue als auch alte Werte verschlüsselt. Weitere Informationen zu geprüften Feldern finden Sie unter Auditing.
Schätzen Sie die maximale Anzahl der Audit-Datensätze	Geschätzte maximale Anzahl geprüfter Datensätze, die verarbeitet werden sollen. Wird nach Auswahl von **Geschätzte Anzahl der Datensätze** ausgefüllt. Dieses Feld ist nur sichtbar wenn **Historische Aufzeichnungen verarbeiten** ausgewählt ist. **Hinweis:** Die Schätzung kann größer sein als die tatsächliche Anzahl der verarbeiteten Datensätze.
Ausführen	Wählen Sie den Zeitraum zwischen den Auftragsausführungen.
Wird gestartet	Geben Sie das Datum und die Uhrzeit ein, zu der der Auftrag zum ersten Mal ausgeführt werden soll.

5. Klicken Sie auf das Menüsymbol in der Formular-Kopfzeile und wählen Sie **Speichern**.
6. Um eine geschätzte Anzahl von Datensätzen anzuzeigen, die aktualisiert werden sollen, klicken Sie auf **Die Anzahl der Datensätze schätzen**.
7. Um den Auftrag sofort auszuführen, klicken Sie auf **Jetzt ausführen**.

Einen Entschlüsselungsauftrag planen

Sie können einen Auftrag zum Entschlüsseln von Daten in einem verschlüsselten Feld einplanen, um klare Daten in der Instanz zu speichern.

Vorbereitungen

Hinweis: Sie müssen den Verschlüsselungsdatensatz für das Feld als inaktiv markieren (deaktivieren Sie das Feld **Aktiv**), um den Entschlüsselungsauftrag auszuführen.

Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Konfiguration der Edge Encryption** > **Verschlüsselungskonfigurationen** > **Alle** um einen Auftrag für ein Feld oder zu erstellen **Konfiguration der Edge Encryption** > **Konfiguration der Variablenverschlüsselung** um einen Auftrag für eine Variable zu erstellen.
2. Klicken Sie auf das Feld, das Sie entschlüsseln möchten.
3. Klicken Sie unter **Zugehörige Links** auf **Massenentschlüsselungsauftrag planen**.

   Das Formular **Geplanter Verschlüsselungsauftrag** wird mit allen Feldern angezeigt. Am unteren Rand des Formulars werden Datensätze für vorherige Auftragsausführungen angezeigt.

4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Wert
Name	Geben Sie einen beschreibenden Namen ein.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
Auftragsart	Wählen Sie **Entschlüsselung**.
Aktiv	Deaktivieren Sie dieses Kontrollkästchen, wenn Sie diesen Auftrag deaktivieren möchten.
Tabelle	Wählen Sie eine Tabelle.
Spalte	Wählen Sie eine Spalte.
Geschätzte Anzahl der Datensätze	Geschätzte Gesamtzahl der zu verarbeitenden Datensätze. Wird nach Auswahl von **Geschätzte Anzahl der Datensätze** ausgefüllt.
Historische Datensätze verarbeiten	Wählen Sie diese Option aus, um historische Datensätze in der Audit-Tabelle zu verarbeiten, wenn das Feld geprüft wird. Wenn Sie historische Datensätze für ein Feld in der Audit-Tabelle verschlüsseln, werden sowohl neue als auch alte Werte verschlüsselt. Weitere Informationen zu geprüften Feldern finden Sie unter Auditing.
Schätzen Sie die maximale Anzahl der Audit-Datensätze	Geschätzte maximale Anzahl geprüfter Datensätze, die verarbeitet werden sollen. Wird nach Auswahl von **Geschätzte Anzahl der Datensätze** ausgefüllt. Dieses Feld ist nur sichtbar wenn **Historische Aufzeichnungen verarbeiten** ausgewählt ist. **Hinweis:** Die Schätzung kann größer sein als die tatsächliche Anzahl der verarbeiteten Datensätze.
Ausführen	Wählen Sie den Zeitraum zwischen den Auftragsausführungen.
Wird gestartet	Geben Sie das Datum und die Uhrzeit ein, zu der der Auftrag zum ersten Mal ausgeführt werden soll.

5. Klicken Sie auf das Menüsymbol in der Formular-Kopfzeile und wählen Sie **Speichern**.
6. Um eine geschätzte Anzahl von Datensätzen anzuzeigen, die aktualisiert werden sollen, klicken Sie auf **Die Anzahl der Datensätze schätzen**.
7. Um den Auftrag sofort auszuführen, klicken Sie auf **Jetzt ausführen**.

Anhänge mithilfe der Standardverschlüsselung verschlüsseln

Sie können Anhänge für bestimmte Tabellen verschlüsseln.

Alle Anhänge für eine Tabelle verwenden denselben Verschlüsselungstyp. Verschlüsselte Anhänge werden bei der Textsuche nicht durchsucht. Für Anhänge sind nur die Standardverschlüsselungstypen zulässig. Die ordnungs- und gleichstellungserhaltenden Verschlüsselungstypen sind nicht zulässig.

Für eine Sitzung unter Umgehung des Edge Encryption Proxy:

- Auf einem Datensatz mit aktivierter Anhangsverschlüsselung:
  - Der Benutzer kann Anhänge und die Namen der Anhänge sehen.
  - Der Benutzer kann keine neuen Anhänge hinzufügen.
- Auf einem Datensatz ohne aktivierte Anhangsverschlüsselung:
  - Der Benutzer kann vorhandene Anhänge öffnen und herunterladen.
  - Der Benutzer kann neue Anhänge hinzufügen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für eine Sitzung, die den Verschlüsselungsproxy verwendet, kann der Benutzer bestehende Anhänge öffnen und herunterladen sowie neue Anhänge hinzufügen.

Die Anhangsverschlüsselung konfigurieren

Wählen Sie die Tabellen aus, deren Anhänge verschlüsselt werden sollen, und geben Sie den Verschlüsselungstyp an.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Konfigurationen der Edge Encryption** > **Neu erstellen:**an.
2. Füllen Sie die entsprechenden Felder im Formular aus.

Konfiguration der Edge Encryption

Feld	Beschreibung
Tabelle	Wählen Sie eine Tabelle aus, deren Anhänge verschlüsselt werden sollen.
Typ	Ob eine Tabellenspalte oder Anhänge für die Tabelle verschlüsselt werden sollen. Wählen Sie **Anhang**.
Spalte	Das zu verschlüsselnde Tabellenfeld. Dieses Feld wird angezeigt, wenn der **Typ Spalte** und nicht **Typ Anhang** ist.
Verschlüsselungstyp	Der zu verwendende Verschlüsselungstyp. Für Anhänge sind nur Standard AES128 und Standard AES256 zulässig.

3. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Nachdem der Verschlüsselungsdatensatz hinzugefügt wurde, können Sie einen Anhangsverschlüsselungsauftrag erstellen, um vorhandene Anhänge zu verschlüsseln. Wenn Sie keinen Verschlüsselungsauftrag für Anhänge ausführen, verschlüsselt das System neue Anhänge, wenn Sie sie anhängen.

Hinweis: Wenn Sie das *Attribut „edge_encryption_clear_attachment_allowed* “ im Sammlungswörterbucheintrag der Tabelle als **true** markieren, werden unverschlüsselte Anhänge einer Tabelle mithilfe von Edge Encryption hinzugefügt, um Anhänge zu verschlüsseln. Wenn Sie dieses Attribut aktivieren, sollten Sie einen Anhangsverschlüsselungsauftrag einrichten, damit alle hinzugefügten unverschlüsselten Anhänge verschlüsselt werden.

Einen Anhangsverschlüsselungsauftrag planen

Sie können einen Auftrag so planen, um unverschlüsselte Anhänge für eine angegebene Tabelle zu suchen und zu verschlüsseln. Verwenden Sie dazu den für die Tabelle konfigurierten Standard-Verschlüsselungsschlüssel.

Vorbereitungen

Erforderliche Rolle: security_admin

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Konfiguration der Edge Encryption** > **Verschlüsselungskonfigurationen** > **Alle**an.
2. Klicken Sie auf die Tabelle, für die Sie einen Verschlüsselungsauftrag planen möchten.
3. Klicken Sie unter **Zugehörige Links** auf **Massenverschlüsselungsauftrag planen**.

   Das Formular **Geplanter Verschlüsselungsauftrag** wird mit allen Feldern angezeigt. Am unteren Rand des Formulars werden Datensätze für vorherige Auftragsausführungen angezeigt.
4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Wert
Name	Geben Sie einen beschreibenden Namen ein.
Aktiv	Deaktivieren Sie dieses Kontrollkästchen, wenn Sie diesen Auftrag deaktivieren möchten.
Auftragsart	Wählen Sie **Anhangsverschlüsselung**.
Tabelle	Wählen Sie eine Tabelle.
Ausführen	Wählen Sie den Zeitraum zwischen den Auftragsausführungen.
Wird gestartet	Geben Sie das Datum und die Uhrzeit ein, zu der der Auftrag zum ersten Mal ausgeführt werden soll.

5. Klicken Sie auf das Menüsymbol in der Formular-Kopfzeile und wählen Sie **Speichern**.
6. Um eine geschätzte Anzahl von Datensätzen anzuzeigen, die aktualisiert werden sollen, klicken Sie auf **Die Anzahl der Datensätze schätzen**.
7. Um den Auftrag sofort auszuführen, klicken Sie auf **Jetzt ausführen**.

Einen Anhangsentschlüsselungsauftrag planen

Sie können einen Auftrag planen, um alle verschlüsselten Anhänge für eine bestimmte Tabelle zu entschlüsseln und klare Anhänge in der Instanz zu speichern.

Vorbereitungen

Hinweis: Sie müssen den Verschlüsselungsdatensatz für die Tabelle als inaktiv markieren (deaktivieren Sie das Feld **Aktiv**), um den Entschlüsselungsauftrag auszuführen, da ansonsten nichts passieren wird.

Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Konfiguration der Edge Encryption** > **Verschlüsselungskonfigurationen** > **Alle**an.
2. Klicken Sie auf die Tabelle mit den Anlagen, die Sie entschlüsseln möchten.
3. Klicken Sie unter **Zugehörige Links** auf **Anhangsmassenentschlüsselungsauftrag planen**.

   Das Formular **Geplanter Verschlüsselungsauftrag** wird mit allen Feldern angezeigt. Am unteren Rand des Formulars werden Datensätze für vorherige Auftragsausführungen angezeigt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Wert
Name	Geben Sie einen beschreibenden Namen ein.
Auftragsart	Wählen Sie **Anhangsentschlüsselung**.
Aktiv	Deaktivieren Sie das Häkchen, wenn Sie diesen Auftrag deaktivieren möchten.
Tabelle	Wählen Sie eine Tabelle.
Ausführen	Wählen Sie den Zeitraum zwischen den Auftragsausführungen.
Wird gestartet	Geben Sie das Datum und die Uhrzeit ein, zu der der Auftrag zum ersten Mal ausgeführt werden soll.

5. Klicken Sie auf das Menüsymbol in der Formular-Kopfzeile und wählen Sie **Speichern**.
6. Um eine geschätzte Anzahl von Datensätzen anzuzeigen, die aktualisiert werden sollen, klicken Sie auf **Die Anzahl der Datensätze schätzen**.
7. Um den Auftrag sofort auszuführen, klicken Sie auf **Jetzt ausführen**.

Den Verschlüsselungstyp eines Felds oder Anhangs ändern

Sie können den Verschlüsselungstyp eines Felds oder eines Anhangs ändern, indem Sie im vorhandenen Verschlüsselungskonfigurationssatz einen neuen Verschlüsselungstyp auswählen. Eine bestimmte Tabellen- und Feldkombination kann jeweils nur eine aktive Konfiguration haben.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Konfiguration der Edge Encryption** > **Verschlüsselungskonfigurationen** > **Alle**an.
   Die Liste **Edge Encryption-Konfigurationen** wird angezeigt.
2. Öffnen Sie den Datensatz für die zu ändernde Verschlüsselungskonfiguration.
3. Klicken Sie auf die Dropdown-Liste **Verschlüsselungstyp** und wählen Sie einen neuen Verschlüsselungstyp.

   Hinweis: Für Anhänge sind nur Standard AES128 und Standard AES256 zulässig.

4. Führen Sie, falls erforderlich, einen Auftrag zur Verschlüsselung oder Anhangsverschlüsselung aus.
   Es ist nicht notwendig, einen Verschlüsselungsauftrag auszuführen. Wenn Sie keinen Verschlüsselungsauftrag ausführen, wird das Feld oder der Anhang bei der nächsten Änderung des Felds oder des Anhangs mit dem neuen Verschlüsselungstyp verschlüsselt.

Zeichenketten mithilfe von Verschlüsselungsmustern tokenisieren

Sie können Zeichenkettenmuster durch Token ersetzen, bevor sie an die Instanz gesendet und dort gespeichert werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Um Verschlüsselungsmuster verwenden zu können, müssen Sie eine MySQL-Datenbank in Ihrem Netzwerk installieren und einrichten. Dies ist die gleiche Datenbank, die für die ordnungserhaltende Verschlüsselung verwendet wird. Um Verschlüsselungsmuster erstellen oder bearbeiten zu können, müssen Sie über den Proxy mit der Instanz verbunden sein.

Erforderliche Rolle: security_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können Basissystemmuster verwenden oder eigene Muster erstellen. Basissystemmuster sind erweiterte Muster. Verschlüsselungsmuster enthalten die folgenden Einschränkungen.

- Ein Muster aller Alpha-Zeichen ist nicht zulässig.
- Die minimale Mustergröße beträgt fünf Zeichen. Sie können diese Einstellung mithilfe einer Systemeigenschaft ändern.
- Die Quantifizierer * und + sind in Verschlüsselungsmustern nicht zulässig.
- Verschlüsselungsmuster stimmen mit vollständigen Wörtern überein, nicht mit Teilen von Zeichenfolgen, die in eine größere Zeichenfolge eingebettet sind. Wörter werden durch Leerzeichen und Zeichen definiert, die nicht in ein Muster eingefügt werden können.
- Wenn dieselbe Zeichenfolge mehrmals an die Instanz gesendet wird, wird sie durch das gleiche Token ersetzt.
- Die Textsuche nach exakten Übereinstimmungen wird unterstützt. Die Abfragezeichenfolge wird mit einem Token ausgetauscht, wenn sie an die Instanz gesendet wird, die Suche nach Token durchgeführt wird und wenn die Suchergebnisse an den Proxy-Server zurückgegeben werden, werden die Token durch den Klartext ersetzt. Features wie Stemming werden nicht unterstützt.

Bei der Verwendung von Mustern verlässt der Klartext niemals Ihr Netzwerk. Wenn der Proxy-Server mit einem Muster in einer Anforderung übereinstimmt, die an die Instanz gerichtet ist, ersetzt der Proxy die Zeichenfolge durch ein Token derselben Größe. Das Token wird anstelle der Klartextzeichenfolge an die Instanz gesendet. Wenn die Antwort von der Instanz an den Proxy-Server gesendet wird, ersetzt der Proxy das Token durch die Zeichenfolge. Bei Anzeige über den Proxy-Server wird die Zeichenfolge als Klartext angezeigt.

Hinweis: Verschlüsselte Felder werden nicht auf Verschlüsselungsmuster geprüft.

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Verschlüsselungsmuster** > **Neu erstellen:**an.
   Alternativ können Sie zu **Erweiterte Muster** navigieren, um ein vorkonfiguriertes Muster zu aktivieren oder zu bearbeiten.
2. Geben Sie den Musternamen ein.
3. Definieren Sie den **Eingabetyp für Edge-Muster**.

Option	Bezeichnung
Basis	Eine Reihe von Zeichentypen. Klicken Sie in der Registerkarte **Eingabe Basismuster** auf die Registerkarte **Hinzufügen** und wählen Sie einen Zeichentyp. Das **Beispielmuster** zeigt das Muster an, wenn Zeichen hinzugefügt werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	Klicken Sie auf **Neuer Block**, um das nächste Zeichen in die nächste Zeile zu verschieben. Auf diese Weise können Sie Zeichen in einem langen Muster gruppieren. Klicken Sie auf **X**, um das letzte Zeichen im Muster zu löschen.
Erweitert	Ein Java-RegEx-Ausdruck. Wenn „Erweitert“ ausgewählt ist, können Sie den Eingabetyp nicht wieder in „Basis“ ändern. Geben Sie im Feld **Beispielmuster** ein Muster ein, um den RegEx-Ausdruck zu testen. Geben Sie im Feld **Muster** einen Java-RegEx-Ausdruck ein. Klicken Sie auf **Bestätigen**, um zu überprüfen, ob der Ausdruck mit dem Muster übereinstimmt.

Der Eingabetyp legt fest, wie Sie das Muster eingeben. Die Verwendung des Musters wird dadurch nicht beeinflusst.

4. Klicken Sie auf **Absenden**.

Ordnungserhaltend verschlüsselte Daten reparieren oder wiederherstellen

Wenn Sie die Rolle Security-Admin haben, können Sie vom Edge Encryption Proxy ausgeführte Aufträge planen, um Felder zu reparieren oder wiederherzustellen, die ordnungserhaltende Verschlüsselung verwenden.

Aufgaben planen für:

- Auftragstoken zu reparieren
- Die Proxy-Datenbank neu zu erstellen.

Das Ausführen dieser Aufträge kann ein zeitaufwändiger Vorgang sein, der sich auf die Leistung des Edge Encryption -Proxy auswirken kann. Planen Sie diese Jobs zu einem Zeitpunkt ein, zu dem keine Benutzer oder eine minimale Anzahl von Benutzern das System nutzen, z. B. am Wochenende um Mitternacht.

Einen Reparaturauftrag für ein Auftragstoken planen

Sie können einen Auftrag planen, um Felder zu finden und zu reparieren, in denen das Auftragstoken fehlt.

Vorbereitungen
Erforderliche Rolle: security_admin

Warum und wann dieser Vorgang ausgeführt wird
Verwenden Sie diese Aufträge, um einzelne Felder in einer Tabelle zu reparieren oder um alle Felder unter Verwendung der ordnungserhaltenden Verschlüsselung zu reparieren. Führen Sie diesen Auftrag aus, wenn die Proxy-Datenbank während der Ausführung der Instanz offline war. Dies führt zu ordnungserhaltenden Feldern, deren Auftragstoken fehlen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Reserviert** > **Plantafel Tokenreparatur**an.
2. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Wert
Name	Geben Sie einen beschreibenden Namen ein.
Auftragsart	Wählen Sie **Reparatur von Reihenfolge-Token**.
Alle Felder	Aktivieren Sie dieses Kontrollkästchen, um alle Tabellen zu reparieren.
Tabelle	Wählen Sie eine Tabelle.
Spalte	Wählen Sie eine Spalte.
Aktiv	Deaktivieren Sie dieses Kontrollkästchen, wenn Sie diesen Auftrag deaktivieren möchten.
Ausführen	Wählen Sie den Zeitraum zwischen den Auftragsausführungen.
Wird gestartet	Geben Sie das Datum und die Uhrzeit ein, zu der der Auftrag zum ersten Mal ausgeführt werden soll.

3. Klicken Sie auf das Menüsymbol in der Formular-Kopfzeile und wählen Sie **Speichern**.
4. Um eine geschätzte Anzahl von Datensätzen anzuzeigen, die aktualisiert werden sollen, klicken Sie auf **Geschätzte Datensatzanzahl**.

Einen Proxy-Datenbank-Wiederherstellungsauftrag planen

Führen Sie diesen Auftrag aus, wenn die Proxy-Datenbank Daten verloren hat. Dieser Auftrag findet alle Datensätze, die mit einem Token verschlüsselt wurden (ordnungserhaltender Verschlüsselungstyp), und sendet sie an den Proxy, damit die Proxy-Datenbank neu erstellt werden kann.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Reserviert** > **Datenbankwiederherstellung planen**an.
2. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Wert
Name	Geben Sie einen beschreibenden Namen für diesen Auftrag ein.
Auftragsart	Wählen Sie **Datenbankwiederherstellung**.
Aktiv	Deaktivieren Sie dieses Kontrollkästchen, wenn Sie diesen Auftrag deaktivieren möchten.
Ausführen	Wählen Sie den Zeitraum zwischen den Auftragsausführungen.
Wird gestartet	Geben Sie das Datum und die Uhrzeit ein, zu der dieser Auftrag zum ersten Mal ausgeführt werden soll.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf das Menüsymbol in der Formular-Kopfzeile und wählen Sie **Speichern**.
4. Um eine geschätzte Anzahl von Datensätzen anzuzeigen, die aktualisiert werden sollen, klicken Sie auf **Die Anzahl der Datensätze schätzen**.

Konfigurieren Sie die Deny-Liste für IP-Adressen

Verhindern, dass eine IP-Adresse in Ihrem Netzwerk Anforderungen an Ihre -Instanz sendet

Vorbereitungen

Erforderliche Rolle: security_admin
Da sich der Edge Encryption Proxy-Server in Ihrem Netzwerk befindet, kann er Schwachstellen-Scans durch Ihre Netzwerksoftware unterzogen werden. Um zu verhindern, dass IP-Scanner-Anforderungen oder andere Anforderungen an Ihre Instanz ServiceNow weitergeleitet werden, können Sie IP-Adressen, IP-Bereiche oder Netzwerkmasken zu einer Deny-Liste hinzufügen. Jede Verbindung zum Proxy-Server von einer in der Deny-Liste aufgeführten Adresse wird beendet und nicht an Ihre Instanz weitergeleitet.

Um eine IP-Adresse auf eine Deny-Liste zu setzen, müssen Sie über den Proxy-Server bei Ihrer -Instanz angemeldet sein.

Wichtig: Stellen Sie sicher, dass Sie Ihre Netzwerktopologie verstehen, bevor Sie IP-Adressen in Ihrem Netzwerk zu einer Deny-Liste hinzufügen. Wenn der Deny-Liste eine IP-Adresse hinzugefügt wird, wird jeder Benutzer mit dieser IP-Adresse für den Zugriff auf den Proxy-Server Edge Encryption gesperrt.

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Wartung** > **IP-Adressen auf Deny-Liste**an.
   Die Listenansicht „Encryption-Proxy-IP-Denylisten“ [edge_encryption_ip_blacklist] wird geöffnet.
2. Klicken Sie auf **Neu**.
3. Füllen Sie das Formular aus.

Feld	Beschreibung
Proxy-Server	Der Proxy-Server Edge Encryption, der keine Anforderungen von Adressen auf der Deny-Liste weiterleiten darf.
IP, IP-Bereich oder Netzwerkmaske	Anfragen von dieser IP-Adresse, diesem Bereich oder dieser Netzwerkmaske werden nicht an Ihre ServiceNow-Instanz weitergeleitet. Beispielwerte sind: ◦ IP-Adresse: 10.10.10.5 ◦ IP-Bereich: 10.10.10.1-15 ◦ Netzwerkmaske: 10.10.10.0/24 **Hinweis:** Sie können entweder IPv4- oder IPv6-Adressen verwenden
Aktiv	Ob der Datensatz aktiv ist Nur IP-Adressen aus aktiven Datensätzen können keine Anfragen an die Instanz senden.
Beschreibung	Beschreibung des Deny-Listendatensatzes.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Absenden**.
5. Wiederholen Sie diese Schritte für alle anderen Proxys, denen eine IP-Adresse verweigert werden soll.

Ergebnisse

Der -Proxyserver Edge Encryption beendet jede Verbindung von IP-Adressen, Bereichen oder Netzwerkmasken in der Deny-Liste und kann die Anforderung nicht an die -Instanz weiterleiten.

Daten von einem Datensatzersteller verschlüsseln

Konfigurieren Sie Ihren Edge Encryption -Proxy-Server so, dass Einfügungen von einem Datensatzersteller erlaubt werden, indem Sie Verschlüsselungsregeln aus dem Datensatz des Datensatzerstellers erstellen.

Vorbereitungen

Erforderliche Rolle: security_admin
Datensatzersteller ermöglichen Endbenutzern das Erstellen von aufgabenbasierten Datensätzen, z. B. Servicekatalog und Serviceportal. Wenn ein Datensatzersteller versucht, Daten in ein für die Verschlüsselung markiertes Feld einzufügen, wird eine ungültige Einfügemeldung angezeigt und die Daten werden nicht im Feld gespeichert.

Das Verschlüsseln von Daten von einem Datensatzersteller erfordert eine für das Zielfeld definierte Verschlüsselungskonfiguration. Stellen Sie sicher, dass Sie eine Verschlüsselungskonfiguration für das Zielfeld und die Zieltabelle erstellt haben, bevor Sie eine Verschlüsselungsregel von einem Datensatzersteller erstellen. Weitere Informationen finden Sie unter Erstellen Sie eine Feldverschlüsselungskonfiguration. Um Anhänge eines Datensatzerstellers zu verschlüsseln, Die Anhangsverschlüsselung konfigurieren.

Prozedur

1. Melden Sie sich über den Edge Encryption Proxy-Server bei der Instanz an.
2. Navigieren zu **Servicekatalog** > **Katalogdefinitionen** > **Datensatzersteller**an.
3. Erstellen Sie einen Datensatz für einen Datensatzersteller, oder öffnen Sie einen vorhandenen Datensatz für einen Datensatzersteller.
4. Wählen Sie unter **Zugehörige Links Eine Edge Encryption-Regel erstellen**.
   Es werden automatisch zwei inaktive Verschlüsselungsregeln erstellt, um Daten zu verschlüsseln, die vom Datensatzersteller an das für die Verschlüsselung markierte Feld gesendet werden.

Verschlüsselungsregel	Beschreibung
<RecordProducerName>	Regel erstellt, um POST-Parameter von Servicekatalog zu verarbeiten und Variablen den Feldern in der Instanz zuzuordnen.
<RecordProducerName>Json	Regel, die erstellt wurde, um eine JSON-Nutzlast von Serviceportal zu verarbeiten und Variablen den Feldern in der Instanz zuzuordnen.

5. Aktivieren Sie die erforderlichen Verschlüsselungsregeln, die vom Datensatzersteller erstellt wurden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren zu **Konfiguration der Edge Encryption** > **Regeln** > **Alle**an.

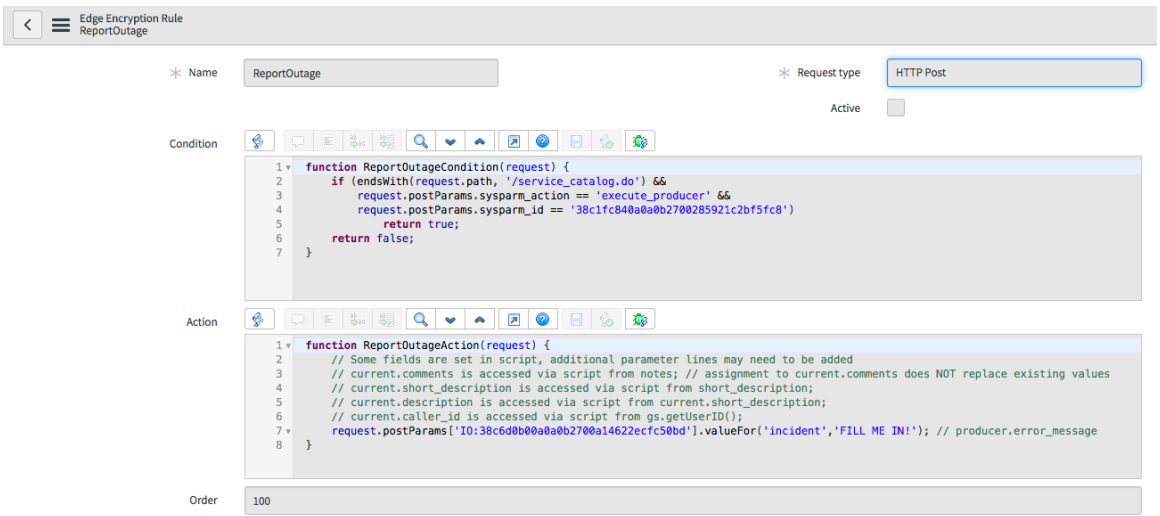
b. Öffnen Sie je nach Verwendungsort des Datensatzerstellers die zugehörige vom Datensatzersteller erstellte Verschlüsselungsregel und wählen Sie die Option **Aktiv**. Bei Verwendung des Datensatzerstellers im Servicekatalog aktivieren Sie die Verschlüsselungsregel <RecordProducerName>. Bei Verwendung des Datensatzerstellers im Serviceportal aktivieren Sie die Verschlüsselungsregel <RecordProducerName>Json.

6. Wahlweise: Untersuchen Sie das **Aktion** der Verschlüsselungsregel und fügen Sie die erforderlichen Feldnamen oder Anweisungen hinzu.

   (Optional) Wenn ein Datensatzersteller eine Variable direkt einem Feld in einer Tabelle zuordnet, ordnet die Verschlüsselungsregel die Variable automatisch dem richtigen Feld zu. Wenn eine Variable jedoch indirekt durch verschiedene Skripts auf der Plattform zugeordnet wird, müssen Sie möglicherweise die Regeln aktualisieren, um jede Variable dem richtigen Feld zuzuordnen.

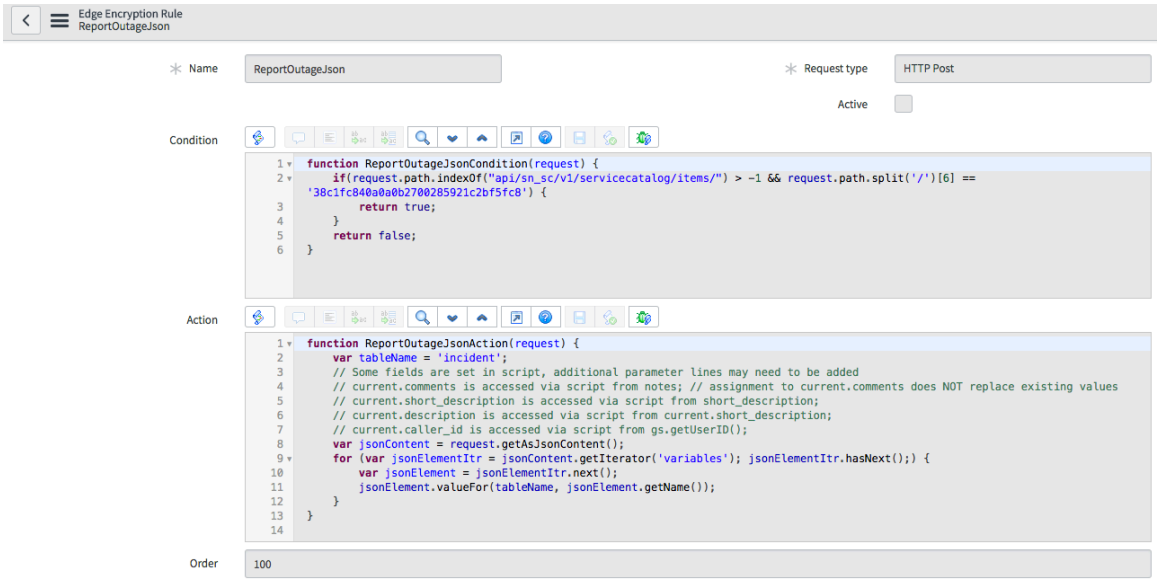
   Example

   (Optional) Die folgende Verschlüsselungsregel wurde aus dem Datensatzersteller „Report Outage“ erstellt und verarbeitet die POST-Parameter von Servicekatalog, um Variablen den Feldern in der Instanz zuzuordnen. Ersetzen Sie `„FÜLL MICH AUS“` mit dem Zielfeld.



   Die folgende Verschlüsselungsregel wurde aus dem Datensatzersteller „Report Outage“ erstellt und verarbeitet die JSON-Payload von Serviceportal, um Variablen den Feldern in der Instanz zuzuordnen. Fügen Sie zusätzliche Anweisungen hinzu, um alle Skriptvariablen den Zielfeldern zuzuordnen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Wenn die Nutzdaten des Datensatzerstellers geprüft werden, enthält das Element error_message den Wert für das Feld short_description. Durch Hinzufügen der folgenden Anweisung können Sie die Skriptvariable error_message dem Feld short_description zuordnen.

```
if (jsonElement.getName() == 'error_message')
        jsonElement.valueFor(tableName, 'short_description');
```

Der Wert des Feldes **Aktion** ändert sich zu:

```
function ReportOutageJsonAction(request) {
 var tableName = 'incident';
 // Some fields are set in script, additional parameter lines may need
 to be added
 // current.comments is accessed via script from notes; // assignment
 to current.comments does NOT replace existing values
 // current.short_description is accessed via script from
 short_description;
 // current.description is accessed via script from
 current.short_description;
 // current.caller_id is accessed via script from gs.getUserID();
 var jsonContent = request.getAsJsonContent();
 for (var jsonElementItr = jsonContent.getIterator('variables');
 jsonElementItr.hasNext();;) {
  var jsonElement = jsonElementItr.next();
  if (jsonElement.getName() == 'error_message')
   jsonElement.valueFor(tableName, 'short_description');
              } else {
          jsonElement.valueFor(tableName, jsonElement.getName());
 }
}
```

Ergebnisse

Die beiden Verschlüsselungsregeln ermöglichen es dem Datensatzersteller, Werte in Felder einzufügen, die entweder vom Servicekatalog oder von Serviceportal zur Verschlüsselung markiert sind.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine benutzerdefinierte Verschlüsselungsregel definieren

Es kann notwendig sein, sensible Informationen in HTTP-Anforderungen auf dem Weg zu Ihrer Instanz zu identifizieren und zu verschlüsseln. Sie können Verschlüsselungsregeln schreiben, um Daten in solchen Anforderungen zu identifizieren, zu interpretieren und zu verschlüsseln, und Felder in der Anforderung zu Tabellenfeldnamen in Ihrer Instanz zuordnen.

Was ist eine Verschlüsselungsregel?

Verschlüsselungsregeln sind Skripts, die auf dem Edge Encryption Proxy-Server ausgeführt werden, um Felder in einer Anforderung Feldern in einer Tabelle in Ihrer ServiceNow-Instanz zuzuordnen. Eine Verschlüsselungsregel weist den Edge Encryption Proxy-Server an, wie Daten in benutzerdefinierten Payloads verschlüsselt werden.

Hinweis: Verschlüsselungsregeln unterstützen nur ECMAScript 3 und niedriger.

Wann werden benutzerdefinierte Regeln verwendet?

Ein Satz von Verschlüsselungsregeln ist im Edge Encryption Plugin enthalten. Diese Regeln behandeln viele Anwendungsfälle der Core-Plattform, z. B.:

- Bearbeiten eines Felds aus dem Listenbearbeitungsformular
- Ein Datensatz wird über das Datensatzformular aktualisiert
- Verwalten des direkten Webservice
- Verarbeiten von Daten über die REST Application Program Interface (API)

Anwendungen, die mit Standardformularen und -listen erstellt wurden, sollten ohne benutzerdefinierte Verschlüsselungsregeln funktionieren.

Wenn Sie Skripts entwickeln, die zu verschlüsselnde Daten enthalten, erstellen Sie Verschlüsselungsregeln, um diese Daten zu finden und den Glide-Tabellenfeldnamen zuzuordnen. Beispiel:

- Geskriptete Prozessoren
- Scripted Web Services
- Geskriptete REST APIs, UIs oder Ajax-Skripts

Format einer Verschlüsselungsregel

Regeln bestehen aus drei Teilen:

- **Bedingung**: Gibt die Art der Anforderung an.
- **Aktion**: Ordnet Felder in der Anforderung Feldern in einer Tabelle zu und verschlüsselt Werte, die Feldern mit definierten Verschlüsselungskonfigurationen zugeordnet sind.
- **Reihenfolge**: Priorität der Regel. Die Regel mit der niedrigsten Priorität mit einer erfüllten Bedingung ist die einzige ausgeführte Regel. Wie Business Rules laufen die Regeln vom niedrigsten zum höchsten.

Mit Ausnahme von Anhangsanforderungen werden HTTP-Anforderungen vom Proxyserver Edge Encryption ausgewertet. Der Edge Encryption -Proxyserver wertet alle Verschlüsselungsregelbedingungen in der Prioritätsreihenfolge aus, bis entweder alle Bedingungen „falsch“ oder eine Bedingung „wahr“ zurückgibt. Wenn eine Bedingung „true“ zurückgibt, wird die Aktion für die Anforderung ausgeführt und das Ergebnis an die Instanz weitergeleitet. Andere Bedingungen werden nicht bewertet. Daher sollten die Bedingungen für die Verschlüsselungsregeln so genau wie möglich sein. Eine generische Regel kann für

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

eine Anforderung, die von einer anderen Regel verarbeitet werden soll, als „Wahr“ bewertet werden, was dazu führt, dass die Anforderung durch die falsche Aktion verarbeitet wird. Wenn eine generische Bedingung unvermeidbar ist, sollte die Regel mit einem Wert höherer Ordnung markiert werden, damit spezifischere Regeln zuerst ausgewertet werden.

Richtlinien zum Erstellen von Verschlüsselungsregeln

Durch das Erstellen effizienter, optimierter Verschlüsselungsregeln kann die Verarbeitungszeit für die Skriptvalidierung reduziert werden.

Allgemeine Richtlinie: Wenn Regeln lang werden, versuchen Sie, die Anzahl der Blöcke zu minimieren, und teilen Sie die Regeln nach Möglichkeit auf. Im Idealfall sollten benutzerdefinierte Regeln für bestimmte Anwendungsfälle gelten, anstatt mehrere Fälle zu umfassen, mit den Anweisungen `Falls` oder „Switch“ im Aktionsskript.

1. Teilen Sie die Regeln, wann immer möglich. Beispiel:
   - Erstellen Sie unterschiedliche Regeln für verschiedene Tabellen und stellen Sie sicher, dass jede Regel nur für die jeweilige Tabelle ausgeführt wird.
   - Erstellen Sie unterschiedliche Regeln für jeden Zieldatensatzersteller oder zumindest für jede Teilmenge von Datensatzerstellern. Anstelle einer Regel, die auf Dutzende von `sys_ids` abzielt, können Sie mehrere verschiedene Regeln erstellen, die auf kleinere Teilmengen von Datensatzerstellern abzielen, oder sogar eine Regel pro `sys_id` erstellen.

     Hinweis: Das Erstellen mehrerer Regeln erfordert mehr Wartung. Der Nachteil ist, dass mehrere, einfachere Regeln effizienter validiert werden können als längere, komplexere Regeln.

2. Minimieren Sie die Anzahl der Blöcke. Da das Verarbeitungsmodul jeden Block während der Auswertung von Skripts durchsucht, führt eine große Anzahl von Blöcken zu Verzögerungen bei der Validierung. Beispiel:
   - Ersetzen Sie alle `Falls`-Blöcke durch ein Array-Lookup, und ersetzen Sie alle Blöcke im Array-Lookup durch nur einen `Falls`-Block.
   - Kombinieren Sie `if` -Blöcke, wann immer sie gruppiert werden können.

Verschlüsselungsregel-APIs

Verschlüsselungsregeln werden in JavaScript geschrieben und verwenden Edge Encryption APIs zum Auffinden und Verschlüsseln sensibler Informationen im Hauptteil einer Anforderung. Die API verwendet ähnliche Ausdrücke wie xPath, um durch JSON- und XML-Inhalte zu navigieren.

Edge Encryption APIs verarbeiten die Anforderung aus dem Stream, während sie in den Ausgabestream geschrieben wird. Durch die Stream-Analyse können Verschlüsselungsregeln netzwerkleistungsfähig sein. Das mehrmalige Abrufen und Analysieren von Inhalten aus dem Körper kann jedoch zu unerwarteten Ergebnissen führen. Um dieses potenzielle Problem zu vermeiden, sollten Anforderungen von der Aktion in einem einzigen Vorgang verarbeitet werden.

Beim Erstellen von Verschlüsselungsregeln können Sie keine Glide APIs, Skripteinbindungen, Geschäftsregeln oder globale Parameter wie *`current`*verwenden. Da die Regeln für HTTP-Objekte erstellt werden, ist ein globales Objekt *`Anforderung`* verfügbar.

Beim Erstellen von Verschlüsselungsregeln können Sie keine APIs aus dem Allow-Listen-Manager oder bereichsbezogenen Anwendungen verwenden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fehlerbehandlung

Wenn eine Bedingung oder Aktion einer Verschlüsselungsregel eine Ausnahmebedingung auslöst, überprüfen Sie das Proxy-Protokoll auf Informationen zur Problembehandlung.

Die Client-Anforderung überprüfen

Bevor Sie eine benutzerdefinierte Verschlüsselungsregel erstellen, müssen Sie das Format der Client-Anforderung festlegen, die auf dem Edge Encryption Proxy-Server eingegeben wird.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Da Verschlüsselungsregeln Client-Anforderungen durchlaufen und bestimmen, was ggf. verschlüsselt werden muss, müssen Sie den Typ der Anforderung kennen, für die Sie eine Regel erstellen. Das Format der Client-Anforderung bestimmt die Struktur Ihrer Verschlüsselungsregel und die zur Verwendung in der Regel verfügbaren APIs.

Prozedur

1. Überprüfen Sie die Client-Anforderung.

   Abhängig von der Quelle der Anforderung stehen die folgenden Tools zur Verfügung, um die Anforderung zu überprüfen und das Format zu bestimmen.

Quelle der Anforderung	Verfügbare Tools
Client-Browser	Verwenden Sie die Entwicklerkonsole in Ihrem Browser, um die Client-Anforderung zu überprüfen. Zu den nützlichen Tools gehören: ◦ Firefox Netzwerkmonitor ◦ Chrome Netzwerkbereich
Drittanbieter/externe Quelle	Verwenden Sie ein HTTP-Protokollanalysegerät, um die Anforderung zu überprüfen. Zu den nützlichen Tools gehören: ◦ Wireshark ◦ HTTP Scoop Alternativ können Sie häufig Dokumentation für die externe Quelle verwenden, um das Format der Anforderung zu bestimmen.

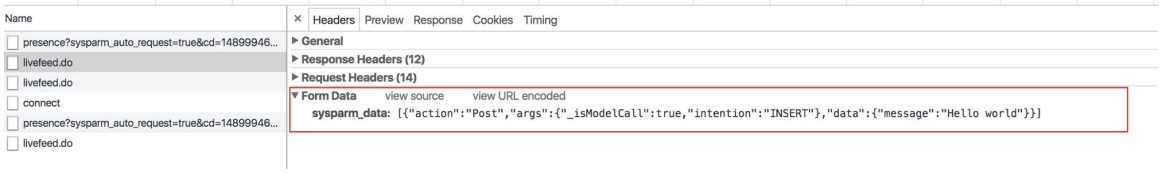
2. Überprüfen Sie das Paket in der Client-Anforderung und stellen Sie Folgendes fest:
   ◦ Die Methode der Client-Anforderung
   ◦ Der URL-Pfad der Anforderung

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die URL-Parameter
- Die POST-Parameter, falls vorhanden
- Das Format des Anforderungstextes, falls vorhanden

Example



Ergebnisse

Durch Überprüfen der Anforderung erhalten Sie Informationen zu den Feldern, die Sie in Ihrer Verschlüsselungsregel filtern und iterieren müssen. Hinweise zum besseren Verständnis der Felder im Objekt *Anforderung* finden Sie unter Anforderung.

Eine Verschlüsselungsregel erstellen

Der Proxy verwendet Verschlüsselungsregeln, um Inhalte in HTTP-Anforderungen zu finden, die verschlüsselt werden sollen.

Vorbereitungen

Erforderliche Rolle: security_admin
Bevor Sie eine Verschlüsselungsregel erstellen, müssen Sie Die Client-Anforderung überprüfen, um das Format zu bestimmen.

Warum und wann dieser Vorgang ausgeführt wird

Um Verschlüsselungsregeln erstellen oder bearbeiten zu können, müssen Sie über einen Verschlüsselungs-Proxy mit der Instanz verbunden sein.

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Regeln** > **Neu erstellen:**an.
2. Geben Sie im Feld **Name** einen Namen ein.
3. Wählen Sie unter **Anfragetyp** eine HTTP-Methode aus.
   - **HTTP Post**
   - **HTTP Get**
   - **HTTP Put**
   - **HTTP Patch**
   - **HTTP Delete**

   Hinweis: Vorinstanzen vorJakarta lassen nur **HTTP-Get-** und **HTTP-Post-** Methoden zu.
4. Geben Sie im Feld **Bedingung** eine JavaScript-Anweisung ein, die festlegt, wann die Regel ausgeführt werden soll.
5. Geben Sie im Feld **Aktion** eine JavaScript-Funktion ein, die ausgeführt werden soll, wenn die Bedingung erfüllt ist.
6. Geben Sie im Feld **Auftrag** die relative Priorität der Regel ein.
7. Klicken Sie auf **Absenden** oder speichern Sie das Formular.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bedingungen für Verschlüsselungsregeln

Die Bedingungen für die Verschlüsselungsregeln bestimmen, ob die Regel ausgeführt werden soll.

Eine Bedingung für eine Verschlüsselungsregel muss „Wahr“ zurückgeben, wenn die Regel die HTTP-Anfrage behandeln soll; andernfalls muss sie „Falsch“ zurückgeben.

Beachten Sie beim Erstellen Ihrer Bedingung, dass pro Anforderung nur eine Regel ausgeführt wird. Daher muss die Bedingung so allgemein oder spezifisch sein, dass sie unter den vorgesehenen Umständen ausgeführt werden kann.

Hinweis: Seien Sie vorsichtig, wenn Sie Überprüfungen des Inhalts in der Bedingung durchführen. Übermäßige Überprüfungen können für den Proxy-Server teuer sein und zu einer erhöhten Latenzzeit bei der Bearbeitung komplexer Anfragen führen.

Die Bedingung kann den Methodentyp, den Inhaltstyp, den URL-Pfad oder beliebige URL-Abfragezeichenfolgeparameter verwenden, um zu bestimmen, ob die Regel die Anforderung verarbeiten soll. Die Bedingung hat auf diese Felder über das Objekt Anforderung Zugriff. Stellen Sie sicher, dass Sie vor dem Erstellen einer Verschlüsselungsregel die Client-Anforderung überprüft haben und die für das Auslösen der Regel erforderlichen Bedingungen kennen.

Hinweis: Um effiziente Regeln zu erstellen, sollten Sie einfache Möglichkeiten berücksichtigen, Anforderungen auszuschließen, die nicht von einer Regel ausgewertet werden sollen. Erstellen Sie Ihre Bedingung, um zuerst für diese Anforderungen „Falsch“ zurückzugeben. Diese Methode erhöht die Leistung und leitet die Anforderung schneller an die richtige Regel weiter.

Verschlüsselungsregelobjekte und APIs sind für Verschlüsselungsregelbedingungen verfügbar.

Beispiel mit Pfad und Postparametern

```
/*This condition checks if the request coming in has a path ending in
"/sample_processor.do" and if a post parameter exists in that request
 called myPostParam */

function SampleCondition(request) {
   if (endsWith(request.path, "/sample_processor.do") &&
 request.postParams.myPostParam) {
       return true;
   }
   return false;
}
```

Beispiel mit urlParams und contentType

```
/* This condition checks if a url parameter exists in the query called
myUrlParam and if the content type contains 'xml'
(if so, you can expect the body to be an XML payload).
Then, it checks if the xml payload contains myXmlTag */

function SampleCondition2(request) {
   if (request.urlParams.myUrlParam && request.contentType.indexOf('xml')
 > -1 && request.xmlContains('myXmlTag')) {
       return true;
   }
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
 return false;
}
```

Aktionen für Verschlüsselungsregeln

Eine Verschlüsselungsregel ordnet Felder in einer Client-Anforderung Feldern in einer Tabelle in Ihrer Instanz zu und identifiziert Felder, die für die Verschlüsselung markiert sind.

Eine Verschlüsselungsregelaktion wird nur ausgeführt, wenn die Bedingung der Verschlüsselungsregel „Wahr" zurückgibt. Eine Verschlüsselungsregel gibt die Daten an, die in Ihrer Anforderungs-Payload verschlüsselt werden sollen. Da die Regel den Inhalt im Anforderungsobjekt durchläuft, müssen Sie das Formular und die Struktur des Anforderungstexts verstehen und bestimmen, welche Elemente in der Anforderung verschlüsselt werden müssen. Die zu verschlüsselnden Daten befinden sich möglicherweise in:

- einem POST- oder URL-Parameter,
- einem JSON- oder XML-Inhalt in einem POST- oder URL-Parameter,
- einer JSON-Payload,
- einer XML-Payload.

Stellen Sie vor dem Schreiben einer Verschlüsselungsregelaktion Folgendes sicher:

- Die Client-Anforderung überprüfen.
- Stellen Sie fest, wo sich die sensiblen Daten im Objekt Anforderung befinden.
- Bestimmen Sie das Feld und den Tabellennamen, in das Daten eingefügt werden sollen, oder verstehen Sie, wie man dies dynamisch aus der Anforderung entnimmt.

Verschlüsselungsregelobjekte und APIs stehen für Verschlüsselungsregelaktionen und -bedingungen zur Verfügung.

Verschlüsselungsregelobjekte und APIs

Verwenden Sie Verschlüsselungsregel-APIs, um Werte in Anforderungen zu analysieren und zu verschlüsseln, die sich durch den Edge Encryption Proxy-Server zur Instanz bewegen.

Die für Ihre Verschlüsselungsregel verfügbaren APIs hängen vom Format des Anforderungsobjekts ab. Wenn der contentType-Parameter des Anforderungsobjekts beispielsweise XML ist, können Sie XML-APIs verwenden, um Werte in der Payload zu analysieren und zu verschlüsseln. Nachdem Sie den Objekttyp in Ihrer Anforderung ermittelt haben, können Sie eine Verschlüsselungsregel mit den verfügbaren APIs erstellen.

Verschlüsselungsregel-APIs sind sowohl in den Bedingungen für Verschlüsselungsregeln als auch in Aktionsskripts verfügbar.

Anforderung

Das Objekt *`Anforderung`* ist ein globales Objekt, das in Edge Encryption Regelaktionen und Bedingungsskripts verfügbar ist.

Das Objekt *`Anforderung`* ist ein JavaScript-Objekt, das die Client-Anforderung darstellt, die an den Edge Encryption Proxy-Server gesendet wird. Sie müssen Ihre Verschlüsselungsregel erstellen, um das Objekt *`Anforderung`* zu analysieren, die Objektwerte *`Anforderung`* Feldern in einer Tabelle in der Instanz zuordnen und alle sensiblen Daten im Objekt *`Anforderung`* verschlüsseln.

Das Objekt *`Anforderung`* enthält die folgenden Attribute und Daten aus der Client-Anforderung:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anforderungsobjektfelder

Feld	Beschreibung
Pfad	Der Pfadbestandteil der URL.
requestMethod	GET, POST, PUT, PATCH, DELETE.
contentType	Das Kopfzeilenfeld „Content-Type“.
urlParams	Die Parameter in der Abfragezeichenfolge. Dies kann auch als String ausgewertet werden.
postParams	Wenn es sich um einen Formular-Post handelt, enthält dieser die Post-Parameter.

Anforderung – getAsJsonContent()

Gibt die Anforderung als iterierbares Objekt vom Typ `JsonNode` zurück.

Diese Methode ist nur in einer Edge Encryption-Regel verfügbar, wenn der Anforderungstext eine gültige JSON-Payload ist. Wenn Sie nicht sicher sind, in welchem Format der Anforderungstext enthalten ist, überprüfen Sie das Feld „contentType“ im Objekt `Anforderung`.

Sobald die Anforderung als `JsonNode`-Objekt zurückgegeben wird, können Sie mit Hilfe von JSON-APIs über das Objekt iterieren und Felder verschlüsseln.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
JsonNode	Die Anforderung als iterierbarer `JsonNode`.

Anforderung – getAsXmlContent()

Gibt den Anforderungsinhalt als iterierbares Objekt vom Typ `XMLContent` zurück.

Diese Methode ist nur in einer Edge Encryption-Regel verfügbar, wenn der Anforderungstext eine gültige XML-Payload ist. Wenn Sie nicht sicher sind, in welchem Format der Anforderungstext enthalten ist, überprüfen Sie das Feld „contentType“ im Objekt `Anforderung`.

Sobald die Anfrage als `XMLContent`-Objekt zurückgegeben wird, können Sie mit Hilfe von XML-APIs über die Objekt- und Verschlüsselungsfelder iterieren.

Parameter

Name	Typ	Beschreibung
Keine		

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Typ	Beschreibung
XMLContent	Die Anforderung als iterierbares Objekt vom Typ *XMLContent*.

Anforderung – XMLContains (Zeichenfolgenpfad)

Gibt „Wahr“ zurück, wenn der angegebene Pfad im XML DOM vorhanden ist.

Diese Methode ist nur verfügbar, wenn der Anforderungstext eine gültige XML-Payload ist. Wenn Sie nicht sicher sind, in welchem Format der Anforderungstext enthalten ist, überprüfen Sie das Feld „contentType“ im Objekt *Anforderung*.

Parameter

Name	Typ	Beschreibung
Pfad	Zeichenfolge	XPath-Anweisung, nach der Sie suchen.

Ergebnisse

Typ	Beschreibung
Boolean	Gibt an, ob der angegebene Pfad im XML DOM vorhanden ist.

POST- und URL-Parameter-APIs

POST- und URL-Parameter können als Eigenschaften des Objekts *Anforderung* über `request.postParams` und `request.urlParams` aufgerufen werden.

Auf jeden einzelnen Parameter kann als Eigenschaft der übergeordneten Objekte *postParams* und *urlParams* durch Aufrufen von `request.postParams.myParam` zugegriffen werden. Jeder Parameter, auf den auf diese Weise zugegriffen wird, ist ein Objekt der zugrunde liegenden Klasse *ParameterValue*. Alle APIs in dieser Klasse können für jeden Parameter aufgerufen werden.

Nach dem Überprüfen der Client-Anforderung kann es notwendig sein, auf Parameterwerte aus dem Objekt *Anforderung* zuzugreifen und diese zu verschlüsseln. Abhängig von den Daten in der Clientanforderung können Sie Werte auf mehrere Arten verschlüsseln und sie Feldern in der Instanz zuordnen.

Den Wert einer bekannten Tabelle und eines Felds verschlüsseln

Wenn Sie den Namen der Instanztabelle und des Felds kennen, in dem die verschlüsselten Daten gespeichert werden sollen, können Sie sie explizit in der Verschlüsselungsregel definieren. Möglicherweise wissen Sie beispielsweise, dass die Anforderung in der Instanz verarbeitet wird, um einen Incident zu erstellen, und Sie möchten den Parameter **Text** im Beschreibungsfeld verschlüsseln. In diesem Fall können Sie die folgende Aktion erstellen.

```
function SampleAction1() {
    request.postParams.text.valueFor('incident', 'description');
}
```

Den Wert einer dynamisch definierten Tabelle und eines Felds verschlüsseln

Wenn Sie andererseits den Namen des Feldes nicht kennen, das die verschlüsselten Daten füllen sollen, können Sie sie mit **tableName** und **fieldName** dynamisch definieren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Im folgenden Beispiel wird eine generische Anforderung verarbeitet, in der möglicherweise Daten in verschiedenen Aufgabentabellen (z. B. Incident, Problem und Change_request) in der Instanz gespeichert werden.

```
function SampleAction2() {
    var tableName = request.urlParams.table;
    for (var parameter in request.postParams) {
        var currentParam = request.postParams[parameter];
        var fieldName = currentParam.toString();
        if (fieldName == 'text') {
            currentParam.valueFor(tableName, 'description')
        } else {
            currentParam.valueFor(tableName, fieldName);
        }
    }
}
```

Diese Aktion:

- Ruft die Zieltabelle aus den URL-Parametern ab.
- Iteriert über die URL-Parameter.
- Fordert den Edge Encryption Proxy-Server auf, jeden URL-Parameter mit einem Namen zu verschlüsseln, der einem für die Verschlüsselung markierten Feld entspricht.
- Sucht nach einem bestimmten Parameter namens *Text* und fordert den Edge Encryption Proxy auf, den Wert basierend auf der Verschlüsselungskonfiguration für das Beschreibungsfeld in der Incident-Tabelle zu verschlüsseln.

In diesem Beispiel führt die Methode valueFor() eigentlich keine Verschlüsselung durch. Vielmehr fordert das Verfahren den Edge Encryption Proxy-Server auf, zu prüfen, ob das Tabellen-/Feldpaar im Anforderungsobjekt mit einer Verschlüsselungskonfiguration zur Verschlüsselung vorgemerkt ist, und gegebenenfalls zu verschlüsseln.

JSON oder XML innerhalb eines Parameters verschlüsseln

Ein POST- oder URL-Parameter kann JSON- oder XML-Inhalte enthalten. In diesem Fall können Sie den Inhalt innerhalb des Parameters verarbeiten, die Werte durchlaufen und die erforderlichen Felder verschlüsseln. In diesem Beispiel wird weiterhin über einen POST-Parameter auf **tableName** zugegriffen, aber der Wert des Feldes ist das JSON-Objekt **Daten**.

```
function SampleAction3() {
    var tableName = request.postParams.table;
    var data = request.postParams.data;
    var dataIterator = data.getAsJsonContent().iterator();
    while (dataIterator.hasNext()) {
        var jsonElement = dataIterator.next();
        var fieldName = jsonElement.getName();
        if (fieldName == 'text') {
            jsonElement.valueFor(tableName, 'description');
        } else {
            jsonElement.valueFor(tableName, fieldName);
        }
    }
}
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein Beispiel für eine Verschlüsselungsregelaktion, die XML innerhalb eines POST-Parameters verarbeitet.

```
function SampleAction4() {
    var tableName = request.postParams.table;
    var data = request.postParams.data;
    var dataIterator =
 data.getAsXmlContent().getIteratorOverAllChildren();
    while (dataIterator.hasNext()) {
        var jsonElement = dataIterator.next();
        var fieldName = jsonElement.getName();
        if (fieldName == 'text') {
            jsonElement.valueFor(tableName, 'description');
        } else {
            jsonElement.valueFor(tableName, fieldName);
        }
    }
}
```

Eine Anforderung verschlüsseln

In einer Client-Anforderung, die vertrauliche Daten enthält, tritt möglicherweise eine verschlüsselte Abfrage in einem Parameter auf. Um ein Feld in einer Abfrage einem verschlüsselten Wert in der Instanzdatenbank zuzuordnen, müssen Sie eine Verschlüsselungsregel erstellen, die den Proxy-Server auffordert, zu prüfen, ob ein Feld in der Abfrage für die Verschlüsselung markiert ist. Die Methode encodedQueryFor() analysiert eine verschlüsselte Abfrage für eine bestimmte Tabelle und prüft, ob Felder in der Abfrage Verschlüsselungskonfigurationen enthalten.

In diesem Beispiel durchläuft die Regel die Parameter und sucht den Parameter **Filter**, der voraussichtlich eine Glide-codierte Abfrage ist.

```
function SampleAction5() {
    var tableName = request.urlParams.table;
    for (var parameter in request.postParams) {
        var currentParam = request.postParams[parameter];
        var fieldName = currentParam.toString();
        if (fieldName == 'filter') {
            currentParam.encodedQueryFor(tableName);
        } else {
            currentParam.valueFor(tableName, fieldName);
        }
    }
}
```

Wenn beispielsweise der Wert von **Filter** `short_description=My sensitive information^number=INC000056^category=Outage` ist, würde die Abfrage in der Instanz zu `short_description=<Encrypted(My sensitive information)>^number=INC000056^category=Outage` werden.

ParameterValue - toString()

Konvertiert den POST- oder URL-Parameterwert in eine Zeichenfolge.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
Zeichenfolge	Der Parameterwert als Zeichenfolge.

ParameterValue - getAsJsonContent()

Gibt die Anforderung als iterierbares Objekt vom Typ `JsonNode` zurück.

Diese Methode ist nur in einer Edge Encryption-Regel verfügbar, wenn der Anforderungstext eine gültige JSON-Payload ist. Wenn Sie nicht sicher sind, in welchem Format der Anforderungstext enthalten ist, überprüfen Sie das Feld „contentType“ im Objekt `Anforderung`.

Sobald die Anforderung als `JsonNode`-Objekt zurückgegeben wird, können Sie mit Hilfe von JSON-APIs über das Objekt iterieren und Felder verschlüsseln.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
JsonNode	Die Anforderung als iterierbarer `JsonNode`.

ParameterValue - getAsXmlContent()

Gibt den Anforderungsinhalt als iterierbares Objekt vom Typ `XMLContent` zurück.

Diese Methode ist nur in einer Edge Encryption-Regel verfügbar Diese Methode setzt voraus, dass der Anforderungstext eine gültige XML-Payload ist. Sie können den contentType überprüfen, um sicherzustellen, dass dies der Fall ist.

Sobald die Anfrage als `XMLContent`-Objekt zurückgegeben wird, können Sie mit Hilfe von XML-APIs über die Objekt- und Verschlüsselungsfelder iterieren.

Parameter

Name	Typ	Beschreibung
Keine		

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Typ	Beschreibung
XMLContent	Die Anforderung als iterierbares Objekt vom Typ `XMLContent`.

ParameterValue - encodedQueryFor(String tableName)

Gibt an, dass der Wert des Elements eine codierte Abfrage für die angegebene Tabelle ist.

Durch Aufrufen dieser Funktion für einen Parameter wird dem Proxy mitgeteilt, dass der Wert des Parameters eine codierte Abfragezeichenfolge für die angegebene Tabelle ist. Der Proxy analysiert die verschlüsselte Abfrage und verschlüsselt die Felder in der verschlüsselten Abfrage, die verschlüsselt werden müssen.

Parameter

Name	Typ	Beschreibung
tableName	Zeichenfolge	Die Tabelle, auf der die Abfrage ausgeführt werden soll.

Ergebnisse

Typ	Beschreibung
void	

ParameterValue - valueFor(String tableName, String fieldName)

Gibt an, dass der Wert des Elements dem angegebenen Feld in der angegebenen Tabelle zugeordnet ist.

Durch Aufrufen dieser Methode für einen Elementwert wird dem Proxy mitgeteilt, dass der Wert für dieses Element dem angegebenen Feld in der angegebenen Tabelle zugeordnet ist. Der Proxy prüft dann, ob das Feld verschlüsselt werden muss.

Parameter

Name	Typ	Beschreibung
tableName	Zeichenfolge	Der Tabellenname.
fieldName	Zeichenfolge	Der Feldname.

Ergebnisse

Typ	Beschreibung
void	

XML-APIs

XML-APIs können nach dem Aufrufen von `getAsXmlContent()` entweder über das Objekt `Anforderung` oder eine Eigenschaft `ParameterValue` verwendet werden.

Wenn Sie XML-APIs zum Schreiben Ihrer Verschlüsselungsregel verwenden, können Sie ein allgemeines Format verwenden:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Aufrufen von `getAsXmlContent()` über das Objekt `Anforderung` oder die Eigenschaft `ParameterValue`. Dies gibt ein iterierbares Objekt der zugrunde liegenden Klasse `XMLContent` zurück.
2. Aufrufen von `getIterator()` oder `getIterator(String xPath)` im Objekt `XMLContent`. Dies gibt ein Objekt `XMLElementIterator` zurück, das zum Iterieren von XML-Elementen verwendet werden kann.
3. Aufrufen der Methode `hasNext()` im Objekt `XMLElementIterator`, um zu bestimmen, ob ein anderes Element verfügbar ist.
4. Aufrufen von `next()` im Objekt `XMLElementIterator`, um das nächste XML-Element zurückzugeben. Sie können `next()` erst nach Aufrufen von `hasNext()` aufrufen.
5. Aufruf von `valueFor(String tableName, String fieldName)` auf dem XML-Element. Diese Methode teilt dem Proxy mit, dass der Wert für dieses Element dem angegebenen Feld in der angegebenen Tabelle zugeordnet ist. Der Proxy prüft dann, ob das Feld verschlüsselt werden muss.

> **Hinweis:** Um festzustellen, ob Sie `valueFor(String tableName, String fieldName)` auf einem XML-Element aufrufen möchten, können Sie die Methode `getName()` verwenden, um den Namen des Elements zurückzugeben.

Zu einem bekannten Tabellenfeld in der Instanz zuordnen

In diesem Beispiel wird die XML-Payload auf der Instanz verarbeitet, um Datensätze in die Incident-Tabelle einzufügen. Das Beschreibungsfeld füllt den Incident mit short_description aus.

```
<data>
    <record>
        <name>'Test Record 1'</name>
        <description>'Test Record 1 Description'</description>
        <tag>critical</tag>
    </record>
    <record>
        <name>'Test Record 2'</name>
        <description>'Test Record 2 Description'</description>
        <tag>security</tag>
    </record>
</data>
```

Die folgende Verschlüsselungsregelaktion kann angewendet werden:

```
function sampleXmlAction1() {
    var xmlContent = request.getAsXmlContent();
    // This loop iterates over all description tags that match the given
 path
    var xmlElementIterator =
 xmlContent.getIterator('data/record/description');
    while (xmlElementIterator.hasNext()) {
        var xmlElement = xmlElementIterator.next();
        xmlElement.valueFor('incident', 'short_decription');
    }
}
```

Diese Aktion iteriert das Tag **Beschreibung** und fordert den Proxy-Server auf, die Werte zu verschlüsseln und sie in der Instanz in instance.short_description einzufügen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Diese Regel findet alle Tags **Beschreibung** in allen Tags **Datensatz** in der XML-Payload. Wenn es nur ein einziges Vorkommen eines zu verschlüsselnden Tags gibt, verwendet die Regel weiterhin die xPath- und Iteratorstruktur. Es iteriert jedoch nur einmal in der Schleife.

Zu einem unbekannten Tabellenfeld in der Instanz zuordnen

In diesem Beispiel iteriert die Regel die Tags **Datensatz**, weiß jedoch nicht, welche Tags innerhalb des Tags **Datensatz** zu erwarten sind. Es ist nur bekannt, dass die Tags innerhalb der Tags **Datensatz** mit den Namen der in der Tabelle „URL-Parameter“ angegebenen Spalten übereinstimmen.

Die Regel legt außerdem fest, dass bei Vorliegen einer Incident-Tabelle, die Daten im Tag **Beschreibung** verschlüsselt und im Feld short_description der Instanz gespeichert werden sollen.

```
function sampleXmlAction2() {
    var xmlContent = request.getAsXmlContent();
    var tableName = request.urlParam.table;
    // This first iterator will iterate over all record elements
    var xmlElementIterator = xmlContent.getIterator('data/record');
    while (xmlElementIterator.hasNext()) {
        encryptFieldsInRecord(xmlElementIterator.next());
    }
}
function encryptFieldsInRecord(xmlElement) {
    //Then, iterate over all tags representing fields in the table
    var fieldIterator = xmlElement.getIteratorOverAllChildren();
    while (fieldIterator.hasNext()) {
        var field = fieldIterator.next();
        var fieldName = childElement.getName();
        //if table is incident, then description is encrypted for the
 short_description field
        if (tableName == 'incident' && fieldName == 'description') {
            field.valueFor(tableName, 'short_description');
        } else {
            //if table is not incident, ask the proxy to check if the
 given field is encrypted for the given table
            field.valueFor(tableName, fieldName);
        }
    }
}
```

In der Funktion *encryptFieldsInRecord()* wird die Methode *valueFor()* für eine Tabelle und ein Feld aufgerufen, die aufgrund der Anforderung dynamisch zugewiesen werden. Obwohl sich die Tabellen- und Feldnamen ändern können, fordert die Regel den Proxy auf, zu prüfen, ob das Feld in der Tabelle aufgrund der definierten Verschlüsselungskonfigurationen verschlüsselt werden muss.

Wenn das Feld nicht für die Verschlüsselung konfiguriert ist oder das Tag nicht mit einem Feld in der Tabelle übereinstimmt, überspringt der Proxy dieses Tag. Wenn das Tag mit einem für die Verschlüsselung markierten Feld übereinstimmt, verschlüsselt der Edge Encryption Proxy-Server den Wert.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine verschlüsselte Abfrage verwenden

In diesem Beispiel haben alle Tags das Attribut **Filter**, das angibt, ob das Tag eine verschlüsselte Abfrage enthält.

```
<data>
    <record>
        <name filter="false">'Test Record 1'</name>
        <description filter="false">'Test Record 1
 Description'</description>
        <query filter="true">category=1^name=edge</query>
    </record>
    <record>
        <name filter="false">'Test Record 2'</name>
        <description filter="false">'Test Record 2
 Description'</description>
        <query filter="true">category=2^severity=3</query>
   </record>
</data>
```

Die folgende Verschlüsselungsregelaktion kann angewendet werden:

```
function sampleXmlAction3() {
   var xmlContent = request.getAsXmlContent();
   var tableName = request.urlParam.table;
   // This first iterator will iterate over all record elements
   var xmlElementIterator = xmlContent.getIterator('data/record');
   while (xmlElementIterator.hasNext()) {
       encryptFieldsInRecord(xmlElementIterator.next());
   }
}
function encryptFieldsInRecord(xmlElement) {
   //this time we want to iterate over all tags representing fields in
 the table
   var fieldIterator = xmlElement.getIteratorOverAllChildren();
   while (fieldIterator.hasNext()) {
       var field = fieldIterator.next();
       var fieldname = childElement.getName();
       //let's look at the filter attribute, if true, then encrypt as
 encoded query
       if (field.getAttributeValue('filter') == 'true') {
           field.encodedQueryFor(tableName);
       } else {
           //if it is false then check if the field should be encrypted
           field.valueFor(tableName, fieldName);
       }
   }
}
```

Wenn das Attribut **Filter** „Wahr“ ist, fordert die Regel den Proxy-Server auf, die Werte in der verschlüsselten Abfrage zu verschlüsseln. Bei „falsch“ fordert die Regel den Proxy auf, zu prüfen, ob das Feld verschlüsselt werden soll.

XMLContent

Ein globales Objekt, das Methoden zum Iterieren des XML-Inhalts bereitstellt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können auf ein Objekt `XMLContent` zugreifen, indem Sie getAsXmlContent() auf einem Objekt `Anforderung` aufrufen.

Sie greifen auf XML-Daten in einem POST- oder URL-Parameter zu, indem Sie `request.postParams.<parameter name>.getAsXmlContent()` oder `request.urlParams.<parameter name>.getAsXmlContent()` aufrufen.

XMLContent - getIterator()

Gibt ein Objekt `XMLElementIterator` für den XML-Inhalt zurück.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
XMLElementIterator	Ein Objekt, das zum Iterieren von Elementen im Objekt `XMLContent` verwendet werden kann.

XMLContent - getIterator(String xPath)

Gibt ein Objekt `XMLElementIterator` für den XML-Inhalt basierend auf dem angegebenen Parameter zurück.

Parameter

Name	Typ	Beschreibung
xPath	Zeichenfolge	Ein xPath-ähnlicher Ausdruck, der angibt, wo im Objekt `XMLContent` begonnen werden soll.

Ergebnisse

Typ	Beschreibung
XMLElementIterator	Ein Objekt, das zum Iterieren von Elementen im Objekt `XMLContent` verwendet werden kann.

XMLElementIterator

Stellt Methoden zum Iterieren von XML-Elementen bereit.

Sie erhalten ein Objekt `XMLElementIterator`, indem Sie die Methode `getIterator()` in der Klasse `XMLContent` aufrufen.

XMLElementIterator - hasNext()

Bestimmt, ob ein anderes Element verfügbar ist.

Parameter

Name	Typ	Beschreibung
Keine		

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Typ	Beschreibung
Boolean	„Wahr“, wenn ein anderes Element verfügbar ist.

XMLElementIterator - next()

Gibt das nächste Element im Iterator zurück.

Sie können `next()` erst nach Aufrufen von `hasNext()` aufrufen.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
XMLElement	Das nächste XML-Element.

XMLElement

Stellt Methoden zum Iterieren von XML-Elementen und zum Zuordnen von Werten zu Feldern in einer Tabelle bereit.

Sie erhalten ein Objekt `XMLElement`, indem Sie die Methode `next()` eines Objekts `XMLElementIterator` aufrufen.

XMLElement - getIterator(String xPath)

Gibt ein Objekt `XMLElementIterator` für das XML-Element basierend auf dem angegebenen Parameter zurück.

Parameter

Name	Typ	Beschreibung
xPath	Zeichenfolge	Ein xPath-ähnlicher Ausdruck, der angibt, wo im Objekt `XMLElement` begonnen werden soll.

Ergebnisse

Typ	Beschreibung
XMLElementIterator	Ein Objekt, mit dem über Elemente im Objekt `XMLElement` iteriert werden kann.

XMLElement - getIteratorOverAllChildren()

Gibt ein Objekt `XMLElementIterator` zurück, das alle Unterelemente des XML-Elements basierend auf dem angegebenen Parameter enthält.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
XMLElementIterator	Ein Objekt, mit dem über Elemente im Objekt `XMLElement` iteriert werden kann.

XMLElement - valueFor(String tableName, String fieldName)

Gibt an, dass der Wert des Elements dem angegebenen Feld in der angegebenen Tabelle zugeordnet ist.

Durch Aufrufen dieser Methode für einen Elementwert wird dem Proxy mitgeteilt, dass der Wert für dieses Element dem angegebenen Feld in der angegebenen Tabelle zugeordnet ist. Der Proxy prüft dann, ob das Feld verschlüsselt werden muss. Wenn die Tabellen- und Feldnamen unbekannt sind, können Sie die Methode `valueFor()` auf einer Tabelle und einem Feld mit der Bezeichnung Dynamisch zugeordnet basierend auf der Anfrage aufrufen.

Parameter

Name	Typ	Beschreibung
tableName	Zeichenfolge	Der Tabellenname.
fieldName	Zeichenfolge	Der Feldname.

Ergebnisse

Typ	Beschreibung
void	

XMLElement - encodedQueryFor(String tableName)

Gibt an, dass der Wert des Elements eine codierte Abfrage für die angegebene Tabelle ist.

Durch Aufrufen dieser Funktion für ein Element wird dem Proxy mitgeteilt, dass der Wert des Elements eine codierte Abfragezeichenfolge für die angegebene Tabelle ist. Der Proxy analysiert die verschlüsselte Abfrage und verschlüsselt die Felder in der verschlüsselten Abfrage, die verschlüsselt werden müssen.

Parameter

Name	Typ	Beschreibung
tableName	Zeichenfolge	Die Tabelle, auf der die Abfrage ausgeführt werden soll.

Ergebnisse

Typ	Beschreibung
void	

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

XMLElement - getName()

Gibt den Elementnamen zurück.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
Zeichenfolge	Der Elementname.

XMLElement - getAttributeValue(String attribute)

Gibt den Wert des angegebenen Attributs zurück.

Parameter

Name	Typ	Beschreibung
Attribut	Zeichenfolge	Der Attributname.

Ergebnisse

Typ	Beschreibung
Zeichenfolge	Der Attributwert.

JSON-APIs

JSON-APIs können nach dem Aufrufen von `getAsJsonContent()` entweder über das Objekt `Anforderung` oder eine Eigenschaft `ParameterValue` verwendet werden.

Wenn Sie JSON-APIs zum Schreiben Ihrer Verschlüsselungsregel verwenden, können Sie ein allgemeines Format verwenden:

1. Aufrufen von `getAsJsonContent()` im Objekt `Anforderung`. Dies gibt ein iterierbares Objekt der zugrunde liegende Klasse `JsonNode` zurück.
2. Rufen Sie für das `JsonNode`– Objekt „iterator `()` “ oder „`getIterator(String xPath)` “ auf. Dies gibt ein Objekt `JsonNodeIterator` zurück, das zum Iterieren von Knoten im JSON-Objekt verwendet werden kann.
3. Aufrufen der Methode `hasNext()` im Objekt `JsonNodeIterator`, um zu bestimmen, ob ein anderes Element verfügbar ist.
4. Aufrufen von `next()` im Objekt `JsonNodeIterator`, um das nächste JSON-Element zurückzugeben. Sie können `next()` erst nach Aufrufen von `hasNext()` aufrufen.
5. Aufrufen von `valueFor(String tableName, String Feldname)` auf dem JSON-Element. Diese Methode teilt dem Proxy mit, dass der Wert für dieses Element dem angegebenen Feld in der angegebenen Tabelle zugeordnet ist. Der Proxy prüft dann, ob das Feld verschlüsselt werden muss.

> **Hinweis:** Um festzustellen, ob Sie `valueFor(String tableName, String fieldName)` auf einem JSON-Element aufrufen möchten, können Sie die Methode `getName()` verwenden, um den Namen des Elements zurückzugeben.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zu einem bekannten Tabellenfeld in der Instanz zuordnen

In diesem Beispiel wird die JSON-Payload auf der Instanz verarbeitet, um Datensätze in die Incident-Tabelle einzufügen. Das Beschreibungsfeld füllt den Incident mit short_description aus.

```
{
    data: {
        records: [
            {
                "name": "Test Record 1",
                "description": "Test Record 1 Description",
                "tag": "security"
            },
            {
                "name": "Test Record 1",
                "description": "Test Record 1 Description",
                "tag": "security"
            }],
        "query":
 "assigned_to=3D4860165813e63a00d00abd322244b092^category=vulnerability"
    },
    "source": "10.11.13.14"
}
```

Die folgende Regel kann gelten:

```
function sampleJsonAction1() {
    var jsonContent = request.getAsJsonContent();
    // This loop iterates over all description elements in the records
 array
    var jsonNodeIterator =
 jsonContent.getIterator('/data/records/description');
    while (jsonNodeIterator.hasNext()) {
        var jsonNode = jsonNodeIterator.next();
        jsonNode.valueFor('incident', 'short_decription');
    }
}
```

Diese Aktion iteriert die Knoten **Beschreibung** und fordert den Proxy-Server auf, die Werte zu verschlüsseln und sie in instance.short_description auf der Instanz einzufügen.

Hinweis: Diese Regel findet alle Knoten **Beschreibung** innerhalb der JSON-Payload. Wenn nur ein Knoten zu verschlüsseln ist, verwendet die Regel weiterhin die xPath- und Iterator-Struktur. Es iteriert jedoch nur einmal in der Schleife.

Zu einem unbekannten Tabellenfeld in der Instanz zuordnen

In diesem Beispiel wird die Regel **Datensätze** iteriert. Es ist jedoch nicht bekannt, welche Knoten zu erwarten sind. Es ist nur bekannt, dass für jedes Objekt innerhalb von **Datensätze** die Knoten mit den Namen der im URL-Parameter der Tabelle angegebenen Spalten übereinstimmen.

Die Regel legt außerdem fest, dass bei Vorliegen einer Incident-Tabelle, die Daten im Knoten **Beschreibung** verschlüsselt und im Feld short_description der Instanz gespeichert werden sollen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
function sampleJsonAction2() {
    var jsonContent = request.getAsJsonContent();
    var tableName = request.urlParam.table;
    // This first iterator will iterate over all record elements
    var jsonNodeIterator = jsonContent.getIterator('data/records');
    while (jsonNodeIterator.hasNext()) {
            encryptFieldsInRecord(jsonNodeIterator.next());
    }
}
function encryptFieldsInRecord(jsonNode) {
    //this time we want to iterate over all nodes
    var fieldIterator = jsonNode.iterator();
    while (fieldIterator.hasNext()) {
            var field = fieldIterator.next();
            var fieldname = childElement.getName();
            if (fieldName == 'description') {
                field.valueFor(tableName, 'short_description');
            } else {
                field.valueFor(tableName, fieldName);
            }
    }
}
```

In der Funktion *encryptFieldsInRecord()* wird die Methode *valueFor()* für eine Tabelle und ein Feld aufgerufen, die aufgrund der Anforderung dynamisch zugewiesen werden. Obwohl sich die Tabellen- und Feldnamen ändern können, fordert die Regel den Proxy auf, zu prüfen, ob das Feld in der Tabelle aufgrund der definierten Verschlüsselungskonfigurationen verschlüsselt werden muss.

Wenn das Feld nicht für die Verschlüsselung konfiguriert ist oder der Knotenname nicht mit einem Feld in der Tabelle übereinstimmt, überspringt der Proxy diesen Knoten. Wenn der Knotenname mit einem für die Verschlüsselung markierten Feld übereinstimmt, verschlüsselt der Proxy den Wert.

Eine verschlüsselte Abfrage verwenden

```
function sampleJsonAction3() {
    var jsonContent = request.getAsJsonContent();
    var tableName = request.urlParam.table;
    // This first iterator will iterate over all record elements
    var jsonNodeIterator = jsonContent.getIterator('data');
    while (jsonNodeIterator.hasNext()) {
        var jsonNode = jsonNodeIterator.next();
        if (jsonNode.getName() == 'records')
            encryptRecors(jsonNodeIterator.next());
        else if (jsonNode.getName() == 'query')
            jsonNode.encodedQueryFor(tableName);
    }
}
function encryptRecords(jsonNode) {
    //we iterate over all fields in the node
    var recordIterator = jsonNode.iterator();
    while (recordIterator.hasNext()) {
        encryptFieldsInRecord(recordIterator.next());
    }
}
function encryptFieldsInRecord(jsonNode) {
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
    //this time we want to iterate over all nodes
    var fieldIterator = jsonNode.iterator();
    while (fieldIterator.hasNext()) {
            var field = fieldIterator.next();
            var fieldname = childElement.getName();
            field.valueFor(tableName, fieldName);
    }
}
```

In diesem Beispiel wird die Regel **Daten** iteriert. Mit Auffinden von **Datensätzen** wird die gleiche Logik wie im zweiten Beispiel ausgeführt, wobei die Felder in jedem Knoten iteriert werden. Nach Auffinden des Knotens **Abfrage** wird `encodedQueryFor()` aufgerufen, um Werte verschlüsseln, die in der Abfrage verschlüsselt werden sollen.

JsonNode

Ein globales Objekt, das Methoden zum Durchlaufen des JSON-Inhalts bereitstellt.

Sie können auf ein Objekt `JsonNode` zugreifen, indem Sie getAsJsonContent() in einem Objekt `Anforderung` aufrufen.

Sie haben Zugriff auf JSON-Inhalte von einem POST- oder URL-Parameter, indem Sie `request.postParms.<parameter name>.getAsJsonContent()` oder `request.urlParms.<parameter name>.getAsJsonContent()` aufrufen.

JsonNode - getIterator(String xPath)

Gibt ein Objekt `JsonNodeIterator` für den JSON-Inhalt zurück.

Diese Methode kann nur für den Stammknoten verwendet werden, kann jedoch auch verwendet werden, um tief in das JSON-Objekt zu gelangen. Nachfolgende Traversen müssen die Methode `Iterator()` verwenden.

Parameter

Name	Typ	Beschreibung
xPath	Zeichenfolge	Ein xPath-Ausdruck.

Ergebnisse

Typ	Beschreibung
JsonNodeIterator	Ein Objekt, das Knoten im JSON-Objekt iterieren kann.

JsonNode - iterator()

Gibt ein Objekt `JsonNodeIterator` zurück, das alle untergeordneten Knoten des aktuellen Knotens iteriert.

Parameter

Name	Typ	Beschreibung
Keine		

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Typ	Beschreibung
JsonNodeIterator	Ein Objekt, das Knoten im JSON-Objekt iterieren kann.

JsonNode - getAsString()

Gibt den aktuellen Knotenwert als Zeichenfolge zurück.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
Zeichenfolge	Der aktuelle Knotenwert.

JsonNode - getAsString(String propertyName)

Gibt den Zeichenfolgenwert der angegebenen Eigenschaft zurück.

Parameter

Name	Typ	Beschreibung
propertyName	Zeichenfolge	Der Name der Eigenschaft.

Ergebnisse

Typ	Beschreibung
Zeichenfolge	Der Eigenschaftswert.

JsonNode - getName()

Gibt den Namen des aktuellen JSON-Knotens zurück.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
Zeichenfolge	Name des aktuellen JSON-Knotens.

JsonNode - valueFor(String tableName, String fieldName)

Gibt an, dass die JSON-Eigenschaft dem angegebenen Feld in der angegebenen Tabelle zugeordnet ist.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Durch Aufrufen dieser Methode für eine JSON-Eigenschaft wird dem Proxy mitgeteilt, dass der Wert für diese Eigenschaft dem angegebenen Feld in der angegebenen Tabelle zugeordnet ist. Der Proxy entscheidet dann, ob das Feld verschlüsselt werden muss. Wenn die Tabellen- und Feldnamen unbekannt sind, können Sie die Methode `valueFor()` auf einer Tabelle und einem Feld mit der Bezeichnung Dynamisch zugeordnet basierend auf der Anfrage aufrufen.

Parameter

Name	Typ	Beschreibung
tableName	Zeichenfolge	Der Tabellenname.
fieldName	Zeichenfolge	Der Feldname.

Ergebnisse

Typ	Beschreibung
void	

JsonNode - encodedQueryFor(String tableName)

Gibt an, dass der Wert der JSON-Eigenschaft eine codierte Abfrage für die angegebene Tabelle ist.

Durch Aufrufen dieser Funktion auf einem JSON-Knoten wird dem Proxy mitgeteilt, dass der Wert eine codierte Abfragezeichenfolge für die angegebene Tabelle ist. Der Proxy analysiert die verschlüsselte Abfrage und verschlüsselt die Werte für Felder in der verschlüsselten Abfrage, die verschlüsselt werden müssen.

Parameter

Name	Typ	Beschreibung
tableName	Zeichenfolge	Die Tabelle, auf der die Abfrage ausgeführt werden soll.

Ergebnisse

Typ	Beschreibung
void	

JsonNodeIterator

Sie erhalten ein Objekt `JsonNodeIterator`, indem Sie die Methoden `getIterator()` oder `iterator()` der Klasse `JsonNode` aufrufen.

JsonNodeIterator - hasNext()

Bestimmt, ob eine andere Eigenschaft verfügbar ist.

Parameter

Name	Typ	Beschreibung
Keine		

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Typ	Beschreibung
Boolean	„Wahr“, wenn eine andere Eigenschaft verfügbar ist.

JsonNodeIterator - next()

Gibt die nächste Eigenschaft im Iterator zurück.

Sie können `next()` erst nach Aufrufen von `hasNext()` aufrufen.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
JsonNode	Der nächste `JsonNode`.

print(String message)

Gibt eine Nachricht an die Wrapper-Protokolldatei aus: `<proxy server directory>/logs/wrapper_<date>.log`.

Diese Methode ist nur in einem Edge Encryption-Regelaktionsskript verfügbar

Parameter

Name	Typ	Beschreibung
Nachricht	Zeichenfolge	Die Nachricht, die in die Wrapper-Protokolldatei geschrieben werden soll.

Ergebnisse

Typ	Beschreibung
void	

Nicht zulässige Schlüsselwörter

Der Edge Encryption Proxy überprüft Verschlüsselungsregelskripts, bevor die Regel gespeichert wird. Viele JavaScript-Stichwörter sind in Verschlüsselungsregelskripts nicht zulässig.

Nicht zulässige Schlüsselwörter

Stichwort
__DIR__
__FILE__
__LINE__

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nicht zulässige Schlüsselwörter (Fortsetzung)

Stichwort
__parent__
__proto__
Fehler
Ausw
getClass
getPrototypeOf
Java
javax
javafx
JavaImporter
laden
loadWithNewGlobal
neu
Pakete
Objekt
Prototyp
RegExp
setPrototypeOf
diese
werfen

Attribute für das Edge-Encryption-Dictionary

Fügen Sie Tabellen und Feldern Wörterbuchattribute hinzu, um zu steuern, wie sie mit Edge Encryption funktionieren.

Um ein Wörterbuchattribut auf „wahr“ zu setzen, müssen Sie im Feld „ **Attribute** “ `Attribut=wahr` eingeben. Informationen zum Hinzufügen eines Dictionary-Attributs zu einem Datensatz finden Sie unter Tabellen und Felder mithilfe von Wörterbuchattributen ändern .

Edge Encryption ausgeschlossen [edge_encryption_excluded]

Bestimmt, ob das Feld von der Verschlüsselung ausgeschlossen ist.

Bei Festlegung auf „ `wahr`“ kann das Feld oder die Tabelle nicht verschlüsselt werden. Bei Festlegung auf `false`kann das Feld verschlüsselt werden.

- Wert: wahr/falsch
- Zielelement: Feld oder Tabelle
- Standardwert: false

Edge Encryption aktiviert [edge_encryption_enabled]

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bestimmt, ob das Feld für die Verschlüsselung durch eine Verschlüsselungskonfiguration geeignet ist.

Bei Festlegung auf `true`ist das Feld für die Verschlüsselung geeignet. Bei Festlegung auf `„false“`ist das Feld nicht für die Verschlüsselung geeignet. Da dieses Attribut vom System verwendet wird und nicht geändert werden kann, wird es dem Anwender nicht angezeigt.

Hinweis: Dieses Attribut gibt nicht an, dass ein Feld verschlüsselt ist, und löst auch keine Verschlüsselungslogik für das Feld aus. Das Attribut bestimmt vielmehr die Möglichkeit, dass das Feld von einem Benutzer verschlüsselt wird.

- Wert: wahr/falsch
- Zielelement: Feld
- Standardwert: true für Zeichenfolgenfelder

Klartext für die Edge Encryption zulässig [edge_encryption_clear_text_allowed]

Legt fest, ob serverseitige Skripts unverschlüsselte Daten an eine verschlüsselte Zeichenfolge innerhalb des Felds für Benutzeraktionen anhängen dürfen, die über den Proxy-Server ausgeführt werden, oder serverseitige automatisierte Skripts, z. B. geplante Aufgaben.

Bei Festlegung auf `true`ist das Anfügen von Daten zulässig. Bei Festlegung auf „ `false`“ ist das Anfügen von Daten nicht zulässig.

- Wert: wahr/falsch
- Zielelement: Feld
- Standardwert: falsch

Domain Separation und Edge Encryption

Domain Separation wird unter bestimmten Umständen mit Edge Encryptionunterstützt. Edge Encryption bietet die Möglichkeit, Daten aus der Umgebung des Kunden mithilfe spezifischer Konfigurationen, Regeln und Schlüssel zu verschlüsseln, die im Proxy Edge Encryption definiert sind. Der Edge Encryption Proxy ist nicht domänenabhängig und unterstützt keine domänenspezifischen Einstellungen. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Kein Support

- Das Feld „Domäne“ kann in Datentabellen vorhanden sein, es ist jedoch keine Geschäftslogik zum Verwalten der Daten vorhanden.
- Diese Ebene wird nicht als domänengetrennt betrachtet.

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

Funktionsweise der Domänentrennung in der Edge Encryption

Die Edge Encryption kann verwendet werden, wenn keine domänenspezifischen Schlüssel, Konfigurationen und Regeln erforderlich sind.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Domänentrennung für Service Provider

Datenintegration mit Edge Encryption

Um Daten von Drittanbietern mit einer Instanz über Edge Encryption zu integrieren, müssen Sie die Daten über den Edge Encryption Proxy-Server mit unterstützten Integrationen weiterleiten. Unterstützte Integrationen verwenden Verschlüsselungsregeln des Basissystems, die Daten in jeder Payload auf Felder in einer Tabelle abbilden.

Daten in für die Verschlüsselung markierte Felder hochladen

Edge Encryption unterstützt nicht den Import von Daten aus oder den Export von Daten nach Excel, CSV, XML oder anderen Dateitypen in oder aus Feldern mit definierten Verschlüsselungskonfigurationen.

ODBC-Treiber

Verschlüsseln Sie Anforderungen und Datenabfragen über den Edge Encryption Proxy-Server mit dem ODBC-Treiber.

Weitere Informationen: Edge Encryption ODBC-Treiberintegration

MID-Server

Sie können MID-Server so konfigurieren, dass Daten über einen Edge Encryption Proxy-Server geleitet werden. Es gelten jedoch einige Einschränkungen.

Weitere Informationen: Edge Encryption MID-Server-Integration

REST/SOAP Web Services

Verwenden Sie REST/SOAP Web Services zum Aktualisieren oder Abrufen von Datensatzdaten über den Edge Encryption Proxy-Server.

Weitere Informationen: Webservices

JSONv2-Webservice

Verwenden Sie JSONv2-Webservice-APIs zum Aktualisieren oder Abrufen von Datensatzdaten über den Edge Encryption Proxy-Server. Verschlüsselungsregeln des Basissystems unterstützen APIs zum Abrufen und Ändern von Daten.

- Um einen einzelnen Datensatz über die Datenänderungs-API einzufügen, verwenden Sie die Methoden `insert()` oder `insertMutiple()`.
- Um mehrere Datensätze über die Datenänderungs-API einzufügen, verwenden Sie die Methode `insertMultiple()`.

Weitere Informationen: JSONv2-Webservice

Um Daten von benutzerdefinierten Drittanbieter-Integrationen zu verschlüsseln, die oben nicht aufgeführt sind, erstellen Sie benutzerdefinierte Verschlüsselungsregeln. Weitere Informationen finden Sie unter Eine benutzerdefinierte Verschlüsselungsregel definieren.

Anhänge zu zur Verschlüsselung markierten Datensätzen hochladen

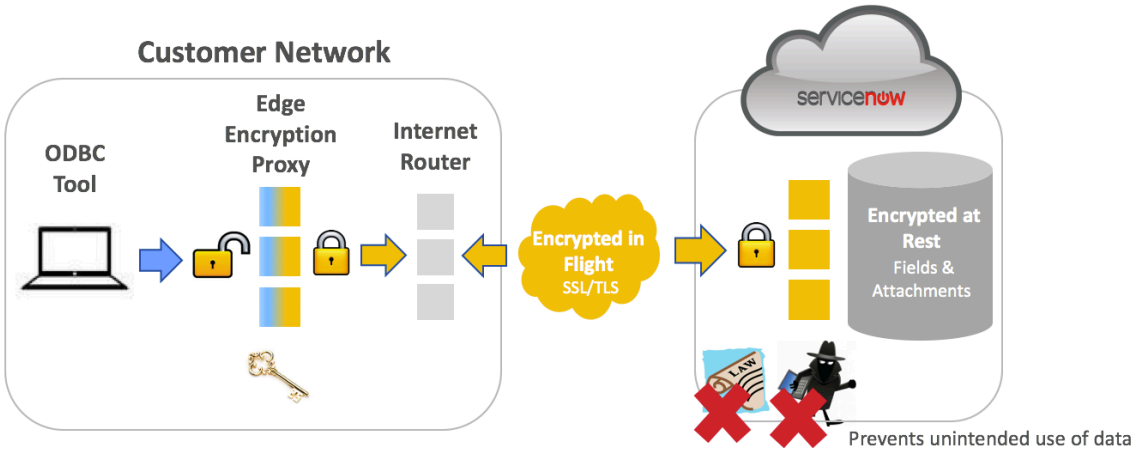
Anhänge können in Tabellen hochgeladen werden, wobei die Anhangsverschlüsselung mithilfe von REST und SOAP Web Services konfiguriert wird.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Edge Encryption ODBC-Treiberintegration

Konfigurieren Sie Ihren ODBC-Treiber für die Abfrage von Daten, die mit Edge Encryption verschlüsselt sind. Der Edge Encryption Proxy-Server verschlüsselt ODBC-Treiberanfragen an die ServiceNow-Instanz, wenn Edge Encryption mit dem ODBC-Treiber integriert ist.

Verschlüsselte Antworten von der Instanz werden über den Edge Encryption Proxy-Server entschlüsselt, bevor sie an den ODBC-Treiber in Ihrem Netzwerk weitergeleitet werden.



Für eine erfolgreiche Integration muss der ODBC-Treiber dem Zertifikat des Edge Encryption Proxy-Servers vertrauen. Wenn das Zertifikat des Edge Encryption Proxy-Servers von einer Zertifizierungsstelle signiert wird, die vom ODBC-Treiber vertraut wird, wird dem Proxy-Server Edge Encryption automatisch vertraut. Wenn jedoch eine Zertifizierungsstelle, der der ODBC-Treiber vertraut, das Edge Encryption Proxy-Server-Zertifikat nicht signiert hat, müssen Sie das selbstsignierte Zertifikat in den ODBC-Truststore importieren.

Ein selbstsigniertes Zertifikat in den ODBC-Truststore importieren

Wenn eine Zertifizierungsstelle, der der ODBC-Treiber vertraut, das Edge Encryption Proxy-Server-Zertifikat nicht signiert hat, müssen Sie ein selbst signiertes Zertifikat in den ODBC-Truststore importieren. Sie können das Zertifikat vom Edge Encryption Proxy-Server exportieren und in den ODBC-Truststore importieren.

Vorbereitungen

Erforderliche Rolle: admin

Um festzustellen, ob eine vom ODBC-Treiber vertrauenswürdige Zertifizierungsstelle das Zertifikat des Edge Encryption Proxy-Servers signiert hat, führen Sie den folgenden Befehl im Schlüsselspeicherverzeichnis im Stammverzeichnis des Proxys aus, um eine Liste der vom ODBC-Treiber vertrauenswürdigen Zertifizierungsstellen anzuzeigen:

```
keytool -keystore "<ODBC directory>\ip\Java\jre\lib\security\cacerts"
 -list
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

In den meisten Fällen stellt der Client über ein Lastenausgleichsmodul eine Verbindung zu den Proxys Edge Encryption her, sodass das Zertifikat das im Lastenausgleichsmodul konfigurierte Zertifikat ist.

Wenn kein Lastenausgleichsmodul zwischen Client und Edge-Proxy-Server vorhanden ist, ist das Zertifikat das vom Edge-Proxy vorgelegte Zertifikat und wird in der Datei *edgeencryption.properties* konfiguriert.

```
edgeencryption.proxy.https.port = 9090
edgeencryption.proxy.https.keystore.path = keystore/keystore
edgeencryption.proxy.https.keystore.password = password
edgeencryption.proxy.https.cert.alias = jetty
```

Einzelheiten zum Bearbeiten von Eigenschaften finden Sie unter Zusätzliche Eigenschaften in der Eigenschaftendatei mit Edge Encryption konfigurieren

Prozedur

1. Wechseln Sie in das Schlüsselspeicherverzeichnis im Proxy-Stammverzeichnis.
2. Überprüfen Sie den Schlüsselspeicher auf das selbstsignierte Zertifikat.

   a. Um den Schlüsselspeicher für das Zertifikat zu überprüfen, können Sie den folgenden Befehl ausführen, um alle Elemente im Schlüsselspeicher aufzulisten.

   ```
   keytool -list -keystore keystore.jceks -storetype jceks -v
   ```

   b. Suchen Sie den Schlüsselalias in der Liste der Elemente.

3. Exportieren Sie das Zertifikat mithilfe des Schlüsselalias in eine CER-Datei.

   ```
   keytool -export -alias <key alias> -keystore keystore.jceks -storetype
    jceks -rfc -file <file name>.cer
   ```

4. Wechseln Sie in Ihr ODBC-Truststore-Verzeichnis: `ODBC\ip\Java\jre\lib\security\cacerts`.
5. Importieren Sie das Zertifikat in Ihren ODBC-Truststore.

   ```
   keytool -keystore cacerts -importcert -alias $<key alias> -file <file
    name>.cer
   ```

Die ODBC-Treibereigenschaften festlegen

Legen Sie die ODBC-Treibereigenschaften so fest, dass Anforderungen über den Edge Encryption Proxy-Server geleitet werden.

Vorbereitungen

Erforderliche Rolle: admin

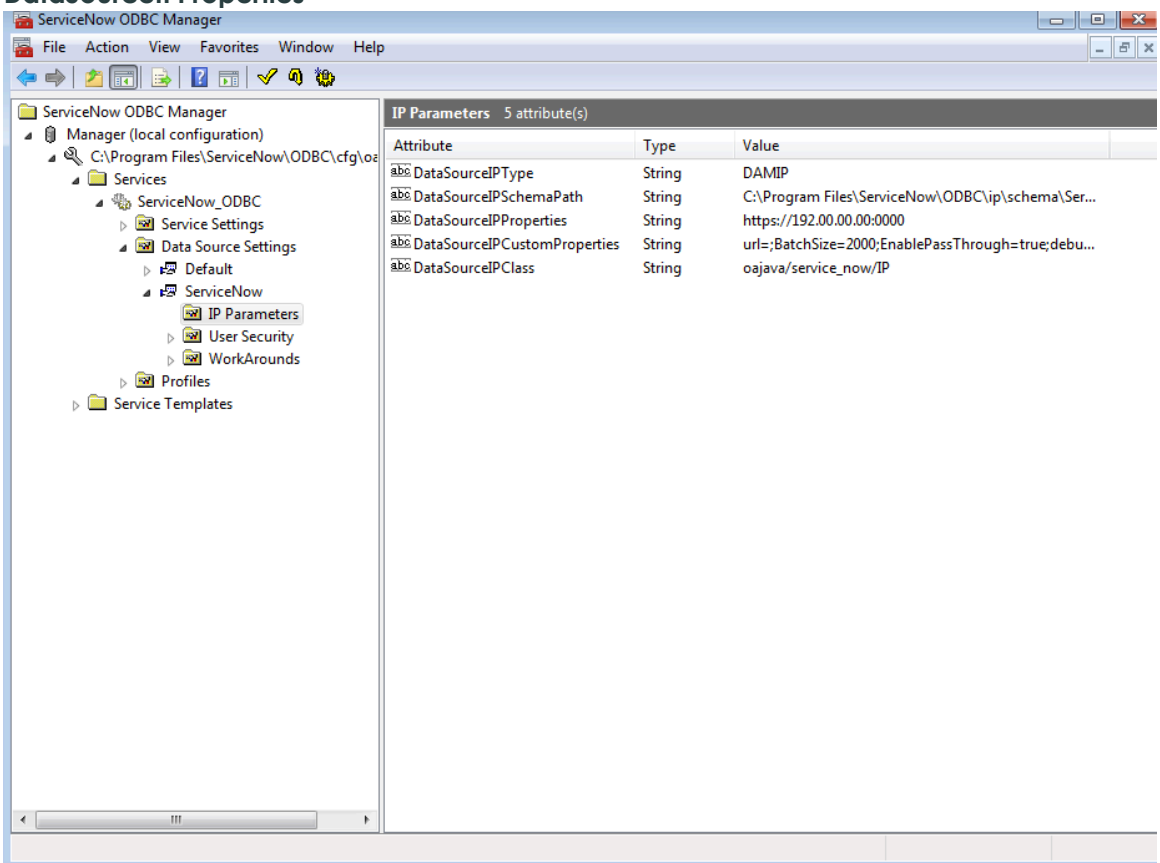
Prozedur

1. Navigieren Sie in Windows zu **Start** > **Programme** > **ServiceNow ODBC Management Console**an.
2. Erweitern Sie das Stammverzeichnis der Konsolenstruktur um: `ServiceNow ODBC Manager\Manager\<installation location>\Services\ServiceNow_ODBC\Data Source Settings\ServiceNow\IP Parameters`.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Doppelklicken Sie auf das Attribut **DataSourceIPProperties**.
4. Ändern Sie den **Wert** auf die URL Ihres Edge Encryption Proxy-Servers, wie z. B. `https://<IP address>:<port>`

DataSourceIPProperties



5. Klicken Sie auf **OK**.

Nächste Maßnahme

Der ODBC-Treiber ist jetzt so konfiguriert, dass Anforderungen an die Instanz über den Edge Encryption Proxy-Server weitergeleitet werden.

Edge Encryption MID-Server-Integration

Konfigurieren Sie MID-Server so, dass Daten über den Edge Encryption Proxy-Server geleitet werden.

Bei der Integration mit MID-Server fungiert der Edge Encryption Proxy-Server als Endpunkt des MID-Server. Der Edge Encryption Proxy-Server verschlüsselt und entschlüsselt dann die zwischen der ServiceNow-Instanz und dem MID-Server übertragenen Daten.

Einschränkungen bei der Integration mit dem MID-Server

Wenn die Daten von MID-Server so konfiguriert sind, dass sie den Edge Encryption Proxy-Server durchlaufen, gelten die folgenden Einschränkungen:

- Die Verschlüsselung der ECC-Warteschlangenfelder wird nicht unterstützt.
- Verschlüsselte Daten können nicht mit Discovery oder Service-Mapping verwendet werden.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Den MID-Server auf den Edge Encryption Proxy-Server verweisen

Um Daten von MID-Server über den Edge Encryption Proxy-Server zu übertragen, aktualisieren Sie die MID-Server-Konfigurationsdatei, um MID-Server auf den Edge Encryption Proxy-Server zu verweisen.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn MID-Server so konfiguriert ist, das der Edge Encryption Proxy-Server durchlaufen wird, können Sie die Web-Proxy-Eigenschaften in der MID-Server-Konfigurationsdatei nicht verwenden, um den Datenverkehr über den Edge Encryption Proxy-Server zu Ihrer Instanz zu leiten. Stattdessen müssen Sie den Edge Encryption Proxy-Server als den Endpunkt von MID-Server einstellen.

Prozedur

1. Navigieren Sie zum lokalen MID-Server-Verzeichnis und öffnen Sie die Datei `config.xml`.
2. Suchen Sie das Element `<parameter name="url" value="https://YOUR_INSTANCE.service-now.com" />` und ändern Sie die Eigenschaft „Wert“ auf die URL Ihres Edge Encryption Proxy-Servers.
   Beispiel: `http://hostname.mycompany.com:8081`
   Mit diesem Schritt wird MID-Server angewiesen, den Datenverkehr an den Edge Encryption Proxy-Server und nicht an die Instanz zu leiten. Der Edge Encryption Proxy-Server wiederum verschlüsselt alle erforderlichen Felder und leitet die Nutzdaten an die Instanz weiter.
3. Speichern und schließen Sie die Datei.
4. Starten Sie den MID-Server neu, wenn schon in Ausführung.

Diagnose und Leistung der Edge Encryption

Überwachen sie Performance-Trends des Edge Encryption Proxy-Servers und untersuchen Sie die vom Edge Encryption Proxy-Server generierten Fehler.

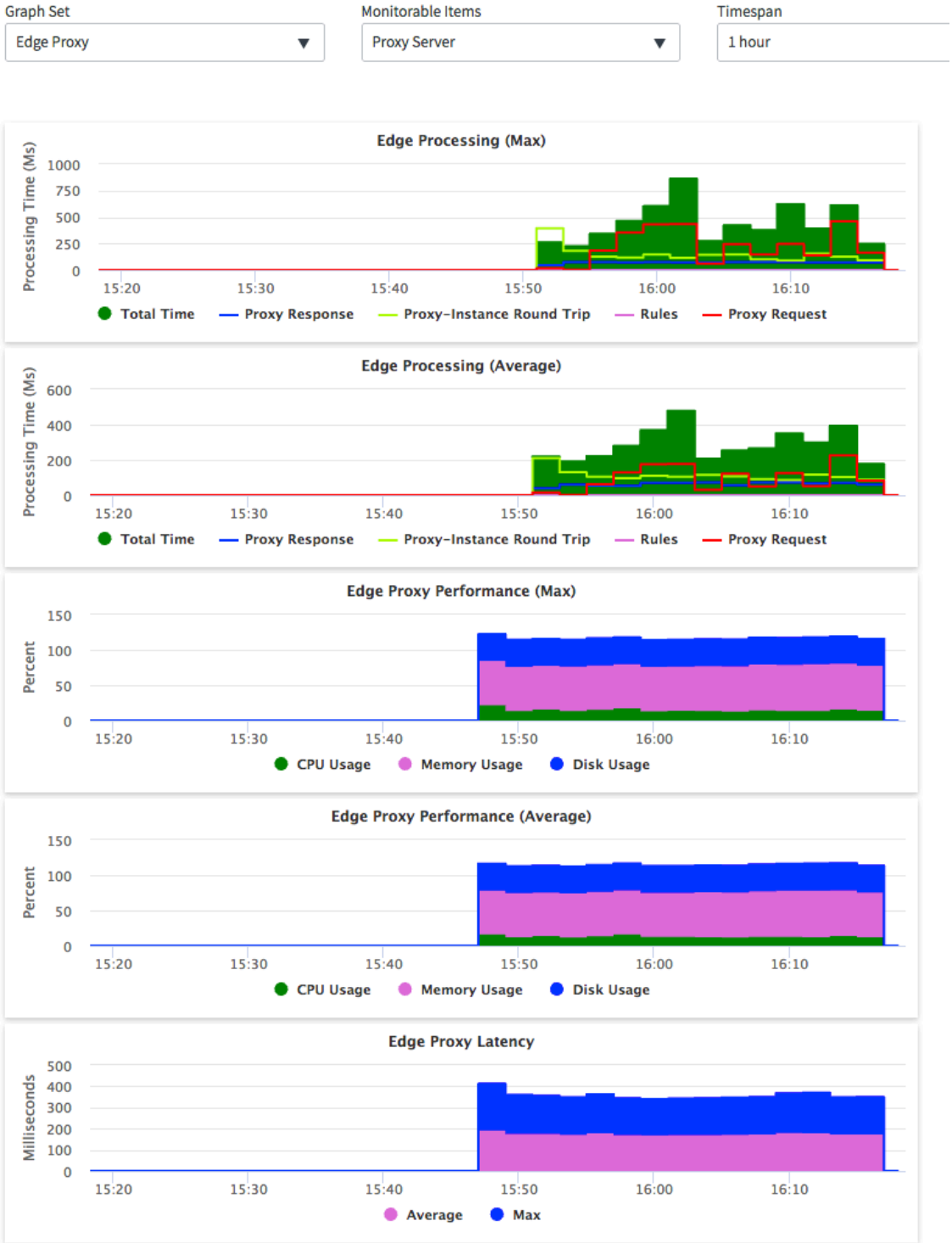
Edge-Proxy-Leistung

Sehen Sie sich die wichtigsten Performance-Trends des Edge Encryption Proxy-Servers mithilfe des Edge-Proxy-Diagramms auf der ServiceNow Performance-Homepage an. Überwachte Trends umfassen:

- Maximale und durchschnittliche Antwortzeit zwischen Client, Proxy-Server und Instanz.
- CPU, Speicherplatz und Speicherplatz des Host-Computers.
- Maximale und durchschnittliche Netzwerklatenz zwischen dem Proxy-Server und der ServiceNow-Instanz.

Hinweis: Edge Encryption Proxy-Server mit doppelten Namen melden keine Performance-Trends.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Edge-Verarbeitung (Maximum und Durchschnitt)

Maximale und durchschnittliche Zeit in Millisekunden für die Verarbeitung einer Anforderung. Diese Datenpunkte sind allgemeine Trends im Zeitablauf.

- **Gesamtzeit**: Zeit, in der der Proxy-Server eine Anforderung von einem Client erhält und eine Antwort sendet. Dieser Datenpunkt ist die Summe der nachfolgenden Datenpunkte.
- **Proxy-Antwort**: Zeit, in der der Proxy-Server eine Antwort der Instanz verarbeitet.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Proxy-Instanz-Rundlauf**: Zeit, in der der Proxy-Server eine Anforderung an die Instanz sendet und eine Antwort erhält. Enthält die Netzwerklatenz zwischen dem Proxy-Server und der Instanz sowie die Zeit, die die Instanz für die Verarbeitung der Anforderung benötigt.
- **Regeln**: Zeit, die der Proxy-Server benötigt, um eine Anforderung anhand definierter Verschlüsselungsregeln auszuwerten.
- **Proxy-Anforderung**: Zeit, in der der Proxy-Server eine Client-Anforderung verarbeitet und an die Instanz weiterleitet.

Edge Proxy-Performance (Maximum und Durchschnitt)

Maximaler und durchschnittlicher Prozentsatz der auf dem Host-Computer verwendeten Ressourcen.

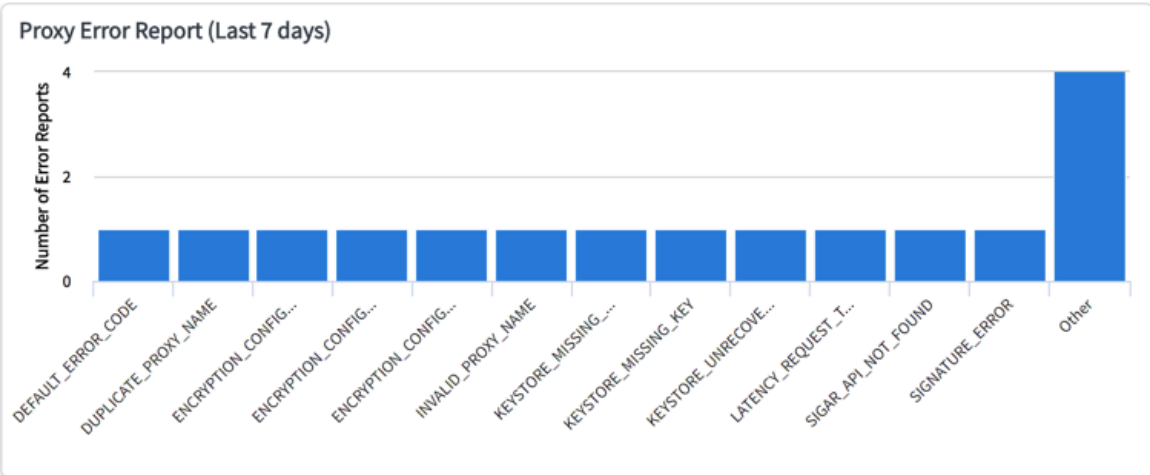
- CPU-Auslastung
- Speicherauslastung
- Festplattenauslastung

Edge-Proxy-Latenzzeit

Maximale und durchschnittliche Netzwerklatenz in Millisekunden zu einem bestimmten Zeitpunkt. Die Latenz wird durch die Rundlaufzeit bestimmt, die ein Proxy-Server benötigt, um einen einfachen Ping an die Instanz zu senden und eine Antwort zu empfangen.

Proxy-Fehlerberichte

Navigieren zu **Konfiguration der Edge Encryption** > **Diagnose und Fehlerbehebung** > **Proxy-Fehlerberichte** um alle in den letzten sieben Tagen erfassten Proxyserverfehler anzuzeigen.



Fehler werden über einen Zeitraum von einer Minute erfasst. Jede Minute wird ein Fehlerbericht generiert. Die vertikale Achse zeigt die Anzahl der Fehlerberichte der letzten sieben Tage an, die jeden Fehler enthalten. Selbst wenn beispielsweise der Fehler DEFAULT_ERROR_CODE über einen Zeitraum von einer Minute mehrmals ausgelöst wird, erreicht die Leiste DEFAULT_ERROR_CODE nur einen Fehler auf der Achse **Anzahl der Fehlerberichte**.

In dieser Ansicht können Sie:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Auf die einzelnen Proxy-Fehlercodeleisten klicken, um den Bericht über einen einzelnen Fehler für jeden Proxy-Server anzuzeigen. In dieser Ansicht können Sie erneut auf die Leiste klicken, um den Fehlertext in der Edge Encryption Proxy-Statistiktabelle [edge_encryption_stat] anzuzeigen. Folgen Sie den Links im Fehlertext, um weitere Informationen und mögliche Schritte zur Fehlerbehebung anzuzeigen.
- Klicken Sie auf **Andere**, um die zweite Seite des Fehlerberichts zu sehen.

Hinweis: Wenn Sie mehr als einen Proxy-Server mit demselben Namen haben, wird im Proxy-Fehlerbericht ein einzelner Fehler DUPLICATE_PROXY_NAME angezeigt. Für Proxy-Server mit doppelten Namen werden keine anderen Fehler gemeldet. Wenn dieser Fehler auftritt, stellen Sie sicher, dass alle Proxy-Server eindeutige Namen haben.

Zusätzlich Überwachungsressourcen

Die Instanz verfolgt alle Verschlüsselungsproxys. Jeder Edge Encryption Proxy-Server registriert sich beim Start. Die Instanz wird benachrichtigt, wenn:

- Ein neuer Edge Encryption Proxy-Server gestartet wird.
- Ein Edge Encryption Proxy-Server absichtlich heruntergefahren wird.

Wenn ein Edge Encryption Proxy-Server versucht, sich bei einer Instanz zu registrieren, die Edge Encryption nicht installiert hat, wird der Proxy nicht gestartet.

Alle Verschlüsselungskonfigurationsdateien werden geprüft. Gelöschte Datensätze werden für alle Verschlüsselungskonfigurationsdateien geprüft. Audit-Datensätze werden in der Tabelle sys_audit abgelegt. Um den Verlauf eines bestimmten Konfigurationsdatensatzes anzuzeigen, zeigen Sie den Datensatz an, und klicken Sie auf **Verlauf** > **Liste** im Menü. Der Massenverschlüsselungsauftrag wird keinem Audit unterzogen.

Verwenden Sie die folgenden zusätzlichen Ressourcen, um Ihre Proxy-Server zu überwachen.

Tabelle	Beschreibung
Ungültige Einfügeversuche [sys_edge_encryption_invalid_insert_log]	Liste der Versuche, die folgenden Daten in verschlüsselten Feldern zu speichern: • Nicht verschlüsselte Daten. • Daten, die nicht von einem Edge Encryption Proxy stammen. Die Instanz lehnt alle Versuche ab, diese Daten zu speichern, und protokolliert sie anschließend. Wenn Sie die Rolle Security-Admin haben, können Sie die Protokolle in der Liste „Ungültige Einfügeversuche“ anzeigen.
Auftragsfehler [sys_encryption_job_execution]	Eine Liste der Aufträge, die nicht erfolgreich ausgeführt wurden.
Systemprotokolle	Die Instanz sucht regelmäßig nach Nachrichten von jedem registrierten Proxy-Server. Wenn ein Proxy-Server im erforderlichen Zeitraum keine Nachricht gesendet hat, wird ein Fehler protokolliert. Die Protokollnachricht enthält Informationen zum Verschlüsselungs-Proxy und den letzten Zeitpunkt, zu dem der Proxy die Instanz gepingt hat. Wenn die Instanz feststellt, dass keiner der Verschlüsselungsproxys

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
	online ist, protokolliert sie eine Nachricht. Diese Meldungen werden zum Systemprotokoll hinzugefügt.

Die Edge Proxy-Statistikerfassung deaktivieren oder reduzieren

Verhindern Sie, dass der Edge Encryption Proxy-Server Edge Proxy Diagrammsatz-Statistiken an die ServiceNow Performance-Homepage sendet, oder reduzieren Sie die Häufigkeit der statistischen Erfassung.

Vorbereitungen

Erforderliche Rolle: admin oder security_admin

Warum und wann dieser Vorgang ausgeführt wird

Durch das Hinzufügen von Eigenschaften in der Konfigurationsdatei `edgeencryption.properties` können Sie:

- Den Edge Proxy-Diagrammsatz deaktivieren.
- Das Intervall ändern, in dem die Statistiken vom Edge Encryption Proxy-Server erfasst werden. Standardmäßig werden Statistiken alle 30 Sekunden erfasst.

Prozedur

1. Öffnen Sie in Ihrem Installationsverzeichnis des Proxy-Servers die Konfigurationsdatei `edgeencryption.properties` im Ordner `<installation directory>/conf/`.
2. Fügen Sie eines der Eigenschaften des Edge Encryption Proxy-Servershinzu .
3. Starten Sie den Proxy-Server neu.

Erhöhen Sie die Debug-Protokollierung für den Edge Encryption -Proxy

Erhöhen Sie die Protokollierungsebene, um Protokolle zu interpretieren und Probleme mit dem Proxy zu debuggen.

Es gibt derzeit drei Optionen zum Erhöhen der Debug-Protokollierung im Edge Encryption -Proxy. Erhöhen Sie die Protokollierungsebene, um Probleme zu debuggen, und stellen Sie dem technischen Support mithilfe ausführlicherer Protokollanweisungen Informationen zur Untersuchung des Problems zur Verfügung.

Richten Sie abhängig vom zu debuggenden Problem die Debug-Protokollierung auf eine von drei Arten ein:

- Andere Debugging-Probleme als SSL-Konnektivität
- Protokollierung von Zeitmetriken für Anforderungen über den Proxy
- Beheben von Problemen mit der SSL-Konnektivität zwischen dem Edge Encryption-Proxy und der Instanz

Für alle Debug-Fälle können Sie die Protokolle in Ihrem eigenen anzeigen und interpretieren oder einen Incident öffnen, um eine Interpretation vom technischen Support von ServiceNow zu erhalten, die das Problem beschreibt und beschreibt, wie es reproduziert wird.

Beheben von Problemen mit der Anwendung Edge Encryption außer SSL-Konnektivität

Verwenden Sie diese Methode, um Probleme mit der Anwendung Edge Encryption zu debuggen, ohne den Proxy anzuhalten und neu zu starten. Diese Schritte erhöhen die Protokollierungsebene und helfen bei der Suche nach der Ursache durch ausführlichere Protokollanweisungen.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: admin

Hinweis: Änderungen an der Datei „`$proxy_installation_location/conf/log4j2.properties` “ werden innerhalb von etwa 60 Sekunden, nachdem Sie Ihre Änderungen vorgenommen haben, vom Proxy übernommen. Sie müssen die Proxys nicht neu starten.

Prozedur

1. Suchen Sie in der Datei `$proxy_installation_location/conf/log4j2.properties` nach der folgenden Zeile.

```
logger.edge.level=info
```

2. Ändern Sie die obige Zeile wie folgt ab:

```
logger.edge.level=debug
```

3. Speichern Sie den Change.
   Es kann bis zu 60 Sekunden dauern, bis die Änderung wirksam wird. Dazu ist jedoch kein Proxy-Neustart erforderlich.
4. Reproduzieren Sie Ihr Problem.
5. Suchen Sie in der Datei `$proxy_installation_location/logs/edgeencryption.log` nach Debug-Protokollanweisungen im Zusammenhang mit der Anwendung.

Ergebnisse
Nachdem Sie die Eigenschaft geändert haben, können Sie zusätzliche Details in der Datei `$proxy_installation_location/logs/edgeencryption.log anzeigen`.
Wenn Sie das Debugging abgeschlossen haben, machen Sie die an der Datei `$proxy_installation_location/conf/log4j2.properties vorgenommene Änderung rückgängig`.

Protokollierung von Zeitmetriken für Anforderungen über den Proxy

Aktivieren Sie die Protokollierung von Zeitmetriken, um für jede vom Edge Encryption -Proxy verarbeitete Anforderung eine Metrikanweisung hinzuzufügen. Jede dieser Protokollanweisungen für Zeitmetriken enthält nützliche Informationen über die Anforderung, z. B. Verarbeitungszeiten und verwendete Verschlüsselungsregel.

Vorbereitungen
Erforderliche Rolle: admin

Hinweis:

Die zusätzlichen Protokollierungseinstellungen werden der Datei `$proxy_installation_location/conf/log4j2.properties hinzugefügt`.
Vorgenommene Änderungen werden vom Proxy dynamisch innerhalb von etwa einer Minute übernommen, sodass Sie die Proxys nicht neu starten müssen.

Prozedur

1. Ändern Sie die Datei `$proxy_installation_location/conf/log4j2.properties`, indem Sie die folgenden Zeilen am Ende der Datei hinzufügen

```
appender.timinglog.type=RollingFile
appender.timinglog.name=TimingLog
appender.timinglog.fileName=../logs/edgenetwork.log
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
appender.timinglog.filePattern=../logs/$
${date:yyyy-MM}/edgenetwork-%d{yyyy-MM-dd-HH}-%i.log.gz
appender.timinglog.layout.type=PatternLayout
appender.timinglog.layout.pattern=%d [%t] %-5p %m%n
appender.timinglog.policies.type=Policies
appender.timinglog.policies.size.type=SizeBasedTriggeringPolicy
appender.timinglog.policies.size.size=500MB
appender.timinglog.strategy.type=DefaultRolloverStrategy
appender.timinglog.strategy.max=4

logger.timing.name=com.snc.edgeencryption.metrics.EdgeEncryptionTimingM
etricCache
logger.timing.level=debug
logger.timing.additivity=false
logger.timing.appenderRef.rolling.ref=TimingLog
```

2. Speichern Sie die Datei.

Ergebnisse

Nach dem Speichern der Datei „`log4j.properties` “ werden in der `Protokolldatei` „`$proxy_installation_location/logs/edgenetwork.log` “ für Netzwerkzeiten die folgenden Arten von Nachrichten angezeigt.

```
2022-07-21 12:56:15,783 [qtp1971991758-7700] DEBUG
 com.snc.edgeencryption.metrics.EdgeEncryptionTimingMetricCache -
 request_uri=/api/now/ui/presencesysparm_auto_request=true&cd=1658433375
754 request_method=POST client_request_received="2022-07-21 12:56:15,015"
 proxy_request_processing_time=6 all_rules_processing_time=0
 rule_executed="REST JSON" rule_execution_time=1
 proxy_instance_round_trip=14 proxy_response_processing_time=1
 total_time_from_proxy=21 reponse_code=201
 glide_user=SCv3_1:BAz1ZK7ee9XoroG2nvMlixHpgTvsT4fY2bwQvnH2WdU=:y5HGsTTqo
3Pjq6G0xk4LoazCwCiWRJk4/6SpbXuBzqg=:6816f79cc0a8016401c5a33be04be441
 jsessionid_suffix=037A66
```

Die Werte in den Protokollnachrichten lauten wie folgt:

```
request_uri: The URI being requested

request_method: The HTTP method being used, for example, GET, POST, PUT,
 PATCH, DELETE

client_request_received: The timestamp noting when the HTTP client
 request arrived at the Edge proxy

proxy_request_processing_time: How long the Edge proxy took to process
 the request in milliseconds

all_rules_processing_time: Total time it took to execute all of the Edge
 Encryption rules for the request in milliseconds

rule_executed: The name of the encryption rule that was executed

rule_execution_time: How long it took to execute listed rule_executed in
 milliseconds
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
proxy_instance_round_trip: The time from when the Edge proxy sent the
 request to the instance until the instance sent the response and was
 received by the edge proxy in milliseconds

proxy_response_processing_time: How long the Edge proxy took to process
 the response in milliseconds

total_time_from_proxy: The total time from when the Edge proxy received
 the request from the client and returned the response to the client in
 milliseconds

response_code: HTTP response code

glide_user: The glide_user cookie value

jsessionid_suffix: The JSession cookie suffix associated with the request
```

Debuggen Sie Probleme mit der SSL-Konnektivität zwischen dem Edge Encryption -Proxy und der -Instanz

Verwenden Sie diese Methode, um Probleme mit der SSL-Konnektivität zwischen dem Proxy Edge Encryption und Ihrer -Instanz zu debuggen, z. B. wenn der Zugriff auf die Instanz über den Proxy fehlschlägt. Diese Schritte erhöhen die Protokollierung und helfen beim Auffinden der ausführlichen Protokollanweisungen.

Vorbereitungen

Erforderliche Rolle: admin

Hinweis: SSL-Konnektivitäts-Debugging ist nur bei der Behebung von Problemen mit dem TLS-Konnektivitätstyp relevant. In der Praxis ist dies nicht üblich und wird nur selten benötigt.

Prozedur

1. Den Proxy-Server stoppen.
2. Fügen Sie der Datei `$proxy_installation_location/conf/wrapper.conf`, einer Java-Starteigenschaft, die folgende Zeile hinzu:

   ```
   wrapper.java.additional.<next available number in sequence> =
    -Djavax.net.debug=all
   ```

   Beispiel:

   ```
   For example: wrapper.java.additional.4 = -Djavax.net.debug=all
   ```

3. Speichern Sie die Änderung, und starten Sie den Proxy-Server neu.
4. Reproduzieren Sie Ihr Konnektivitätsproblem.

Ergebnisse

Nach dem Reproduzieren des Problems finden Sie Debug-Protokollanweisungen im Zusammenhang mit dem SSL-Austausch unter `$proxy_installation_location/logs/wrapper_` <current date> .log -Datei. Wenn Sie mit dem Debuggen fertig sind. Sie können die zusätzliche Protokollierung remote durchführen, indem Sie die in den vorherigen Schritten erstellte Zeile entfernen oder auskommentieren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenbankverschlüsselung

ServiceNow® bietet Datenbankverschlüsselungsmethoden (Database Encryption, DBE) und Festplattenverschlüsselungsmethoden für Kunden mit gesetzlichen Verpflichtungen zum Datenschutz an, die möglicherweise den Schutz aller Daten im Ruhezustand erfordern.

Wichtig: Ab Release Washington DC wird die Datenbankverschlüsselung auf ihre künftige Einstellung vorbereitet. Cloud Encryption ist die Ersatzlösung für die Verschlüsselung von Daten im Ruhezustand. Einzelheiten finden Sie unter Cloud-Verschlüsselung mit Schlüsselverwaltung

Untersuchen



Lernen Sie die wichtigsten Funktionen und den Geschäftsnutzen von Database Encryption kennen.

Anforderung



Erfahren Sie mehr darüber, wie Sie die Rotation des Datenbankschlüssels anfordern.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Referenz



Database Encryption with Customer-Controlled Switch (DBE-CCS) ist eine Verschlüsselungslösung, die alle Daten im Ruhezustand verschlüsselt, wenn sie nicht in der Datenbank verwendet werden.

Datenbankverschlüsselung erkunden

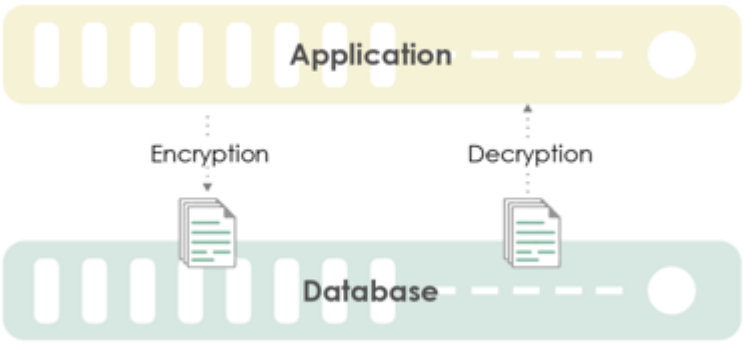
ServiceNow® bietet Datenbankverschlüsselungsmethoden (Database Encryption, DBE) und Festplattenverschlüsselungsmethoden für Kunden mit gesetzlichen Verpflichtungen zum Datenschutz an, die möglicherweise den Schutz aller Daten im Ruhezustand erfordern.

Wichtig: Ab Release Washington DC wird die Datenbankverschlüsselung auf ihre künftige Einstellung vorbereitet. Cloud Encryption ist die Ersatzlösung für die Verschlüsselung von Daten im Ruhezustand. Einzelheiten finden Sie unter Cloud-Verschlüsselung mit Schlüsselverwaltung

Mit der Datenbankverschlüsselung können alle Daten mit symmetrischer AES-256-Verschlüsselung geschützt werden, unabhängig davon, ob die Datenbank online oder offline ist. Aus der Perspektive Now Platform fließen alle Daten in entschlüsselt.

- Die Datenbankverschlüsselung unterstützt die Verschlüsselung aller gespeicherten Daten in Echtzeit und bietet Schutz für Daten online und offline ohne Verlust der Funktionalität.
- Die vollständige Festplattenverschlüsselung schützt Offline-Daten bei Verlust oder Diebstahl eines Datenträgers.

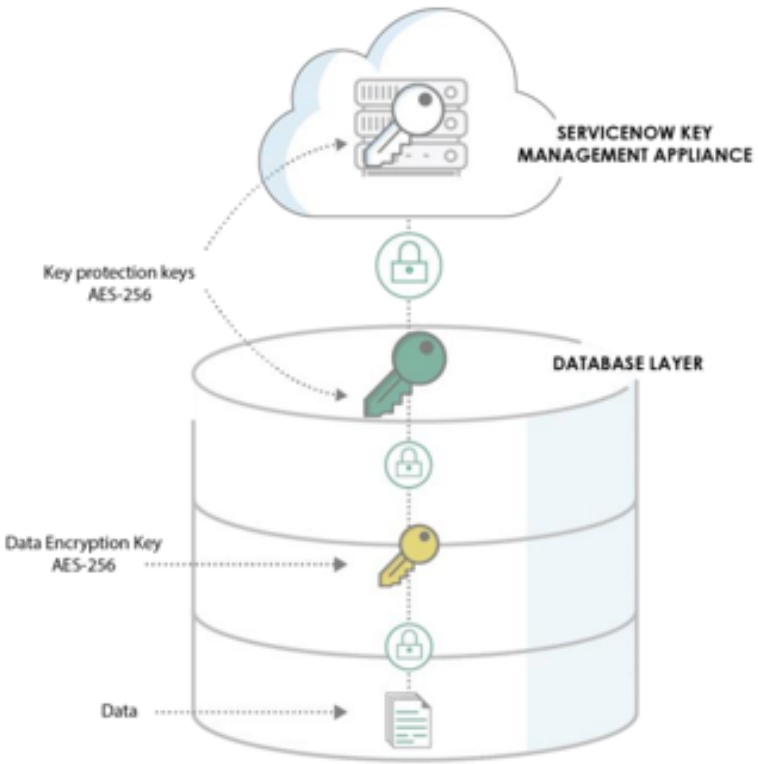
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Mit der Datenbankverschlüsselung werden alle gespeicherten Daten verschlüsselt, und einzelne Datensätze oder Tabellen werden während des Zugriffs im Arbeitsspeicher entschlüsselt. Neue oder geänderte Daten werden verschlüsselt, wenn sie in eine Tabelle eingegeben werden, und zugehörige Aktivitätsprotokolldateien (bin, wiederholen, rückgängig machen und Fehler) werden ebenfalls verschlüsselt.

Die Datenbankverschlüsselung ist für Benutzer transparent, ohne Funktionalitätsverlust. Bei Verwendung dieser Funktion werden alle Instanzen zusammen mit dem Replikationsdatenverkehr und den Sicherungen verschlüsselt. Das Klonen von Instanzen ist weiterhin verfügbar mit einer geringfügigen Auswirkung auf die Leistung bei Verwendung der Datenbankverschlüsselung von bis zu 5 %. Sowohl neue als auch vorhandene Instanzen in unterstützten Releases von Now Platform können die Datenbankverschlüsselung nutzen.

Wie dargestellt, speichert und verwaltet ServiceNow Schlüssel mithilfe einer Schlüsselhierarchie auf drei Ebenen:



© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Ein kundenspezifischer AES-256-Schlüssel wird von der Datenbank-Engine erstellt und zum Verschlüsseln der Daten verwendet.
2. Ein zweiter kundenspezifischer AES-256-Schlüssel wird von der Datenbank-Engine erstellt und dient zum Schutz des Schlüssels der ersten Ebene.
3. Ein dritter AES-256-Schlüssel wird von erstellt und in FIPS 140-validierten Schlüsselverwaltungs-Appliances in den Rechenzentren ServiceNow gespeichert. Dieser Schlüssel schützt den Schlüssel der zweiten Ebene und ist für jede Kundeninstanz eindeutig.

Now Platform unterstützt auch die Datenbankverschlüsselung mit einem vom Kunden bereitgestellten Switch, DBE with CCS. Dies ist eine Verschlüsselungslösung, die alle Daten im Ruhezustand verschlüsselt, wenn sie in der Datenbank nicht verwendet werden. Es verwendet die AES-Verschlüsselung nach Industriestandard ohne Auswirkungen auf die Funktionalität. Die Datenbank verschlüsselt Daten, während sie auf den Datenträger geschrieben werden, und entschlüsselt Daten, während sie vom Datenträger gelesen werden. Das bedeutet, dass Anwendungen immer über die Daten in einem unverschlüsselten Zustand verfügen, um die erforderliche Logik und Funktionen ohne Auswirkungen auszuführen.

Hinweis: Datenbankverschlüsselung wird für lokale Instanzen nicht unterstützt.

Wenn Sie eigene Schlüssel für die Datenbankverschlüsselung verwenden, finden Sie weitere Informationen unter Datenbankverschlüsselung mit kundengesteuertem Switch.

Datenbankschlüsselrotation wird angefordert

Lassen Sie den Datenbankschlüssel jährlich oder nach Bedarf rotieren, indem Sie eine Anforderung an den Support senden.

Vorbereitungen

Erforderliche Rolle: admin

Wichtig: Ab Release Washington DC wird die Datenbankverschlüsselung auf ihre künftige Einstellung vorbereitet. Cloud Encryption ist die Ersatzlösung für die Verschlüsselung von Daten im Ruhezustand. Einzelheiten finden Sie unter Cloud-Verschlüsselung mit Schlüsselverwaltung

Warum und wann dieser Vorgang ausgeführt wird

Die Schlüsselrotation erfolgt in der Nacht innerhalb von 24 Stunden vor dem Ablaufdatum und unterbricht den Service für die Instanz nicht.

Hinweis: Derzeit ist die Schlüsselrotation nur in ServiceNow Kommerziellen, Behörden- und Community-Cloud-Umgebungen (GCC), Frankreich und Singapur verfügbar.

Prozedur

Wenden Sie sich an Kundenservice und Support, um eine der folgenden Schlüsselrotationsaktionen anzufordern:

- Registrieren Sie sich, um die jährliche Schlüsselrotation auf allen festgelegten Instanzen durchzuführen.
- Rufen Sie einen Verlaufsbericht der letzten drei Schlüsselrotationen ab, der Folgendes enthält:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Name der Instanz.
- Schlüsselname und -version.
- Datum und Uhrzeit der Rotation.

- Planen Sie eine frühe Schlüsselrotation außerhalb der geplanten Jahresrotation.

Datenbankverschlüsselung mit kundengesteuertem Switch

Database Encryption with Customer-Controlled Switch (DBE-CCS) ist eine Verschlüsselungslösung, die alle Daten im Ruhezustand verschlüsselt, wenn sie nicht in der Datenbank verwendet werden.

Übersicht

Bei der Datenbankverschlüsselung mit vom Kunden gesteuertem Switch wird die branchenübliche AES-Verschlüsselung verwendet, ohne dass die Funktionalität beeinträchtigt wird. Die Datenbank verschlüsselt Daten, während sie auf den Datenträger geschrieben werden, und entschlüsselt sie, während sie vom Datenträger gelesen wird. Anwendungen verfügen immer über die Daten in einem unverschlüsselten Status, um die erforderliche Logik und Funktionen auszuführen.

DBE-CCS nutzt native Datenbanktechnologie, häufig als Tablespace-Verschlüsselung oder transparente Datenverschlüsselung bezeichnet. Weitere Informationen zur Technologie finden Sie auf der MariaDB-Website unter „Tablespace Encryption“.

DBE-CCS erfordert die Einrichtung eines HTTPS-REST-Serviceendpunkts, der regelmäßig den geheimen Schlüssel für die Instanz ServiceNow bereitstellt. Der CCS-Endpunkt gibt dann den geheimen Kundenschlüssel zurück, der mit dem öffentlichen Schlüssel der Datenbankinstanz verschlüsselt ist.

Kundenendpunkt

Wichtig: Ihre Organisation ist allein für die Einrichtung und Wartung Ihres CCS-Endpunkts verantwortlich. Die Kundenendpunktspezifikation wird in KB0789788 bereitgestellt.

Der Technologiepartner von ServiceNow Fortanix ist verfügbar, um Ihren Kundenendpunkt für Sie zu implementieren. Wenden Sie sich direkt an den Technologiepartner, um Details zur Integration zu erfahren. Einzelheiten hierzu finden Sie unter Fortanix Data Security Manager mit ServiceNow verwenden .

Unterstützung mehrerer ServiceNow -Versionen

Wichtig: Datenbankverschlüsselung ist ein kostenpflichtiges Infrastrukturangebot, das unabhängig von der Version ist. Die Anwendung kann auf jedes unterstützte Release sowie auf neue oder vorhandene Instanzen angewendet werden.

Andere Referenzen

Weitere Informationen zu DBE mit CCS finden Sie in den folgenden Referenzen:

Referenz	Beschreibung
KB0993681	Architektur des vom Kunden gesteuerten Switches für die Datenbankverschlüsselung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Referenz	Beschreibung
KB0789788	Implementierungsleitfaden für DBE mit CCS

Hinweis: Um auf KB-Artikel zuzugreifen, müssen Sie sich zuerst bei Now Supportauthentifizieren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugriffsverwaltung

Die Zugriffsverwaltung ermöglicht Ihnen einen sicheren Zugriff auf die Instanz ServiceNow®.

Zero Trust-Zugriff



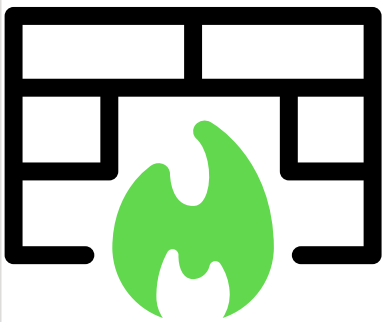
Zero Trust Access stellt sicher, dass jeglicher Zugriff auf Anwendungen und Daten erst nach Verifizierung der Identität und Risikobewertung des Anwenders auf Basis der geringsten Berechtigungen gewährt wird.

Domain Separation



Mit der Now Platform können Service Provider (SPs) ihren Kunden ein schnelleres Onboarding ermöglichen, Compliance-Vorgaben erfüllen und ihre Daten durch Domain Separation schützen.

Authentifizierung

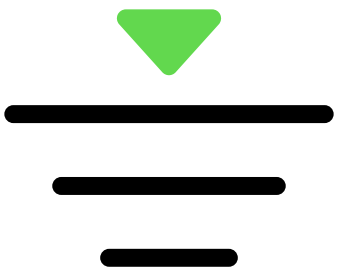


Die Authentifizierung von ServiceNow validiert die Identität eines Benutzers, der auf eine Instanz zugreift, und autorisiert den Benutzer dann für Funktionen, die der Rolle oder Jobfunktion des Benutzers entsprechen.

ACL



Datenfilterung



Verwenden Sie die Datenfilterung, um bei Leseabfragen den Zugriff auf Tabellen und Datensätze basierend auf Themenattributen zu steuern.

Sicherheitsrollen



Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regeln für Zugriffssteuerungslisten (ACLs) schränken den Zugriff auf Daten ein, indem sie von Anwendern die Erfüllung einer Reihe von Anforderungen verlangen, bevor sie mit der Interaktion beginnen können.

Sicherheitsrollen bieten zusätzliche Sicherheit. Jeder Anwender muss über mindestens eine Rolle verfügen, damit die Instanz zwischen internen und externen Anwendern unterscheiden kann.

Verbindung und Anmeldeinformationen



Anmelde- und Verbindungsinformationen sind erforderlich, um auf einen Computer oder ein Netzwerkgerät für Discovery, Service-Mapping und Cloud-Management zuzugreifen oder um mit Orchestration zu arbeiten.

Zugriffssteuerung von ServiceNow



Mit dem Plugin „SNC Access Control“ können Sie steuern, welche Kundenservice- und Supportmitarbeiter wann auf Ihre Instanz zugreifen können.

Zero Trust-Zugriff

Zero Trust Access (ZTA) ist ein Sicherheitsmodell, bei dem davon ausgegangen wird, dass standardmäßig keinem Benutzer oder Gerät vertraut wird.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Untersuchen



Lernen Sie die Funktionen und den Geschäftsnutzen von Zero Trust Access kennen.

Aktivieren



Erfahren Sie, wie Sie Zero Trust-Zugriffe aktivieren.

Konfigurieren



Konfigurieren Sie den Zero Trust-Zugriff.

Referenz: Eigenschaften



Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zero Trust-Zugriff erkunden

Zero Trust Access (ZTA) ist ein Sicherheitsmodell, bei dem davon ausgegangen wird, dass standardmäßig keinem Benutzer oder Gerät vertraut wird.

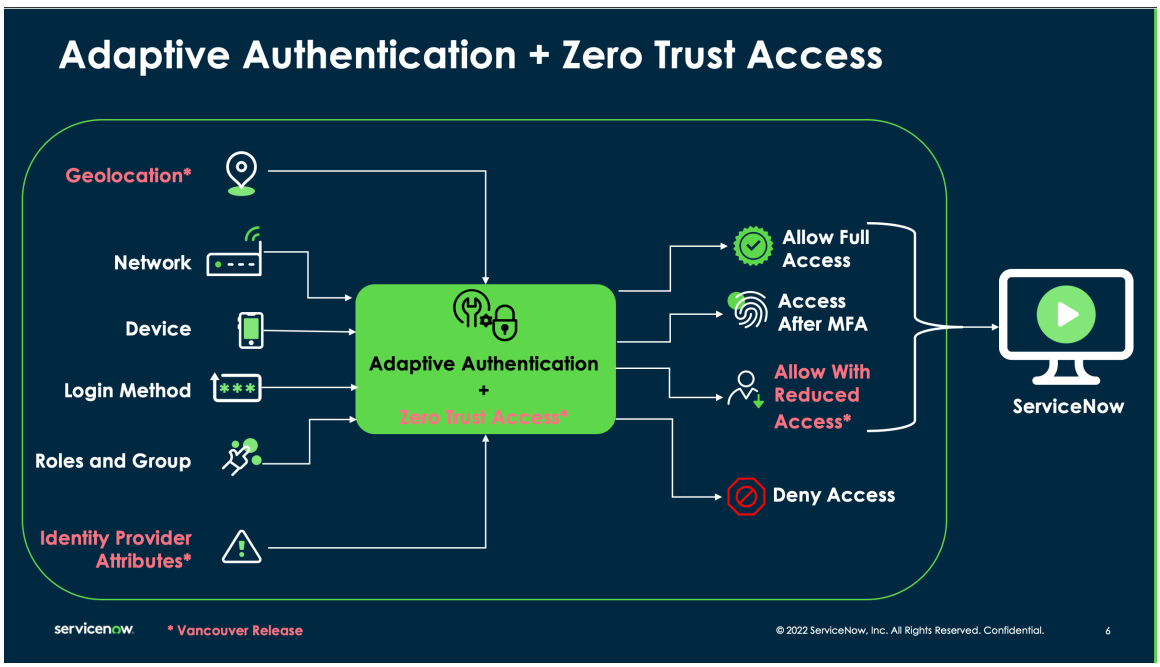
ZTA stellt sicher, dass jeglicher Zugriff auf Anwendungen und Daten erst nach Überprüfung der Identität des Benutzers und Risikobewertung auf Basis der geringsten Berechtigungen gewährt wird.

Zero Trust: Richtlinienbasierter Sitzungszugriff

ServiceNow Mit Zero Trust – Richtlinienbasierter Sitzungszugriff (Sitzungszugriff) können Organisationen die Anwenderberechtigung in einer Websitzung basierend auf einer Vielzahl von Faktoren dynamisch reduzieren, einschließlich IP-Adresse, Standort, Authentifizierungsmethode, Rolle des Anwenders, Gruppe, Anwender mit MFA und von geteilten Attributen Identitätsanbieter (IDP). Dies kann dazu beitragen, Organisationen vor nicht autorisiertem Zugriff und Datenschutzverletzungen zu schützen, selbst wenn Benutzer mit hohen Berechtigungen von nicht vertrauenswürdigen Geräten oder Standorten auf Anwendungen zugreifen.

Zero Trust: Richtlinienbasierter Sitzungszugriff

Sie ermöglicht es Sicherheitsadministratoren, den Benutzerzugriff in einer Sitzung basierend auf IP-Adresse, Standort, Identitätsanbieterattributen und Benutzerattributen mithilfe von Richtlinien für adaptive Authentifizierung zu reduzieren oder zu beschränken.



© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Konfigurationen des Sitzungszugriffs können nur mit der Rolle „ `security_admin` “ durchgeführt werden. Sie müssen Ihre Rolle auf `security_admin`erhöhen.
- Der Sitzungszugriff unterstützt keine Integrationen.
- Der Sitzungszugriff hat keine Auswirkungen, wenn die reduzierte oder eingeschränkte Rolle keinem Anwender zugewiesen ist. In diesem Fall gibt es keine Änderungen an der angemeldeten Sitzung. Der Benutzer greift weiterhin mit den zugewiesenen Rechten auf die Instanz zu.
- Der Sitzungszugriff hat keine Auswirkungen, wenn der Benutzer bereits bei der Instanz angemeldet ist und gleichzeitig der Administrator die Richtlinie konfiguriert. Der Benutzer muss sich von der Sitzung abmelden, damit die Richtlinie wirksam wird.
- Der Sitzungszugriff hat keine Auswirkungen, wenn sich der Benutzer in einem vertrauenswürdigen Netzwerk befindet und später innerhalb einer Sitzung zu einem VPN wechselt (Orts- oder Netzwerkänderung).
- Der Sitzungszugriff wird zum Zeitpunkt der Anmeldung erzwungen. Jede Änderung der Risikoparameter während der Sitzung führt nicht zu einem reduzierten Zugriff. Wenn beispielsweise ein Benutzer nach dem Herstellen der Sitzung vom Unternehmensnetzwerk zu einem nicht vertrauenswürdigen Netzwerk wechselt, wird der Zugriff nur eingeschränkt, wenn er sich abmeldet und erneut anmeldet.

Anwendungsfall

Im Folgenden finden Sie einige Anwendungsfälle für Zero Trust Access:

- Reduzieren Sie Berechtigungen basierend auf dem mit der Sitzung verbundenen Risiko. Beispielsweise kann ein Benutzer mit einer Erfüllerrolle, der sich von außerhalb des vertrauenswürdigen Netzwerks anmeldet, so konfiguriert werden, dass er nur die Rolle des Anforderers für die Sitzung hat.
- Reduzieren Sie den Zugriff basierend auf der IdP-Antwort für eine Benutzersitzung, wenn der Benutzer ein nicht vertrauenswürdiges Gerät verwendet. Weitere Informationen finden Sie unter Konfigurieren Sie das IDP-Attribut für den Sitzungszugriff.

Diese Rollenzuweisung stellt sicher, dass der Benutzer über keine anderen Berechtigungen in einer Sitzung verfügt. Wenn sich der Benutzer aus einem vertrauenswürdigen Netzwerk anmeldet, werden alle vorhandenen Berechtigungen für eine Sitzung zugewiesen.

Als Teil der Richtlinie können mehrere IP-Bedingungen und mehrere Rollen- oder Gruppenzuweisungen definiert werden.

Zero Trust-Zugriff – Mobile

Sie können die Richtlinie „Zero Trust-Zugriff – Sitzungszugriff“ innerhalb der Richtlinie „Adaptive Authentifizierung“ verwenden, um die Rollen oder Berechtigungen der jeweiligen Sitzung in Mobile zu reduzieren.

Zero Trust-Zugriff – Sitzungszugriff für Mobilgeräte kann aktiviert werden, indem **glide.authenticate.session_access.mobile.enabled** in der Systemeigenschaftentabelle aktiviert wird.

Um Zero Trust-Zugriff – Sitzungszugriff für Mobilgeräte mit den IDP-Attributen zu verwenden, können Sie das Feld **„glide.authenticate.session_access.mobile.refresh_token_interval** “ konfigurieren. Dies ermöglicht es Administratoren, den Sitzungszugriff basierend auf dem Aktualisierungstoken effektiv zu steuern.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen finden Sie unter Konfigurieren Sie den Zero Trust-Zugriff für Mobilgeräte .

Zero Trust-Zugriff wird aktiviert

Aktivieren Sie die **Richtlinie „Zero Trust – Richtlinienbasierter Sitzungszugriff** `com.snc.zero_trust_session_access` “, damit Sicherheitsadministratoren den Benutzerzugriff in einer Sitzung basierend auf IP-Adresse, Standort, Attributen des Identitätsanbieters und Benutzerattributen mithilfe von Richtlinien für adaptive Authentifizierung reduzieren oder einschränken können.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie das Plugin **„Zero Trust – Richtlinienbasierter Sitzungszugriff“** (`com.snc.zero_trust_session_access`) mithilfe der Filterkriterien und der Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: `Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.`

   Nach Abschluss der Installation wird eine Meldung angezeigt.

Konfigurieren der Rolle für den Sitzungszugriff

Konfigurieren Sie den Sitzungszugriff, um den Benutzerzugriff in einer Sitzung basierend auf IP, Standort, Identitätsanbieterattributen und Benutzerattributen mithilfe von Richtlinien für adaptive Authentifizierung zu reduzieren.

Vorbereitungen

Erforderliche Rolle: security_admin

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Konfigurationen des Sitzungszugriffs können nur mit der Rolle „ `security_admin` “ durchgeführt werden. Sie müssen Ihre Rolle auf `security_admin`erhöhen.
- Der Sitzungszugriff unterstützt keine Integrationen.
- Der Sitzungszugriff hat keine Auswirkungen, wenn die reduzierte oder eingeschränkte Rolle keinem Anwender zugewiesen ist. In diesem Fall gibt es keine Änderungen an der angemeldeten Sitzung. Der Anwender greift weiterhin mit den ihm zugewiesenen Berechtigungen auf die Instanz zu.
- Der Sitzungszugriff hat keine Auswirkungen, wenn der Benutzer bereits bei der Instanz angemeldet ist und gleichzeitig der Administrator die Richtlinie konfiguriert. Der Benutzer muss sich von der Sitzung abmelden, damit die Richtlinie wirksam wird.
- Der Sitzungszugriff wird zum Zeitpunkt der Anmeldung erzwungen. Jede Änderung der Risikoparameter während der Sitzung führt nicht zu einem reduzierten Zugriff. Wenn beispielsweise ein Benutzer nach dem Herstellen der Sitzung vom Unternehmensnetzwerk zu einem nicht vertrauenswürdigen Netzwerk wechselt, wird der Zugriff nur eingeschränkt, wenn er sich abmeldet und erneut anmeldet.

Prozedur

1. Navigieren zu **Alle** > **Zero Trust-Zugriff** > **Konfigurationen der Sitzungszugriffsrolle**an.
2. Um eine Konfiguration für eine Sitzungszugriffsrolle zu erstellen, wählen Sie **Neu**aus.
3. Füllen Sie im Formular die folgenden Felder aus:

Konfiguration der Sitzungszugriffsrolle

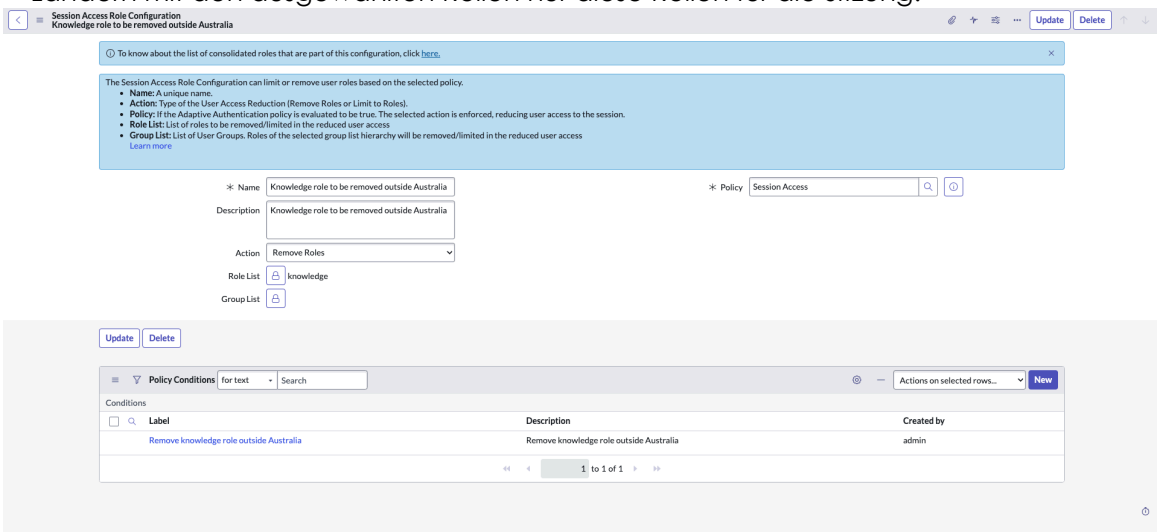
Feld	Beschreibung
Name	Name der Konfiguration
Beschreibung	Kurze Beschreibung der Konfiguration.
Richtlinie	Wählen Sie die Richtlinie für adaptive Authentifizierung. Verwenden Sie das Suchsymbol, um die Liste der Richtlinien anzuzeigen.
Aktion	**Rollen entfernen** oder **Auf Rollen beschränken**. ◦ **Rollen entfernen**: Wenn sich der konfigurierte Anwender anmeldet, wird die Liste der in der Rollen- oder Gruppenliste angegebenen Rollen für die Sitzung entfernt. ◦ **Auf Rollen beschränken**: Wenn sich der konfigurierte Anwender anmeldet, werden ihm nur die ausgewählten Rollen bereitgestellt und alle anderen Rollen werden für die Sitzung entfernt.
Rollenliste	Wählen Sie Rollen aus der Rollenliste aus.
Gruppenliste	Wählen Sie in der Gruppenliste die Rollen aus, die Sie entfernen oder auf den Anwender beschränken möchten.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Auswählen, **Absenden**.

Die Anmeldung für Benutzer erfolgt basierend auf den konfigurierten Ländern wie folgt:

- In **„Rollen entfernen“**haben die Benutzer aus den konfigurierten Ländern mit den ausgewählten Rollen diese Rollen für die Sitzung nicht mehr.
- In **Limit To Roles**(Auf Rollen beschränken) haben die Benutzer aus den konfigurierten Ländern mit den ausgewählten Rollen nur diese Rollen für die Sitzung.

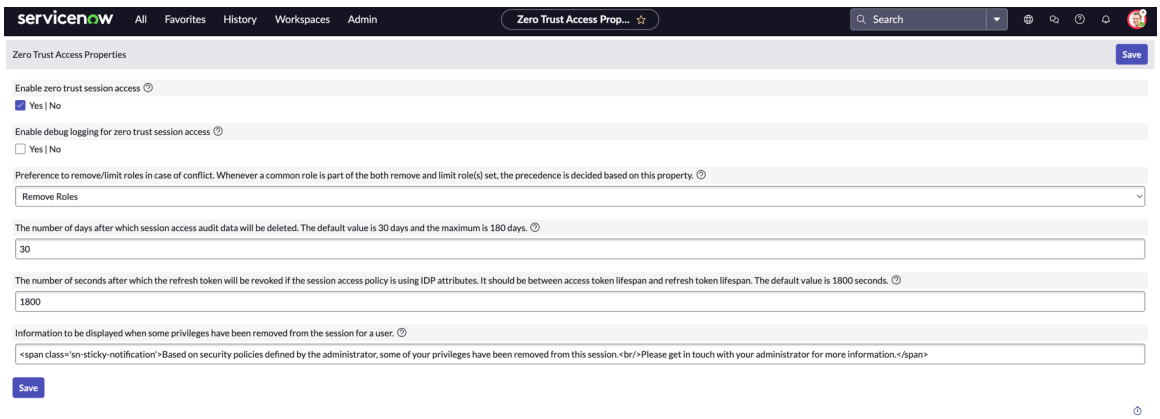


Weitere Informationen zum Entfernen oder Einschränken von Rollen für eine Sitzung, die anhand eines Beispielanwendungsfalls erläutert wird, finden Sie unter Lernprogramm: Verwenden Sie Zero Trust-Zugriff.

Systemeigenschaften für Zero Trust-Zugriff

Verwenden Sie die Systemeigenschaften, um den Zero Trust-Zugriff zu aktivieren und an Ihre Sicherheitsanforderungen anzupassen.

Eigenschaften



© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Systemeigenschaften für Zero Trust-Zugriff

Eigenschaft	Beschreibung
Aktiviert Zero Trust-Sitzungszugriff	Option, mit der Administratoren die Funktion „Zero Trust-Sitzungszugriff“ verwenden können. Standardmäßig lautet der Wert `false`.
Aktivieren Sie die Debug-Protokollierung für Zero Trust-Sitzungszugriff	Option zum Aktivieren der Debug-Protokollierung für Zero Trust-Sitzungszugriff.
Einstellung zum Entfernen/Einschränken von Rollen im Konfliktfall. Immer wenn eine allgemeine Rolle Teil des Satzes „Rolle(n) entfernen“ und „Rolle(n) beschränken“ ist, wird die Rangfolge basierend auf dieser Eigenschaft festgelegt.	**Rollen entfernen** oder **Rollen einschränken**
Die Anzahl der Tage, nach der Audit-Daten zum Sitzungszugriff gelöscht werden. Der Standardwert beträgt 30 Tage, der Höchstwert 180 Tage.	Standardmäßig sind es 30 Tage.
Die Anzahl der Sekunden, nach der das Aktualisierungstoken widerrufen wird, wenn die Sitzungszugriffsrichtlinie IDP-Attribute verwendet. Sie sollte zwischen der Lebensdauer des Zugriffstokens und der Lebensdauer des Aktualisierungstokens liegen. Der Standardwert beträgt 1800 Sekunden.	Standardmäßig sind es 1800 Sekunden.
Informationen, die angezeigt werden sollen, wenn für einen Anwender einige Berechtigungen aus der Sitzung entfernt wurden.	Beschreibung, die Sie Ihren Anwendern bezüglich der Einschränkung oder des Entzugs von Berechtigungen anzeigen möchten. Beispielbeschreibung: `Basierend auf den vom Administrator definierten Sicherheitsrichtlinien wurden einige Ihrer Rollen aus dieser Sitzung entfernt. Wenden Sie sich an Ihren Administrator, um weitere Informationen zu erhalten.`

Audits des Sitzungszugriffs

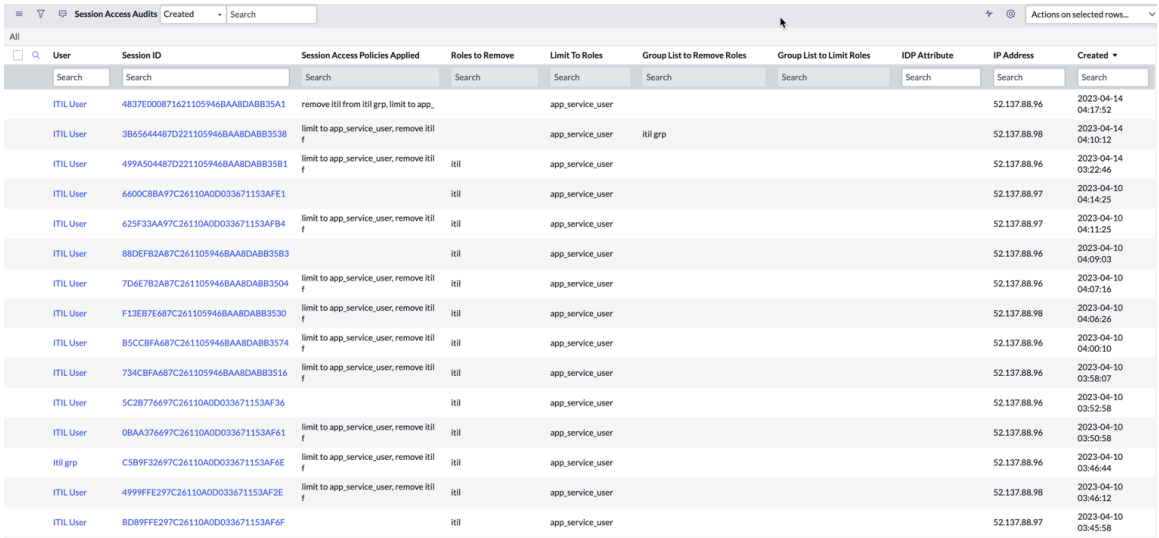
Audits des Sitzungszugriffs zeigen die Sitzungszugriffsprotokolle und Informationen zur Sitzung eines Benutzers an.

Audits

Das Audit des Sitzungszugriffs zeigt Audit-Informationen wie folgt an:

Hinweis: Verwenden Sie die Eigenschaft „`glide.authenticate.session_access.log_audit_event`“, um die Audit-Informationen auszufüllen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Audits des Sitzungszugriffs

Feld	Beschreibung
Anwender	Details des Anwenders.
Sitzungs-ID	Details zur Sitzung, die als eindeutige ID angezeigt werden.
Mobile-Client	Die Mobile-Client-Details. **ServiceNow Agent** (Now Agent) und **ServiceNow Request** (Now Mobile).
Sitzungszugriffsrichtlinien angewendet	Die angewendete Richtlinie für den Sitzungszugriff.
Zu entfernende Rollen	Rollen, die dem Anwender während der Protokollierung entzogen wurden.
Auf Rollen beschränken	Rollen, die bei der Protokollierung auf den Anwender beschränkt waren.
Gruppenliste zur Entfernung von Rollen	Informationen zur Gruppe, die Rollen für den Anwender entfernt hat.
Gruppenliste zur Beschränkung von Rollen	Informationen zur Gruppe, die über eingeschränkte Rollen für den Anwender verfügt.
Mobile-Client	Details des über das Mobilgerät angemeldeten Anwenders mit reduziertem oder entferntem Zugriff.
IDP-Attribut	Der für diese Sitzung verwendete IdP.
IP-Adresse	Details der IP-Adresse, die der Anwender für die Anmeldung verwendet hat.
Erstellt	Details zu Datum und Uhrzeit der Erstellung des Anwenderdatensatzes.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Lernprogramm: Verwenden Sie Zero Trust-Zugriff

Verfahren zur Verwendung der Zero Trust Access-Funktion mit einem End-to-End-Anwendungsfall.

Vorbereitungen

Erforderliche Rolle: security_admin

Aktivieren Sie die **Eigenschaft „Sitzungszugriff aktivieren“**.

Hinweis:

- Konfigurationen des Sitzungszugriffs können nur mit der Rolle „ `security_admin` “ durchgeführt werden. Sie müssen Ihre Rolle auf `security_admin`erhöhen.
- Der Sitzungszugriff unterstützt keine Integrationen.
- Der Sitzungszugriff hat keine Auswirkungen, wenn die reduzierte oder eingeschränkte Rolle keinem Anwender zugewiesen ist. In diesem Fall gibt es keine Änderungen an der angemeldeten Sitzung. Der Anwender greift weiterhin mit den ihm zugewiesenen Berechtigungen auf die Instanz zu.
- Der Sitzungszugriff hat keine Auswirkungen, wenn der Benutzer bereits bei der Instanz angemeldet ist und gleichzeitig der Administrator die Richtlinie konfiguriert. Der Benutzer muss sich von der Sitzung abmelden, damit die Richtlinie wirksam wird.
- Der Sitzungszugriff wird zum Zeitpunkt der Anmeldung erzwungen. Jede Änderung der Risikoparameter während der Sitzung führt nicht zu einem reduzierten Zugriff. Wenn beispielsweise ein Benutzer nach dem Herstellen der Sitzung vom Unternehmensnetzwerk zu einem nicht vertrauenswürdigen Netzwerk wechselt, wird der Zugriff nur eingeschränkt, wenn er sich abmeldet und erneut anmeldet.

Der Sitzungszugriff ist eine Funktion, mit der Administratoren einen Satz von Rollen für den Anwender dynamisch reduzieren oder einschränken können, wenn der Anwender versucht, sich aus verschiedenen Umgebungen bei der Instanz anzumelden, z. B. über das nicht vertrauenswürdige Netzwerk oder von einem anderen Gerät usw.

Der Sitzungszugriff kann durch die erstellte Richtlinie und die ausgewählte Aktion bei der Konfiguration gesteuert werden. Einige der Szenarien sind wie folgt:

- Wenn die Richtlinie auf true festgelegt ist und die Aktion für Rollen auf **Rollen entfernen**festgelegt ist, werden die ausgewählten Rollen und die zugehörigen untergeordneten Rollen für den Benutzer entfernt, wenn er versucht, sich bei der Instanz anzumelden.
- Wenn die Richtlinie auf true festgelegt ist und die Aktion für Rollen auf **Auf Rollen beschränken**festgelegt ist, werden dem Benutzer nur die ausgewählten Rollen und die zugehörigen untergeordneten Rollen zugewiesen, wenn er versucht, sich bei der Instanz anzumelden.

Im folgenden Verfahren wird eine End-to-End-Konfiguration für den Sitzungszugriff erläutert, auf deren Grundlage die Rolle auf den Benutzer beschränkt wird, der sich bei der Instanz anmeldet. Auf ähnliche Weise können Sie auch Rollen entfernen, indem Sie während der Konfiguration die Option **Rollen** entfernen auswählen.

Prozedur

1. Navigieren zu **Alle** > **Sitzungszugriff** > **Konfigurationen der Sitzungszugriffsrolle**an.
2. Wählen Sie auf der Seite Konfigurationen der Sitzungszugriffsrolle **Neu**.
3. Um eine Rolle für den Anwender einzuschränken, füllen Sie im Formular die Felder aus:

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Name
- Beschreibung
- Richtlinie
- Aktion
- Rollenliste
- Gruppenliste

a. Wählen Sie **Auf Rollen** beschränken, um die Rollen für den Benutzer zu beschränken. Beispiel: **itil**.

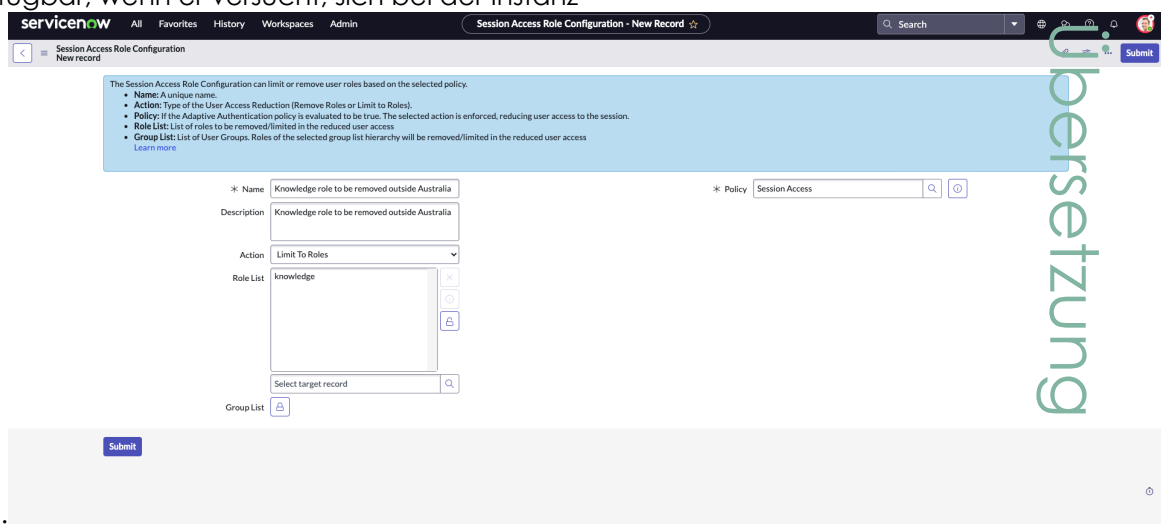
b. Wählen Sie eine **Wissensrolle** aus der Rollenliste aus.

c. Wählen Sie die **Richtlinie**aus.

Sie können die Richtlinie für den Sitzungszugriff mithilfe von Authentifizierungsrichtlinien und Filterkriterien (Rolle, Gruppe, IP, Standort) mit Richtlinieneingaben und -bedingungen erstellen.

Verwenden Sie die Richtlinie in der Konfiguration des Sitzungszugriffs. Beispielsweise möchten Sie die Rolle (Wissen) auf den Benutzer beschränken, der sich außerhalb des Standorts (Australien) anmeldet.

d. Wählen Sie Aktion als **Auf Rollen begrenzen**.
Wenn die Richtlinie auf „true“ festgelegt ist, sind nur die ausgewählten Rollen und die zugehörigen untergeordneten Rollen für den Benutzer verfügbar, wenn er versucht, sich bei der Instanz



anzumelden.

e. Wählen Sie **Absenden**.

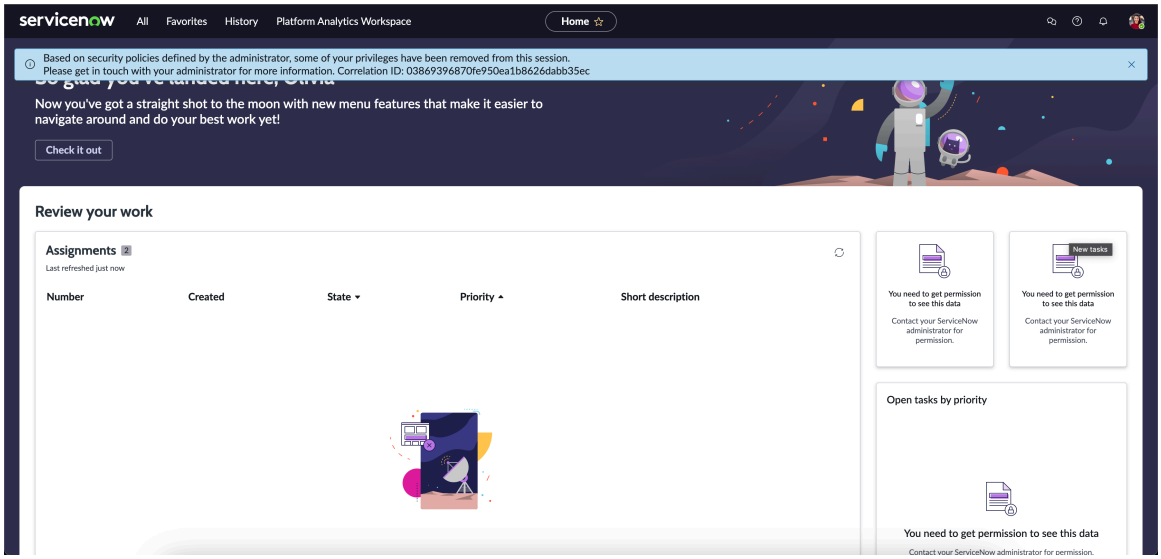
Ebenso können Sie die Gruppe aus der Gruppenliste auswählen, um Rollen für die Benutzer innerhalb der Gruppe einzuschränken oder zu entfernen.

Wenn sich der Anwender bei der Instanz außerhalb Australiens anmeldet, werden nur die Rolle **„Knowledge** “ und die zugehörigen untergeordneten Rollen für die protokollierte Sitzung zugewiesen, und andere Rollen sind für den Anwender eingeschränkt.

Nach der Anmeldung wird dem Benutzer im Profilabschnitt der Plattform die folgende Fehlermeldung angezeigt:

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Der Benutzer kann sich an die Administratoren wenden und die Korrelations-ID für Untersuchungen angeben.

Hinweis: Die Korrelations-ID ist die sys_id des entsprechenden Audit-Datensatzes in der Audit-Tabelle für den Sitzungszugriff.

Konfigurieren Sie das IDP-Attribut für den Sitzungszugriff

Verwenden Sie das Attribut Identity Provider (IDP), das aus der Antwort der Security Assertion Markup Language (SAML) erstellt wurde, um den Zugriff von Anwendersitzungen auf die Instanz zu entfernen oder einzuschränken.

Vorbereitungen

Erforderliche Rolle: security_admin

Aktivieren Sie die **Eigenschaft „Sitzungszugriff aktivieren“**.

Hinweis: Um die Rollenkonfiguration für den Sitzungszugriff zu verwenden, müssen Sie Ihre Rolle auf `security_admin`erhöhen.

Der Sitzungszugriff kann durch die erstellte Richtlinie und die ausgewählte Aktion bei der Konfiguration gesteuert werden. Einige der Szenarien sind wie folgt:

- Wenn die Richtlinie auf „true“ festgelegt ist und die Aktion „ **Rollen“ zusammen mit der IDP-Attributeingabe und -bedingung auf „Rollen entfernen** “ festgelegt ist, werden die ausgewählten Rollen und die zugehörigen untergeordneten Rollen für den Anwender entfernt, wenn er versucht, sich bei der Instanz anzumelden.
- Wenn die Richtlinie auf „true“ festgelegt ist und die Aktion für **Rollen** zusammen mit der IDP-Attributeingabe und -bedingung auf Auf Rollen beschränken festgelegt ist, werden dem Anwender nur die ausgewählten Rollen und die zugehörigen untergeordneten Rollen zugewiesen, wenn er versucht, sich bei der Instanz anzumelden.

Das folgende Verfahren zeigt Schritte zum Konfigurieren des IDP-Attributs aus der SAML-Antwort einer Richtlinieneingabe zur Steuerung des Sitzungszugriffs.

Prozedur

1. Navigieren zu **Alle** > **Sitzungszugriff** > **Konfigurationen der Sitzungszugriffsrolle**an.
2. Wählen Sie auf der Seite Konfigurationen der Sitzungszugriffsrolle **Neu**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Um eine Rolle für den Anwender zu entfernen, füllen Sie im Formular die folgenden Felder aus:
   - Name
   - Beschreibung
   - Richtlinie
   - Aktion
   - Rollenliste
   - Gruppenliste

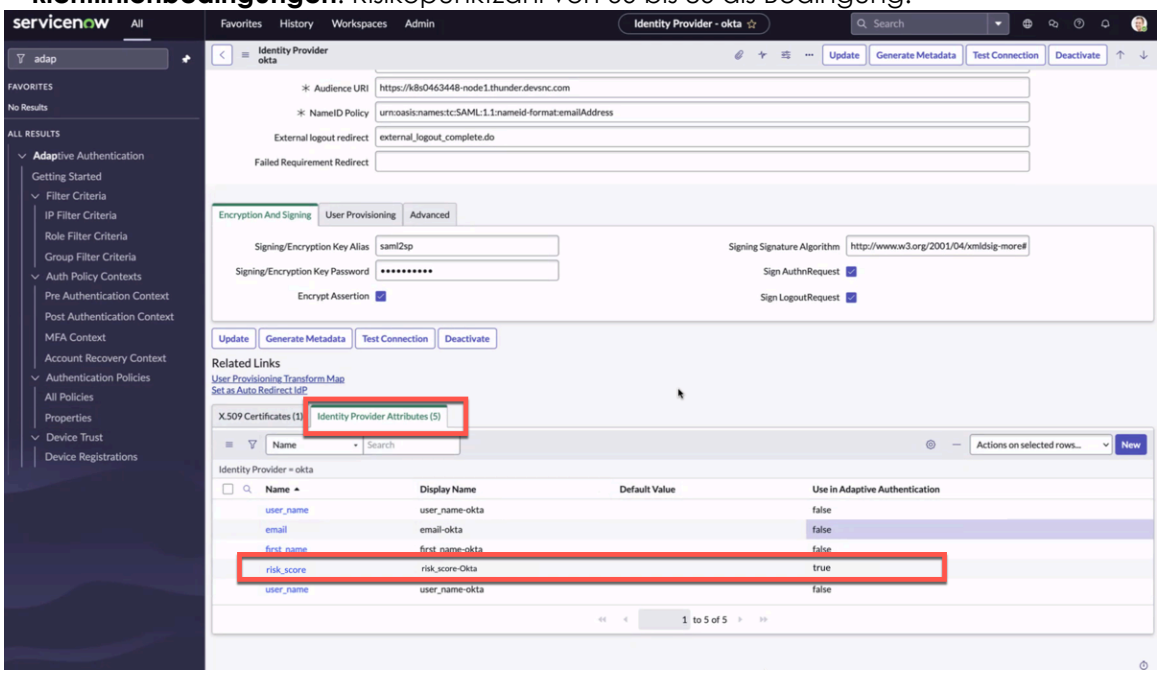
a. Wählen **Sie Rollen** entfernen aus, um Rollen für den Anwender zu entfernen.
Beispiel: **itil**.

b. Wählen Sie die Rolle **itil** aus der Rollenliste aus.

c. Wählen Sie die **Richtlinie**aus.
Weitere Informationen zum Erstellen von Richtlinien mit verschiedenen Filterkriterien bei der Richtlinienerstellung für die adaptive Authentifizierung finden Sie unter Filterkriterien.

d. Wählen Sie als Aktion Rollen entfernen aus.
Wenn die Richtlinie auf true festgelegt ist und die Aktion für Rollen auf **Rollen entfernen**festgelegt ist, werden die ausgewählten Rollen für den Benutzer entfernt, wenn er versucht, sich bei der Instanz anzumelden.

e. Erstellen Sie in der Richtlinieneingabe die Richtlinieneingabe und die Richtlinienbedingung.
Beispiel:
- **Richtlinieneingabe**: Risikopunktzahlattribut von Okta (IDP).
- **Richtlinienbedingungen**: Risikopunktzahl von 60 bis 80 als Bedingung.



Wenn der Attributwert der Risikopunktzahl von Okta (IDP) basierend auf dieser Konfiguration 80 übersteigt, wird der Benutzer nicht mit den Rollen (**Mitarbeiter**) und den

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

untergeordneten Rollen authentifiziert, die für die Instanz entfernt wurden, sondern nur mit anderen Rollen zugewiesen. Wenn die Risikopunktzahl zwischen 60 und 80 liegt, wird der Benutzer bei der Instanz mit allen Rollen authentifiziert.

Weitere Informationen zum Erstellen der Richtlinie des Nachauthentifizierungskontexts mit Richtlinieneingaben und Bedingung finden Sie unter Kontext nach der Authentifizierung.

Hinweis: Wenn die Eigenschaft **„Sitzungszugriff aktivieren“** inaktiv ist, schränkt die Konfiguration für den Sitzungszugriff die Rollen des Anwenders nicht ein oder entfernt sie.

f. Wählen Sie **Absenden**.

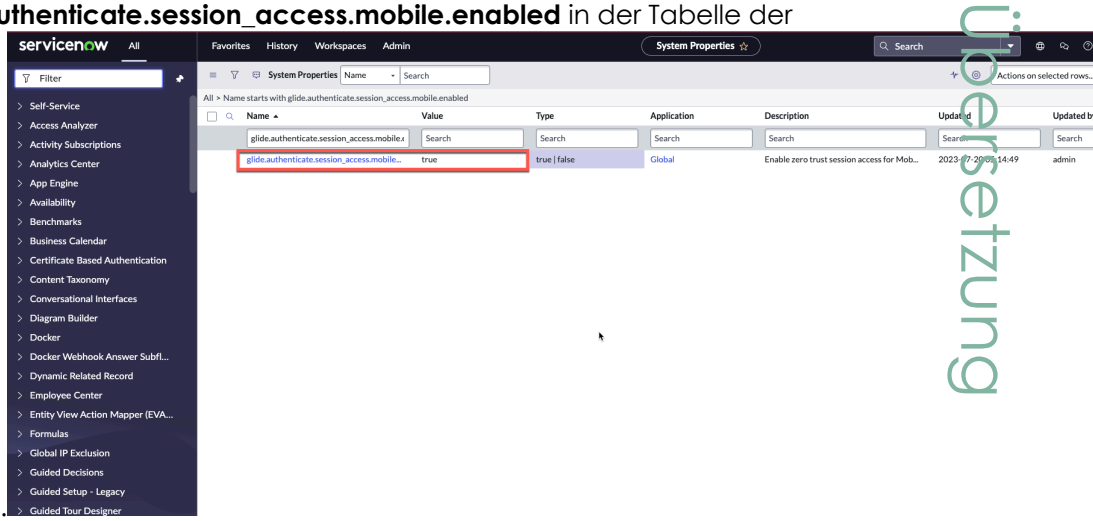
Zero Trust-Zugriff für Mobilgeräte

Zero Trust Access (ZTA) ist ein Sicherheitsmodell, bei dem davon ausgegangen wird, dass standardmäßig keinem Benutzer oder Gerät vertraut wird.

Sie können die Richtlinie Zero Trust-Zugriff – Sitzungszugriff innerhalb der Richtlinie „Adaptive Authentifizierung“ verwenden, um die Rollen oder Berechtigungen der jeweiligen Sitzung in Mobile für Anwender zu reduzieren.

Um Zero Trust-Zugriff für Mobilgeräte zu aktivieren, müssen Sie die folgenden Aufgaben ausführen:

- Konfigurationen des Sitzungszugriffs können nur mit der Rolle „ `security_admin` “ durchgeführt werden. Sie müssen Ihre Rolle auf `security_admin`erhöhen.
- Aktivieren Sie die **Richtlinie Zero Trust – Richtlinienbasierter Sitzungszugriff** `com.snc.zero_trust_session_access`.
- **Aktivieren Sie glide.authenticate.session_access.mobile.enabled** in der Tabelle der Systemeigenschaften.

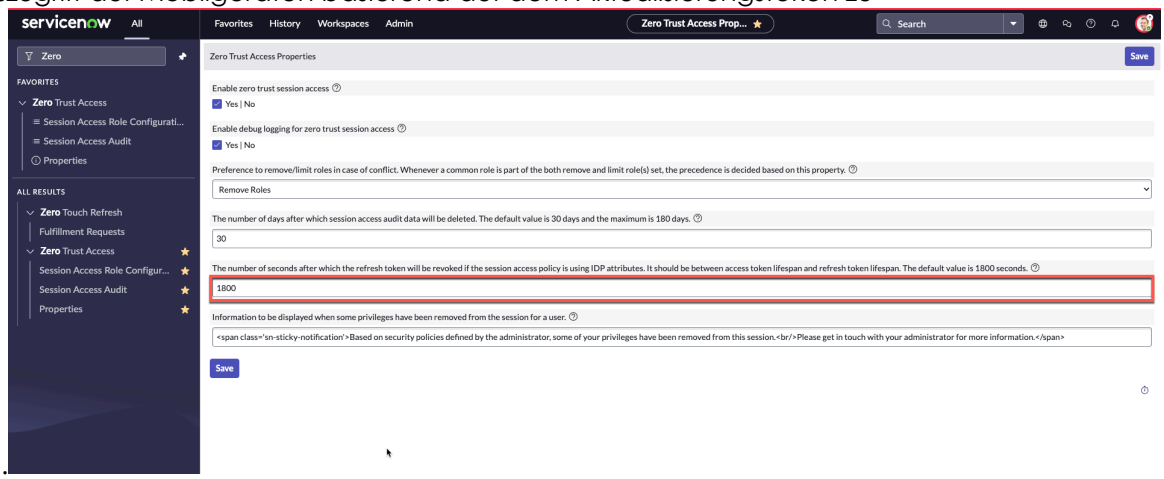


- Konfigurieren Sie das Feld **„glide.authenticate.session_access.mobile.refresh_token_interval“**, um den

Automatische Übersetzung

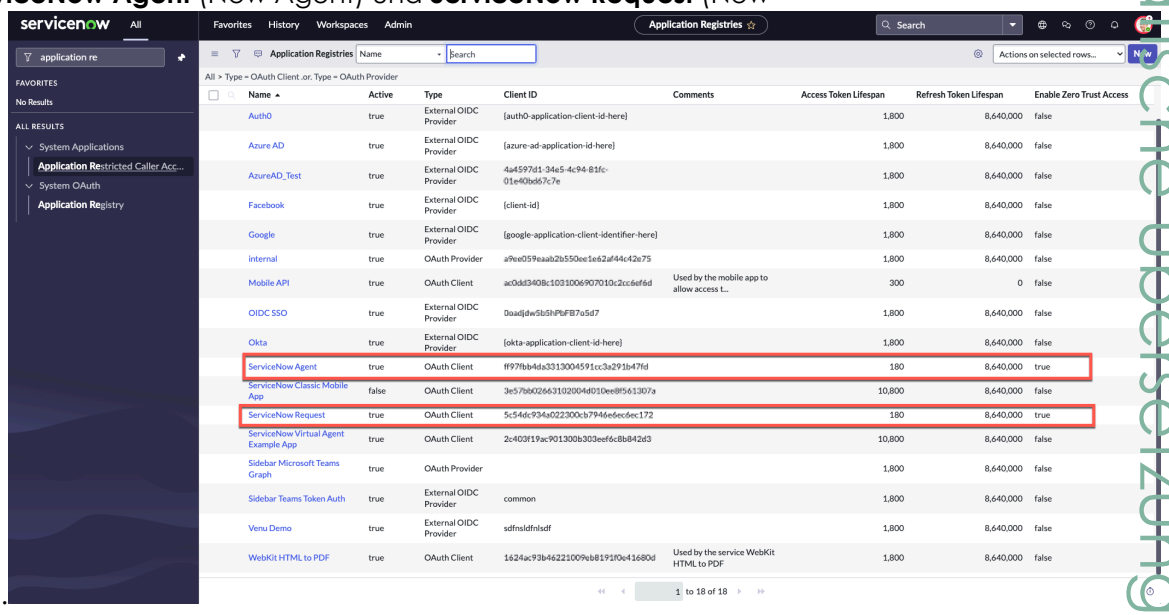
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sitzungszugriff auf Mobilgeräten basierend auf dem Aktualisierungstoken zu steuern.



Hinweis: Sie müssen die Aktualisierungstokensekunden konfigurieren, wenn Sie einen IdP für Anmeldungen bei der mobilen App verwenden. Standardmäßig werden Anwender nach 1800 Sekunden (30 Minuten) von den Mobile-Apps abgemeldet.

- „Zero Trust-Zugriff aktivieren“ ist unter „ **Anwendungsregistrierungen“** für die Mobile-Client-Anwendung (OAuth-Client) aktiviert. In diesem Fall **ServiceNow Agent** (Now Agent) und **ServiceNow Request** (Now Mobile).



- Konfigurieren Sie die Rolle „Sitzungszugriff“, um die Rollen für die Anwender, die sich anmelden, basierend auf den Richtlinieneingaben und -bedingungen entweder zu reduzieren oder zu entfernen. Weitere Informationen zur Konfiguration finden Sie unter Konfigurieren der Rolle für den Sitzungszugriff.

Die Konfiguration wertet die Anmeldung aus, um die Rollen der Benutzer, die auf Ihre Instanz ServiceNow® zugreifen, basierend auf den Richtlinienfiltern und -bedingungen zu reduzieren oder zu entfernen. Weitere Informationen finden Sie unter Konfigurieren Sie den Zero Trust-Zugriff für Mobilgeräte .

Domänentrennung für Service Provider

Mit der ServiceNow Platform können Service Provider (SPs) ihren Kunden ein schnelleres Onboarding bieten, die Compliance erfüllen und ihre Daten durch Domänentrennung

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

schützen. Sie können Client-Daten, Prozesse und Berichte in logische Gruppierungen unterteilen, die als Domänen bezeichnet werden. SPs steuern, wer welche Inhalte sieht und darauf zugreifen kann.

Untersuchen	Konfigurieren
	
Erfahren Sie mehr über Domain Separation.	Konfigurieren Sie Domain Separation.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Referenz



Ruft Details zu Domain Separation ab.

Analysieren



Erfahren Sie mehr über die Analyse von Domain Separation

Domain Separation erkunden

Mithilfe von Domain Separation können Sie Daten, Prozesse und administrative Aufgaben in logisch definierte Domänen aufteilen.

Die Domänentrennung ist am besten geeignet für Kunden, die:

- absolute Datentrennung zwischen Business-Entitäten (Datentrennung) benötigen.
- Geschäftsprozessdefinitionen und Benutzerschnittstellen für jede Domäne anpassen möchten (delegierte Verwaltung).
- einige globale Prozesse und globale Berichte in einer einzigen Instanz verwalten.
- Trennen Sie Daten nach Service Providern, Kunden, Partnern oder Unterorganisationen.
- geringfügige oder moderate Prozessunterschiede zwischen Kunden aufweisen.

Domänentrennung im Vergleich zu separaten Instanzen

Die Domänentrennung bietet zwar Unterstützung für mehrere Mandanten, die Mehrmandantenfähigkeit ist jedoch auch weiterhin in einer einzelnen Instanz enthalten. Einige globale Eigenschaften, Daten und Prozesse werden über alle Domänen hinweg gemeinsam genutzt. Zum Beispiel ist die Angabe von Benutzernamen speichern auf der *Anmeldeseite* des Systems global und kann nicht pro Domäne angegeben werden.

Wenn Sie eine vollständige Trennung aller Systemeigenschaften benötigen und weder globales Reporting noch globale Prozesse benötigen, sind separate Instanzen die beste Option.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datentrennung

Mitglieder einer Domäne sehen nur die Daten, die in ihrer Domäne oder in den untergeordneten Domänen enthalten sind, die sich in der Domänenhierarchie niedriger befinden. Standardmäßig sind alle Benutzer und alle Datensätze Mitglieder der globalen Domäne, es sei denn, ein Administrator weist sie einer bestimmten Domäne zu. Sobald Sie einer Domäne einen Benutzer oder einen Datensatz zugewiesen haben, vergleicht die Instanz die Domäne des Benutzers mit der Domäne des Datensatzes, um zu bestimmen, ob der Benutzer den Datensatz aufrufen kann.

ServiceNow-Anwendungen werden mit den folgenden inkrementellen Supportstufen definiert. Diese Ebenen basieren auf der Perspektive der tatsächlichen Anwendungsfälle und Personas.

Datentrennung: Mandanten sehen nur Daten, für die sie berechtigt sind. Mandanten können Zugriff auf andere Mandantendaten erhalten, können jedoch keine Mandantendaten abfragen, wenn sie keinen Zugriff haben.

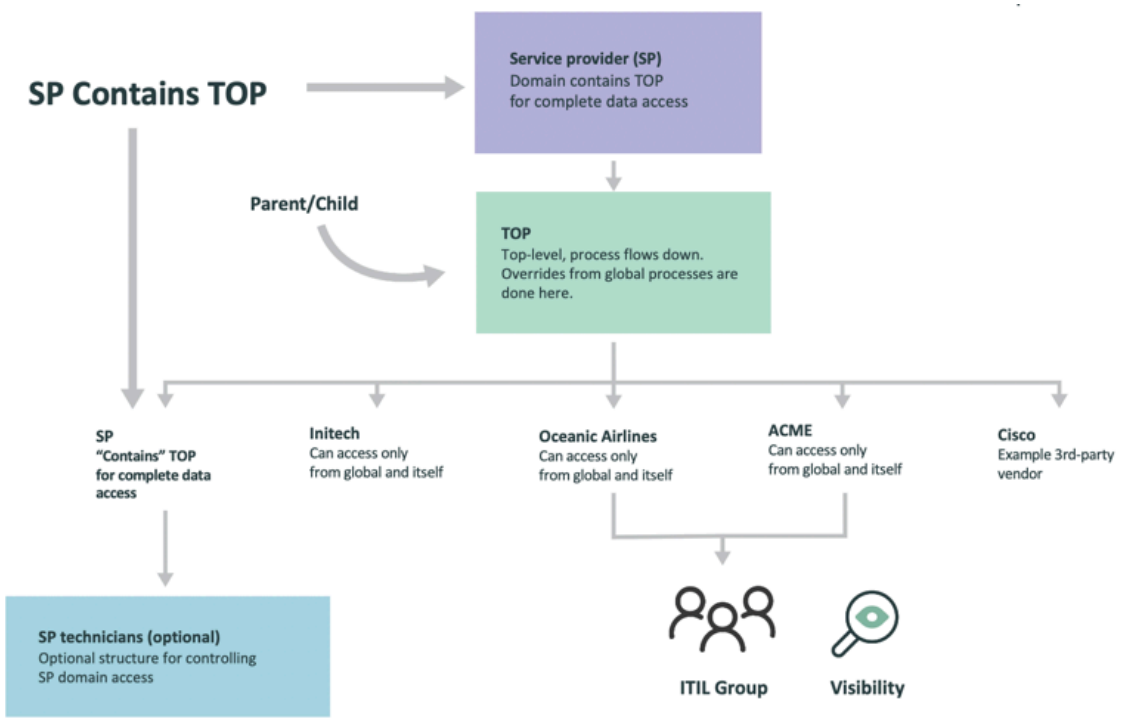
UI-Trennung: Unterstützt eine mandantenspezifische Experience für UI-Elemente wie Ansichten, Listen, Bezeichnungen usw.

Business Logic Separation: Sie können mandantenspezifische Systemrichtlinien wie E-Mail-Benachrichtigungen, Geschäftsregeln, Client-Skripts, UI-Richtlinien und UI-Aktionen erstellen.

Hierarchische Modellierung: Geschachtelte Mehrinstanzfähigkeit, sodass übergeordnete Mandanten auf untergeordnete Mandantenressourcen zugreifen können. Geschäftslogik für übergeordnete Mandanten wird für untergeordnete Mandanten automatisch ausgeführt und kann auf jeder Ebene überschrieben werden.

Mandantenübergreifende Intelligenz (Domänenbereich): Verarbeitet automatisch die Daten, Metadaten, die Geschäftslogik und den Verarbeitungskontext für Mandanten, die Zugriff auf zusätzliche Mandantendaten haben.

Im Allgemeinen sind Daten, die auf einer höheren Ebene in der Domänenhierarchie definiert sind, auf niedrigeren Ebenen in der Hierarchie nicht sichtbar.



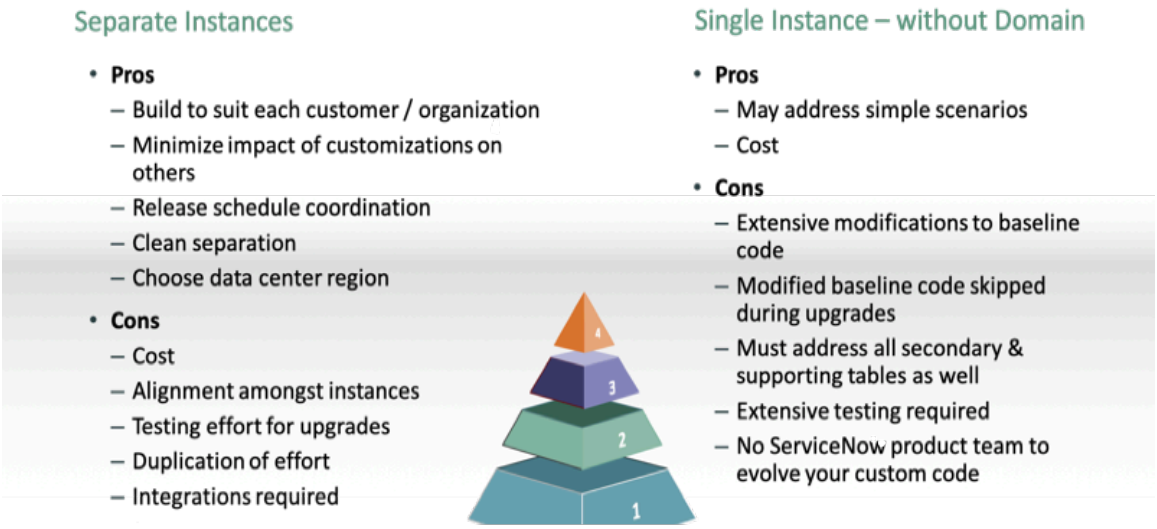
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Domänenpfadmigration

Domänenpfade werden für alle Kunden verwendet. Es wird keine Domänennummerierung verwendet. Kundenservice und Support kann beim Upgrade helfen.

Alternativen zu Domain Separation

Getrennte Instanzen sind eine gängige Alternative zur Domänentrennung. Dies bietet ein hohes Maß an Flexibilität bei der Erfüllung der Anforderungen für Kunden und Stakeholder mit geringen bis keinen Auswirkungen auf andere.



Warnung: Wenden Sie sich vor der Aktivierung von Domain Separation an Ihren Vertreter, um sicherzustellen, dass sie für Ihre Umgebung geeignet ist. Domain Separation verursacht eine zusätzliche Administrationsebene. Obwohl es deaktiviert werden kann, kann es nicht aus einer Instanz entfernt werden.

Zugehörige Informationen

Empfohlene Domain Separation-Verfahren für Service Provider

Domain Separation-Plugin

Konfiguration, die an interne oder externe Kunden delegiert werden kann

Domain Separation soll ServiceNow® Service Providern (SPs) die Möglichkeit geben, die Services zu konfigurieren, die sie ihren Kunden anbieten. Sie ist nicht dazu vorgesehen, Kunden die Möglichkeit zu geben, diese Services selbst zu verwalten, außer in einigen Bereichen, die in diesem Thema behandelt werden.

Übersicht

Für SP-Kunden ist es sicher, Daten zu verwalten, die in ihrer Domäne enthalten sind und sich nicht auf die Lizenzierung oder andere Kunden auswirken. Beispielsweise ist es für Kunden sicher, neue Berichte zu erstellen oder Konfigurationselemente zu verwalten, aber es ist für Kunden nicht sicher, Felder, Auswahlmöglichkeiten, Geschäftsregeln und andere Prozesse anzupassen, wenn sie sich auf andere Kunden in derselben Instanz auswirken können.

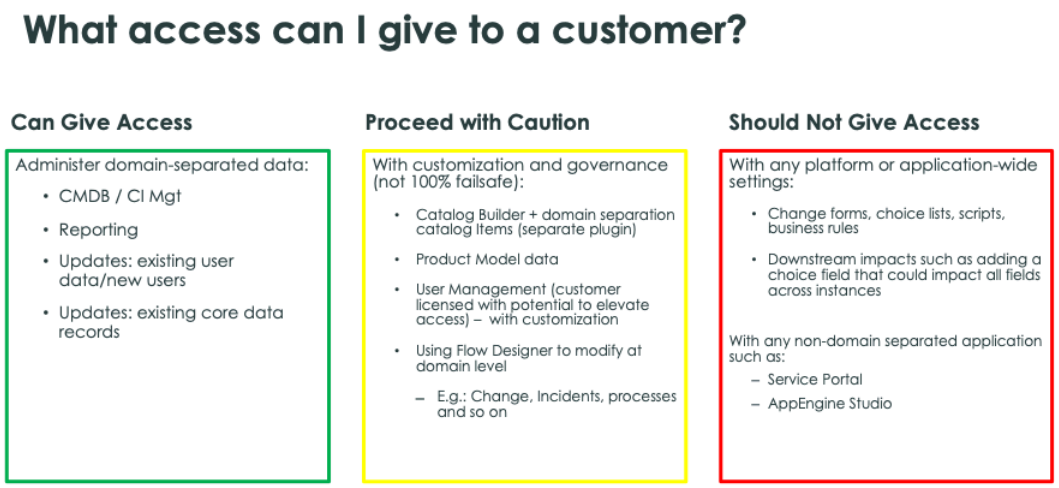
Die -Administratorrollen für das Basissystem von [ServiceNow und ihre Zugriffssteuerungen auf der Plattform ServiceNow sind für ein einzelnes Administratorteam pro Instanz vorgesehen. Beispielsweise wird die Rolle „domain_admin“ einer der Ressourcen des SP gewährt, um alle Domäneneinstellungen für die Instanz zu verwalten und neue Domänen zu erstellen. Für alle domänenspezifischen Administratoraufgaben sollte der SP nach Bedarf neue

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

„Kundenadministrator“-Rollen und Zugriffssteuerungen erstellen, um seinen Kunden spezifischen Zugriff zu gewähren.

Die folgende Abbildung zeigt eine Übersicht über allgemeine Administratorfunktionen in verschiedenen Kategorien dessen, was für einen Kunden sicher ist.



Kann Zugriff gewähren

Beispiele:

- CI-Datenverwaltung in der CMDB
- Berichterstellung
- Aktualisierungen vorhandener Anwenderdaten oder neuer Anwender ohne Rollen
- Aktualisierungen vorhandener Kerndatensätze wie Abteilung, Gruppe, Standort, Kostenstelle oder neuer Gruppen ohne Rollen und neuer Abteilungen/Kostenstellen/ Standorte.

„Mit Vorsicht fortfahren“.

Beispiele:

- Katalogelemente: Um kundenspezifische Katalogelemente zu erstellen, die vom Kunden aktualisiert werden können, können zwei Fähigkeiten zusammen verwendet werden: Domänentrennung für Katalogelemente (Domänentrennung und Servicekatalog) ermöglicht es dem Besitzer der -Instanz, Elemente in der Domäne des Kunden zu erstellen. Der Besitzer der Instanz kann eine Rolle erstellen, mit der Kunden sichere Felder wie Preis, Beschreibung und Bilder aktualisieren können. Der Katalog-Generator (neu im Quebec-Release) gibt dem SP-Administratorteam die Möglichkeit, Artikelvorlagen zu erstellen, die sicher an Kunden verteilt werden können, um neue Elemente in ihrer Domäne innerhalb einer verbindlichen UI-Experience zu erstellen.
- Anwender-/Gruppenverwaltung: Es ist sicher, die Rolle „Kundenadministrator“ zu erstellen, mit der Anwenderdatensätze erstellt und geändert werden kann. Das Hinzufügen und Entfernen von Rollen kann sich jedoch auf die Sicherheit und die Lizenzierung auswirken. Im Basissystem gibt es keine Möglichkeit, Rollen zu unterteilen, die für einen Kunden sicher sind. Dasselbe gilt für das Erstellen und Ändern von Gruppen. Während die Gruppe selbst geändert werden kann, sollte das Hinzufügen oder Entfernen von Rollen gesteuert werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Flow Designer : ServiceNow Flow Designer ist das Erstellungstool, das zum Erstellen von Prozessen (Workflows) für Tabellen verwendet wird. Die Rolle „flow_designer“ gewährt Kunden skriptfreien Zugriff zum Erstellen von Flows. Sie können jeden Flow in Domänen über ihnen in der Hierarchie lesen und klonen. Sie können Flows in ihrer Domäne erstellen und ändern. In einem Silos ist dies jedoch nicht möglich. Jeder, der sich auf den Prozess auswirken kann, muss dem globalen Admin-Team für Governance hinzugefügt werden, damit sich Prozesse nicht gegenseitig aufheben oder andere Konflikte verursachen.

Kein Zugriff gewähren

Zu verstehen, wie Auswahlfelder funktionieren, ist hilfreich, um zu verstehen, warum sie nur vom SP-Administratorteam verwaltet werden sollten.

- Aufbau eines Auswahlfelds: Auswahlfeldwerte werden in der Tabelle „sys_choice“ gespeichert und basierend auf Tabelle, Domäne und Sprache gruppiert.

  Beispielsweise ist das **Feld** „Status“ in einer Aufgabe für jede Tabelle verfügbar, die eine Aufgabe erweitert. Das bedeutet, dass jede Tabelle ihre eigenen Werte haben kann, dass diese Werte mit der Domäne multipliziert werden können und die Domänenwerte mit der Sprache multipliziert werden können.

  Alle Werte für den **Status** in allen Tabellen, Domänen und Sprachen werden als Werte für das **Feld „** Status“ betrachtet.

- Funktionsweise von Änderungen an Auswahlfeldern: Wenn ein Auswahlfeld aktualisiert wird, wird eine Nutzlast mit allen Werten für dieses Feld (Tabellen, Domänen, Sprachen) erstellt. Wenn Sie diese Nutzlast in einer Instanz installieren, werden alle vorhandenen Werte für das Feld gelöscht und die neuen Werte geladen. Dadurch wird sichergestellt, dass keine doppelten Einträge oder Werte übrig bleiben, die nicht mehr gültig sind.

  Aus diesem Grund ist es unmöglich, einem Kunden in einer domänengetrennten Instanz die Möglichkeit zu geben, Auswahlfelder direkt zu aktualisieren, da dies die gesamte Instanz betreffen würde. Darüber hinaus können Sie Auswahlmöglichkeiten nicht direkt in einer Produktionsinstanz aktualisieren, da alle importierten Update Sets, die sich auf dieses Feld auswirken, die vorhandenen Auswahlmöglichkeiten überschreiben würden. In einigen Fällen können Auswahlfelder selbst Prozesse steuern, die abbrechen würden, wenn ein Kunde diese Felder ändern würde.

Weitere Informationen finden Sie unter:

- Benutzerverwaltung erkunden
- Eine ACL-Regel erstellen
- Lernpfad für Service Provider auf Now Learning
- Domänentrennung für Service Provider
- Service Provider-Konzepte
- Anwendungssupport für Domain Separation
- Versionshinweise zur Domain Separation

Domänenzuweisung

Standardmäßig fügt Domain Separation Tabellen und ihren Erweiterungen ein Domänenfeld hinzu.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können Domain Separation auch auf alle neu erstellten Tabellen erweitern, indem Sie der Wörterbuchdefinition der Tabelle ein Feld **sys_domain** hinzufügen. Standardmäßig trennt das System nur Plattform- und Baselineanwendungstabellen nach Domäne, sofern angemessen.

> ⚠ **Warnung:** ServiceNow empfiehlt keine domänentrennenden Plattformtabellen (Tabellen mit dem Präfix sys_, z. B. die Tabellen Wörterbucheintrag [sys_dictionary] und Wörterbucheintragsüberschreibung [sys_dictionary_override]), da dies zu unerwarteten Ergebnissen führen kann.

Jeder Datensatz wird einer einzelnen Domäne zugewiesen.Diese Domäne wird im Feld **sys_domain**gespeichert.Mehrere Tabellen haben standardmäßig die Spalte **„sys_domain“** und sind bereits domänengetrennt.

Der Wert des **Felds sys_domain** enthält die Domäne, die dem Datensatz durch eine der folgenden Optionen zugewiesen wurde:

- Unternehmen, dem der Benutzer angehört
- Business-Regel beim Erstellen des Datensatzes
- Modul, das beim Erstellen des Datensatzes verwendet wird
- Formularvorlage, die beim Erstellen des Datensatzes verwendet wird
- Domäne des übergeordneten Datensatzes
- Dem Benutzerdatensatz zugewiesene Domäne
- Domäne des Benutzers, der sie erstellt

Das System verhindert, dass die folgenden Tabellen domänengetrennt werden:

- Zugriffssteuerung `[sys_security_acl]`
- `Skripteinbindung [sys_script_include]`
- Systemeigenschaft `[sys_properties]`
- Entitäten auf der Sicherheitsausschluss-/Einschlussliste `[sys_security_restricted_list]`
- Wörterbucheintrag `[sys_dictionary]`
- Wörterbucheintrag `–Überschreibung [sys_dictionary_override]`

Zuweisen von Benutzern zu Unternehmen

Administratoren können Benutzer schnell einer Domäne zuweisen, indem sie sie einem Unternehmen zuweisen. Nachdem Benutzer einer Domäne zugewiesen wurden, erben Datensätze automatisch die Domäne des Benutzers.

Wenn Sie beispielsweise Base Base dem ACME-Unternehmen zuweisen, wird er automatisch der ACME-Domäne zugewiesen. Wenn SieDon Goodliffe dem Unternehmen Initech zuweisen, wird er automatisch der Domäne Initech zugewiesen. Alle von ihnen erstellten Datensätze werden automatisch der entsprechenden Domäne hinzugefügt.

Geschäftsregeln zum Zuweisen von Domänen verwenden

Administratoren können eine Geschäftsregel verwenden, um beim Erstellen eines Datensatzes automatisch einen Domänenwert festzulegen. Die Geschäftsregel muss einen Wert im Feld **„sys_domain“ festlegen**. Administratoren müssen sicherstellen, dass für die Tabelle des Datensatzes eine Spalte „ **sys_domain“** verfügbar ist. Siehe Empfohlene Domain Separation-Verfahren für Service Provider für weitere Informationen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mithilfe von Modulen Domänen zuweisen

Administratoren können den URL-Parameter **sysparm_domain** verwenden, um aus einem Modul automatisch einer bestimmten Domäne neue Datensätze zuzuweisen. Administratoren müssen ein Modul mit dem folgenden **Argumentwert** erstellen: `sysparm_domain=sys_ID of domain`.

Formularvorlagen zum Zuweisen von Domänen verwenden

Administratoren können eine Formularvorlage verwenden, um einer bestimmten Domäne automatisch neue Datensätze zuzuweisen. Administratoren müssen dem Formular das Feld **„sys_domain“** hinzufügen und einen Domänenwert auswählen. Wenn Sie beispielsweise das Feld **„sys_domain“** auf **TOP/ACME-Domäne** festlegen, werden alle Datensätze aus dieser Vorlage automatisch der TOP/ACME-Domäne zugewiesen.

Domänenvererbung für Tabellen

Standardmäßig erben zugehörige Datensätze die Domäne des übergeordneten Datensatzes. Beispiel:

- Ein Change-Aufgabendatensatz erbt die Domäne des übergeordneten Change-Anforderungsdatensatzes.
- Ein Problemdatensatz erbt die Domäne des übergeordneten Incident-Datensatzes.

Automatische Domänenzuweisung basierend auf Benutzerdomänen

Wenn keine anderen Domänenbedingungen zutreffen, erbt ein Datensatz automatisch die Domäne des Benutzers, der ihn erstellt.

Sichtbarkeitsdomänen und Enthält Domänen

Sichtbarkeitsdomänen steuern, was ein bestimmter Benutzer oder eine bestimmte Gruppe von Benutzern sehen kann. „Enthält“-Domänen steuern, was eine ganze Domäne von Anwendern sehen kann.

Sichtbarkeitsdomänen

Das Element „Sichtbarkeitsdomänen“ bestimmt, ob Benutzer aus einer Domäne auf Datensätze einer anderen Domäne zugreifen können. Ordnen Sie dieses Element den Datensätzen „Anwender“ [sys_user] und „Gruppe“ [sys_user_group] in zugehörigen Listen für diese Datensätze zu. Gruppen gewähren ihren Mitgliedern die Sichtbarkeitsdomänen der Gruppe. Wenn ein Benutzer eine Gruppe verlässt, verliert er die Sichtbarkeitsdomänen der Gruppe. Durch die Gewährung einer Sichtbarkeitsdomäne werden Benutzern alle Rechte für die Datensätze in dieser Domäne basierend auf ACL-Regeln (Zugriffssteuerungsliste) gewährt.

Eine Sichtbarkeitsdomäne:

- Ist eine Anwender-zu-Domäne-Beziehung und wird explizit gewährt.
- Ist keine untergeordnete Domäne.
- Wird nicht durch die Auswahl in der Domänenauswahl gesteuert. Benutzer mit Zugriff auf eine Sichtbarkeitsdomäne sehen immer Daten in dieser Domäne und ihren untergeordneten Domänen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Eine übermäßige Verwendung von Sichtbarkeitsdomänen wird nicht empfohlen. Obwohl Transparenz eine Methode ist, um Benutzern den Zugriff auf Datensätze zu ermöglichen, ist es am besten, für eine robustere Steuerung Domänen zu verwenden, die Domänen enthält.

Enthält Domänen

Normalerweise definieren Übergeordnet/Untergeordnet-Beziehungen die Domänenhierarchie. Mit einer Domäne, die enthält, können Sie Domänen nach Bedarf verknüpfen, unabhängig von über- und untergeordneten Beziehungen. Enthält jedoch Domänen, die nur Domänendaten sichtbar sind. Prozesse sind von Beziehungen, die enthalten, nicht betroffen.

Eine enthält Domäne:

- Eine m:n-Beziehung zwischen Domänen
- Kann untergeordnete Domänen haben. Wenn eine Domäne ausgewählt wird, können Sie die Daten dieser Domäne und ihrer untergeordneten Elemente anzeigen.
- Wird durch die Auswahl in der Domänenauswahl gesteuert.

Hinweis: Wenn Sie den Domänendatensatz öffnen, wird der Bereich auf die Domäne dieses Datensatzes festgelegt, sodass Sie nur untergeordnete Domänen sehen können. Wählen Sie **Domänenbereich** ein/aus aus dem Menü, um die zugehörige Liste auszufüllen.

Enthält ein Domänenbeispiel

Wenn die Stammdomäne eines Benutzers A ist und die Domäne A die Domänen B und C enthält, werden alle Benutzer zu Peer-Domänen. Das bedeutet, dass der Benutzer Daten aus den Domänen A, B und C sieht, während er sich in seiner Stammdomäne A befindet. Wenn Benutzer Domänen mit der Domänenauswahl zu Domäne B ändern, werden nur Daten in Domäne B angezeigt. Wenn Benutzer mit einem Datensatz aus Domäne B interagieren oder Domäne C direkt sind, sehen sie nur Daten für diese Domäne.

Beispiel für die Sichtbarkeitsdomäne

Wenn sich die Domänentransparenz anwendet: Wenn sichDon Goodliffe in der Datenbankdomäne und BOW Runneri in der Netzwerkdomäne befindet und sich keine Incidents in der globalen Domäne befinden, kann DO aufgrund der Datentrennung nicht auf die Incidents von BO zugreifen.

Sichtbarkeitsdomänen werden basierend auf der Gruppenmitgliedschaft geerbt

Wenn Sie die Domänentabelle auf die Tabelle „Gruppe“ [sys_user_group] festlegen, können Benutzer Domänen mit Sichtbarkeit basierend auf ihrer Gruppenmitgliedschaft erben.

Zugehörige Informationen

Enthält Abfragen und Domänenzugriff

Empfohlene Domain Separation-Verfahren für Service Provider

Domänenbereich

Der Domänenbereich definiert, worauf Benutzer zugreifen können und was nicht.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Jeder Benutzer hat zwei Domänenbereiche, wenn er eine Sitzung in einer domänengetrennten Instanz herstellt.

- Der*Sitzungsumfang* wird beim Herstellen der Sitzung auf die Domäne festgelegt, die im Benutzerdatensatz des Benutzers aufgeführt ist. Benutzer können den Bereich ihrer Sitzungsdomäne manuell über die Domänenauswahl ändern.
- Der*Datensatzbereich* verwendet die Domäne des Datensatzes und ist aktiv, wenn das Formular eines Datensatzes angezeigt wird.

Standardmäßig hat der Datensatzumfang Vorrang vor dem Sitzungsumfang, sodass Anwender in Domänen höherer Ebenen die Daten- und Prozessbeschränkungen der einzelnen Datensätze einhalten. Diese Benutzer können jedoch den Domänenumfang erweitern oder einklappen, um Daten aus anderen Domänen anzuzeigen oder auszublenden. Beispielsweise hat ein Benutzer in der Domäne des Service Providers (SP) auch Einblick in untergeordnete Domänen wie die ACME-Domäne. Wenn Sie einen Incident-Datensatz aus der ACME-Domäne anzeigen, können Sie den Domänenbereich erweitern, um Werte aus der SP-Domäne anzuzeigen, oder den Domänenbereich reduzieren, um nur Datensatzwerte anzuzeigen, die der ACME-Domäne des Datensatzes entsprechen.

Hinweis: Benutzer haben immer Zugriff auf Daten aus Domänen, die ihnen durch die Domänensichtbarkeit explizit gewährt wurden.

Benutzer mit der Anwenderrolle „ **domain_expand_scope** “ können den Domänenbereich aus der UI-Aktion „Domänenbereich ein/aus“ im Formular auswählen. Wenn der Datensatzbereich aktiviert ist, klicken Sie auf die UI-Aktion, um ihn auf den Sitzungsbereich zu erweitern und alle verfügbaren Daten basierend auf der Domäne und den untergeordneten Domänen des Benutzers anzuzeigen. Wenn der Sitzungsbereich aktiviert ist, klicken Sie auf die UI-Aktion, um sie auf den Datensatzbereich zu reduzieren und nur Daten anzuzeigen, die der Domäne des aktuellen Datensatzes entsprechen.

Hinweis: Ein Datensatz zeigt die UI-Aktion zum Umschalten des Domänenbereichs nicht an, wenn sich der Datensatz in der globalen Domäne befindet oder wenn die Domäne des Benutzers mit der Domäne des Datensatzes übereinstimmt.

Datensatzwertauswahl aus anderen Domänen

Benutzer, die mehrere Domänen sehen können, haben die Möglichkeit, Datensatzwerte aus einer Domäne auszuwählen, die sich von der Domäne des Datensatzes unterscheidet.

Beispielsweise möchten Service Desk-Mitarbeiter, die für einen Service Provider arbeiten, möglicherweise sich selbst bestimmte Incidents zuweisen, um Probleme im Namen ihrer Kunden zu lösen. In diesem Fall enthält das Feld Incident **Zugewiesen an** möglicherweise einen Benutzer aus der SP-Domäne, auch wenn der Incident-Datensatz selbst einer untergeordneten Domäne wie ACME zugeordnet ist.

Durch Auswählen eines Datensatzwerts aus einer anderen Domäne wird die Domäne des Datensatzes nicht geändert. Der Datensatz behält seine ursprüngliche Domäne bei. Wenn ein Benutzer einen Datensatz mit Werten aus mehreren Domänen anzeigt, bestimmt die Sichtbarkeit der Domäne, was angezeigt wird.

Auswahl des Datensatzwerts

Wenn diese Bedingungen erfüllt sind	Der Benutzer hat Zugriff auf diese UI-Elemente
Der Benutzer hat Zugriff auf die Domäne des aktuellen	Der Benutzer kann:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auswahl des Datensatzwerts (Fortsetzung)

Wenn diese Bedingungen erfüllt sind	Der Benutzer hat Zugriff auf diese UI-Elemente
Datensatzes, auf den in einem Feld verwiesen wird.	• Siehe Anzeigewert des Referenzfelds. Beispielsweise sieht den Benutzernamen im Feld **Zugewiesen an**. • Siehe Referenzdatensatz über Symbol. Beispielsweise zeigt den Benutzerdatensatz für den Benutzer im Feld **Zugewiesen an an**. • Wählen Sie Werte aus einer beliebigen sichtbaren Domäne aus. Beispielsweise kann Benutzer aus der SP-Domäne und der ACME-Domäne auswählen.
Der Benutzer hat keinen Zugriff auf die Domäne des aktuellen Datensatzes, auf den in einem Feld verwiesen wird.	Der Benutzer kann: • Anzeigewerte des Referenzfelds nicht sichtbar. (Dies ist der Fall, wenn Domain Separation in Madrid oder späteren Releases aktiviert wurde und der Benutzer keinen Zugriff auf die Domäne dieses Datensatzes hat.) • Wählen Sie nur Werte aus der Domäne des Datensatzes aus. Beispielsweise können nur Benutzer aus der ACME-Domäne ausgewählt werden.

Domänen und zugehörige Unternehmen

Mit Domain Separation können Sie Änderungen, die Sie an einem Unternehmensdatensatz vornehmen, auf die Domäne und andere dem Unternehmen zugeordnete Datensätze kaskadieren.

Standardmäßig weist das System Benutzer automatisch derselben Domäne zu wie ihrem Unternehmen. Beispielsweise werden alle Benutzer des Unternehmens ACME automatisch Mitglieder der TOP/ACME-Domäne.

Hinweis: Benutzer mit der Rolle admin können ihre eigenen Benutzerdatensätze und damit die Domäne ändern. Service Provider möchten möglicherweise entweder die delegierte Administration deaktivieren oder einen Genehmigungsprozess einrichten, um zu überprüfen, ob der Benutzer die Administratorrolle benötigt.

Wenn Sie die Domäne eines Unternehmens ändern, ändert die Instanz automatisch die Domäne der folgenden zugeordneten Datensätze in die neue Domäne des Unternehmens.

- Standorte
- Abteilungen
- Gruppen
- Anwender

Hinweis: Die Instanz ändert die Domäne von Datensätzen, für die Sie das Kontrollkästchen **Verwaltete Domäne** aktiviert haben, nicht automatisch.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Domänendeaktivierung und zugehörige Unternehmen

Wenn Sie eine Domäne deaktivieren, führt die Instanz auch automatisch die folgenden Aktionen aus.

- Deaktiviert alle Unternehmen in der Domäne.
- Verhindert, dass sich alle Benutzer anmelden, die dem inaktiven Unternehmen zugewiesen sind.

Hinweis: Wenn ein Benutzer aus einem inaktiven Unternehmen versucht, sich anzumelden, erhält er eine ähnliche Fehlermeldung wie `Unternehmen inaktiv - Ihr Zugriff auf diese Instanz ist nicht autorisiert.`

Wenn Sie beispielsweise die ACME-Domäne aus den Beispieldaten deaktivieren, deaktiviert die Instanz auch das ACME-Unternehmen, und die drei Beispielbenutzer werden gesperrt.

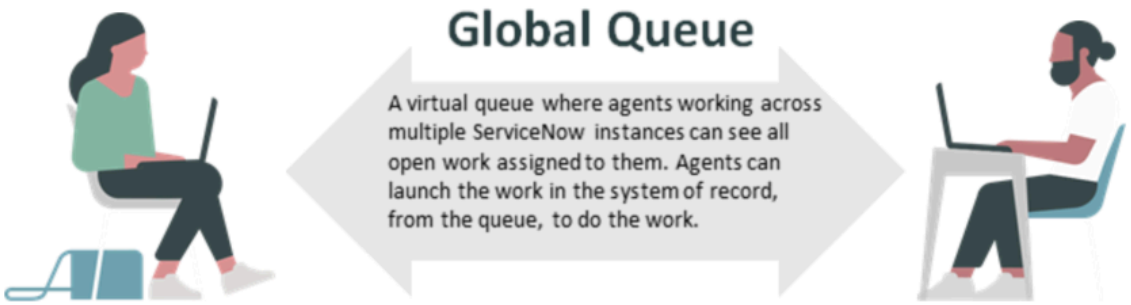
Konzepte für Service Provider

Diese Konzepte funktionieren mit den vorhandenen Fähigkeiten der Plattform ServiceNow, um Sie bei der Lösung allgemeiner Anwendungsfälle zu unterstützen.

Globale Warteschlange v.2

Das Konzept der globalen Warteschlange bietet eine einheitliche virtuelle Ansicht von Aufgaben, die sich in mehreren Instanzen befinden. Das Konzept erstellt eine anwenderdefinierte Anwendung, um eine Erfülleransicht der Arbeit bereitzustellen, die sich in mehreren Instanzen befindet, ohne dass Aufgaben oder Daten repliziert werden müssen.

Übersicht



Service Provider, deren Service Desk-Mitarbeiter an Aufgaben aus mehreren Systemen arbeiten, integrieren die Daten in der Regel zurück in eine zentrale Instanz oder einen „Stuhl“ zwischen Instanzen. Obwohl diese Methode in einigen Fällen angemessen sein könnte, kann sie in Bezug auf Erstellung und Wartung teuer und zeitaufwändig sein. Diese Methode öffnet den Anbieter auch für potenzielle Überlegungen zu Audits und Datenanforderungen wie die Datenschutz-Grundordnung (DSGVO) in allen Instanzen, in denen sich die Daten jetzt befinden.

Eine Alternative bietet die globale Warteschlange v.2: Mit dieser Methode können Service Desk-Mitarbeiter die ihnen zugewiesenen Daten aus einer einzelnen Instanz anzeigen, ohne dass souveräne Daten in der Instanz, bei der sie sich anmelden, beibehalten werden. Wenn Kunden beispielsweise Anforderungen an den Datenspeicherort haben, aber den Zugriff durch Service Desk-Mitarbeiter aus anderen Ländern zulassen, kann der Anbieter beispielsweise einen „Follow-the-Sun“-Helpdesk mit globaler Warteschlange v.2 verwenden.

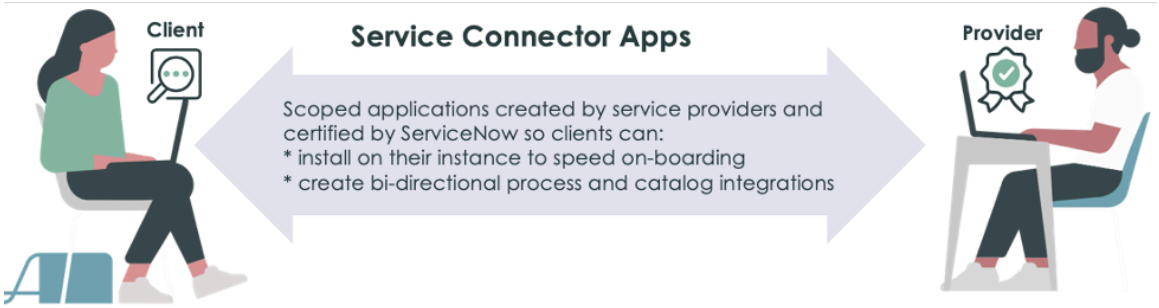
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zum Proof of Concept für Global Queue v.2 finden Sie auf der Knowledge-Website ServiceNow.

Hinweis: Ab dem Quebec-Release wurde der Proof of Concept der globalen Warteschlange auf globale Warteschlange v. 2 aktualisiert.

Service Provider-Connector

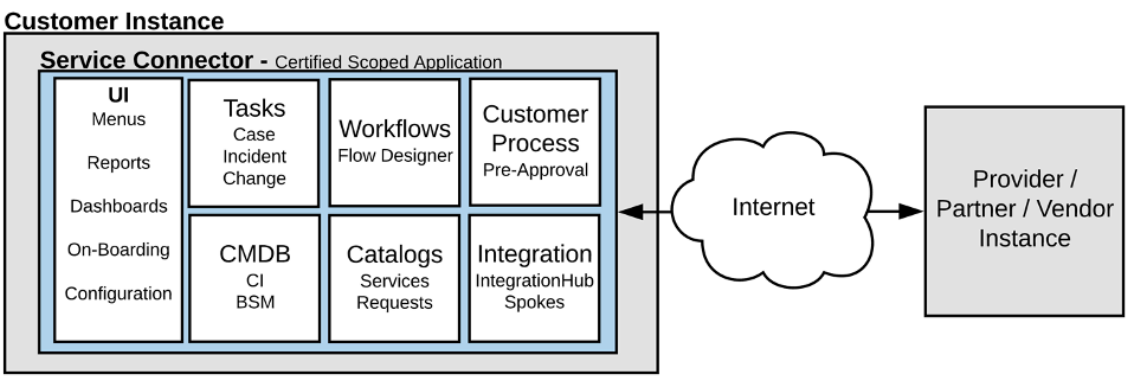
Die Anwendung Service Provider Connector ist ein Referenzdesign zum Erstellen einer ServiceNow Store App für Ihre Kunden zur Integration in Ihre Systeme. Service Provider-Anwendungen helfen Ihnen, das Onboarding zu beschleunigen und standardisierte Integrationen zu erstellen.



Vorteile von Service Connectors

Wenn Service Provider (Lieferanten, Lieferanten, Partner) Connectors veröffentlichen, erfolgt das Onboarding von Kunden schneller und entsprechend schneller die Abrechnung. Integrierte Instanzen von erhöhen die Produktivität und verbessern die Transparenz im ServiceNow -Ökosystem sowie die Vorteile von Partnerprogrammen. Spezifische Vorteile sind:

- Benutzerdefinierte Integrationen eliminieren, einschließlich der Kosten für Services, die für ihre Bereitstellung und Wartung erforderlich sind.
- Services werden innerhalb ihrer ServiceNow -Instanzen vom Anbieter definiert und machen die Komplexität und die Kosten benutzerdefinierter Integrationen überflüssig.
- Workflows und Kataloganforderungen können synchronisiert werden, wobei die Prozesse und Genehmigungen des Kunden den Prozessen des Anbieters vorausgehen, sodass Kunden ihre eigenen Prozesse verfolgen können.
- Alle Daten, die in der Instanz des Providers für den Kunden erstellt oder geändert wurden (z. B. CIs), können zu ihrer Sichtbarkeit und Verwendung in Prozessen wieder mit der Instanz des Kunden synchronisiert werden.



© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schlüsselfunktionen

Funktion	Beschreibung
Anwenderoberfläche	Ein Service Connector sollte mindestens die folgenden UI-Komponenten enthalten: • Berichte/Dashboards: Von Personas vordefinierte Berichte und Dashboards helfen bei der Transparenz. • Menü und Module: Der Kunde sollte die Anwendung über das beschreibende Menü **Provider XYZ Services**finden können. • Rollen: Jeder Connector benötigt Anwender- und Administratorrollen, um sicherzustellen, dass der Zugriff vom Kunden gesteuert werden kann. Beispiel: „x_snc_xyz_user“ oder „x_snc_xyz_admin“. • Onboarding: Ein schnelles Onboarding ist für eine gute Kunden-Experience von entscheidender Bedeutung und sollte über ein Playbook, ein geführtes Setup oder ein Katalogelement so erfolgen, dass keine professionellen Services erforderlich sind, damit der Kunde live gehen kann. (Professional Services sind verfügbar, das Onboarding ist jedoch auch ohne sie möglich). • Konfiguration – Datenpunkte sollten in Prozesse integriert werden, um den Großteil der normalen Prozesskonfiguration zu berücksichtigen, die ein Kunde erreichen muss. Dadurch werden professionelle Services so weit wie möglich eliminiert. • Dokumentation: Eine gründliche Dokumentation erhöht die Kundenzufriedenheit und ist anwenderfreundlich. • Supportintegration oder Kontaktinformationen: Der Kunde benötigt eine einfache Möglichkeit, bei Problemen, Fragen oder Anforderungen mit dem Service Provider in Kontakt zu bleiben.
Aufgaben	Die Verwendung der Anwendung Service Bridge (veraltet) für Aufgaben wie Incidents, Fälle, Changes, Probleme usw. sollte im Connector vordefiniert sein. Diese Integrationen werden mit Flow Designer und IntegrationHub erstellt, um ein Höchstmaß an Resilienz und Leistung sicherzustellen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Funktion	Beschreibung
CMDB	Es werden Kerndaten synchronisiert, z. B. müssen die für ordnungsgemäße ITIL-Prozesse erforderlichen CIs zwischen Anbieter- und Kundeninstanzen synchron gehalten werden.
Workflows	Alle -Workflows sollten in Flow Designer entworfen werden, um Resilienz und Leistung sicherzustellen.
Kataloge	Der Katalog des Anbieters, von dem der Kunde anfordert, sollte als datensatzerzeugender Katalog in die Anwendung aufgenommen werden. Die vom Element in der Instanz des Kunden generierte Anforderung sollte mit den Instanzen des Anbieters verbunden werden. Die Workflows des Anbieters halten die Anforderung auf dem neuesten Stand und synchronisieren sie zurück mit der Instanz des Kunden.
Kundenprozesse	Alle Mechanismen zum Synchronisieren von Anforderungen mit der Instanz des Anbieters sollten es Kundenprozessen ermöglichen, mit den Anforderungen zu interagieren, bevor sie an die Instanz des Anbieters gesendet werden. Während der Verarbeitung des Anbieters können bei Bedarf Genehmigungen an die Instanz des Kunden gesendet werden.
Integration	Integrationen sollten mit Flow Designer und IntegrationHub erstellt werden, um ein Höchstmaß an Resilienz und Leistung sicherzustellen.

Mögliche Komponenten, die Sie in einen Service Connector aufnehmen können

Komponente	Beschreibung
Instanzdatenreplikation (IDR)	Wenn Replikation das Ziel ist: • Kann für die Prozessintegration verwendet werden, kann jedoch je nach Komplexitätsintegrationslogik basierend auf dem Statusübergang zu streng sein • Weitere Informationen finden Sie unter Instanzdatenreplikation
IntegrationHub	Wenn Prozessintegration das Ziel ist:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Komponente	Beschreibung
	• Einfacher mitten in einen Prozess einzufügen, als Teil eines komplexen oder bedingten Schritts in der Mitte eines Flows • Weitere Informationen finden Sie unter IntegrationHub
Globale Arbeitswarteschlange (virtuell)	Wenn die Aufgabenvereinigung das Ziel ist und die externe Speicherung von Daten nicht zulässig ist: • Wird verwendet, wenn Service Desk-Mitarbeiter in mehreren Instanzen ServiceNow arbeiten und alle ihnen zugewiesenen offenen Arbeiten sehen müssen • Die zurückgegebenen Zeilen sollten auf weniger als 1000 beschränkt sein • Weitere Informationen finden Sie unter Globale Arbeitswarteschlange
Remotetabellen	Wenn die Nutzung externer Daten ohne Speicher das Ziel ist: • Wird verwendet, um eine Instanz mit Drittanbieterquellen oder einer anderen Instanz zu verbinden, externe Daten abzurufen und optional im Arbeitsspeicher zwischenzuspeichern. Die Daten werden in der Instanz für schreibgeschützte Zwecke wie Gruppieren, Sortieren, Aggregieren und Filtern als Tabelle behandelt. • Weitere Informationen finden Sie unter Externe Daten mithilfe von Remotetabellen und -skripts abrufen
Flow Designer	Wenn Prozessdesign das Ziel ist • Wird zur Automatisierung von Prozessen in einer einheitlichen Designumgebung verwendet. Prozessverantwortliche können natürliche Sprache verwenden, um Genehmigungen, Aufgaben, Benachrichtigungen und Datensatzvorgänge ohne Codierung zu automatisieren. • Weitere Informationen finden Sie unter Flow Designer .

Weitere Informationen zum Proof of Concept von Service Connector finden Sie auf der Knowledge-Website ServiceNow.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installiert mit Domain Separation

Mehrere Plattformkomponenten werden bei Domain Separation hinzugefügt oder geändert.

Rollen

Rolle	Beschreibung
domain_admin	Kann Domänen erstellen, bearbeiten und löschen.

Ergänzungen zu Feldern [sys_domain].

Das Feld „sys_domain“ wird den folgenden Tabellen hinzugefügt:

Tabellen mit dem Feld „sys_domain“

Tabellen
sys_attachment
sys_user_has_role
sys_group_has_role
sys_email
sys_user_group
core_company
cmn_location
cmn_department
sys_gage
sys_report
kb_feedback
sysapproval_approver
sys_user_grmember

Feld für die Aufgabentabelle

MSP-Erweiterungen fügen der Aufgabentabelle ein Feld „task_for“ hinzu. Dieses Referenzfeld bezieht sich auf die Benutzertabelle.

Optionen für den Gruppentyp

MSP-Erweiterungen fügen dem Typfeld der Gruppentabelle mehrere neue Standardoptionen hinzu. Fügen Sie diese Typen nach Bedarf hinzu, oder aktualisieren Sie sie, um Ihre Domänen zu unterstützen.

Tabellen
Sicherheit
Support

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabellen
Sichtbarkeit

Business-Regeln

Name	Tabelle	Beschreibung
Domäne: Aktivieren/ deaktivieren	core_company	Aktiviert die zugehörige Domäne, wenn mindestens eines ihrer Unternehmen aktiv ist. Deaktiviert die zugehörige Domäne, wenn alle zugehörigen Unternehmen inaktiv sind.
Domäne: kaskadierendes Unternehmen	core_company	Hält die Domäne eines Unternehmens mit seinen Benutzern, Gruppen, Abteilungen und Standorten synchronisiert.
Domäne – Kaskadierende Domäne – E-Mail	sys_email	Hält die Domäne einer E-Mail mit ihren Anhängen synchron.
Domäne – Kaskadierende Domäne – Gruppe	sys_user_group	Hält die Domäne einer Gruppe mit ihren geerbten Rollen (sys_group_has_role-Datensätze) synchron.
Domäne – Kaskadierende Domäne – Wissen	kb_knowledge	synchronisiert die Domäne eines Wissensartikels mit dem zugehörigen Feedback.
Domäne – Kaskadierende Domäne – Aufgabe	Aufgabe	Hält die Domäne mit zugehörigen Aufgaben für „wf_context“, „wf_executing“, „wf_history“, „attachments“, „emails“, „task_sla“ und ihren Workflow, „sysapproval_approver“ und ihren Workflow sowie „sysapproval_group“ und ihren Workflow synchron.
Domäne – Kaskadierende Domäne – Anwender	sys_user	Hält die Domäne eines Anwenders mit den Datensätzen seiner Gruppenmitgliedschaft (sys_user_grmember) und Rolle (sys_user_has_role) synchronisiert.
Domäne – Kaskadierende Domäne – Version	wf_workflow_version	Hält die Synchronisierung von Domänen mit zugehörigen Workflow-Versionen für wf_activity und wf_transition aufrecht

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Tabelle	Beschreibung
Domäne: Unternehmen deaktivieren	Domäne	Deaktiviert zugehörige Unternehmen, wenn eine Domäne deaktiviert wird.
Domäne – Standard – Aufgabe	Aufgabe	Legt die Aufgabendomäne basierend auf der Aufgabe für die Domäne des Benutzers fest. Wenn diese Domäne global wäre, wird die Domäne stattdessen auf Standard festgelegt.
Domäne – Standard – Anwender	sys_user	Legt die Domäne eines Anwenders als Standard fest, wenn die Domäne andernfalls global wäre.
Domäne: Globaler Domänendatensatz nicht zulassen	Domäne	Verhindert die Erstellung einer Domäne mit dem Namen global.
Domäne: Kopie überschreiben	sys_app_application	Wenn eine Anwendung für eine Domäne überschrieben wird, erstellt eine Kopie ihrer Module für die neue Anwendung.
Domäne: Kopie überschreiben	sys_data_policy2	Wenn eine Datenrichtlinie für eine Domäne überschrieben wird, erstellt eine Kopie ihrer Datenrichtlinienregeln für die neue Datenrichtlinie.
Domäne: Kopie überschreiben	sys_gage	Wenn eine Anzeige für eine Domäne überschrieben wird, wird von eine Kopie der Anzeigeanzahl für die neue Anzeige erstellt.
Domäne: Kopie überschreiben	sys_ui_action	Wenn eine UI-Aktion für eine Domäne überschrieben wird, erstellt eine Kopie ihrer UI-Aktionsansichten für die neue UI-Aktion.
Domäne: Kopie überschreiben	sys_ui_list_control_embedded	Wenn ein eingebettetes Listensteuerelement für eine Domäne überschrieben wird, erstellt eine Kopie seiner Client- und Serverskripts für das neue eingebettete Listensteuerelement.
Domäne: Kopie überschreiben	sys_ui_policy	Wenn eine UI-Richtlinie für eine Domäne überschrieben wird, erstellt eine Kopie ihrer UI-Richtlinienaktionen für die neue UI-Richtlinie.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Tabelle	Beschreibung
Domäne: Legen Sie die Domäne fest – Genehmigungen	sysapproval_approver	Legt die Domäne basierend auf der des genehmigten Datensatzes fest.
Domäne – Domäne festlegen – Anhang	sys_attachment	Legt die Domäne basierend auf der Domäne des übergeordneten Datensatzes fest.
Domäne: Domäne festlegen – CMDB_CI	cmdb_ci	Legt die Domäne eines CI auf die Domäne seines Unternehmens fest.
Domäne: Legen Sie die Domäne fest – Abteilung	cmn_department	Legt die Domäne einer Abteilung auf die ihres Unternehmens fest.
Domäne – Domäne festlegen – Domäne	Domäne	Legt die Domäne einer Domäne auf sich selbst fest.
Domäne: Domäne festlegen – E-Mail	sys_email	Legt die Domäne basierend auf der Domäne des übergeordneten Datensatzes fest. Der übergeordnete Datensatz einer E-Mail ist der im Instanzfeld angegebene Datensatz.
Domäne: Legen Sie die Domäne fest – Feedback	kb_feedback	Legt die Domäne eines Wissensfeedbacks auf die Domäne des zugehörigen Wissensartikels fest.
Domäne – Domäne festlegen – Gruppe	sys_user_group	Legt die Domäne einer Gruppe auf die ihres Unternehmens fest.
Domäne: Domäne festlegen – Gruppengenehmigungen	sysapproval_group	Legt die Domäne basierend auf der des genehmigten Datensatzes fest.
Domäne: Legt die Domäne fest – Gruppenrolle	sys_group_has_role	Legt die Domäne einer Gruppenrolle auf die Domäne ihrer Gruppe fest.
Domäne: Domäne festlegen – Standort	cmn_location	Legt die Domäne eines Standorts auf die Domäne des Unternehmens fest.
Domäne: Domäne festlegen – Aufgaben-SLA	task_sla	Legt die Domäne eines Aufgaben-SLA auf die seiner Aufgabe fest.
Domäne: Domäne festlegen – Anwender	sys_user	Legt die Domäne eines Benutzers auf die Domäne seines Unternehmens fest.
Domäne: Legt die Domäne fest – Anwenderrolle	sys_user_has_role	Legt die Domäne einer Anwenderrolle auf die Domäne ihres Anwenders fest.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Tabelle	Beschreibung
Domäne: Domäne festlegen – WF-Aktivitätsverlauf	wf_history	Legt die Domäne des Workflow-Aktivitätsverlaufs basierend auf der Domäne des übergeordneten Workflow-Kontexts fest.
Domäne: Domäne festlegen – WF-Kontext	wf_context	Legt die Workflow-Kontextdomäne basierend auf der Domäne des referenzierten Datensatzes fest, falls vorhanden.
Domäne – Domäne festlegen – WF-Ausführungsaktivität	wf_executing	Legt die Domäne der Workflow-Ausführungsaktivität basierend auf der Domäne des übergeordneten Workflow-Kontexts fest.
Domäne – Aufgabe festlegen für – Change	Change-Anforderung	Beim Konvertieren eines Tickets in eine Change-Anforderung wird das Feld Angefordert von auf den Wert der Aufgabe für des Tickets festgelegt.
Domäne – Legen Sie die Aufgabe für – Incident fest	Incident	Beim Konvertieren eines Tickets in einen Incident legt das Feld Anrufer auf den Wert Aufgabe für des Tickets fest.
Domäne: Validiert den Standard	Domäne	Stellt sicher, dass nur für eine Domäne das Kontrollkästchen Standard aktiviert ist.
Domäne: Validiert Primär	Domäne	Stellt sicher, dass nur für eine Domäne das Kontrollkästchen Primär aktiviert ist.
Mit dem Domain Support-Plugin installierte Business-Regeln		
Domänensatz ändern	sys_dictionary	Legt den Domänensatz auf die aktuelle Domäne fest.
Eigenschaften der Domänenunterstützung	sys_properties	Legt die Systemeigenschaften so fest, dass sie der Domänenabfragemethode entsprechen (Domänenpfade oder Domänennummerierung).

Client-Skripts

Client-Skript	Beschreibung
Domäne – Unternehmen und Standort festlegen (sys_script)	Überwacht das Feld „Incident-Anrufer“ auf Änderungen. Wenn die Felder „Unternehmen“ und „Standort“ noch keinen Wert aufweisen, fügt das Skript diese Informationen aus dem Anruferdatensatz hinzu. Wenn die Felder „Unternehmen“ und „Standort“ bereits einen Wert enthalten, behält das Skript die vorhandenen Werte bei.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Client-Skript	Beschreibung
Deaktiviertes Skript	
(BP) Legen Sie den Standort auf Benutzer fest	Überwacht das Incident-Standortfeld und legt das Standortfeld auf den Standort des Anrufers fest.

Zugehörige Informationen

Empfohlene Domain Separation-Verfahren für Service Provider

Anwendungssupport für die Domänentrennung

Viele ServiceNow -Anwendungen unterstützen die Domänentrennung im Basissystem, aber nicht alle. Einige unterstützte Anwendungen beinhalten Einschränkungen bei den Daten und administrativen Einstellungen, die domänengetrennt werden können. Diese Definitionen beschreiben die Unterstützungsebenen für Domain Separation aus der Perspektive der tatsächlichen Anwendungsfälle und der Personen, die sie verwenden.

Unterstützungsebenen für Domain Separation

ServiceNow Anwendungen, die die Domänentrennung unterstützen, unterstützen möglicherweise nur die Trennung von Daten und Datenweiterleitung, verfügen über erweiterte Geschäftslogiktrennung oder unterstützen die Verwaltung der Anwendung auf Mandantenebene (Kundenebene). ServiceNow Anwendungen werden mit den folgenden inkrementellen Supportstufen definiert.

Basic	Standard	Enhanced
• Data is domain-separated • Logic exists to ensure proper data routing, caching, rollups, and aggregations • Global configuration operational for multiple tenants	• Application properties are domain-aware as needed • Business logic can be domain-separated by the instance owner per tenant	• Data-driven process enables failsafe configuration by tenants through the UI to drive business logic

Kein Support

- Das Feld „Domäne“ kann in Datentabellen vorhanden sein, es ist jedoch keine Logik zum Verwalten der Daten vorhanden.
- Diese Ebene wird nicht als domänengetrennt betrachtet.

Basis

- Geschäftslogik: Stellen Sie sicher, dass Daten in die richtige Domäne für die Anwendungsfälle des Application Service Providers übertragen werden.
- In der Anwendung berücksichtigen die Benutzeroberfläche, Cache-Schlüssel, Berichterstellung, Rollups, Zusammenfassungen usw. Domänen zur Produktionslaufzeit.
- Der Besitzer der Instanz muss in der Lage sein, die Anwendung so einzurichten, dass sie mandantenübergreifend funktioniert.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel-Anwendungsfall: Wenn ein SP den Chat verwendet, um auf die Nachricht eines Mandanten zu antworten, muss der Client die Antwort des SP sehen können.

Standard

- Umfasst die **Basis**-Support-Stufe.
- Geschäftslogik: Prozesse können vom Service Provider (SP) pro Kunde erstellt oder geändert werden. Die Anwendungsfälle spiegeln die ordnungsgemäße Verwendung der Anwendung durch mehrere SP-Kunden in einer einzigen Instanz wider.
- Der Besitzer der Instanz muss in der Lage sein, die MVP-Geschäftslogik (Minimum des lebensfähigen Produkts) und die Datenparameter pro Mandant wie erwartet für die spezifische Anwendung zu konfigurieren.

Beispiel-Anwendungsfall: Ein -Administrator muss in der Lage sein, Kommentare obligatorisch zu machen, wenn ein Datensatz für einen Mandanten geschlossen wird, aber nicht für einen anderen.

Verbessert

- Umfasst die Stufen **Basis** und **Standard**.
- Ein datengesteuerter Prozess ermöglicht es Service Provider-Kunden, die Geschäftslogik basierend auf definierten Anwendungsfällen zu ändern. Diese Konfigurationen sind UI-basiert und ausfallsicher, sodass Konfigurationen von einem Kunden sich nicht auf einen anderen auswirken können.
- Mandanten der Instanz müssen die MVP-Geschäftslogik (Minimum des lebensfähigen Produkts) und die Datenparameter für sich selbst konfigurieren können. Diese Logik und diese Parameter würden für die normale Funktion der Anwendung erwartet.

Beispiel-Anwendungsfall: Mandanten-Kunden einer gemeinsam genutzten Umgebung müssen in der Lage sein, die Auswirkungs-, Dringlichkeits- oder Prioritätsmatrix zu ändern, um die Priorität in ihrer Domäne festzulegen.

Hinweis: Effektive Domäne (*)

Manchmal kann eine Plattformfunktion oder eine Anwendung SP-Anwendungsfälle auch ohne das Domänen-Framework effektiv unterstützen. Wenn dies der Fall ist, müssen die Anwendungsfälle die Unterstützung von Domain Separation beschreiben. Ein Sternchen (*) hinter der Support-Stufe weist auf diese Art der Konfiguration hin.

Unterstützte Funktion	Standard	Standard	Erweitert
Domänenspalte ist für Basissystem-Anwendungstabellen vorhanden.	●	●	●
Die domänenspezifische Konfiguration wird vom Besitzer der Instanz verwaltet.	●	●	●
Mandantendomänen können ihre eigenen Anwendungsdaten verwalten.		●	●
Anwendungseigenschaften sind bei Bedarf domänenfähig.		●	●

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterstützte Funktion	Standard	Standard	Erweitert
Geschäftslogik und Prozesse können vom Instanzbesitzer domänengetrennt werden.		●	●
Geschäftslogik und -prozesse können von der Mandantendomäne verwaltet werden.			●

Supportstufen nach Anwendung

Produkt-Suite	Anwendung	Support-Stufe
Hyperautomation und Low Code	App Engine Studio	Kein Support
	Automatisierungszentrale	Standard
	Robotic Process Automation (RPA)-Hub	Standard
	Table Builder	Standard
	App Engine Management Center	Kein Support
	Entscheidungstabellen erkunden	Standard
	Enterprise Resource Planning Integration	Kein Support
	Enterprise Resource Planning Customization Mining	Kein Support
	Next Experience UI Builder	Standard
Kundenservice-Management	Communities	Kein Support
	Kundenservice-Management	Standard
	Releasemanagement	Standard*
	Order Management für Customer Service Management	Standard
	Post-Sales Support	Standard
	Domain Separation in Personaloptimierung für den Kundenservice	Standard
DevOps	Domain Separation und DevOps Change-Geschwindigkeit	Kein Support
	Domain Separation und DevOps Config	
Employee Service Management	HR Service Delivery	Standard*
	Arbeitsschutz	Standard
	Legal Service Delivery	Standard

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Produkt-Suite	Anwendung	Support-Stufe
	Procurement Service Management (PSM)	Kein Support
	Safe Workplace Suite	Die einzelnen Supportstufen für Anwendungen finden Sie auf der Website der -Anwendung
	Connector für SharePoint Online-Suchen	Standard
	Universelle Anforderung	Standard
	UR-Aufgabe	Standard
	Personaloptimierung für HR	Standard
Environmental, Social und Governance	Environmental, Social und Governance	Standard
Außendienst-Management	Field Service Management	Standard
Governance, Risk und Compliance	Business Continuity Management	Standard
	Governance, Risk and Compliance (GRC)	Standard
	Operational Resilience	Standard
Branchenprodukte		
• Financial Services	Financial Services Card Operations	Standard
	Financial Services Deposit Operations	Standard
	Financial Services Payment Operations	Standard
	Intelligent Servicing for Fraud	
	Sach- und Unfallversicherungs-Servicing	
	Life Insurance Servicing	
	Versicherungsansprüche	
	Financial Services Know Your Customer	
	Financial Services Credit Operations	
	Financial Services Document Processor	Standard
• Gesundheitswesen und Biowissenschaften	EMR Help	Standard
	Healthcare and Life Sciences Service Management Core	Standard
	Pre-Visit Management	Standard

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Produkt-Suite	Anwendung	Support-Stufe
	Patient Support Services	Standard
	Vaccine Administration Management	Standard
• Fertigungsindustrie	Manufacturing Process Manager Prozessmanager Industrie	Standard
	Operational Technology Manager	Standard
	Operational Technology Vulnerability Response	Standard
	Operational Technology Manager	Standard
IT Asset Management	Cloud Insights	Kein Support
	Hardware Asset Management	Erweitert
	Software Asset Management	Erweitert
	Enterprise Asset Management	Standard
Strategic Portfolio Management	Agile Development	Standard*
	Alignment Planner Workspace	Standard
	Application Portfolio Management	Standard
	Cost Management	Kein Support
	Demand-Management	Standard
	Finanzmanagement	Kein Support
	Investment Funding	Standard
	Projektportfoliomanagement	Standard*
	Releasemanagement	Standard*
	Scaled Agile Framework (SAFe)	Standard*
	Test Management	Standard*
	Ziel-Framework	Standard
IT Operations Management	Cloud Provisioning and Governance	Standard
	Agent Client Collector	Standard
	Discovery	Standard
	Ereignismanagement	Standard
	Service Operations-Arbeitsbereich für ITOM	Standard

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Produkt-Suite	Anwendung	Support-Stufe
	Health Log Analytics	Standard
	Metric Intelligence	Standard
	Service-Zuordnung	Standard
	Bewertung der Cloud-Migration	Standard
	Aktionsbibliothek	Kein Support
	Governance für Cloud-Konfigurationen	Kein Support
	Tag Governance	Standard
	Abrechnung für Cloud-Einblicke	Kein Support
	Cloud Provisioning and Governance: Google Cloud	Standard
	Cloud Provisioning and Governance Terraform	Standard
	Arbeitsbereich für Cloud-Vorgänge	Standard
	Cloud-Discovery	Standard
IT Service Management	Benchmarks	Kein Support
	Change-Management	Standard
	Coaching	Standard
	Management kontinuierlicher Verbesserungen	Standard
	Vertragsmanagement	Kein Support
	Kostenzeile	Kein Support
	Incident Communications Management	Standard
	Incident-Management	Standard
	Facilities Service Management	Standard
	Incident-Management	Standard
	Bereitschaftsplanung	Standard
	Asset-Management	Standard
	Problem-Management	Standard
	Beschaffung	Standard*
	Produktkatalog	Standard
	Anforderungsmanagement	Standard
	Servicekatalog	Standard
	Service-Level-Management	Standard

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Produkt-Suite	Anwendung	Support-Stufe
	Service Portfoliomanagement	Standard*
	Site Reliability Operations	Standard*
	Nichtverfügbarkeit von Aufgaben	Standard
	Domain Separation und Vendor Management-Arbeitsbereich	Kein Support
	Walk-up Experience	Standard
Konfiguration und Navigation für Mobile	Mobil	Standard
Now Intelligence	Dashboards	Standard
	Leistungsanalysen	Erweitert
	Process Optimization	Standard
	Berichterstellung	Standard
	User Experience Analytics	Standard
Die Now Platform	,Administration ,App Engine Studio , Anwenderoberfläche für Now Platform-Fähigkeiten	
	Domänentrennung und Mitarbeiterchat	Standard
	Advanced Work Assignment	Standard
	AI Search	Suchvorgänge berücksichtigen Domänenbeschränkungen aus indizierten Datensätzen
	App Engine Studio	Kein Support
	Application Management	Kein Support
	Bewertungen	Standard
	Automated Test Framework	Standard*
	ServiceNow Voice	
	Codesignatur	Basis-Support
	Contextual Search	Standard
	Configuration Management (CMDB)	Standard
	Content-Management-System	Kein Support
	Anmeldeinformationen und Verbindungen	Standard
	Datenzertifizierung	Standard*
	Data Classification	Erweitert

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Produkt-Suite	Anwendung	Support-Stufe
	Datenschutz	Kein Support
	Datenverwaltung	Standard*
	Delegated Development	Kein Support
	Dependency Views	Standard
	Dokumentenservices	Kein Support
	Dynamische Übersetzung	Standard
	Edge Encryption	Basis-Support
	Verschlüsselung auf Spaltenebene	Kein Support
	Column Level Encryption Enterprise	Kein Support
	Cloud-Verschlüsselung mit Schlüsselverwaltung	Basis-Support
	Feldnormalisierung	Kein Support
	Flow Designer	Standard*
	Geführtes Setup	Kein Support
	Domänentrennung und IntegrationHub	Standard*
	Integrationen mit Anwendungen und Datenquellen von Drittparteien	Grundlegend+Standard
	Knowledge Management	Standard
	Hermes Messaging Service	Kein Support
	Verwaltete Dokumente	Kein Support
	MetricBase	Standard
	Natural Language Understanding	Grundlegend+Standard
	Benachrichtigungen	Standard
	ODBC-Treiber	Standard*
	Orchestration	Standard*
	Password Reset	Standard
	Platform-Sicherheit	Zielseite der Domänentrennung
	Datenschutz	Kein Support
	Predictive Intelligence	Standard
	Proaktive Auslöser	Standard
	Process Automation Designer	Standard
	Remotetabellen	Kein Support

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Produkt-Suite	Anwendung	Support-Stufe
	Zeitpläne	Standard
	Skript-Debugger	Standard
	Suchvorschläge	Kein Support
	Service Portal	Kein Support
	Domain Separation und Sidebar	Standard
	Status-Flows	Kein Support
	Subscription Management	Standard*
	Umfragemanagement	Standard*
	Task Intelligence	Kein Support
	Domänentrennung und Zeitkarten	Standard*
	UI Builder	Standard
	Virtual Agent	Standard
	Visual Task Boards	Standard
	Webservices	Standard*
	Workflow	Standard*
	Arbeitsbereich	Standard
Security Operations	Configuration Compliance	Standard
	Configuration Data Management	Standard
	IBM QRadar Offense Ingestion	Standard
	Integration der Microsoft Graph-Sicherheits-API zur Warnungserfassung	Standard
	Security Incident Response	Standard
	Threat Intelligence	Standard
	Vulnerability Response	Standard
Service Management	Facilities Service Management	Standard
	Geplante Wartung	Standard*
	Proaktive Auslöser	Standard
	NOW Code-Editor	Kein Support
	Personaloptimierung für ITSM	Standard
	Vendor Management-Arbeitsbereich	Standard

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Empfohlene Domain Separation-Verfahren für Service Provider

Sie können Domain Separation für Ihre Anwendungen und Services erstellen, implementieren und verwalten.

Domänengrundlagen

Mit Domain Separation (auch bezeichnet als ServiceNow Multitenant Platform Architecture) können Sie die Anwendungsdaten, die Anwenderoberfläche und die Geschäftslogik in einer einzigen Kundeninstanz trennen, die hierarchische Modellierung mit mandantenübergreifender Intelligenz unterstützt. Die Geschäftslogik beschreibt, wie die Domänentrennung konfiguriert wird und welche Regeln sich auf die Konfiguration auswirken.

Bevor Sie mit der Domain Separation beginnen, finden Sie hier einige bewährte Vorgehensweisen. Wählen Sie die gewünschten Themen aus, oder folgen Sie ihnen der Reihe nach, indem Sie auf die Links unter dem Bild klicken.



Erklärung zu Domain Separation

Mit Domain Separation können Sie Anwendungsdaten, UI und Geschäftslogik, wie z. B. Regeln oder Workflows, in einer einzigen Kundeninstanz trennen. Durch die Aufteilung dieser Elemente in logisch definierte Domänen werden bestimmte Hierarchien für alle Kunden unterstützt, die Ihre Anwendungen verwenden.

Domänengrundlagen

Domain Separation, auch bekannt als ServiceNow Architektur der mehrinstanzenfähigen Plattform, verursacht erheblichen Aufwand für die Verwaltung einer Instanz. Wenn Sie Domain Separation jedoch richtig verwenden, kann dies die Effizienz verbessern, die Sicherheit erhöhen und die Leistung der Instanzen Ihrer Kunden steigern.

Einige globale Standards und Eigenschaften (z. B. Systemeigenschaften und Tabellenschema) können nicht nach Mandanten getrennt werden.

Lesen Sie die folgenden Richtlinien, bevor Sie mit der Trennung von Domänen beginnen.

Automatische Übersetzung

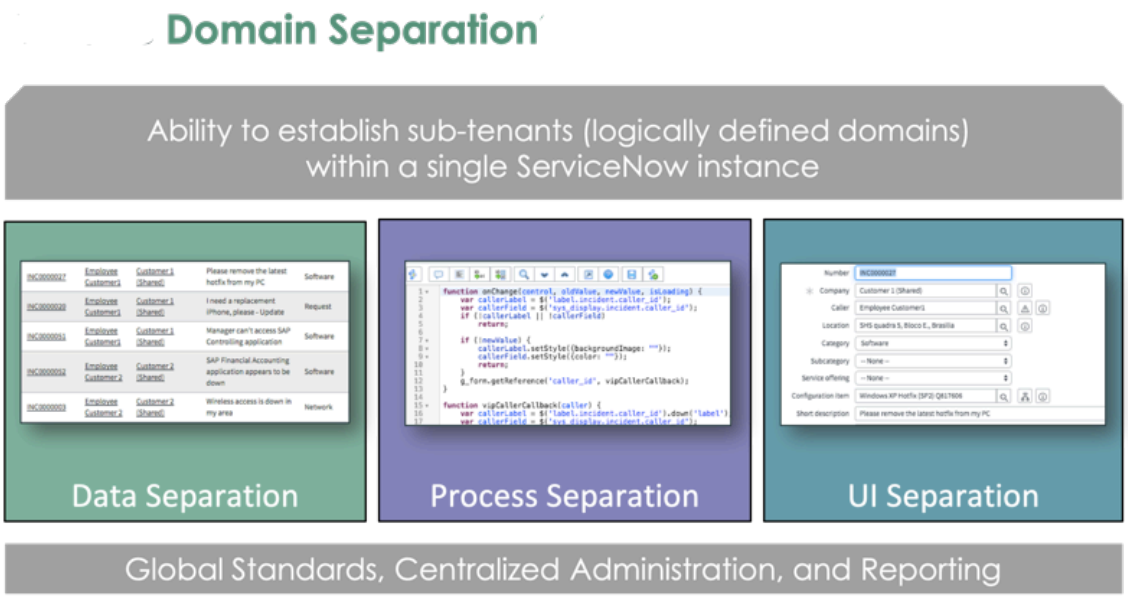
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Möglichkeiten der Domänentrennung

- Datentrennung: Ermöglicht Mandanten der Domäne, nur Daten anzuzeigen, für die sie berechtigt sind. Mandanten können Zugriff auf andere Mandantendaten gewährt werden, sie können jedoch keine Mandantendaten abfragen, auf die sie keinen Zugriff haben.
  - Wenn Sie Datensätze aktualisieren, generieren sie keine Update Set-Datensätze.
  - Benutzer, einschließlich der Kundenkonten, die für Integrationen verwendet werden, sehen nur die Daten in den Domänen, auf die sie zugreifen dürfen.
  - Kunden, Service Desk-Mitarbeiter und Erfüller sehen Daten, die sich auf die von ihnen unterstützten Kunden und Organisationen beziehen.
- UI-Trennung: Unterstützt eine mandantenspezifische Experience für UI-Elemente wie Ansichten, Listen, Bezeichnungen usw.
  - Sie können die browserbasierte Anwenderoberfläche einschließlich Anwendungsmenüs, Listen, Formularen und Dashboards überschreiben. Sie können sie auch für eine bestimmte Domäne oder eine Reihe von Domänen anpassen und gleichzeitig Ihre grundlegende Prozesslogik beibehalten.
  - Service Provider können das angezeigte Branding und die UI-Elemente ändern, um individuelle Kundenbedürfnisse zu erfüllen.
- Geschäftslogiktrennung: Erstellt mandantenspezifische Systemrichtlinien wie E-Mail-Benachrichtigungen, Geschäftsregeln, Clientskripts, UI-Richtlinien und UI-Aktionen.
- Hierarchische Modellierung: Verschachtelt mehrere Mandanten, sodass übergeordnete Mandanten auf untergeordnete Mandantenressourcen zugreifen können. Die Geschäftslogik für übergeordnete Mandanten wird automatisch für untergeordnete Mandanten ausgeführt, die Sie auf jeder Ebene überschreiben können.
- Mandantenübergreifende Intelligenz: Verarbeitet automatisch Daten, Metadaten, Geschäftslogik und Verarbeitungskontext für Mandanten mit Zugriff auf zusätzliche Mandantendaten.

Domain Separation auf einen Blick

Die folgende Grafik zeigt die Aufteilung von Daten, den Prozess und die UI-Trennung. Diese Konzepte werden im Abschnitt „Empfohlene Vorgehensweisen“ ausführlich behandelt.



Automatische Übersetzung

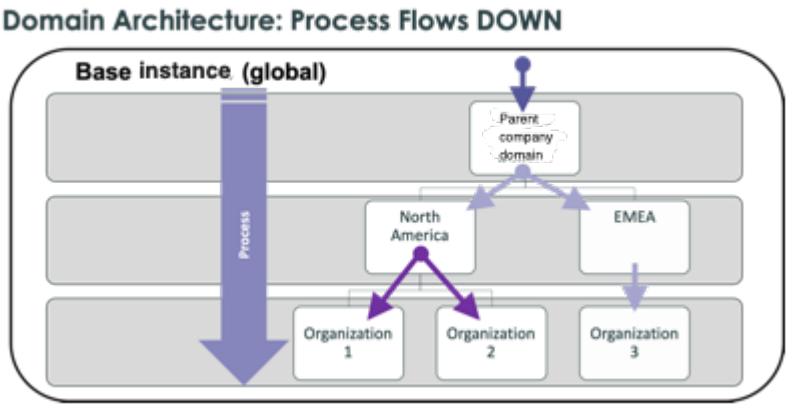
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Domänenarchitektur

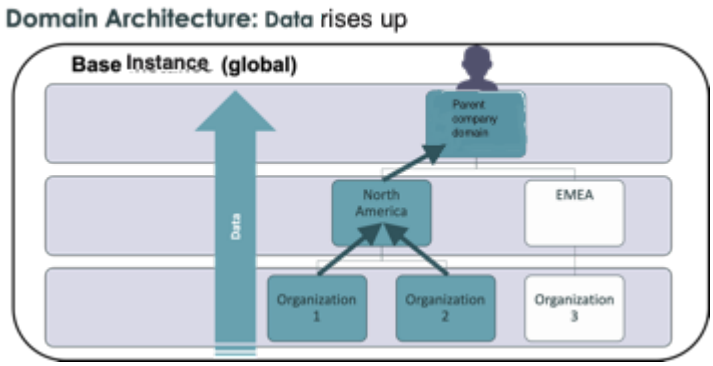
Benutzerdatensätze werden einem Domänenwert zugewiesen, der die Stammdomäne des Benutzers darstellt. Benutzer haben keinen Zugriff auf Daten in übergeordneten Domänen, Peer-Domänen oder Domänen in anderen Verzweigungen der Hierarchie.

Erweiterte Optionen zum Gewähren von zusätzlicher Domänentransparenz finden Sie unter Enthält Abfragen und Domänenzugriff.

Das folgende Diagramm zeigt, wie der Architekturprozess bis zu den untergeordneten



Domänen abläuft.



Wertversprechen für Domain Separation

Mit Domain Separation können Service Provider über eine mehrinstanzenfähige Instanzarchitektur verfügen, die Angebote effizient und sicher für ihre Kunden bereitstellt. Strenge universelle Prozessstandards, datengesteuertes Prozessdesign, strikte Governance und eine zentralisierte Administration tragen dazu bei, diese Vorteile zu maximieren.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorteile von Domain Separation

Die Mandanten einer Domäne profitieren von einem schnellen ROI, einem geringeren Verwaltungsaufwand und der Nutzung der von Instanzbesitzern bereitgestellten Business Services.

Hier erhalten Sie eine kurze Übersicht über diese Vorteile.

Besitzer der Instanz	Domänenmandanten
Mitarbeiterproduktivität des Service Providers	Mehr Sicherheit
Es werden nur Delta-Prozesse verwaltet	Vorgefertigte Prozesse und Funktionen von
Effizienzen der Administration	Weniger Personal erforderlich
Weniger Clientintegrationen	Schnelleres Onboarding
Upgradefähigkeit und Skalierbarkeit	Nutzung der neuesten Releases
Datentrennung	Vom Besitzer der Instanz bereitgestellte Services
Globale Berichterstellung	

Definition von Domain Separation

Mit Domain Separation (auch bekannt als ServiceNow® Multitenant Platform Architecture) können Sie Anwendungsdaten, UI und Geschäftslogik in einer einzigen Kundeninstanz trennen, die hierarchische Modellierung mit mandantenübergreifender (Kunden-)Intelligenz unterstützt.

Eigenschaften für Domain Separation

Domänengetrennte Anwendungen ServiceNow werden mit den folgenden Eigenschaften definiert:

Datentrennung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ermöglicht Kunden, nur die Daten anzuzeigen, für die sie berechtigt sind. Kunden kann Zugriff auf andere Kundendaten gewährt werden, sie können jedoch keine Kundendaten abfragen, wenn sie keinen Zugriff haben.

UI-Trennung

Unterstützt eine kundenspezifische Experience für UI-Elemente wie Ansichten, Listen, Bezeichnungen usw.

Trennung der Geschäftslogik

Unterstützt kundenspezifische Systemrichtlinien wie E-Mail-Benachrichtigungen, Geschäftsregeln, Clientskripts, UI-Richtlinien und UI-Aktionen.

Hierarchische Modellierung

Unterstützt geschachtelte Mehrinstanzenfähigkeit, sodass übergeordnete Mandanten (Kunden) auf untergeordnete Kundenressourcen zugreifen können. Die Geschäftslogik für übergeordnete Kunden wird für untergeordnete Kunden automatisch ausgeführt und kann auf jeder Ebene überschrieben werden.

Kundenübergreifende Intelligenz (Domänenbereich)

Verarbeitet automatisch die Daten, Metadaten, die Geschäftslogik und den Verarbeitungskontext für Mandanten, die Zugriff auf zusätzliche Mandantendaten haben.

Domain Separation-Hierarchien

Erstellen Sie beim Definieren einer Domänenarchitektur eine Hierarchie, um Ihre Prozesse und Workflows zu nachzuverfolgen.

Beispiele für Domain Separation-Hierarchien

Das folgende Diagramm ist ein guter Ausgangspunkt für die Definition der Domänenarchitektur. Es zeigt die Beziehung zwischen den TOP- und den untergeordneten Domänen und wie sich der Prozess, die Daten und die Geschäftsregeln auf die übergeordneten und untergeordneten Domänen auswirken.

- Im folgenden Beispiel ist TOP eine Prozessdomäne. Sie darf keine Benutzer enthalten. Eigentlich sollte TOP die neuen Prozesse enthalten, die die Eigentümer der Instanzen entwickeln, sowie die Überschreibungen zu diesen Prozessen aus der globalen Domäne.
- Nur der Service Provider (SP) hat Zugriff auf die Standarddomäne. Diese Domäne enthält keine aktiven Benutzer. Die Domäne enthält nur die „verlorenen“ Daten, die Sie der richtigen Domäne neu zuweisen müssen.

  Hinweis: Wenn Daten keiner bestimmten Domäne zugewiesen sind, werden sie in die Standarddomäne verschoben. Sie gehen vorübergehend „verloren“ und müssen der richtigen Domäne zugewiesen werden.

- Aufgaben und Benutzer ohne Domäne werden beim Erstellen oder Aktualisieren von Domänen automatisch in der Standarddomäne eingefügt. Sie können diese Aktion überschreiben, indem Sie entweder die Option **Standard** für diesen Datensatz deaktivieren oder die Option **Standard** für einen anderen Domänendatensatz auswählen. Wenn Sie noch keine Standarddomäne festgelegt haben, werden Aufgaben und Benutzer ohne Domäne in die globale Domäne verschoben.
  - Verschieben Sie keine Daten zwischen Domänen, während Sie die Instanz verwenden.
  - Wenn Daten in der Standarddomäne landen, bedeutet dies, dass Sie ein Konfigurations- oder Verfahrensproblem haben.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

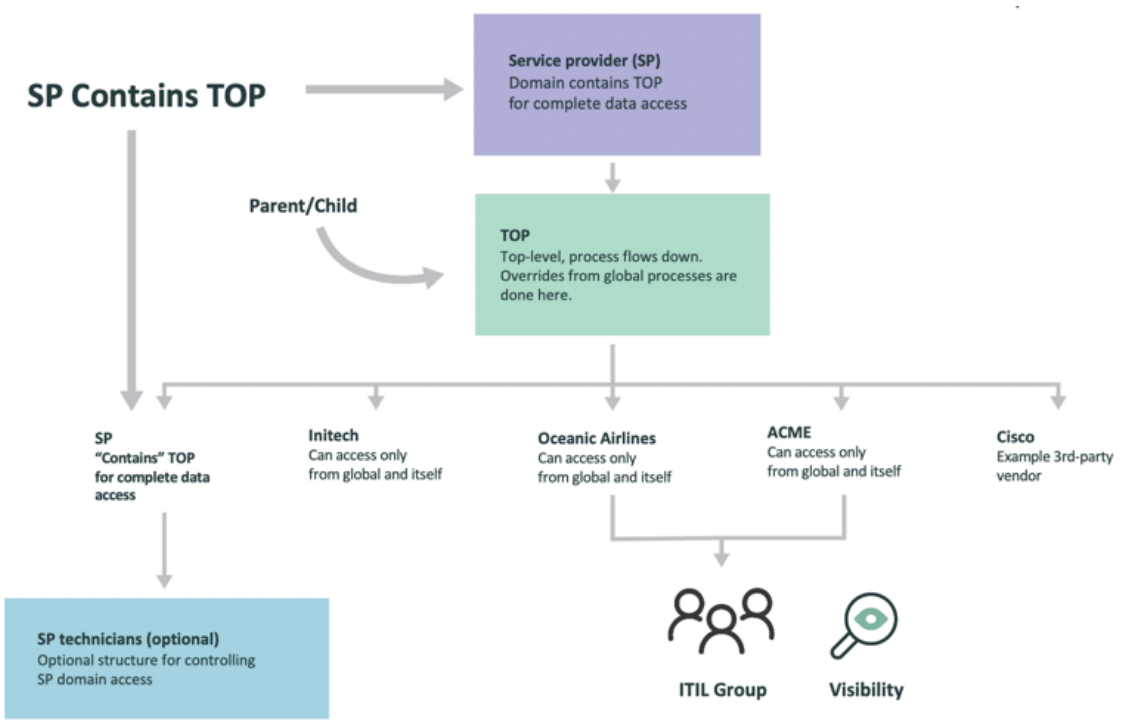
Das Wort „Global“ wird in diesem Diagramm nicht angezeigt, da keine globale Domäne vorhanden ist. Denken Sie daran, dass „global“ das Fehlen einer Domäne in einem Datensatz bezeichnet.

Eine Tabelle ohne Domänenfeld bedeutet beispielsweise, dass die Tabelle alle globalen Datensätze enthält. Eine Tabelle mit einem Domänenfeld bedeutet, dass jeder Datensatz ohne Domäne eine globale Domäne ist.

Das Wort „global“ befindet sich im Domänenfeld. Es wird automatisch dort platziert, wenn der Datensatz keine Domäne hat.

Globale Datensätze sind für alle Benutzer der Instanz verfügbar, sofern sie nicht durch Sicherheitskonfigurationen eingeschränkt werden.

- Verwenden Sie die Standarddomäne, um sicherzustellen, dass Datensätze nicht in der globalen Domäne in Tabellen landen, die niemals globale Datensätze enthalten dürfen.
- Die Besitzer eine Instanz müssen dann die Datensätze in der Standarddomäne selektieren und in die richtige Domäne verschieben.



Domänenhierarchien

- Über-/untergeordnet: betroffener Prozess und betroffene Daten
  - Design, das auf einem Prozess-Flow basiert.
  - Denken Sie daran, dass die übergeordneten Domänen auf alle Daten in den untergeordneten Domänen zugreifen können.
- Domäne „Enthält“: Nur Daten sind betroffen. Beispiel: Wenn SP im Diagramm „TOP“ enthält, werden Prozesse in SP nicht in der Domäne „TOP“ und abwärts ausgeführt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Gewährt Personen in Gruppen Datenzugriffsrechte, die dedizierten Zugriff auf bestimmte Domänen erfordern.
- Enthält Ursachen oder Bedingungen, die Datenbankabfragen hinzugefügt werden sollen, die Leistungsprobleme bei großen Domänen und Datensätzen verursachen können

- Sichtbarkeit: Hierarchie, die für Benutzer immer sichtbar ist, sobald Sie Zugriff gewähren. Nur die Daten sind betroffen, nicht die Prozesse.
  - Gewährt einer anderen Domäne, die beim Erstellen der über- und untergeordneten Hierarchie keinen Zugriff hatte, Datenzugriff auf eine Domäne
  - Ermöglicht es Benutzern, alle Daten in den Domänen zu sehen, für die sie Sichtbarkeitszugriff haben, und zwar jederzeit, unabhängig von dem Datensatz, an dem sie gerade arbeiten

> **Hinweis:** Gehen Sie sparsam damit um, da mit „Sichtbarkeit“ vollständiger Zugriff gewähren werden kann, was Sie möglicherweise nicht beabsichtigen.

Grundprinzipien der Definition einer Domänenhierarchie

Uneingeschränkte und eingeschränkte Anwendungsfälle für Domänentrennung.

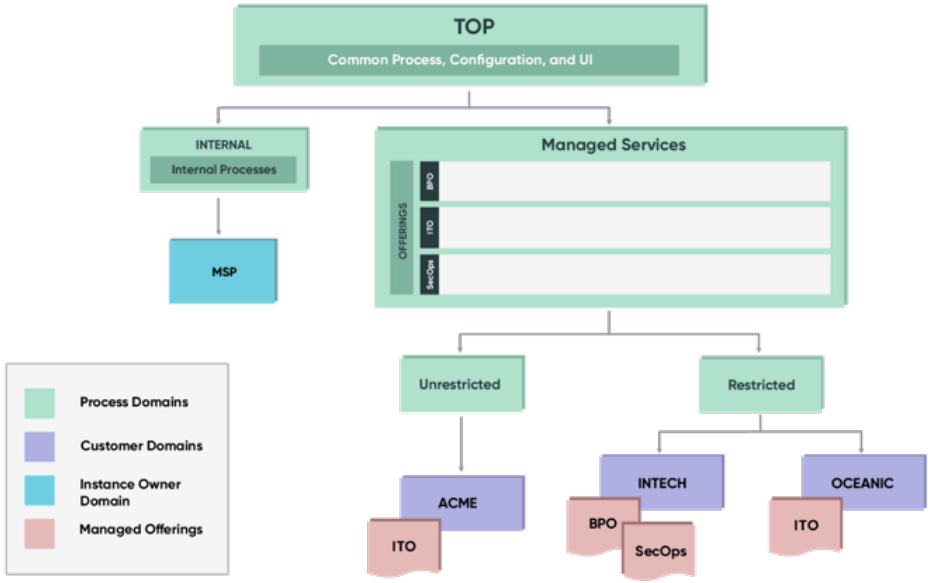
Viele SPs haben Kunden, die implizit angeben, dass der Zugriff auf ihre Domänen streng reguliert werden muss, was die Verwendung der Funktion „Enthält“ in der TOP-Domäne einschränkt. Das folgende Diagramm erläutert, wie diese Regelung durch die Unterteilung der Domänen in eingeschränkte und unbeschränkte Domänen abgeschwächt werden kann.

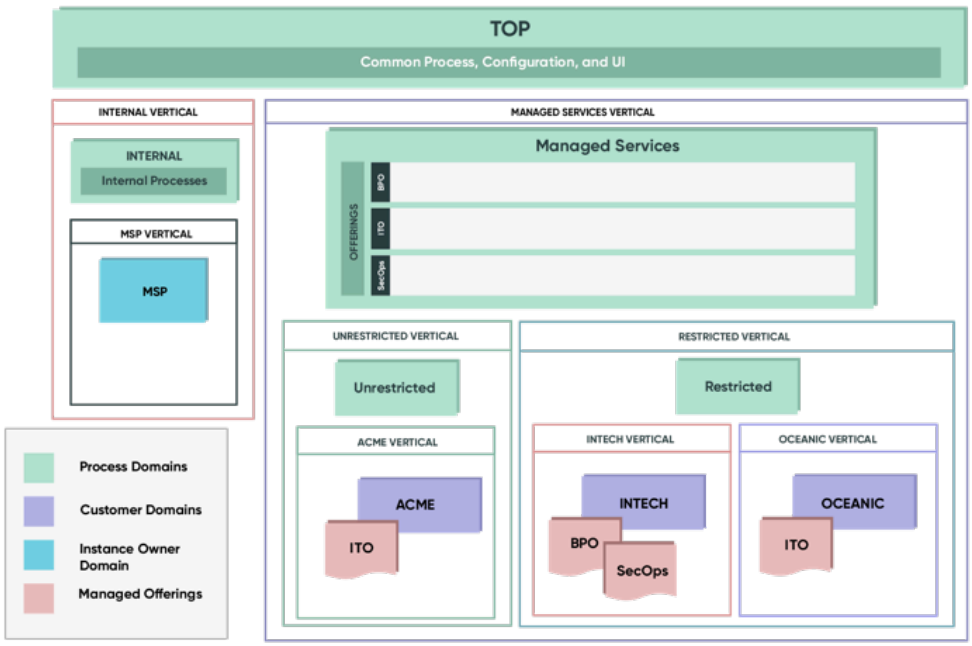
1. Kunden befinden sich in einer bestimmten „Vertikalen“ der Hierarchie der Domänentrennung. Dies bedeutet, dass sie nur Prozesse nutzen, die in ihrer Domäne und allen übergeordneten Domänen in der Hierarchie definiert sind. Alle Prozesse, die in Domänen definiert sind, die sich nicht in ihrer linearen Übergeordnet-Untergeordnet-Hierarchie befinden, gelten nicht.

   > **Hinweis:** Kunden oder „Mandanten“ sind Entitäten, die vollständig voneinander getrennt sind, nicht wie Abteilungen oder Geschäftsbereiche, die Ressourcen gemeinsam nutzen.

2. Strikt vertikale Einheiten (beschränkt, Managerservices usw.) sind zulässig, solange die Kunden nur zu einer von ihnen gehören.
3. Services, Produkte oder Angebote, die für alle Kunden horizontal verfügbar sein müssen, werden nicht in separaten Domänenhierarchien definiert.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.





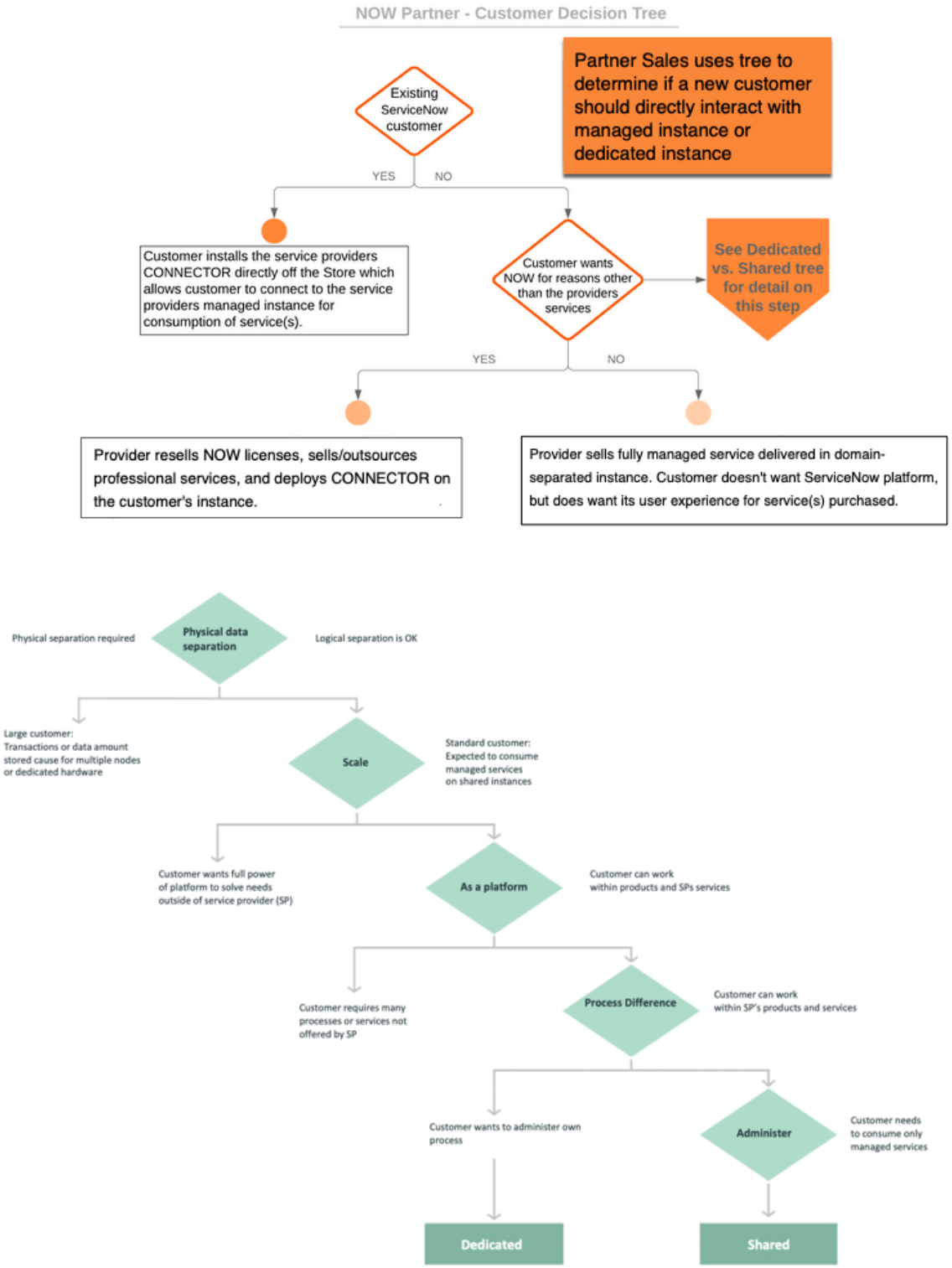
Hier sind einige beispielhafte Anwendungsfälle:

- Sie können beispielsweise unter TOP zwei Domänen erstellen: Nicht beschränkt und Beschränkt.
  - Platzieren Sie Kunden, die keine SP-Sichtbarkeitsbeschränkungen haben, zusammen mit ihren Domänen unter „Nicht beschränkt“.
  - Platzieren Sie Kunden, die diese Anforderung haben, zusammen mit ihren Domänen unter „Beschränkt“.
- Systemadministratoren können dann die Funktionen „Enthält“ und „Sichtbarkeit“ effizient und gezielt verwenden.
  - Wenden Sie „Enthält“ auf „Nicht beschränkt“ an, sodass ein einziges „Enthält“ den meisten Kunden Sichtbarkeit gewähren kann.
  - Wenden Sie die Domänensichtbarkeit bei Bedarf mithilfe von „Domänensichtbarkeitsgruppen“ auf bestimmte Domänen an.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kundenentscheidungsbäume

Das folgende Diagramm zeigt, wie Sie das richtige Hierarchiemodell auswählen. Sie können separate Hierarchien, Hybrid-Hierarchien oder freigegebene Hierarchien auswählen, je nachdem, welche Prozesse und Funktionen Sie in Ihren Domänenstrukturen benötigen.



Weitere Informationen zur Hierarchiearchitektur finden Sie unter Referenzarchitektur des Service Providers.

Automatische Übersetzung

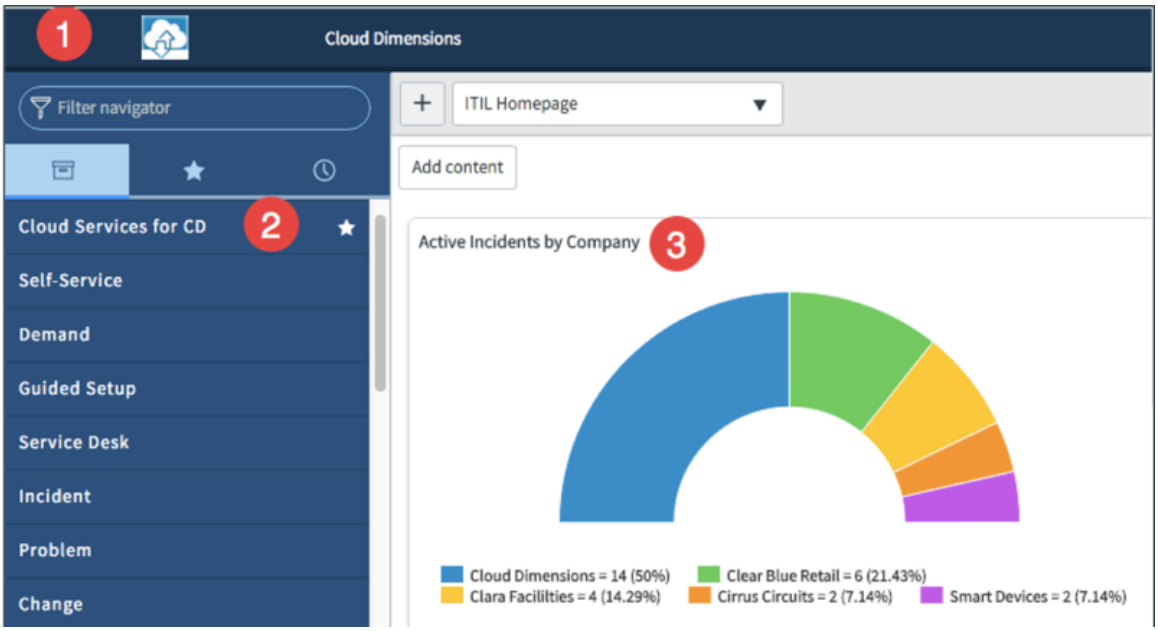
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kontext- und Domänentrennung

Der Kontext der Sitzung eines Benutzers bestimmt die Prozesse, Daten und die Anwenderoberfläche (UI), wenn der Benutzer durch Listenansichten, Homepages, Berichte und Wissensartikel navigiert. Der Kontext wird durch die von Ihnen erstellten Prozesse, die von Ihnen festgelegten Geschäftsregeln, Ihre Workflows und andere Faktoren bestimmt.

Anwendersitzungskontext

Viele Faktoren bestimmen den Kontext einer Benutzersitzung, z. B. Benutzerprofile, Gruppen, Unternehmenskriterien usw. Im folgenden Diagramm sehen Sie, dass die von einem Unternehmen erstellten Incidents Teil des -Kontexts sind.



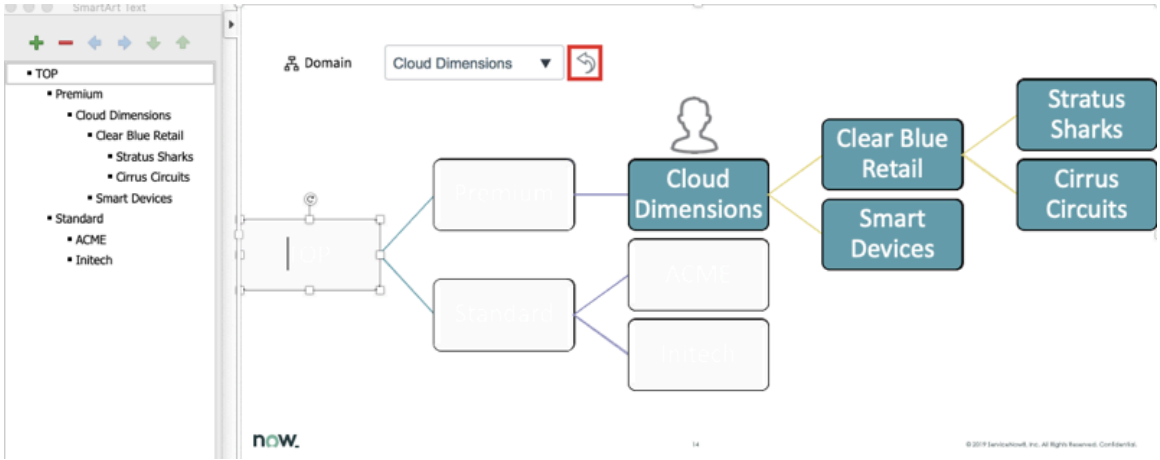
Der Benutzer in diesem Beispiel hat eine Stammdomäne von Cloud Dimensions.

1. Das Branding spiegelt die Einstellungen in der Cloud Dimensions-Domäne und im Unternehmensdatensatz wider.
2. Der Anwendungsnavigator zeigt die Elemente, die von Domänen höherer Ebenen übernommen werden, sowie die Module, die in der Domäne „Cloud Dimensions“ definiert sind.
3. Die Homepages und Listendaten spiegeln die Daten wider, die für den Benutzer sichtbar sind. Diese Daten basieren auf dem Sitzungskontext des Anwenders. In diesem Fall kann der Benutzer in der Cloud Dimensions-Domäne die Daten in Cloud Dimensions, in untergeordneten Domänen und in der globalen Domäne anzeigen.

Der Kontext der Benutzersitzung beginnt in der Stammdomäne

Im folgenden Diagramm sehen Sie die Elemente des -Kontexts.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Der Systemadministrator legt die Stammdomänen von Benutzern in ihren Benutzerdatensätzen fest. In der Regel wird für die Stammdomäne eines Benutzers dieselbe Domäne verwendet wie für die Domäne des Unternehmens. Wenn sich der Benutzer anmeldet, wird die Domänenauswahl automatisch auf die Stammdomäne des Benutzers festgelegt. Benutzer können jederzeit zu ihrer Stammdomäne zurückkehren, indem sie in der Domänenauswahl auf das Pfeilsymbol klicken.

Die Liste der Domänenauswahl enthält Domänen innerhalb des Sitzungskontexts des Benutzers. Benutzer können ihren Sitzungskontext weiter einschränken, indem sie mit der Auswahl untergeordnete Domänen auswählen.

Der Kontext der Benutzersitzung umfasst die Stammdomäne des Benutzers und alle untergeordneten Domänen. Dieser Satz von Domänen im Sitzungskontext des Benutzers wird automatisch an jede Abfrage angehängt, die an die Datenbank gesendet wird. Auf diese Weise werden die Ergebnisse auf die Daten in diesen Domänen und auf globale Daten beschränkt. Dieser Prozess ist in den kompilierten Code eingebettet, auf den nicht zugegriffen werden kann.

Servicekonten, die für Integrationen verwendet werden, verfügen ebenfalls über einen Benutzersitzungskontext. Es gibt einen Benutzerkontext und einen Datensatzkontext mit jeweils eigenen Daten in einer eigenen Domäne. Diese Kontexte wirken sich auf die Integrationen aus. Datenbankabfragen (Datensätze) sind genauso eingeschränkt wie interaktive Anwender (Anwender), was bedeutet, dass sie normal funktionieren, aber durch die vom Entwickler konfigurierten Einschränkungen eingeschränkt werden.

Weitere Informationen zum Hinzufügen von Domänen zum Sitzungskontext eines Benutzers finden Sie unter Referenzarchitektur des Service Providers.

Datensatzkontext

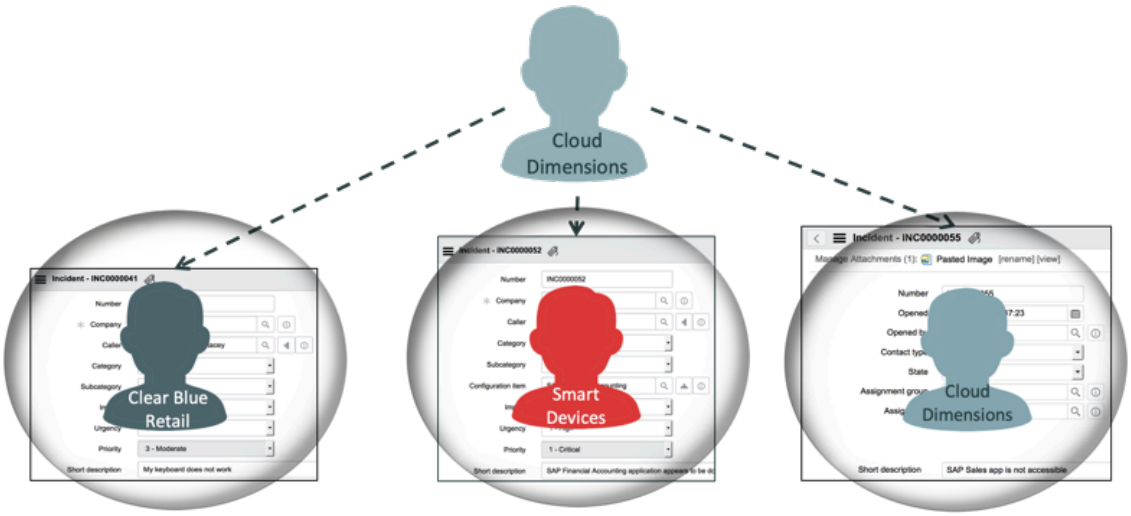
Wenn ein Benutzer einen Drilldown in einzelne Datensätze durchführt, wird der Datensatzkontext aktiviert. Der Datensatzkontext bestimmt die UI-Elemente und Prozesse, die auf den Datensatz angewendet werden sollen.

Die Domäne eines Datensatzes bestimmt den Prozess, die Daten und die Verfügbarkeit von UI-Elementen innerhalb des Datensatzes.

Hinweis:

- Der Datensatzkontext bleibt erhalten, auch wenn sich die Domäne des Benutzers ändert.
- Benutzer können Datensätze gleichzeitig auf mehreren Browserregisterkarten anzeigen und dabei ihren eigenen Datensatzkontext beibehalten.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

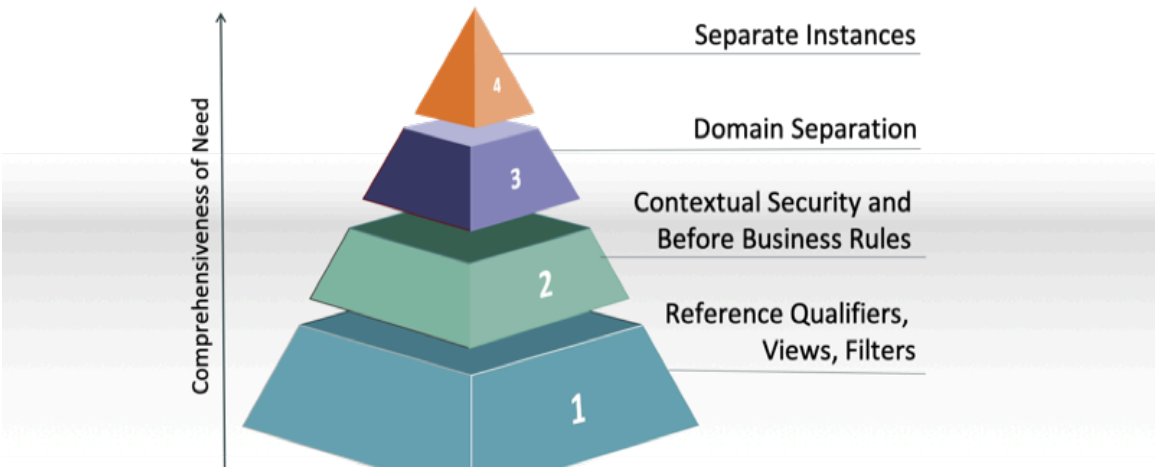


Daten durch Domain Separation trennen und sichern

Abhängig von den Anforderungen Ihrer Kunden können Sie Daten auf der Plattform ServiceNow auf verschiedene Arten trennen und schützen.

Daten werden auf mehrere Arten getrennt

Das folgende Diagramm zeigt vier Möglichkeiten zum Trennen von Daten. Sie können separate Instanzen, Domänentrennung, kontextbezogene Sicherheits- und Geschäftsregeln sowie die Referenzarchitektur selbst verwenden, um Daten zu trennen.



Sie können Daten auf die folgenden vier Arten trennen:

1. Anpassung der Referenzarchitektur mit Qualifizierern und Filtern, damit sich Abteilungen und Gruppen innerhalb eines Unternehmens auf ihre eigene Arbeit konzentrieren können Durch die Trennung der Daten zwischen diesen Abteilungen oder Gruppen kann eine Abteilung oder Gruppe die Datensätze einer anderen Abteilung oder Gruppe nicht anzeigen.
2. Hinzufügen von Kontextsicherheit und Business-Regeln „Vor Abfrage“ als zusätzliche Sicherheitsebenen zum Schutz vor Datenschutzverletzungen. Weitere Informationen zu

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Domain Separation und Geschäftsregeln finden Sie unter Kontext- und Domänentrennung und Business-Regeln „Vor Abfrage“..

3. Hinzufügen einer weiteren Sicherheitsebene in einem Unternehmen durch Domänentrennung. Die Daten aus jeder Datenbankabfrage sind auf die Daten beschränkt, die in einer Domäne sichtbar sind, bevor kontextbezogene Sicherheits- und Business-Regeln ausgeführt werden.
4. Durch die Verwendung separater Instanzen zur Trennung der Daten auf Datenbank- und Anwendungsebene

Getrennte Instanzen, Domänentrennung, kontextbezogene Sicherheits- und Geschäftsregeln sowie die Referenzarchitektur sind Möglichkeiten zur Trennung von Daten. Diese vier Möglichkeiten stehen miteinander in Beziehung, wie durch den Pfeil für die Vollständigkeit des Bedarfs im Diagramm angezeigt. Wie jede Ebene mit den anderen Ebenen interagiert, hängt davon ab, wie Sie Ihre Domain Separation-Konfiguration einrichten.

Nicht alle Organisationen benötigen Domain Separation. Möglicherweise finden Sie andere Alternativen, z. B. separate Instanzen oder eine einzelne Instanz ohne Domäne. Weitere Informationen zu diesen Alternativen finden Sie unter Bewertung der Notwendigkeit einer Domänentrennung.

Mandantenübergreifende Intelligenz

Bei einer Multi-Mandanten-Architektur werden mehrere Mandanten von einer einzigen Instanz bedient. Daten, Metadaten, Geschäftslogik und Verarbeitungskontext für Mandanten werden automatisch mit Zugriff auf zusätzliche Mandantendaten behandelt.

Einzel- oder Mehrfachmandanten

Instanz mit einem Mandanten

Sie sind Kunde von ServiceNow, haben die -Lizenzen erworben, und Sie können entscheiden, welche Services Sie wünschen. Sie können bei Bedarf ein Upgrade durchführen, Vorschauen auf die tollen neuen Funktionen anzeigen und Ihre Instanz sofort konfigurieren. Als Einzelmandant gelten die folgenden Vorteile und Einschränkungen:

- Die Vorlaufkosten und der Verwaltungsaufwand sind zwar höher, aber die Möglichkeiten zur Umgestaltung und Erweiterung sind größer.
- Die Anschaffung und Wartung der Instanz und des Verwaltungspersonals sind höher. Sie können die Umgebung zwar nach Bedarf gestalten, Sie müssen jedoch die ServiceNow empfohlenen Vorgehensweisen und Standards einhalten.

Instanz mit mehreren Mandanten

Eine andere Person besitzt die Instanz, möglicherweise ein Service Provider mit mehreren Kunden. Sie upgraden, wann sie möchten, und fügen neue Services für die Instanz hinzu, wenn sie möchten. Wenn Sie Kunde eines Service Providers sind, befinden Sie sich höchstwahrscheinlich in dessen Instanz, weil Sie möchten, was der Service Provider anbietet. Für mehrere Mandanten gelten die folgenden Vorteile und Einschränkungen:

- Konfigurationen, Integrationen und Upgrades werden von einem zentralen -Mitarbeiter verwaltet.
- Der Besitzer der Instanz stellt zusätzliche Services bereit.
- Domänenmandanten haben geringere Anschaffungskosten für die Nutzung der Plattform ServiceNow, niedrigere monatliche Kosten, da sie die Plattform

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

mit vielen Mandanten gemeinsam nutzen, und müssen keine Mitarbeiter für die Verwaltung der Umgebung einstellen.

- Vorteile, die aus Anforderungen oder Changes geteilt werden, die von anderen Mandanten initiiert werden.

Alternativen zu Domain Separation

Alternativ zur Domänentrennung können Sie für Ihre Kunden eine separate Instanz verwenden. Eine separate Instanz bietet Ihnen die Flexibilität, die Anforderungen für die Datentrennung innerhalb der Gruppen und Abteilungen in einer Organisation mit minimalen bis keinen Auswirkungen auf andere zu erfüllen.

Separate Instanzen

Vor- und Nachteile separater Instanzen

Separate Instanz	Einzelne Instanz – ohne Domäne
Vorteile	**Vorteile**
Passt auf jeden Kunden/jede Organisation zu	Kann einfache Szenarien behandeln
Minimieren Sie die Auswirkungen der Anpassung auf andere	Kosten
Release-Zeitplankoordination	**Kons**
Ordnungsgemäße Trennung	Umfangreiche Änderungen am Baselinecode
Wählen Sie die DATACENTER-Region	Geänderter Basissystemcode während Upgrades übersprungen
Kons	Muss auch alle sekundären und unterstützenden Tabellen behandeln
Kosten	Umfangreiche Tests erforderlich
Ausrichtung von Instanzen	Kein ServiceNow -Produktteam für die Entwicklung Ihres anwenderdefinierten Codes
Testaufwand für Upgrades	
Doppelter Aufwand	
Integrationen erforderlich	

Sie können den Zeitpunkt für Upgrades und Releases für jede Instanz separat festlegen. Wenn Sie sich jedoch für die Verwendung separater Instanzen entscheiden, müssen Sie sich intensiv mit anderen Personen abstimmen, die die Instanzen verwalten. Durch die Konfiguration einer Instanz mit kontextbezogener Sicherheit, Formularansichten, Referenzqualifizierern, Filtern und robusten Bedingungen müssen Sie in Ihrem Unternehmen keine Domänentrennung verwenden.

Mit einer separaten Instanz können Sie die Trennung von Daten und Prozessen ermöglichen, die Besitzer der Instanz müssen jedoch die umfangreichen Anpassungen verwalten, die für separate Instanzen erforderlich sind.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Kontext- und Domänentrennung

Referenzarchitektur des Service Providers

Bewertung der Notwendigkeit einer Domänentrennung

Sie werden möglicherweise feststellen, dass die Domänentrennung für die Organisationen Ihrer Kunden nicht immer funktioniert. Am besten stützen Sie Ihre Entscheidung für Domain Separation auf die Bedürfnisse Ihrer Kunden.

Bewertung der Notwendigkeit einer Domänentrennung

Gründe für Domain Separation

Die folgenden Faktoren können Ihnen bei der Entscheidung für Domain Separation für die Organisationen Ihrer Kunden helfen:

- Ihre Kunden haben eine moderate Ausrichtung der Prozesse und allgemeinen Plattformanforderungen.
- Ihre Kunden planen, an Aufgaben als Erfüller und nicht als anfordernde Personen zu arbeiten.
- Ihre Kunden haben eine vertragliche Vereinbarung, die die Isolierung von Datensätzen erfordert, aber der Besitzer der Instanz hat festgestellt, dass die Anforderung möglicherweise an anderer Stelle in der Konfiguration behandelt wird.
- Die Instanzbesitzer Ihres Unternehmens haben ganze Entitäten, die als physisch getrennte Organisationen arbeiten und keine Daten gemeinsam nutzen. Eine vollständige Berichterstellung ist jedoch erforderlich. Getrennte Domänen würden bei richtiger Konfiguration Datentransparenz ermöglichen.

Gründe für keine Domänentrennung

Die folgenden Faktoren können auf Gründe hinweisen, warum die Organisationen Ihrer Kunden möglicherweise keine Domänentrennung einrichten möchten:

- Ihre Kunden möchten ihre Umgebung verwalten, vollständig besitzen und die Roadmap für Erweiterungen festlegen.
- Ihre Kunden möchten, dass die Daten und Prozesse auf physischer Ebene oder Datenbankebene vollständig isoliert sind.

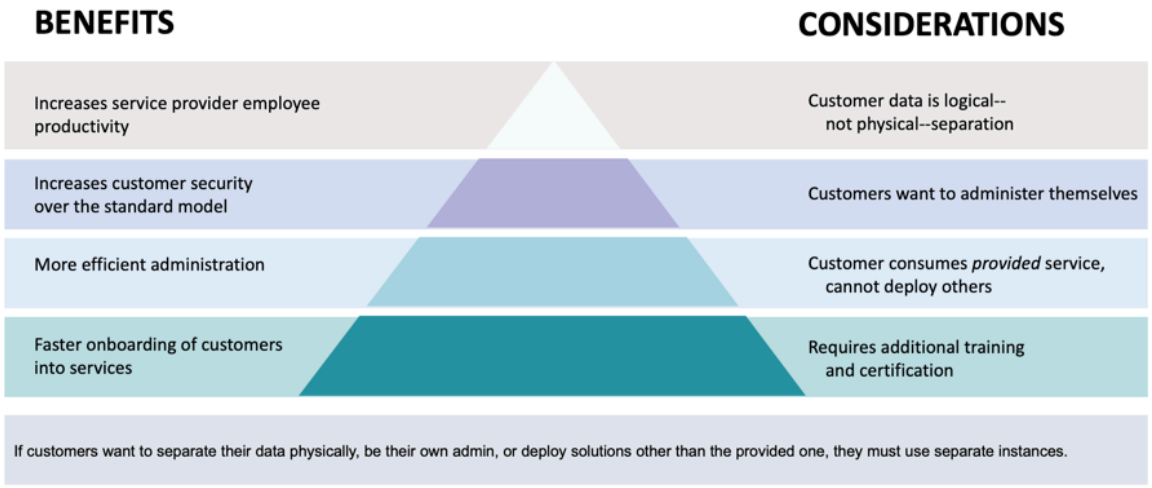
Hinweis:

Domänengetrennte Instanzen enthalten eine gemeinsam genutzte Datenbank, sodass die Isolationsanforderung unterminiert wird.

- Abteilungen in der Organisation Ihrer Kunden möchten Datensätze isolieren. (Zugriffssteuerungen können ausreichen.)
- Ihre Kunden möchten alle ihre eigenen Prozesse, Geschäftsregeln und Workflows.
- Die Unternehmenskultur ist gekennzeichnet durch die Nichtzusammenarbeit zwischen den Organisationen Ihrer Kunden.
- Ihre Kunden interagieren nur mit der Plattform als Endanwender.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

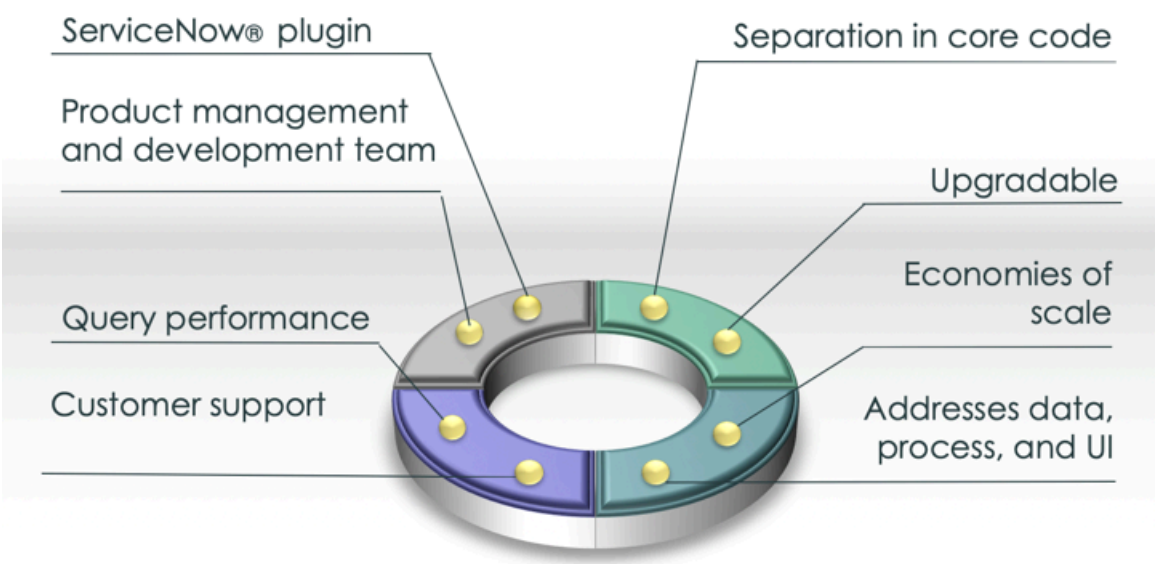


Vorteile von Domain Separation

Domain Separation funktioniert möglicherweise besser für die Organisationen Ihrer Kunden als jede andere Methode zur Trennung der Daten zwischen Gruppen und Abteilungen.

Vorteile der Domänentrennung auf einen Blick

Sie können Domain Separation mit dem Plugin ServiceNow aktivieren, dessen Funktionalität in die Core-Plattform integriert ist. Die Konfiguration der separaten Domänen wird von einem Produktmanager verwaltet, der von einem Entwicklungsteam unterstützt wird. Erweiterungen und Korrekturen für die Funktion zur Domänentrennung sind in den -Releases ServiceNow enthalten und können von Kunden verwendet werden. Zur Unterstützung der Domänentrennung können Ihre Instanzbesitzer -Ressourcen Kundenservice und Support verwenden, z. B. das Serviceportal .



Funktionsweise einer Datenbankabfrage mit Domänentrennung

Durch die Verwendung von Datenbankabfragen mit Domänentrennung in den Anwendungen Ihrer Kunden können Sie ihre Daten schützen. Diese Abfragen beschleunigen dann die Konfigurations- und Build-Prozesse.

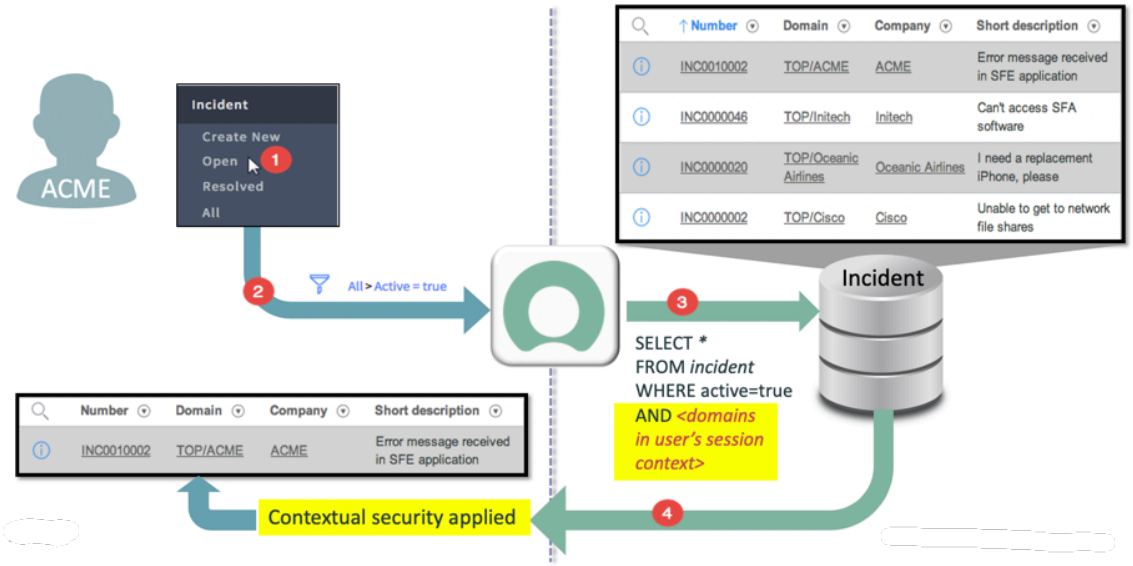
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wie Domain Separation Daten schützt

In der folgenden Abbildung besitzt die Incident-Tabelle [incident] ein Domänenfeld, das von der Aufgabe des incident geerbt wird. Wenn Sie dieses Domänenfeld sehen, wissen Sie, dass die Datensätze in der Tabelle Domänenzuweisungen haben können.

Wenn sich Benutzer anmelden, werden ihre Stammdomäne und die Domänen angezeigt, auf die sie zugreifen können. Dies wird als Sitzungskontext des Benutzers bezeichnet. Weitere Informationen zu Sitzungskontexten finden Sie unter Kontext- und Domänentrennung.

Datenbankabfrage mit Domain Separation



1. In einem Browser wählt der Benutzer von Acme, einem der Unternehmen, das Modul Offene Incidents aus, um alle Incidents anzuzeigen, für die aktiv=wahr ist.
2. Der Filter active=true wird an die Anwendung übermittelt.
3. Die Anwendung sendet dann eine Abfrage an die Datenbank, indem sie eine WHERE-Klausel an active=true anhängt. Die WHERE-Klausel beschränkt die Incident-Datensätze, die zurückgegeben werden, auf die Datensätze, die sich in der Domäne des Benutzers befinden oder in den Domänen, auf die der Benutzer zugreifen kann. Nur die Datensätze in diesen Domänen werden zur Verarbeitung an die Anwendung zurückgegeben.
4. Kontextbezogene Sicherheit wird angewendet, wodurch die Daten, die an den Benutzer zurückgegeben werden, weiter eingeschränkt werden. Die Incident-Datensätze werden in der Liste Offene Incidents angezeigt.

Hinweis:

Wenn Sie kontextbezogene Sicherheit anwenden, erstellen Sie Grenzwerte für die Daten, die an den Benutzer zurückgegeben werden. Diese Grenzwerte schützen andere Inhalte, die Anwender möglicherweise nicht sehen sollen.

Weitere Informationen zur kontextbezogenen Sicherheit finden Sie unter Kontext- und Domänentrennung.

Hinweis: Diese Verarbeitungslogik gilt für alle Abfragen an die Datenbank, einschließlich der Abfragen, die durch Integrationen ausgelöst werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterstützungsebenen für Domänentrennung

Wählen Sie aus drei Kategorien für die Domänentrennung einer Anwendung für die Organisationen Ihrer Kunden aus.

Anwendungen, die die Domänentrennung unterstützen, unterstützen möglicherweise nur die Trennung von Daten und Datenweiterleitung, verfügen über erweiterte Geschäftslogiktrennung oder unterstützen die Verwaltung der Anwendung auf Mandantenebene (Kundenebene). Diese Definitionen beschreiben die Supportstufen aus der Perspektive der tatsächlichen Anwendungsfälle und der Personen, die sie implementieren.

Inkrementelle ServiceNow Supportstufen

Basic	Standard	Enhanced
• Data is domain-separated • Logic exists to ensure proper data routing, caching, rollups, and aggregations • Global configuration operational for multiple tenants	• Application properties are domain-aware as needed • Business logic can be domain-separated by the instance owner per tenant	• Data-driven process enables failsafe configuration by tenants through the UI to drive business logic

Ebene	Typ	Zusammenfassung
Kein Support		• Das Domänenfeld kann in Datentabellen vorhanden sein, es ist jedoch keine Geschäftslogik zum Verwalten der Daten vorhanden. • Diese Ebene wird nicht als domänengetrennt betrachtet.
Standard	Kundendatenverwaltung	• Geschäftslogik: Stellt sicher, dass Daten in die richtige Domäne für die Anwendungsfälle des Service Providers der Anwendung übertragen werden. • In der Anwendung berücksichtigen die Benutzeroberfläche, Cacheschlüssel, Berichterstellung, Rollups, Zusammenfassungen usw. die Eigenschaften der Domäne zur Laufzeit. • Die Besitzer der Instanz müssen in der Lage sein, die Anwendung so einzurichten, dass sie über mehrere Mandanten hinweg normal funktioniert. Anwendungsfall: Wenn ein Service Provider den Chat verwendet, um auf die Nachricht

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ebene	Typ	Zusammenfassung
		eines Kunden zu antworten, muss der Client die Antwort sehen können.
Standard	Kundenprozessmanagement	• Enthält die Basis-Stufe • Geschäftslogik: Prozesse können vom Service Provider pro Kunde erstellt oder geändert werden. Die Anwendungsfälle spiegeln wider, wie die Anwendung von mehreren Service Provider-Kunden in einer einzigen Instanz verwendet wird. • Die Besitzer Ihrer Instanzen müssen in der Lage sein, die MVP-Geschäftslogik (Minimum des lebensfähigen Produkts) und die Datenparameter pro Kunde für die spezifische Anwendung zu konfigurieren. Anwendungsfall: Der Administrator muss in der Lage sein, Kommentare erforderlich zu machen, wenn ein Datensatz für einen Kunden geschlossen wird, aber nicht für einen anderen Kunden.
Erweitert	Selbstverwaltete Konfiguration des Kunden	• Enthält Basis- und Standard-Ebenen • Ermöglicht Kunden von Service Providern, die Geschäftslogik basierend auf definierten Anwendungsfällen zu ändern. Diese Konfigurationen sind UI-basiert und ausfallsicher, sodass Konfigurationen von einem Kunden sich nicht auf einen anderen Kunden auswirken können. • Die Kunden der Instanz müssen in der Lage sein, die MVP-Geschäftslogik und die Datenparameter selbst zu konfigurieren. Anwendungsfall: Der Kunde einer gemeinsam genutzten Umgebung muss in der Lage sein, Änderungen je nach Auswirkung, Dringlichkeit oder Priorität innerhalb einer Domäne vorzunehmen.
Effektive Domäne*		In einigen Fällen kann eine Plattformfunktion oder eine Anwendung Anwendungsfälle von Service Providern unterstützen, auch wenn das Domänen-Framework nicht verwendet wird. Die Anwendungsfälle müssen detailliert sein, um die Domänentrennung zu unterstützen. Ein Sternchen (*) hinter der Supportstufe weist auf diese Art der Konfiguration hin.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ebene	Typ	Zusammenfassung
		Anwendungsfall: Vor dem New York-Release verfügte Servicekatalog über keine Domänenunterstützung, aber die Instanzbesitzer konnten für jeden Mandanten in einer domänengetrennten Instanz mithilfe von Benutzerkriterien separate Kataloge und Elemente konfigurieren. Das Ergebnis war, dass jeder Mandant den Servicekatalog auf der Standardebene verwenden konnte.

Informationen zur Anzeige aller Anwendungen, sortiert nach ihrer Supportstufe, finden Sie unter Anwendungssupport für die Domänentrennung.

Zusammenfassung

Domain Separation ist ein Framework, das Sie verwenden müssen, um Ihre Anwendungen auf die Kunden aufmerksam zu machen.

Berücksichtigen Sie die Fähigkeiten des Domänen-Frameworks, die Geschäftsanwendungsfälle Ihrer Anwendungen, die Personae und ihre Verwendung der Anwendung, bevor Sie das Framework verwenden können, um Ihre Anwendung unterstützt zu machen.

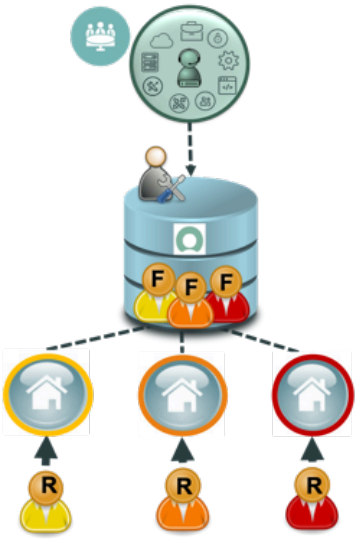
Referenzarchitektur des Service Providers

Ihre Kunden können über ein Portal, über das sie auf ihre domänengetrennte Instanz zugreifen können, auf die Services von Service Providern (SP) zugreifen.

Grundlegende Attribute der Referenzarchitektur des Service Providers

- Sie weisen einer Domäne keine Erfüller zu. Stattdessen geben Sie sie domänenübergreifend frei. Dies erschwert die Überprüfung der Anzahl der Erfüller pro Domäne.
- Sie können die Domänenadministration freigeben und nutzen. Dies bedeutet, dass kein Overhead entsteht und Sie Ihre Lizenzen optimieren können.
- Die Anzahl der Benutzer in der Instanz kann sich ändern, wenn Sie einen neuen Kunden gewinnen. Ein neuer Kunde kann zu zehn- oder sogar hunderttausenden neuen Benutzern im System führen. Die Anzahl der Gesamtbenutzer in einer gemeinsam genutzten Umgebung ist praktisch unbegrenzt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



- SP customers access SP services via a portal to the SP Domain Separated instance
- SP uses ServiceNow shared instance(s) to manage their service delivery
- SP could have a shared instance per region to support data sovereignty requirements

Legend:

Centralized governance at the SP

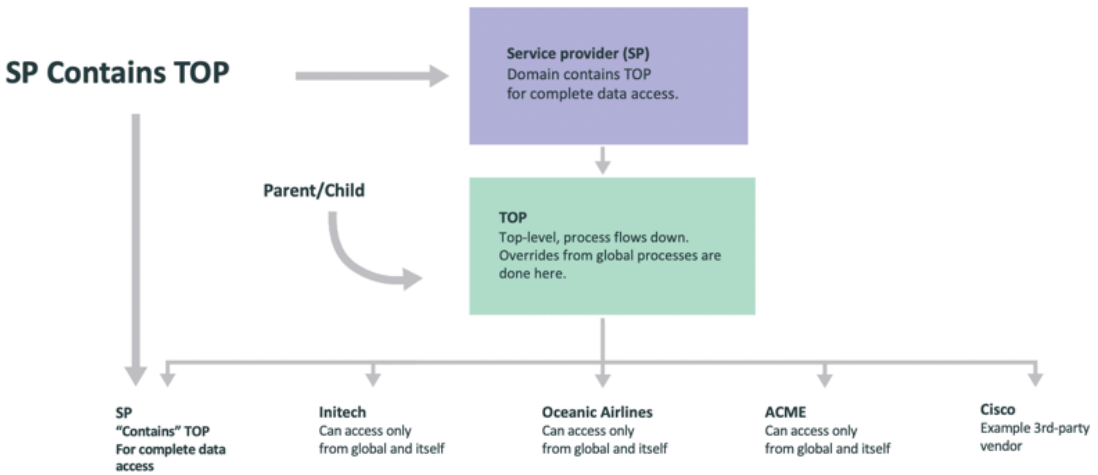
Centralized administration at the SP. Shared business requirements and configurations

Both SP and customer fulfillers on one instance

Customer requesters on each instance

Das Portal für SP-Services ist dediziert oder wird für die gemeinsam genutzte SP-Instanz freigegeben. Service Provider verwenden gemeinsam genutzte Instanzen von ServiceNow, um ihre Servicebereitstellung zu verwalten.

Referenzhierarchie für domänengetrennte Instanzen



© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vergleich der SP-Referenzarchitektur

Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside those offered by SP.	Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.	Global governance & admin for business use case & process can be developed & maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.	Lower administration, transaction, & onboarding costs, & ongoing operational costs for resources & licensing. Faster onboarding = more revenue.	Standardized re-usable services. procedures. processes, & resources delivered on a single ServiceNow instance to multiple Customers.	Services for sole use of customer, offerings specific to industry or vertical solutions, government, or regulatory requirements, applications that do not support Domain Separation.	Multiple best in class Service providers for individual services bringing together tooling, reporting, SLAs, strategy, & design for unified customer experience.	Unified governance across all providers to ensure organization requirements are met & that all providers cooperate on behalf of the customer.

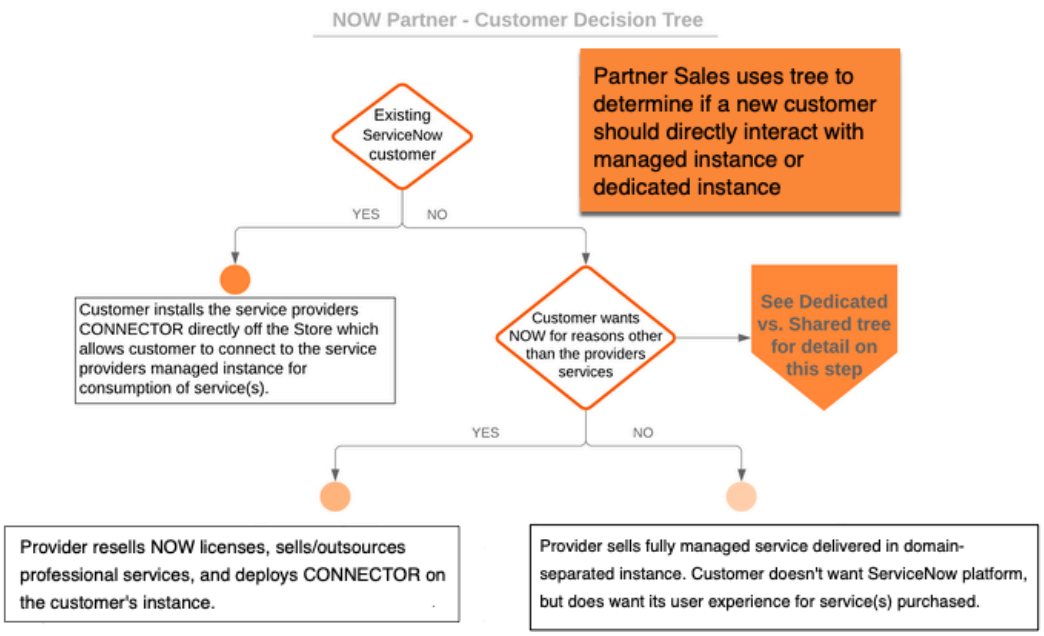
Entscheidungsstrukturen für die Referenzarchitektur des Service Providers

Sie können Entscheidungsstrukturen und ein Vergleichsdiagramm verwenden, um zu bestimmen, ob ein neuer Kunde zu einer gemeinsam genutzten Instanz oder zu seiner eigenen dedizierten Instanz hinzugefügt werden sollte.

Entscheidungsstrukturen

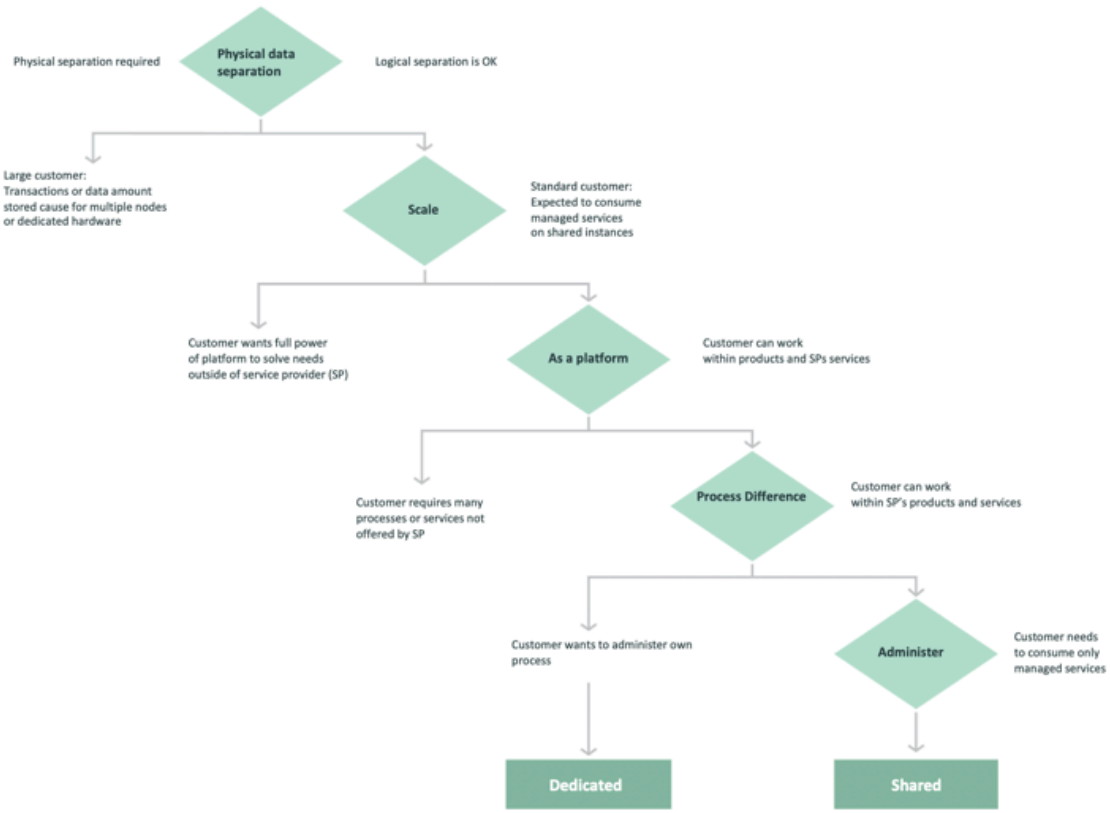
Verwenden Sie diese Entscheidungsstrukturen, um Ihre Kunden bei der Entscheidung zu unterstützen, ob eine verwaltete oder eine dedizierte Instanz verwendet werden soll.

Kundenentscheidungsstruktur



Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Vergleich der SP-Referenzarchitektur

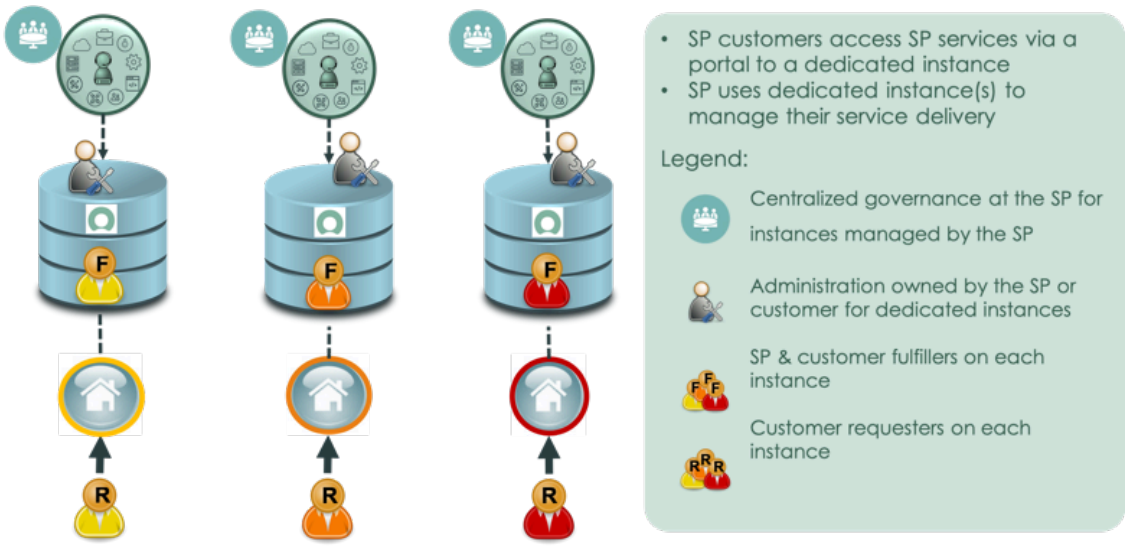
Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside those offered by SP.	Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.	Global governance & admin for business use case & process can be developed & maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.	Lower administration, transaction, & onboarding costs, & ongoing operational costs for resources & licensing. Faster onboarding = more revenue.	Standardized re-usable services. procedures. processes, & resources delivered on a single ServiceNow instance to multiple Customers.	Services for sole use of customer, offerings specific to industry or vertical solutions, government, or regulatory requirements, applications that do not support Domain Separation.	Multiple best in class Service providers for individual services bringing together tooling, reporting, SLAs, strategy, & design for unified customer experience.	Unified governance across all providers to ensure organization requirements are met & that all providers cooperate on behalf of the customer.

Referenzarchitektur des Service Providers für dedizierte Instanzen

Kunden von Service Providern (SP) können über ein Portal zu einer dedizierten Instanz auf SP-Services zugreifen. SPs verwenden diese dedizierten Instanzen, um ihre Servicebereitstellung zu verwalten.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dedizierte Instanzen



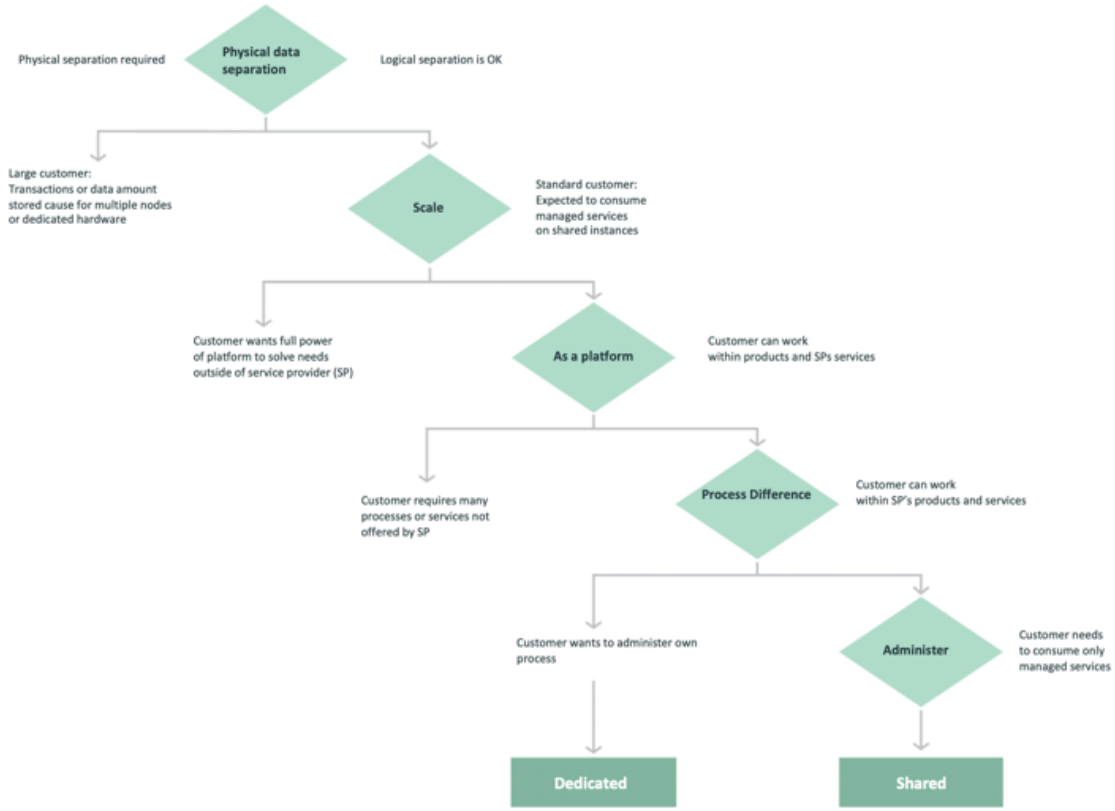
Attribute

- Dedizierte Instanzen erfordern eine separate Verwaltung und dedizierte Teams. Sie benötigen mehrere Lizenzen für die Administratoren und Entwickler, die sich bei mehreren Instanzen anmelden.
- Jede Instanz hat eine begrenzte Anzahl von Anforderern und Erfüllern. Wenn Sie einen neuen Kunden gewinnen, müssen Sie eine Instanz erwerben, die auf der Größe und dem Umfang des Unternehmens Ihres Kunden basiert.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Freigegebene Instanz

Dedizierte vs. gemeinsam genutzte Instanz



Vergleich der SP-Referenzarchitektur

Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside those offered by SP.	Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.	Global governance & admin for business use case & process can be developed & maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.	Lower administration, transaction, & onboarding costs, & ongoing operational costs for resources & licensing. Faster onboarding = more revenue.	Standardized re-usable services. procedures. processes, & resources delivered on a single ServiceNow instance to multiple Customers.	Services for sole use of customer, offerings specific to industry or vertical solutions, government, or regulatory requirements, applications that do not support Domain Separation.	Multiple best in class Service providers for individual services bringing together tooling, reporting, SLAs, strategy, & design for unified customer experience.	Unified governance across all providers to ensure organization requirements are met & that all providers cooperate on behalf of the customer.

Service Provider-Referenzarchitektur für Hybrid

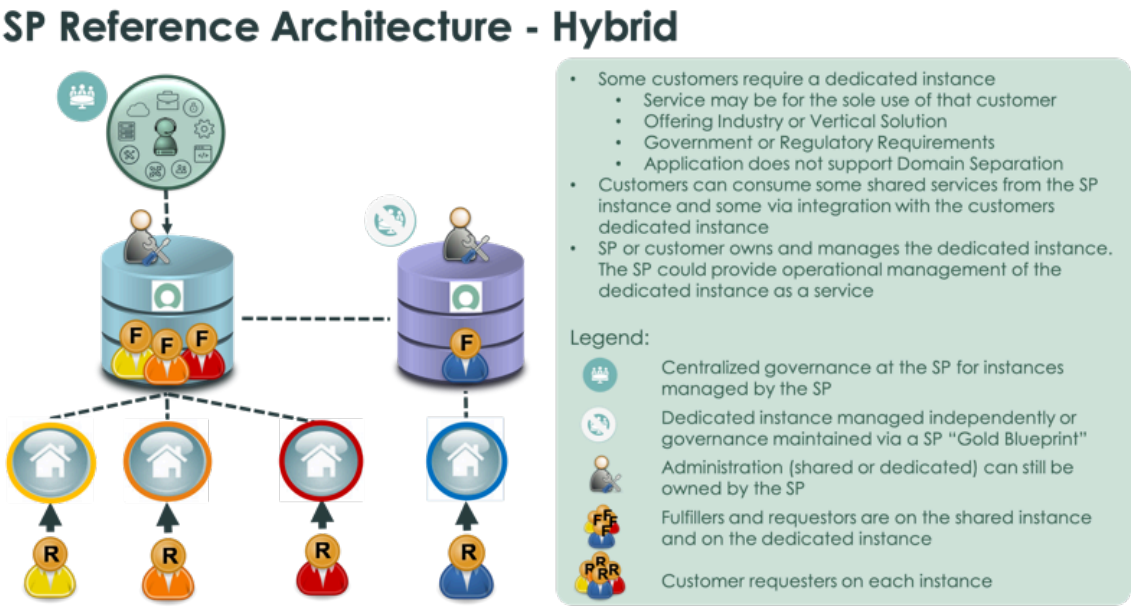
Verwenden Sie die Referenzarchitektur des hybriden Service Providers (SP) für eine anwenderdefinierte Lösung. Ihre Kunden benötigen eine dedizierte Instanz für einen bestimmten Service. Sie können die freigegebene SP-Instanz weiterhin für andere Services verwenden, dies erfordert jedoch die Integration jeder Instanz.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hybridarchitektur

Ihr Kunde ist möglicherweise direkt für die Bereitstellung dieses zusätzlichen Service verantwortlich. Sie müssen eine Hybridlösung mit mehreren Attributen erstellen, die Ihr Kunde bereitstellen kann.



Attribute

- Sie können die Instanz gemeinsam nutzen und verwalten. Dies bedeutet, dass kein Overhead entsteht und Sie Ihre Lizenzen optimieren können.
- Wenn für eine dezentrale Umgebung eine neue Instanz vorhanden ist, ist das Programmteam verantwortlich und wird entsprechend als dedizierter Administratorbenutzer für diese Instanz finanziert. In einer zentralisierten Umgebung, in der alle Instanzen aus einem Blueprint stammen, benötigen Sie doppelte Verwaltungslizenzen.
- Sie weisen einer Domäne keine Erfüller zu. Stattdessen können Sie sie domänenübergreifend freigeben.
- Wenn ein Kunde eine gemeinsam genutzte und eine dedizierte Umgebung gleichzeitig nutzt, benötigt er in beiden Umgebungen einen Erfüller. Das bedeutet mehr Arbeit für jedes Team, da die Prozesse für gemeinsam genutzte und dedizierte Instanzen für jede Instanz andere Arbeit erfordern.
- Die Anzahl der Benutzer in der Instanz kann sich ändern, wenn Sie einen neuen Kunden gewinnen. Ein neuer Kunde kann zu zehn- oder sogar hunderttausenden neuen Benutzern im System führen. Die Anzahl der Gesamtbenutzer in einer gemeinsam genutzten Umgebung ist praktisch unbegrenzt.
- Jede Instanz hat eine begrenzte Anzahl von Anforderern und Erfüllern. Wenn Sie einen neuen Kunden gewinnen, müssen Sie eine Instanz erwerben, die auf der Größe und dem Umfang des Unternehmens Ihres Kunden basiert.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vergleich der SP-Referenzarchitektur

Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside those offered by SP.	Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.	Global governance & admin for business use case & process can be developed & maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.	Lower administration, transaction, & onboarding costs, & ongoing operational costs for resources & licensing. Faster onboarding = more revenue.	Standardized re-usable services. procedures. processes, & resources delivered on a single ServiceNow instance to multiple Customers.	Services for sole use of customer, offerings specific to industry or vertical solutions, government, or regulatory requirements, applications that do not support Domain Separation.	Multiple best in class Service providers for individual services bringing together tooling, reporting, SLAs, strategy, & design for unified customer experience.	Unified governance across all providers to ensure organization requirements are met & that all providers cooperate on behalf of the customer.

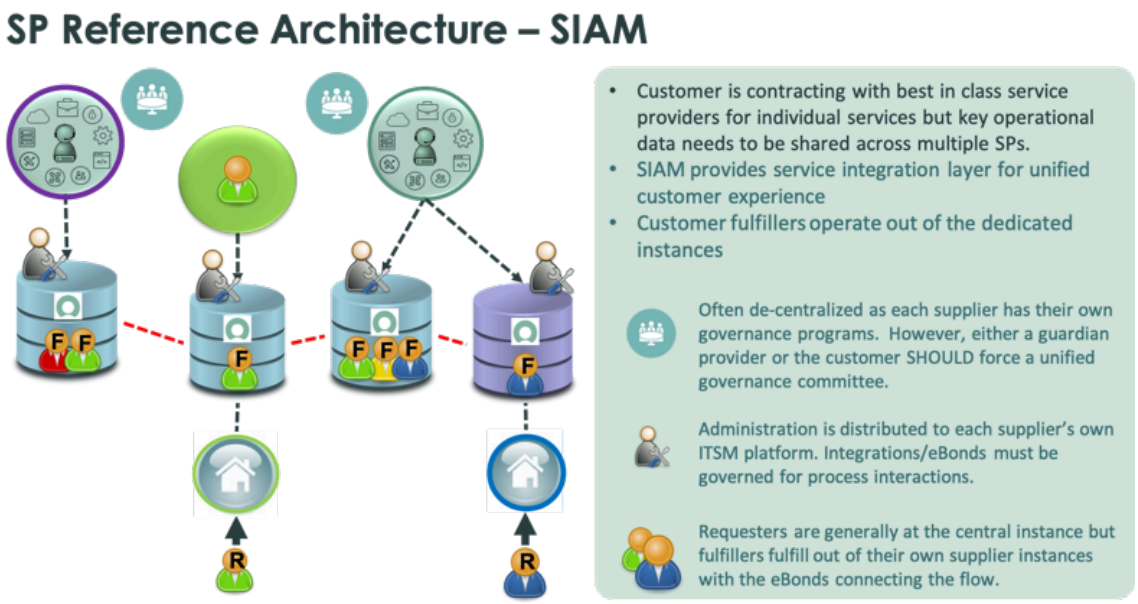
Service Provider-Referenzarchitektur für Verwaltung von Serviceintegrationen (SIAM)

Die Verwaltung von Serviceintegrationen Service Integration and Management-Architektur (SIAM) für Service Provider (SP) integriert Services für eine einheitliche Kunden-Experience.

Attribute der SIAM-Architektur

- Kunden greifen auf SP-Services über ein dediziertes oder gemeinsam genutztes Portal für die gemeinsam genutzte SP-Instanz zu.
- SPs verwenden gemeinsam genutzte ServiceNow Instanzen, um ihre Servicebereitstellung zu verwalten.

SIAM-Architektur auf einen Blick



Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vergleich der SP-Referenzarchitektur

Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside those offered by SP.	Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.	Global governance & admin for business use case & process can be developed & maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.	Lower administration, transaction, & onboarding costs, & ongoing operational costs for resources & licensing. Faster onboarding = more revenue.	Standardized re-usable services. procedures. processes, & resources delivered on a single ServiceNow instance to multiple Customers.	Services for sole use of customer, offerings specific to industry or vertical solutions, government, or regulatory requirements, applications that do not support Domain Separation.	Multiple best in class Service providers for individual services bringing together tooling, reporting, SLAs, strategy, & design for unified customer experience.	Unified governance across all providers to ensure organization requirements are met & that all providers cooperate on behalf of the customer.

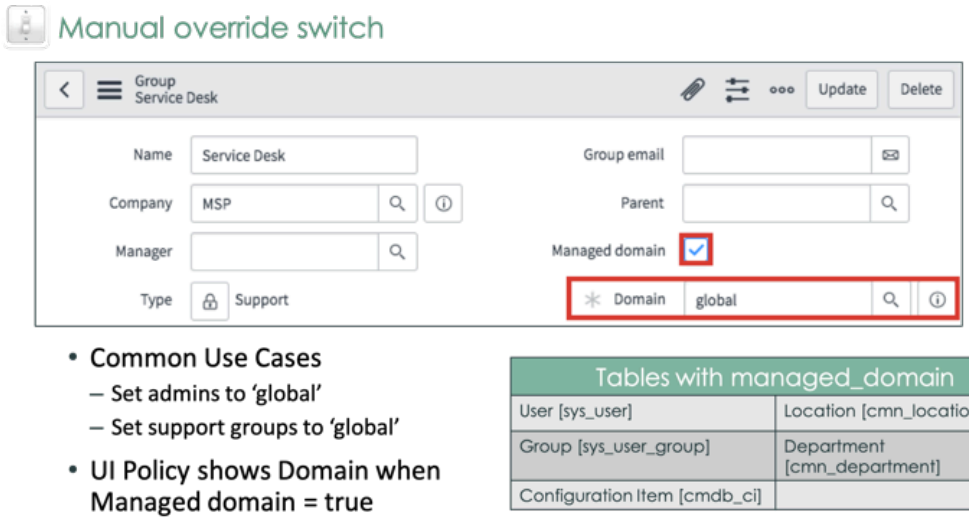
Begriffe für Domänentrennung

Mit einer Instanz ServiceNow können Sie die Effizienz verbessern, die Sicherheit erhöhen und die Leistung Ihrer Kundenorganisationen steigern. Es ist hilfreich, einige der häufigsten Begriffe zu verstehen, wenn Sie Ihre Konfigurationen erstellen.

Verwaltete Domäne

In einer verwalteten Domäne können Domänenadministratoren im Feld **Verwaltete Domäne** manuell eine Domäne für den Benutzer-, Gruppen-, Abteilungs-, Standort- oder CI-Datensatz auswählen, anstatt die Domäne zu verwenden, die automatisch vom Unternehmensdatensatz zugewiesen wird.

Wenn Sie diese Eigenschaften ändern möchten, können Sie sie überschreiben, um die Funktionen der Anwendungen in jeder Ihrer Domänen weiter



anzupassen.

Prozesstabellen

Wenn in Prozesstabellen ein Wert im Feld Überschreibungen **[sys_overrides] angezeigt** wird, ist ein Prozessüberschreibungsdatensatz vorhanden. Das bedeutet, dass die delegierte Administration aktiv ist, d. h. wie Administratoren domänenspezifische Richtlinien

Automatische Übersetzung

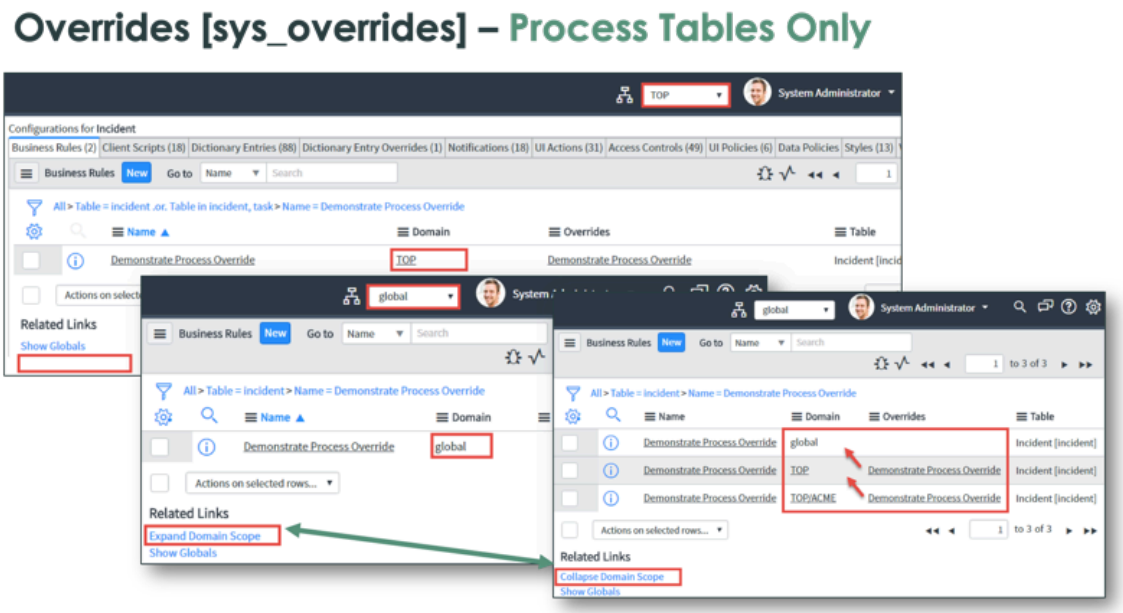
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

festlegen können. Administratoren in der globalen Domäne können den zugehörigen Link „Domänenbereich **erweitern/reduzieren**“ verwenden, um Überschreibungsdatensätze anzuzeigen.

Hinweis: Berichte sind in Domänen unterteilt und enthalten ein Feld „ **Überschreibungen** “. Um alle Berichte aus der globalen Domäne anzuzeigen, verwenden Sie den zugehörigen Link **Domänenbereich erweitern**.

Wenn Sie Prozesstabellen aus einer Domäne anzeigen, werden nur die relevanten Prozessdatensätze für die ausgewählte Domäne angezeigt. Wenn Sie eine Prozesstabelle aus der globalen Domäne anzeigen, wird der zugehörige Link **Domänenbereich erweitern** angezeigt, damit Sie alle Prozessdatensätze (einschließlich Überschreibungen) anzeigen können. Um nur die relevanten Prozessdatensätze für „Global“ erneut anzuzeigen, verwenden Sie den zugehörigen Link **Domänenbereich reduzieren**.

Die Funktion „Domänenbereich“ wird nur für Prozesstabellen verwendet und bewirkt, dass sich die Sichtbarkeit von Daten in der Tabelle in die umgekehrte Richtung verschiebt. Beispielsweise kann ein Datensatz in der übergeordneten Domäne im untergeordneten Datensatz angezeigt werden, ein übergeordneter Datensatz kann jedoch keinen untergeordneten Datensatz anzeigen. Dies ermöglicht einen Flow des Prozesses nach unten zu untergeordneten Domänen.



Arten von Domänen

Verschiedene Arten von Domänen können Ihnen dabei helfen, Ihre Prozesse und Daten und ihre Funktionsweise in der Anwendung oder Funktion zu organisieren.

Kundendomäne

In der Domäne des Kunden befinden sich die Anwenderoberfläche und der Prozess, der steuert, wie die Daten verwendet werden.

Die ACME-Domäne in der folgenden Abbildung ist eine Kundendomäne.

Prozessdomäne

Sie erstellen Prozesse dafür, wie die Daten verwendet werden und was sie in der Domäne tun. Diese Prozesse müssen diese Attribute aufweisen:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Bestimmte Prozesse und UI-Einstellungen für eine Reihe von Domänen
- Keine Kerndaten jeglicher Art (z. B. bestimmte Benutzerdaten).
- Die TOP-Domäne in der folgenden Abbildung ist eine Prozessdomäne.

Datendomäne

Die Datendomäne enthält Daten, die für mehrere Kunden relevant sind. Diese Daten können geteilt werden, ohne die tatsächlichen Kundendomänen freizugeben. Jeder Kunde hat eine eigene Datendomäne und kann darauf zugreifen.

Hinweis:

Diese Art von Domäne ist nicht häufig und kann bei übermäßiger Verwendung zu Leistungsproblemen führen. Wenden Sie sich vor der Verwendung an einen SP-Architekten.

Beispiel: Die Domäne kann Aufgaben enthalten, mit denen ACME, Cisco und der SP interagieren müssen.

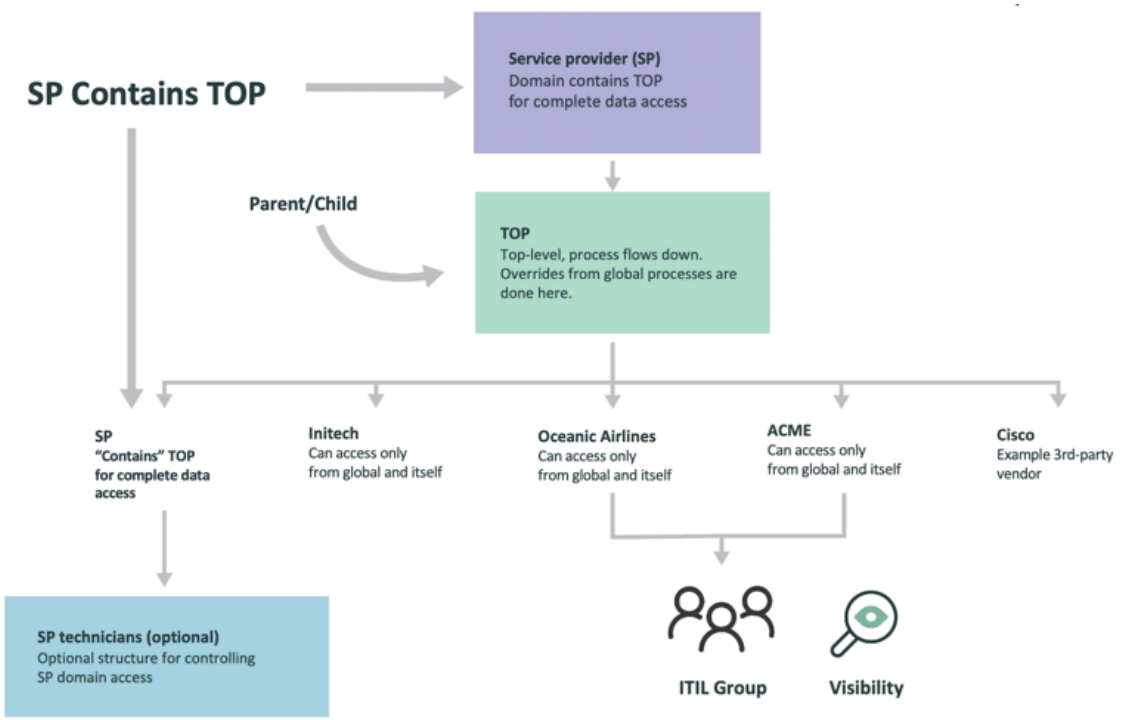
Die Standarddomäne in der folgenden Abbildung ist eine Datendomäne.

Anwenderdaten

Benutzerdatensatzdaten gehören niemals in die globale Domäne oder in eine der Prozessdomänen. Benutzer werden hauptsächlich in Kundendomänen erstellt und können gelegentlich in Datendomänen erstellt werden.

Administratorkonten sind etwas Besonderes, da sie nicht als normale Benutzer der Instanz verwendet werden sollten. Sie sollten sich in der globalen Domäne befinden, um die Verwaltungsfunktionen zu erleichtern.

Domänenhierarchie



© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen, Administrator, globaler Prozess

Listen

Wenn Sie in der globalen Domäne mit der rechten Maustaste auf die Bezeichnung eines Auswahlfelds klicken, Auswahlmöglichkeiten **konfigurieren**auswählen und dann eine neue Auswahl hinzufügen, wird die Auswahl automatisch an alle domänenspezifischen Listen für dieses Feld übertragen. Wenn die neue Option als **Ausgewählt**markiert ist, wird sie als aktiv hinzugefügt. Wenn die neue Option als **Verfügbar**markiert ist, wird sie als inaktiv hinzugefügt.

Instanzenverwaltung

Die Administratoren des Besitzers der Instanz müssen die gesamte normale Prozesserstellung, -änderung und -wartung in einer domänengetrennten Instanz abwickeln. Einzelne Domänenmanager können einige Teile von datengesteuerten Prozessen verwalten.
Die verschiedenen Typen von Domänenmanagern verwalten die Benutzerverwaltung, unterstützen Mitgliedschaften von Supportgruppen und Standorte oder verwalten Anwendungen, die speziell für die Verwaltung von Mandanten entwickelt wurden.

Globaler Prozess/globale Parameter

Sie können den Prozess erstellen und verwalten, der sich auf die globale Domäne auswirkt, sowie die Parameter festlegen. Diese Eigenschaften gelten für alle Benutzer einer domänengetrennten Instanz.

Beispiele: Systemeigenschaften, Außerkraftsetzung des Wörterbuchs, `sys_documentation` (Feldbezeichnungen), Datenmodell (Klassen, CI-Typen usw.), Tabellen und Felder `[sys_dictionary]` (Zugriff kann eingeschränkt sein), Indexierung (Textverzeichnisse sowie Datenbank) , ACLs, Installations-Exits, eingehende Aktionen, öffentliche Seiten und Interceptors.

Trennen Sie eine benutzerdefinierte Tabelle von der Domäne

Möglicherweise müssen Sie anwenderdefinierte Tabellen in separaten Domänen erstellen. Dieses Thema behandelt sowohl das Verfahren als auch das Konzept hinter der Domänentrennung einer benutzerdefinierten Tabelle.

1. Erstellen Sie ein sys_domain-Feld

Hinweis: Wenn eine Systemtabelle oder eine Tabelle nicht durch das Plugin „Domain Separation“ domänengetrennt wurde, sollte sie am besten nicht domänengetrennt werden.

Verwenden Sie diese Punkte als Leitfaden für die Erstellung eines Felds vom Typ sys_domain.

- Erstellen Sie ein neues Feld als Typ *domain_id*.
  - Spaltenname: sys_domain
  - Andere Attribute: Automatisch definiert
- Sys_domain_path wird automatisch erstellt.

Der Spaltenname **sys_domain** ist im Now Platformreserviert, was bedeutet, dass das System ihn erkennt und automatisch den entsprechenden Feldtyp und die entsprechenden Attribute für Sie anwendet. Diese automatische Konfiguration erstellt auch ein entsprechendes Feld **„sys_domain_path“**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Legen Sie den Spaltennamen auf `sys_domain fest`, anstatt die Bezeichnung zu verwenden.
- Domain Separation ist nicht für jede Tabelle geeignet. Wenn eine Tabelle Teil der Basisinstanz ist und diese Tabelle kein **sys_domain** -Feld enthält, sollten Sie dies im Allgemeinen so lassen.

Ein Feld vom Typ „ **sys_domain** " wird automatisch erstellt, wenn Sie ein Feld vom Typ „domain_id" mit dem Namen „sys_domain" erstellen.

2. Fügen Sie eine Geschäftsregel hinzu, um die Domäne festzulegen

Ohne Business-Regeln

Die Domäne wird auf die aktuelle Domäne des Benutzers festgelegt, der den Datensatz erstellt.

Mit Geschäftsregeln

Die Domäne wird mithilfe von Skriptlogik zugewiesen, normalerweise basierend auf dem Feld „Unternehmen".

Zusätzlich zu einem `sys_domain-Feld`benötigen benutzerdefinierte Tabellen eine Geschäftsregel ähnlich der **Domäne – Domäne festlegen – Aufgabe**, um den Wert des Domänenfelds festzulegen. Darüber hinaus benötigen Sie **Domäne – Standard – Aufgabe**, die Datensätze ohne Domäne in die Standarddomäne verschiebt, wenn die erste Regel keine Domäne zuweist.

Überprüfen Sie in der Aufgabentabelle die Geschäftsregeln für die Domäne. Achten Sie besonders auf das Feld Reihenfolge. Die Priorität der Ausführung wird durch das Feld Reihenfolge von niedrig nach hoch angegeben.

Die erste ausgeführte Regel, **Domäne – Domäne festlegen – Aufgabe**, versucht, die Domäne des Datensatzes basierend auf der Unternehmensdomäne des Datensatzes festzulegen.

Wenn die erste Regel keine geeignete Domäne findet, wird die zweite Regel (**Domäne – Standard – Aufgabe**) ausgeführt. Diese Regel legt die Domäne des Datensatzes auf die Standarddomäne fest.

Wenn sich schließlich die Domäne eines Aufgabendatensatzes ändert, ändert die Geschäftsregel **„Domäne – Kaskadierende Domäne – Aufgabe"** die Domäne für alle Datensätze im Zusammenhang mit der Aufgabe, z. B. Workflows, Metriken, SLAs und Anhänge.

3. Fügen Sie eine Geschäftsregel hinzu, wenn Schritt 2 fehlgeschlagen ist

Wenn die ursprüngliche Geschäftsregel keine Domäne festlegen konnte und die Domäne noch leer oder global ist, wird eine zweite Geschäftsregel ausgeführt. Diese Regel untersucht das Feld „`task_for`", das auf dem Feld „Caller" oder „ `requested_for` " basiert. Diese Regel überprüft, ob Sie die Domäne des Datensatzes basierend auf der Domäne des Anwenders festlegen können. Andernfalls legt die Geschäftsregel die Domäne auf die Standarddomäne fest.

Es folgt ein Beispielskript für die Geschäftsregel:

```
/* essentially
If (task_for is set)
  set the domain to the user's domain
ELSE
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
  set the domain to the default domain
*/
```

4. Domäne – Kaskadierungsdomäne – Aufgabe

Aufgaben können viele zugehörige Tabellen haben, die zusammenarbeiten, um Geschäftsziele zu erreichen. Zu diesen zugehörigen Datensätzen gehören Workflow, SLA, Genehmigungen, Anhänge und E-Mail. Wenn sich die Domäne einer Aufgabe ändert, muss sich auch die Domäne der zugehörigen Datensätze ändern, damit sie für Benutzer in der neuen Domäne sichtbar bleiben.

Diese Kaskadierungsregel wird häufig ausgelöst, wenn Sie Datensätze aus der Standarddomäne löschen.

Die zugehörigen Datensätze für eine im Skript enthaltene Kaskadendomäne werden ähnlich wie im folgenden Beispiel dargestellt:

```
/*
* Keep domains in sync w/related records for:
* workflow context
* workflow history
* approver tables and related workflows
* attachments
* emails
*/
```

Eigenschaften und Designs von Domänen anpassen

Sie können die Unternehmenseigenschaften und Designs Ihrer Kunden innerhalb der von Ihnen konfigurierten Domänen anpassen. Durch Anpassungen werden die Instanzen an das allgemeine Erscheinungsbild des Unternehmens angepasst.

Anpassung von Unternehmensdesigns und -logos

Im Unternehmensdatensatz können Sie bestimmte Designthemen und Logos für jedes Unternehmen anpassen.

Passen Sie die Domäne an

Wenn Sie das Service Provider-Plugin installiert haben, wird die Domäne des Datensatzes aufgrund der in den Core-Tabellen enthaltenen Standardgeschäftsregeln standardmäßig auf die Domäne des Unternehmens festgelegt, das dem Datensatz zugeordnet ist. Das Unternehmen kann Tabellen wie Aufgabe, Benutzer, Gruppe, Standort, Abteilung usw. steuern.

Mit allen diesen Tabellen außer der Aufgabentabelle können Sie die Domäne überschreiben, in der ein Datensatz erstellt wird. Dadurch stehen Ihnen weitere Anpassungsoptionen zur Verfügung.

Domain Separation für bestimmte Zwecke verwalten

Sie können separate Domänen für E-Mail-Benachrichtigungen einrichten und die Eigenschaften von Katalogen, Tabellen, Benutzern, Gruppen und Ansichten anpassen. Dadurch können Sie spezifischeres Verhalten in jeder Domäne bereitstellen, was Ihren Kunden mehr Flexibilität verschafft.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

E-Mails

Sie können separate Domänen für E-Mail-Benachrichtigungen und Überschreibungen verwenden. Wenn Sie separate Domänen für Benachrichtigungen verwenden, können Sie eine Überschreibung vornehmen, die nur auf der Domäne des angehängten Datensatzes basiert, nicht auf der gesamten Domäne des Anwenders.

Servicekatalog

Der Servicekatalog ist jetzt domänengetrennt, sodass Ihre Kunden den Katalog anzeigen und darauf zugreifen können. Elemente werden als ODER-Bedingungen verarbeitet, wenn mehrere Elemente verwendet werden. Service Provider sollten die Kategorien und Elemente selbst verwalten, damit sie speziell ihre eigenen Kriterien erfüllen.

Anwender und Gruppen

Verwenden Sie in der globalen Domäne nur Administratorkonten, da Administratoren Zugriff auf alle Domänen benötigen. Führen Sie alle Ihre Anwendungstests in einer tatsächlichen Domäne durch, nicht in der globalen Domäne. Überschreibungen werden in der globalen Domäne nicht ordnungsgemäß verarbeitet. Administratoren müssen auch in der Produktion Benutzeraccounts erhalten, wenn sie die Anwendung verwenden möchten.

Arbeiten mit -Feldern

Bei der Arbeit mit Feldern sind mehrere Punkte zu berücksichtigen. Achten Sie genau auf diese Felder, da sie viele Variationen aufweisen können, die sich auf Ihre Konfigurationen auswirken.

Listen

Es gibt persönliche, globale und Domänenlisten sowie jeweils mehrere Ansichten.

Formulare

Es gibt globale Listen und Domänenlisten sowie jeweils mehrere Ansichten.

Eine Datenbank

Alle von Ihnen erstellten Felder sind für alle Benutzer in einer Datenbank vorhanden. Berücksichtigen Sie die globalen Auswirkungen, bevor Sie eine erstellen.

Hinweis: ACL-Skripts können nicht verhindern, dass ein Feld in einer Liste angezeigt wird, da sie nicht ausgeführt werden. Sie können eine READ ACL hinzufügen, um ein Feld für Benutzer auszublenden, wenn die ACL nur rollenbasiert ist.

Erstellen von Tabellen

Wenn Sie eine Tabelle erstellen, sollten Sie ein Feld „`sys_domain`“ oder „`sys_overrides`“ hinzufügen. Jede Tabelle, die Daten enthält, auf die Ihre Instanzanwender zugreifen müssen, benötigt das Feld `sys_domain`. Tabellen, die Prozesse erweitern oder unterstützen und die in untergeordnete Domänen fließen müssen, benötigen ebenfalls das Feld `sys_domain`.

Domain Separation mit der Domänenauswahl konfigurieren

Verwenden Sie die Domänenauswahl mit Bedacht, und beachten Sie den 80/15/5-Ansatz, damit Sie nicht zu viel anpassen und die Leistung Ihrer Instanz nicht beeinträchtigen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verifizieren Sie Ihre Domäne, bevor Sie Änderungen vornehmen

Die Domänenauswahl fasst alle Domänen in einer Liste zusammen, aus der Sie auswählen können.

Wenn bei Ihrer Sitzung eine Zeitüberschreitung auftritt und Sie nicht abgemeldet werden, greift Ihre Sitzung auf die Domäne in Ihrem Benutzerdatensatz zurück. Gleichzeitig verlieren Sie auch alle erhöhten Rollen. In diesem Fall könnte Ihre Domänenauswahl immer noch die letzte von Ihnen ausgewählte Domäne anzeigen, wenn der obere Frame der Liste nicht neu geladen wurde. Aus diesem Grund sollten Sie Ihre Liste vollständig neu laden, wenn Sie für längere Zeit nicht in der Instanz waren.

Konfiguration in der TOP-Domäne oder der globalen Domäne

Domain Separation funktioniert am besten, wenn Sie Services für Kunden bereitstellen, die in ihrer Konfiguration sowie Benutzer- und Gruppendefinition meist Standard sind. Je mehr Sie „einmalige“ Lösungen anpassen und erstellen, desto höher ist die Toleranz für Fehler. Wenn Sie Ihre Prozesse und Ihre Geschäftslogik erstellen, sollten sich alle Variationen in Eigenschaften befinden, die für jeden Kunden automatisch funktionieren. Prozesse können zwar noch nach Bedarf angepasst werden, aber lassen Sie große Sorgfalt walten, wenn Sie entscheiden, wann und in welchem Umfang Sie eine eindeutige Konfiguration für einen einzelnen Kunden erstellen möchten.

Sie müssen bei der Konfiguration Ihrer Domänen einen „80-15-5“-Ansatz verwenden, um einen zu großen Spielraum für Anpassungen und damit Fehler zu vermeiden.

- Empfohlener Ansatz für die Konfiguration:
  - **80 %** oder mehr **Standard**
  - Mindestens**15 %parametrisch**
  - Weniger als **5 % Konfiguration**
- Legen Sie fest, ob ein vorgeschlagener Change eine globale oder eine konfigurierbare Eigenschaft sein soll.
- Erstellen Sie nicht zu viel, indem Sie immer mehr Anpassungen hinzufügen, die verwaltet werden müssen. Gehen Sie stattdessen wie folgt vor:
  - Beginnen Sie mit den Funktionen des Basissystems, und überprüfen Sie alle Lücken, bevor Sie Änderungen vornehmen.
  - Suchen Sie nach Lösungen ohne Code.
  - Verwenden Sie serverseitige Skripts, erstellen Sie modulare APIs, und integrieren Sie domänengetrennte Eigenschaften.
  - Wenn Sie Client-Skripting verwenden müssen, verwenden Sie nur ServiceNow APIs. Begrenzen Sie "synchrone" Aufrufe (Anrufe, die hin und her von Client zu Server wechseln, auch AJAX genannt).
  - Schreiben Sie alle Skripts logisch, um sie einfach und effektiv zu halten. Erzwingen Sie Peer-Reviews von Codeänderungen, und stellen Sie sicher, dass alle Empfohlene Domain Separation-Verfahren für Service Provider in diesem Abschnitt befolgen.

Leistungsüberlegungen zur Domain Separation

Berücksichtigen Sie bei der Konfiguration der Domänentrennung in Ihrer Anwendung und Ihren Services die Anzahl und die Eigenschaften der von Ihnen erstellten Domänen? Zu viele eigenschaftsintensive Domänen können sich auf die Leistung Ihrer Instanz auswirken.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einschränken von eigenschaftslastigen Domänen

Sie können beliebig viele Domänen erstellen, stellen Sie jedoch sicher, dass Sie keine unnötigen Domänen auf der Instanz erstellen. Wenn Sie in einer Instanz zu viele Domänen mit vielen Eigenschaften gewichten, kann dies die Leistung Ihrer Instanz beeinträchtigen.

Die Anzahl der Domänen wirkt sich nicht auf die Leistung aus, sondern auf der Grundlage ihres Inhalts. Zu viele Eigenschaften können die Domänenauswahlverlangsamen, was wiederum die allgemeine Anwender-Experience Ihrer Kunden verlangsamt. Wenn Sie die Domänenauswahl laden und bereits eine große Anzahl von Domänen mit vielen Eigenschaften haben, muss die Domänenauswahl alle Domänen laden, bevor Sie die Kontrolle über die Sitzung übernehmen. Dieser Prozess kann zu einem Ausfall führen, bei dem Sie bis zum Abschluss der Domänenauswahl nicht auf Elemente in der Instanz zugreifen können. Bevor Sie neue Domänen erstellen, navigieren Sie zur Domänenhierarchie unter **Domänenadministrator** > **Domänenzuordnung** und stellen Sie sicher, dass Sie tatsächlich eine neue Domäne erstellen müssen oder ob eine vorhandene Domänenhierarchie funktionieren kann.

Domänenauswahl Core-UI wird verwendet

Die Domänenreferenz-Auswahl ist in Core-UIverfügbar. Mit der Referenzauswahl werden nicht alle Domänen auf einmal geladen, sondern die Domäne wird durchsucht, während Sie beginnen, den Namen Ihrer Domäne in die Domänenauswahl einzugeben.

Sie aktivieren die Domänenreferenz-Auswahl in Core-UI, indem Sie die folgenden Schritte ausführen:

1. Geben Sie im Anwendungsnavigator `sys_properties.list` ein.
2. Legen Sie die Eigenschaft *`glide.ui.domain_reference_picker.enabled`* auf „Wahr“ fest.
3. Aktualisieren Sie den Browser.

Hinweis: Laden Sie keine große Anzahl von Domänen (über 30) über Integrations- oder Importsätze hoch, ohne zuerst einige Tests durchzuführen, da Sie sonst Ihre Instanz herunterfahren könnten.

Einrichten von Domänenhierarchien

Sie können Verlangsamungen und Auswirkungen auf die Leistung in Ihrer Instanz vermeiden, indem Sie wissen, wie Domänenhierarchien funktionieren, und sie ordnungsgemäß einrichten.

Je nach Domänenhierarchie haben Benutzer Zugriff auf die Daten in ihrer Stammdomäne und in allen untergeordneten Domänen. Der Prozess wird in die untergeordneten Domänen übertragen, und die Daten werden hochgestuft.

Nehmen Sie nur bei Bedarf Änderungen an der vorhandenen Domänenhierarchie vor. Wenn Sie das übergeordnete Element einer Domäne aktualisieren, stellt das System die übergeordnete Domäne mit allen untergeordneten Domänen wieder her, die die Domänenhierarchie ändern. Wenn die Domänenhierarchie aktualisiert wird, löst das System eine kaskadierende Aktualisierung für alle Tabellen aus, die sich auf Domänen beziehen, für die Datensätze, die in dieser Domäne erstellt werden. Daher muss auch eine große Anzahl von unterstützenden Tabellen aktualisiert werden.

Führen Sie aus den gleichen Gründen niemals ein Massenupdate durch, selbst wenn Sie die Domänenhierarchie ändern müssen. Stellen Sie sich die Anzahl der Abfragen vor, die das System ausführen muss, um die Domänenhierarchie zu ändern. Führen Sie Updates immer in kleinen Batches durch. Bevor Sie den nächsten Aktualisierungsbatch starten, stellen Sie sicher,

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

dass DWR-Datensätze (Domain Work Request) verarbeitet werden. DWRs sind Berichte, die anzeigen, ob Fehler aufgetreten sind, nachdem Sie die Domänenhierarchie geändert haben.

Nachverfolgung von DWR-Datensätzen

Suchen Sie in der Tabelle „syslog_domain“ in der Spalte „Nachricht“ für „ **DWR-Ausführung abgeschlossen“ nach einem Informationseintrag.** um zu bestätigen, dass DWR abgeschlossen ist.

Domänenprotokolle werden auf Fehler und Warnungen überprüft

Überprüfen Sie die Domänenprotokolle, um Fehler oder Warnungen in Ihren Domänenpfadprozessen und Hierarchiekonfigurationen zu finden.

Sie finden die Domänenprotokolle in der Tabelle „Domänenprotokoll“ [syslog_domain]. Wenn die Domänenhierarchie aktualisiert wird, löst das System eine geplante Aufgabe aus, um die Domänenpfade neu zu berechnen. Die Tabelle „Domänenprotokolle“ erfasst die Ergebnisse.

Suchen Sie in dieser Tabelle nach Fehlern und Warnungen. Nach Überprüfung dieser Tabelle müssen Sie diese Fehler beheben und die Domänenpfadvalidierung erneut ausführen.

In diesem Beispielprotokoll hat das System zehn verwaiste Datensätze in der Tabelle „sys_ui_list“ erkannt. Die Fehler in diesen Datensätzen müssen behoben werden, bevor der Domänenpfad erfolgreich ausgeführt werden kann.

Error	10 records detected in 'sys_ui_list' that are not in any existing domain and Domain Paths. Fix the domain value in these records & run validator again.	com.glide.domain.validator
Error	10 records detected in 'sys_ui_list' that are not in any existing domain and Domain Paths. Fix the domain value in these records & run validator again. Entries causing the error are as follows:sys_id:1d13ae40470002007f47563dbb9a7170, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:22e34b23470002007f47563dbb9a718c, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:4c85fa809f233100fc6cd4b4232e706b, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:94648b23470002007f47563dbb9a711b, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:a0844b23470002007f47563dbb9a71ef, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:a95ff2c09f233100fc6cd4b4232e7096, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:bd25f4719f233100fc6cd4b4232e70da, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:c1263e809f233100fc6cd4b4232e70f6, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:d8a72c45475002007f47563dbb9a71bb, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:e4c3ce39eb10020045e1a5115206fea0, sys_domain:60e014f69f013100fbf01f80a57fcf00	com.glide.domain.validator

Weitere Informationen zu Fehlern bei der Domänentrennung finden Sie unter Behandeln Sie Domain Separation-Fehler.

Wichtigkeit der Standarddomäne

Das Organisieren Ihrer Domänen ist ein wichtiger Teil des Domänentrennungsprozesses. Wenn Sie keine Standarddomäne festlegen, werden neue Aufgaben und Benutzerdatensätze an die globale Domäne verwiesen. Jeder kann die Datensätze in der globalen Domäne sehen, was bedeutet, dass Daten sichtbar sind, wenn sie es nicht sollen.

Wenn Sie die Standarddomäne festlegen, sind die zugehörigen Datensätze nur für Administratoren sichtbar.

Hinweis: Der Standardzugriff kann geändert werden, indem Benutzern Sichtbarkeit für die Standarddomäne oder die übergeordnete Domäne gewährt wird.

Sie sollten immer eine Standarddomäne für die Domänendatensätze in Ihrer Instanz festlegen. Die Standarddomäne weist das System automatisch Aufgaben- und Benutzerdatensätze zu, die noch keiner Domäne zugewiesen sind.

Wenn Sie eine Standarddomäne im Bildschirm „Domänenverwaltung“ erstellen, fügen Sie im Feld **Name** den Namen Standard hinzu, um sie von anderen Domänen zu unterscheiden. Aktivieren Sie die **Checkbox Standard** für den Datensatz.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwalten Sie die in der Standarddomäne erstellten Datensätze regelmäßig, und verschieben Sie sie in die richtigen Domänen. Wenn Datensätze in der Standarddomäne häufig angezeigt werden, müssen Sie möglicherweise den Grund dafür untersuchen. Im Idealfall sollten Sie sicherstellen, dass alle Datensätze in den entsprechenden Domänen (nicht globalen oder Standarddomänen) erstellt werden.

Enthält Abfragen und Domänenzugriff

Verwenden Sie eine "enthält"-Abfrage nur in Sonderfällen, z. B. wenn Anwender oder Gruppen Daten aus einer Domäne anzeigen müssen, auf die sie keinen Zugriff haben, Sie diese Anwender jedoch nicht in eine Domäne verschieben möchten. Das Erstellen von Domänen „enthält“ und Anwender- oder Gruppenzugriff für eine Domäne sollte nur dann eine Ausnahme sein, wenn dies unbedingt erforderlich ist.

„Enthält“ ist eine Viele-zu-Viele-Beziehung von Domäne zu Domäne, die keine Auswirkungen auf den Prozess-Flow hat. Wenn Sie eine große Anzahl von Domänenbeziehungen erstellen, die einen umfassenden Zugriff bereitstellen, generieren Sie Abfragen mit zu vielen ODER-Bedingungen. ODER-Bedingungen sind langsam und wirken sich auf die Leistung Ihrer Instanz aus. Anstatt zu viele Beziehungen vom Typ „enthält“ zu verwenden, richten Sie Ihre Domänenhierarchie wie folgt ein:

Beispielabfrage

```
SELECT ... FROM task task0 ignore index(number) WHERE task0.`sys_class_name`
= 'incident' AND (task0.`sys_domain_path` = '/' OR task0.`sys_domain_path` LI
KE '!!$/!!(/%' OR task0.`sys_domain_path` LIKE '!!$/!!$/!!&/%') ORDER BY task
0.`number` DESC limit 0,20
```

Bevor Sie Benutzer in eine Domäne verschieben, vergewissern Sie sich, dass sie wirklich Zugriff auf diese Domäne haben. Wägen Sie die Vorteile und Einschränkungen ab. Die obige Abfrage bezieht sich nur auf eine enthält-Beziehung. Wenn Sie eine Domäne haben, die eine andere Domäne enthält und diese Domäne einer Reihe anderer Domänen übergeordnet ist, haben Sie viel mehr ODER-Bedingungen. Gehen Sie beim Erstellen einer Domänenzuordnung vorsichtig vor, damit die Leistung Ihrer Instanz nicht beeinträchtigt wird.

Abfragemethode für Domänenpfade

Sie können effektive Abfragen mit Domänenpfaden erstellen.

Verwenden Sie Domänenpfade anstelle von Domänen-Spooling (`sys_domain`) oder Domänennummerierung. Abfragen, die Domänenpfade verwenden, sind viel schneller als Spooling oder Nummerierung.

Domänenpfade sind die Standardabfragemethode für Instanzen mit aktivierter Domain Separation.

Wenn Sie die Abfragemethode in Ihrer Instanz überprüfen möchten, suchen Sie im Administrator-Dashboard nach den folgenden Systemeigenschaften:

- *If domain path is enabled*: In der Tabelle „Systemeigenschaften“ finden Sie `glide.sys.domain.provider=domain_paths` und `glide.sys.domain.paths.installed=true`.
- *If domain path is not enabled*: In der Tabelle „ `Systemeigenschaften“ wird glide.sys.domain.provider != domain_paths,glide.sys.domain.paths.installed=false angezeigt`

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Langsame Abfragen und SQL-Debugging

Durch das Debuggen von SQL und langsamen Abfragen können Sie Langsamkeitsprobleme in einer Instanz beheben.

Wenn Sie eine Instanz debuggen, können Sie entweder SQL-Debugging aktivieren, um nach langsamen Abfragen zu suchen, oder Sie können nach langsamen Abfragen suchen, indem Sie die Tabelle der langsamen Abfragen [sys_query_pattern] überprüfen, indem Sie zu **Systemdiagnose > Statistiken > Langsame Abfragen**navigieren. In dieser Tabelle werden alle langsamen Abfragen in der Instanz gespeichert.

Wenn Sie die Tabelle durchsuchen, suchen Sie nach Abfragen, die `„domain_path“` enthalten, um zu bestimmen, ob langsame Abfragen auf den Domänenpfad in Ihrer Instanz zurückzuführen sind.

Wenn Sie langsame Abfragen finden, versuchen Sie zu analysieren, warum sie langsam sind.

Häufige Gründe für langsame Abfragen

- Eine Abfrage hat zu viele ODER-Bedingungen (weitere Informationen finden Sie unter Enthält Abfragen und Domänenzugriff). Platzieren Sie in der Domänenhierarchie den Benutzer oder eine Domäne auf einer Hierarchieebene, auf der „enthält“ oder „Transparenz“ nicht erforderlich ist.
- Die Abfragemethode ist nicht die Domänenpfad-Abfragemethode (weitere Informationen finden Sie unter Abfragemethode für Domänenpfade): Wenn Sie nicht die Domänenpfad-Abfragemethode verwenden, wenden Sie sich an Kundenservice und Support.
- Für eine Abfrage muss eine Datenbank indiziert werden, damit Sie schnell sehen können, was in der Datenbank enthalten ist. Wenn Sie die langsame Abfrage identifizieren können, führen Sie „Plan erklären“ aus, um zu sehen, ob Optionen für die Indizierung verfügbar sind. „Erklärungsplan“ ist eine SQL-Funktion, die die Abfrage und was mit ihr passiert.

Business-Regeln „Vor Abfrage“.

Sie können eine Geschäftsregel „Vor Abfrage“ verwenden, um die Datentrennung in einer Instanz zu unterstützen. ServiceNow Anwendungen, die die Domänentrennung unterstützen, unterstützen möglicherweise nur die Trennung von Daten und Datenweiterleitung, verfügen über erweiterte Geschäftslogiktrennung oder unterstützen die Verwaltung der Anwendung auf Mandantenebene (Kundenebene).

Eine Geschäftsregel „Vor Abfrage“ ist ergänzender Code, mit dem Sie die Datentrennung in domänengetrennten Umgebungen unterstützen.

⚠ **Warnung:** Verwenden Sie nicht die Geschäftsregel „Vor Abfrage“ anstelle des Plugins „Domain Separation“. Diese Geschäftsregel verhindert Datenverlust nicht so sicher wie das Plugin.

Verwendung der Geschäftsregel „Vor Abfrage“ für die Datentrennung

In folgenden Situationen können Sie die Geschäftsregel „Vor Abfrage“ mit Datentrennung verwenden:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn die Domänentrennung von einer Anwendung ServiceNow nicht unterstützt wird und Sie einem oder mehreren nicht internen Kunden außerhalb der Organisation des Service Providers Tabellen- oder Zeilenzugriff gewähren oder einschränken müssen.

  Hinweis: Bevor Sie mit der Entwicklung von beginnen, wenden Sie sich bezüglich der Anwendungs-Roadmap für dieses Produkt an den Kundensupport von ServiceNow. Verbesserungen des Domänensupports sind möglicherweise für bevorstehende Releases geplant.

- Wenn eine Tabelle domänengetrennt ist, der Zugriff auf ihre Zeilen jedoch basierend auf bestimmten Bedingungen gewährt oder eingeschränkt werden muss, die nur für eine Reihe von Domänen im System gelten.

  Hinweis: Beispiel: Ein Kunde in der X-Domäne hat mehrere Lieferanten, die diese Domäne unterstützen, und diesen Lieferanten wird nur der Zugriff auf die Datensätze gewährt, die ihnen zugewiesen sind.

Punkte, die vor der Erstellung von Business-Regeln für „Vor Abfrage“ zu berücksichtigen sind

Sie können ein Skript für Business-Regeln vom Typ „Vor Abfrage“ erstellen, um den Zugriff auf über- und untergeordnete Tabellen basierend auf einer Kombination aus Benutzerinformationen, Gruppenmitgliedschaften, Unternehmen, Rollen oder datensatzspezifischen Feldbedingungen zu verhindern. Geschäftsregeln vom Typ „Vor Abfrage“ werden in separaten Domänen platziert und so erstellt, dass sie global für eine bestimmte Verzweigung einer Domänenhierarchie gelten.

- Soweit möglich, erstellen Sie Geschäftsregeln vom Typ „Vor Abfrage“ im niedrigstmöglichen Teil der Domänenhierarchie, damit die Regel nur für Benutzer ausgeführt wird, für die sie gilt.
- Beachten Sie, dass es im System Szenarien gibt, in denen Geschäftsregeln möglicherweise nicht ausgeführt werden oder in denen eine durch einen Benutzer ausgelöste Interaktion möglicherweise keine Ausführung einer Geschäftsregel auslöst. Beispielsweise wird eine Geschäftsregel nicht ausgeführt, wenn Sie Transformationszuordnungen mit deaktivierter Option „Business-Regeln ausführen“ oder Skripts mit deaktiviertem Workflow haben.
- Füllen Sie immer das Bedingungsfeld aus, um anzugeben, wann die Regel ausgeführt wird. Sie können beispielsweise angeben, ob die Geschäftsregel nur für bestimmte Lieferanten in einer Domäne gilt.

  Warnung: Beschränken Sie beim Entwerfen und Codieren von Geschäftsregeln (besonders Abfragegeschäftsregeln) ODER-Klauseln und Suchen in nicht indizierten Feldern. Zu viele ODER-Klauseln und Suchen in nicht indizierten Feldern können Abfragen verlangsamen oder die Leistung Ihrer Instanz beeinträchtigen.

- Verwenden Sie die Geschäftsregeln vom Typ „Vor Abfrage“ nur bei Bedarf. Zu viele Regeln vom Typ „Vor Abfrage“ können sich auf die Leistung Ihrer Instanz auswirken.

Geschäftsregeln vom Typ „Vor Abfrage“ werden vor Zugriffssteuerungslisten (ACLs) ausgeführt und weisen im Allgemeinen eine bessere Leistung auf. Dies gilt insbesondere, wenn Sie die zurückgegebenen Ergebnisse auf die Benutzer in Service Provider-Umgebungen (SP) beschränken, die Zugriff auf mehrere Domänen im System haben.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Das Filtern der Daten erfolgt transparent (im Gegensatz zu ACLs) für Benutzer, die die Nachricht, dass `Datensicherheit beschränkt, nicht sehen.` bei der Interaktion mit Daten.

Wann sollten Business-Regeln und ACLs vom Typ „Vor Abfrage“ nicht verwendet werden?

Seien Sie vorsichtig, wenn Sie Geschäftsregeln und ACLs vom Typ „Vor Abfrage“ verwenden, um Kundendaten zu trennen. Durch die Verwendung von Geschäftsregeln und ACLs erstellen Sie Anpassungen, die Sie dann verwalten müssen. Anpassungen können potenziell zu Leistungsproblemen führen. Ihre Entwicklungsteams sollten Prozesse erstellen, um sicherzustellen, dass das System nicht beschädigt wird.

Domain Separation bietet mit der aktuellen Domänenpfadabfragemethode (v3), einem weithin unterstützten Framework, sowohl Skalierbarkeit als auch Governance. Die Plattform- und App-Teams von ServiceNow sind für die Wartung des Frameworks verantwortlich und entlasten den Kunden.

Bei Unternehmen mit vielen Kunden in vielen Instanzen kann die übermäßige Verwendung von Vor Abfragen und ACLs dazu führen, dass die Datenbankabfragen nicht gut funktionieren.

Wie Domain Separation aktiviert wird

Sie können Domain Separation mit dem Plugin ServiceNow aktivieren. Ein Produktmanager, der von einem Entwicklungsteam unterstützt wird, verwaltet die Funktionalität. Erweiterungen und Korrekturen für die Funktion zur Domänentrennung sind in den Releases ServiceNow enthalten. Instanzbesitzer können sich an Kundenservice und Support -Ressourcen wenden, z. B. Serviceportal, unter https://support.servicenow.com , um Unterstützung bei der Domänentrennung zu erhalten.

Domänenpfad wird in Skripts vermieden

Domänenpfade können dazu führen, dass sich die Werte Ihres Skripts ändern oder sogar ungültig sind. Verwenden Sie sie daher nicht in Skripts.

Ihr Skript darf nicht vom Domänenpfad abhängen, denn wenn Sie die Domänenhierarchie ändern, wird der Domänenpfad neu berechnet und sein Wert geändert. Wenn dies passiert, sind Ihre Skripts nutzlos oder können Fehler auslösen oder abbrechen. Die beste Strategie besteht darin, Ihre Skripts nicht auf Grundlage von Domänenpfaden zu schreiben.

Verwenden Sie das Feld **sys_domain** in Ihren Skripts, anstatt vom Domänenpfad abhängig zu sein. Wenn Sie die Domänenhierarchie ändern, wird der Domänenpfad neu berechnet, und sein Wert ändert sich. Dies kann dazu führen, dass Ihre Skripts unbrauchbar sind, Fehler auslösen oder abbrechen. Suchen Sie nach Geschäftsregeln des Basissystems, die das Feld **„sys_domain“** verwenden, um Ideen zu sammeln, bevor Sie eigene Skripts erstellen.

Die Plattform ServiceNow erfasst die sys_domain_path-Werte in einem Update Set nicht, um Probleme mit Unterschieden in der Domänenhierarchie für jede Instanz zu vermeiden. Daher sollten Sie die Domänenhierarchie validieren, nachdem Sie ein Update Set importiert haben, um sicherzustellen, dass die Domänenpfadwerte für Ihre Datensätze korrekt sind.

Weitere Informationen zum Domänenpfad finden Sie unter Domänentrennung anfordern und Domain Separation Center.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Domänenzuweisungen

Die Art der Zuweisung einer Domäne wirkt sich auf den Wert des Felds „sys_domain“ aus. Die Zuweisungen enthalten Designs und Geschäftseigenschaften, die sich auf die Funktionsweise der Anwendung in den einzelnen Domänen auswirken.

Wert des Felds „sys_domain“.

Der Wert des **Felds sys_domain** enthält die Domäne, die dem Datensatz durch eine der folgenden Optionen zugewiesen wurde:

- Unternehmen, dem der Benutzer angehört
- Geschäftsregel, die beim Erstellen des Datensatzes verwendet wird
- Modul, das beim Erstellen des Datensatzes verwendet wird
- Formularvorlage, die beim Erstellen des Datensatzes verwendet wird
- Domäne des übergeordneten Datensatzes
- Domäne, die dem Benutzerdatensatz zugewiesen ist
- Domäne des Benutzers, der sie erstellt

Stellen Sie sicher, dass Ihre Domänenzuweisungsstrategien und Designs gut dokumentiert und getestet sind, damit Sie Datensätze erstellen, wenn diese Strategien und Designs in die richtige Domäne eingefügt werden. Auf diese Weise können Sie sehen, dass die Eigenschaften jeder Domäne Sie duplizieren oder ändern müssen.

Domain Separation und das Plugin Kundenservice-Management (CSM)

Um das beste Ergebnis zu erreichen, beachten Sie, wie die Eigenschaften im Plugin CSM funktionieren. Wenn das Plugin aktiviert ist, können Sie den Status Ihrer Datensätze in Ihren Domänen anzeigen.

Instanzbesitzer sollten sich an [] wenden, um die Eigenschaft *csm_auto_account_domain_generation*Kundenservice und Support zu aktivieren.

Hinweis: Diese Basissystemeigenschaft befindet sich in der Tabelle „Systemeigenschaften“ und ist verfügbar, nachdem CSM-Plugins aktiviert wurden.

Was die Eigenschaft bewirkt

Wenn in der Anwendung „Customer Service“ ein neuer Account erstellt wird, wird eine Domäne erstellt und unter der TOP-Domäne platziert. Wenn das übergeordnete Feld im Account-Formular ausgefüllt ist und ein neuer Datensatz eingefügt wird, wird dieser Account als Subdomäne des übergeordneten Elements erstellt.

Was geschieht, wenn diese Eigenschaft nicht „wahr“ ist und die Domäne aktiviert ist?

Neue Account-Datensätze in einer domänengetrennten Umgebung werden automatisch in der Standarddomäne platziert.

In der Header-Leiste wird der Status der Datensätze angezeigt, bei denen das Plugin aktiviert ist.

Domain Separation – Hilfe

Zusätzliche Unterstützung zu Domain Separation

Videoübersicht über Domain Separation

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkunden, Lernen, Entwickeln

Empfohlene Vorgehensweisen

Tipps und Tricks zum sinnvollen Erstellen und Entwickeln Ihrer Domänenstruktur

Konzepte für Service Provider

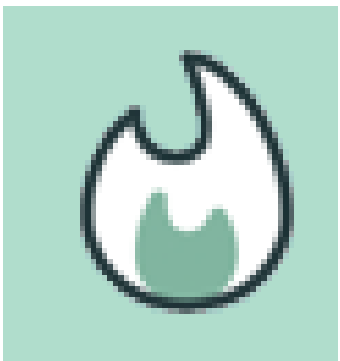
Konzepte, die mit der Plattform ServiceNow funktionieren, um Sie bei der Lösung allgemeiner Anwendungsfälle zu unterstützen

Supportstufen nach Anwendung

Wird Domain Separation für Ihre Anwendung unterstützt? Siehe Supportstufen und Anwendungsfälle.

Klassen

- Für Entwickler: ServiceNow Developer Site Domain Separation
- Für Service Provider: Domain Separation für Service Provider (Now Learning-Anmeldung erforderlich)



Safe Workplace-Suite und Domänentrennung

ServiceNow Safe Workplace-Anwendungen helfen Ihnen, Ihre Arbeitsplätze wieder zu öffnen und die Gesundheit und Sicherheit Ihrer Mitarbeiter nach Notfällen und Pandemien wie COVID-19 zu gewährleisten. Die Suite enthält viele Anwendungen, die Ihr Unternehmen bei der Mobilisierung, Wiederherstellung und Neuerstellung unterstützen.

Setup und Verwaltung

- Upgrades
- Domänentrennung anfordern
- Erstellen Sie eine Domäne

Problembehandlung

- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support
- In der Community Fragen stellen oder beantworten

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

• Konfiguration, die an interne oder externe Kunden delegiert werden kann		

Einrichtung und Verwaltung der Domänentrennung

Das Einrichten von Domain Separation umfasst das Anfordern der Aktivierung eines Plugins, das Festlegen von Optionen und das Zuweisen von Benutzern und Datensätzen zu Domänen.

Gehen Sie wie folgt vor, um Domain Separation einzurichten:

1. Domänentrennung anfordern
2. Erstellen Sie eine Domäne
3. Fügen Sie einer Tabelle ein Domänenfeld hinzu

Sie können die folgenden grundlegenden administrativen Aufgaben auch für Domänen ausführen:

- Aktivieren oder deaktivieren Sie eine Domäne
- Zeigen Sie Domänenbeziehungen an
- Domänenbereich erweitern
- Erstellen Sie eine domänenspezifische Auswahlliste

Unter Erweiterte Verwaltung mit Domänentrennung finden Sie eine Liste der Aufgaben, die Sie ausführen müssen, nachdem Sie Domain Separation eingerichtet und grundlegende Administrationsaufgaben ausgeführt haben.

Domänentrennung anfordern

Alle Domänenunterstützungsfunktionen werden mit dem Plugin „ **Domänensupport – Installationsprogramm**für Domänenerweiterungen“ aktiviert. Administratoren können die Aktivierung dieses Plugins anfordern.

Vorbereitungen

Wenden Sie sich an Ihren ServiceNow-Kundenbetreuer, um ein Abonnement zu erwerben. Der Account Manager sorgt im Allgemeinen innerhalb weniger Tage für die Aktivierung des Plugins *com.glide.domain.msp_extensions.installer* in den Produktions- und Test- und Entwicklungsumgebungsinstanzen Ihrer Organisation.

Wenn Sie keinen Account Manager haben, die Aktivierung nach dem Kauf verzögern oder das Produkt in einer Test- und Entwicklungsumgebung kostenlos testen möchten, führen Sie die folgenden Schritte aus.

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn das Plugin „Domain Support – Domain Extensions Installer“ bereits aktiv ist, werden Inhalte im Plugin „Domain Support – Domain Extensions Installer“ nicht installiert, um einen möglichen Konflikt mit einer vorhandenen Implementierung zu vermeiden.

Domänentrennung ersetzt Unternehmenstrennung. Ab dem Helsinki-Release kann das Plugin „Company Separation“ nicht mehr aktiviert werden. Wenn jedoch die Unternehmenstrennung bereits aktiv ist, wenn Sie die Domänentrennung aktivieren, sind

Automatische Übersetzung

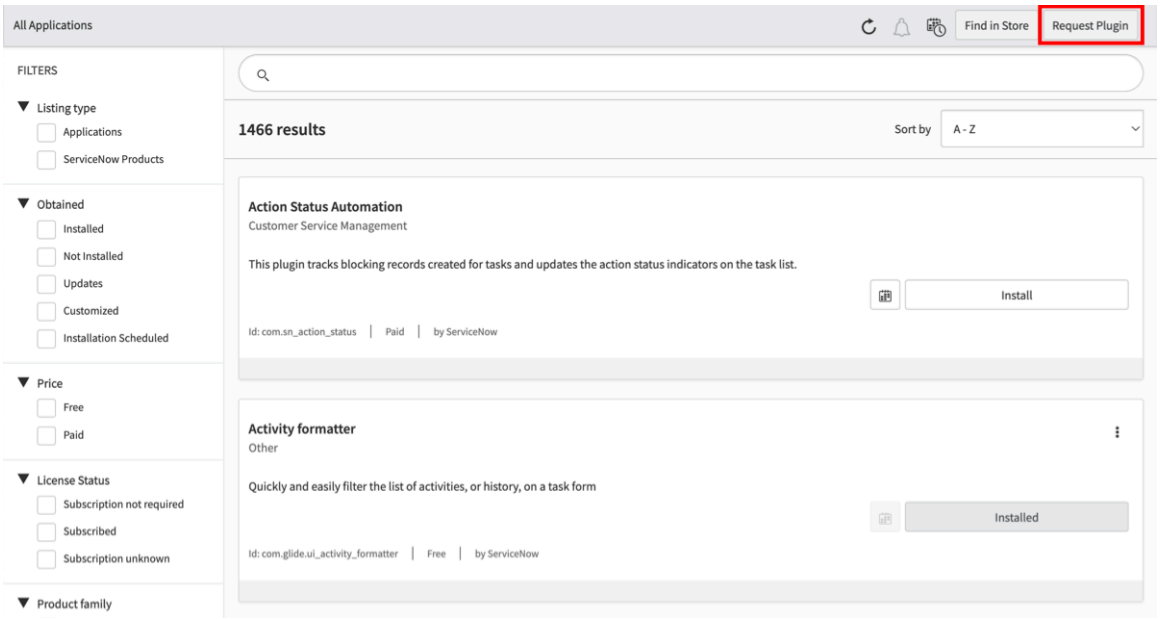
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

beide Plugins gleichzeitig aktiv. Sie können den Aktivierungsstatus der Unternehmenstrennung mit der Eigenschaft *glide.db.separation.field* steuern.

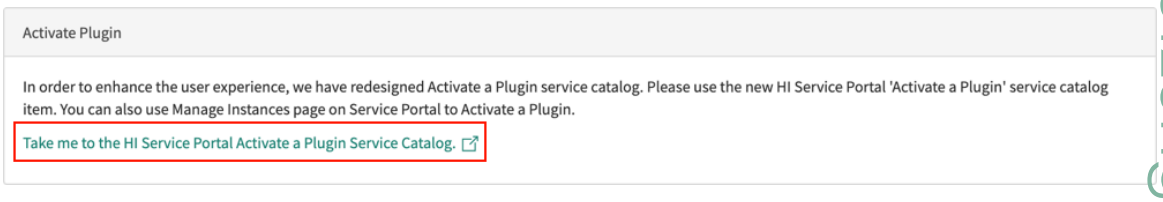
Hinweis: Domänenpfade werden für alle Kunden in Helsinki und höher verwendet. Die Domänennummerierung wird nicht mehr verwendet. Kundenservice und Support kann beim Upgrade helfen.

Prozedur

1. Navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Klicken Sie auf der Seite „Alle Anwendungen“ auf **Plugin anfordern**, um das Formular **Plugin aktivieren** auf Now Support zu öffnen.



3. Wählen Sie unter Now Support den Link aus, um auf Now Support Serviceportal Servicekatalog zuzugreifen.



4. Wählen Sie Ihre Instanz aus.
5. Wählen Sie **Aktionen > Plugin aktivieren** aus.
6. Geben Sie im Formular **Plugin aktivieren** die folgenden Informationen an.

Formular „Plugin anfordern“

Feld	Beschreibung
What is your target instance (Ihre Zielinstanz)	Instanz, auf der das Plugin aktiviert werden soll.

Automatische Übersetzung

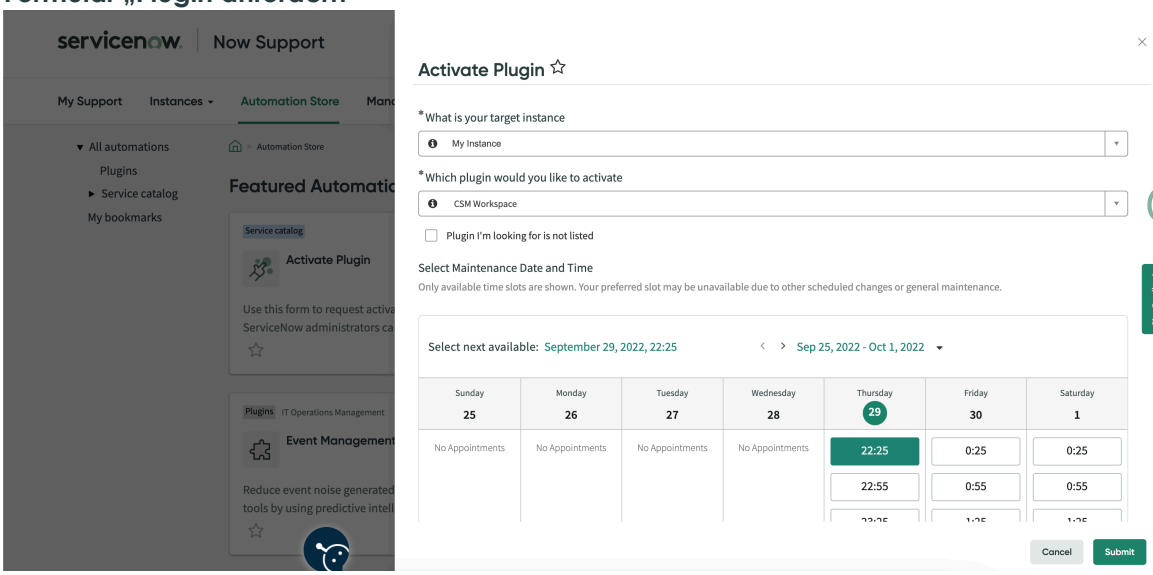
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Which plugin would you like to activate (Welches Plugin möchten Sie aktivieren?)	Name des zu aktivierenden Plugins **Hinweis:** Wenn das System das gewünschte Plugin nicht auflistet oder wenn Sie das Plugin auf einer OEM- oder lokalen Instanz aktivieren, aktivieren Sie das Kontrollkästchen **Plugin I'm looking for is not listed (Gesuchtes Plugin ist nicht aufgelistet)**, und geben Sie dann den Namen des Plugins ein.
Select Maintenance Date and Time (Datum und Uhrzeit der Wartung)	Datum und Uhrzeit zum Aktivieren des Plugins. **Hinweis:** Plugins werden in der pazifischen Zeitzone jeden Werktag in zwei Batches aktiviert, einmal am Morgen und einmal am Abend. Wenn das Plugin zu einem bestimmten Zeitpunkt aktiviert werden muss, geben Sie die Anforderung bei **Grund/ Kommentare** ein.

Example

Betrachten Sie beispielsweise das folgende Formular, um das Plugin „CSM Workspace“ in einer Instanz mit dem Namen „My Instance“ zu aktivieren.

Formular „Plugin anfordern“



7. Wählen Sie **Absenden**.
   Weitere Informationen zum Anfordern eines Plugins finden Sie im Artikel Plugin aus dem Servicekatalog anfordern [KB0751715] in der Now Support Knowledge Base.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse
Durch die Aktivierung des Plugins „Domain Extension Installer“ werden folgende Funktionen aktiviert:

- Die Domänentrennung basiert auf der `Domänentabelle [sys_domain]`.
- Mit der delegierten Verwaltung kann jede Domäne über eine separate Richtlinie verfügen.
- Alle Datensätze sind Teil der globalen Domäne.
- Die Domäne des aktuellen Benutzers bestimmt die zu verwendende Domäne, wenn Sie einen Datensatz in einer anderen Domäne anzeigen oder bearbeiten.

Zugehörige Informationen

Domain Separation-Plugin

Domain Separation-Plugin

Das Plugin „Domain Support – Domain Extensions Installer“ aktiviert mehrere Funktionen und Eigenschaften zur Domänentrennung gleichzeitig. Dieses Plugin wird normalerweise als Domain Separation-Plugin bezeichnet.

Empfohlene Vorgehensweise für die Aktivierung des Domain Separation-Plugins

Im Rahmen der Entwicklung der Domänentrennung müssen Administratoren die Aktivierung dieses Plugins anfordern. Um die besten Ergebnisse zu erzielen, aktivieren Sie das Domain Separation-Plugin zu Beginn des Entwicklungsprozesses, vorzugsweise bevor ein anderes Plugin aktiviert wird.

Wichtig: Fordern Sie die Aktivierung des Plugins „Domain Extensions Installer“ (com.glide.domain.msp_extensions.installer) an, bevor Sie Domain Separation (Plugin com.snc.pa.domain_support) aktivieren.

Wenn Sie Domain Separation gegen Ende der Implementierung von ServiceNow oder nachdem eine Instanz live geschaltet wurde, aktivieren, ist Ihre Anwendung gefährdet in Bezug auf Leistung und Prozess. In etablierten Instanzen könnten je nach Strukturierung der Elemente in der Entwicklung hohe Risiken für die Plattform und ihre Verwendbarkeit bestehen. Weitere Informationen zum Domänentrennungsprozess finden Sie unter Domain Separation erkunden.

Wenn beispielsweise das Plugin „Domain Separation“ aktiviert ist, wird die Spalte „ **Domäne** “ (sys_domain) zur Aufgabentabelle hinzugefügt, und jeder vorhandene Datensatz wird automatisch in „ **Global**“ platziert. Um ein Skript zum Zuweisen aller Datensätze in die richtigen Domänen zu verwenden, ist eine etablierte Hierarchie über- und untergeordneter Elemente erforderlich. Diese Arten von geskripteten Aktionen bergen das Risiko der Beschädigung oder des Verlusts von Daten und mögliche Produktionsausfälle, wenn große Datenmengen verschoben werden. Ein Großteil des Plattformcodes wird ebenfalls im **globalen**platziert, z. B. in Business-Regeln, Client-Skripts, Formularansichten und Workflows.

Wenn ein Kunde Code erstellt oder ServiceNow ändert, besteht ein Risiko für die Leistung und Verwendbarkeit der Plattform. Instanzbesitzer können mit dieser Art von Herangehensweise die Implementierung erheblich verzögern oder zu langen Ausfallzeiten kommen.

Funktionen des Plugins „Domain Separation“.

Diese Funktionen werden aktiviert, wenn Sie das Plugin aktivieren:

- Die Domänentrennung basiert auf der `Domänentabelle [sys_domain]`.
- Mit der delegierten Verwaltung kann jede Domäne über eine separate Richtlinie verfügen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Alle Datensätze sind Teil der globalen Domäne.
- Die Domäne des aktuellen Benutzers bestimmt die zu verwendende Domäne, wenn Sie einen Datensatz in einer anderen Domäne anzeigen oder bearbeiten.

Zugehörige Informationen

Empfohlene Domain Separation-Verfahren für Service Provider

Systemeigenschaften und Benutzereinstellungen für Domänen

Administratoren haben Zugriff auf Eigenschaften und Anwendereinstellungen, die den Domänenbereich steuern.

Eigenschaften

Bei neuen Aktivierungen von Domain Separation wird der Domänenbereich für alle zugehörigen Daten oder Prozesse automatisch auf die Domäne des Datensatzes beschränkt. Wenn der Benutzer einen Datensatz in einem Formular anzeigt, sind die zugehörigen Daten (z. B. Referenzauswahl und zugehörige Listendaten) und angewendeten Prozesse (z. B. Business-Regeln und Client-Skripts) auf den Domänenbereich des Datensatzes beschränkt. Wenn auf mehreren Registerkarten Datensätze vorhanden sind, hat jede Registerkarte einen eigenen Domänenbereich basierend auf dem auf dieser Registerkarte geöffneten Datensatz. Die folgenden Eigenschaften beschränken den Domänenbereich auf die Domäne des Datensatzes und die Domäne der aktuellen Sitzung des Benutzers.

Systemeigenschaften für Domänen

Eigenschaft	Details
glide.sys.domain.use_record_domain_for_processes	Schränkt den Domänenbereich für alle Prozesse auf die Domäne des Datensatzes ein. Diese Eigenschaft gilt nicht für Geschäftsregeln. Geschäftsregeln werden immer vom Domänendatensatz aus verarbeitet. • *Typ*: true | false • *Standardwert*: true • *Speicherort*: Tabelle „Systemeigenschaft“ [sys_properties]
glide.sys.domain.use_record_domain_for_data	Beschränkt den Domänenbereich für alle Daten auf die Domäne des Datensatzes. • *Typ*: true | false • *Standardwert*: „true“ bei Aktivierungen neuer Domänen ab Fuji (Upgrades von Instanzen, die älter als Fuji sind, enthalten diese Eigenschaft nicht in der Tabelle) • *Speicherort*: Tabelle „Systemeigenschaft“ [sys_properties]

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die Eigenschaft *glide.sys.domain.use_record_domain_for_processes* oder *glide.sys.domain.use_record_domain_for_data* auf **true**festgelegt ist, werden die folgenden Eigenschaften unabhängig von ihrer Einstellung nicht verwendet:

- *glide.sys.domain.use_record_domain*
- *glide.sys.domain.use_record_domain_for_client_scripts*
- *glide.sys.domain.domain_change_notify*
- *glide.sys.domain.no_change_roles*

Eine vollständige Liste der Eigenschaften finden Sie unter Verfügbare Systemeigenschaften .

Hinweis:

Bei Neuaktivierungen von Domain Separation ab dem Jakarta-Release bestimmt die Sitzungsdomäne die in der Domänentabelle ausgeführten Geschäftsregeln. In früheren Versionen wurden in der Domänentabelle ausgeführte Geschäftsregeln basierend auf der Hierarchie der neu erstellten Domäne festgelegt. Dieses Verhalten wird durch die Eigenschaft *glide.sys.domain.skip_domain_insert_businessrules* geändert. Durch das Festlegen dieser Eigenschaft auf „wahr“ wird die Leistung beim Einfügen von Domänen erheblich verbessert.

Domänenbereichseigenschaften für Geschäftsregeln, die in der Domänentabelle ausgeführt werden

Eigenschaft	Details
glide.sys.domain.skip_domain_insert_businessrules	Gibt den Domänenbereich für Geschäftsregeln an, die in der Domänentabelle ausgeführt werden. Bei neuen Aktivierungen von Domain Separation ist die Eigenschaft standardmäßig auf „true“ festgelegt, und Geschäftsregeln werden von der Sitzungsdomäne bestimmt. In vorhandenen Implementierungen ist der Standardwert für die Eigenschaft „false“, und die Geschäftsregeln werden durch die Hierarchie der neu erstellten Domäne bestimmt. • *Typ*: true | false • *Standardwert*: „Wahr“ bei neuen Domänenaktivierungen ab Jakarta. False in vorhandenen Implementierungen.
glide.sys.domain.skip_non_global_businessrule_if_ndomain	Stellt sicher, dass nur „bus.rules“ aus der globalen Domäne ausgeführt werden, wenn

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Domänenbereichseigenschaften für Geschäftsregeln, die in der Domänentabelle ausgeführt werden (Fortsetzung)

Eigenschaft	Details
	„queryNoDomain()“ verwendet wird oder wenn die Tabelle nicht domänengetrennt ist, sodass Sie alle anderen Business-Regeln überspringen können • *Typ*: true | false • Wenn Sie die Eigenschaft auf „false“ setzen, wird das alte Verhalten wiederhergestellt und entspricht nicht den ServiceNow® empfohlenen Vorgehensweisen. • Empfohlen: Trennen Sie Ihre Tabellen von der Domäne. Versuchen Sie immer, die Domäne des Datensatzes und nicht die Sitzungsdomäne zu verwenden.

Anwendereinstellungen

Darüber hinaus können Benutzeradministratoren die folgenden Benutzereinstellungen global oder für einzelne Benutzer festlegen:

Benutzereinstellungen für den Domänenbereich

Einstellungen	Kategorie	Aktualisiert von	Details
glide.domain.session_scope	Domäne	Nur Administrator	Bei „wahr“ wird der Standardbereich auf die Sitzungsdomäne des Benutzers und nicht auf die Domäne des Datensatzes festgelegt. Bei „false“ ist der Standardbereich die Domäne des Datensatzes. Benutzer mit der Benutzerrolle „domain_expand_scope“ können den Domänenbereich weiterhin nach Bedarf ändern.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benutzereinstellungen für den Domänenbereich (Fortsetzung)

Einstellungen	Kategorie	Aktualisiert von	Details
			• **Typ**: true | false • **Standardwert**: false
glide.domain.session_scope_notification	Domäne	Nur Administrator	Bei „wahr“ wird ein visueller Hinweis darauf angezeigt, dass Datensatzwerte einen erweiterten Domänenbereich enthalten. Bei „false“ wird die Benachrichtigung ausgeblendet. • **Typ**: true | false • **Standardwert**: true

Zugehörige Informationen

Eigenschaften der Anwendung zur Domänentrennung

Erstellen Sie eine Domäne

Sie können eine Domäne erstellen, indem Sie einen Datensatz in der Tabelle [Domäne] erstellen.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Beachten Sie beim Erstellen einer neuen Domäne Folgendes:

- Nur eine Domäne kann die Standarddomäne sein.
- Nur eine Domäne kann die primäre Domäne sein.

Prozedur

1. Navigieren zu **Alle** > **Domänenadministrator** > **Domänen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die erforderlichen Felder aus (siehe Tabelle).
4. Klicken Sie auf **Absenden**.

Domänenformularfelder

Feld	Beschreibung
Name	Geben Sie einen eindeutigen Namen für die Domäne ein.
Typ	Wählen Sie einen Domänentyp aus, der die Domäne beschreibt. Standardmäßig sind die *Domänentypen Lieferant*, *Kunde*und *MSP*. Sie können auch eigene Auswahlmöglichkeiten hinzufügen.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Primär	Aktivieren Sie das Kontrollkästchen, wenn diese Domäne die Domäne der obersten Ebene in der Hierarchie sein soll. Die Domäne der obersten Ebene hat nur untergeordnete Domänen und keine übergeordneten Domänen.
Standard	Wählen Sie aus, ob diese Domäne die Standarddomäne für Ihre Hierarchie sein soll.
Übergeordnet	Wählen Sie den Namen der Domäne höher in der Hierarchie aus, die diese Domäne enthält. Dieses Feld muss einen Wert aufweisen, damit die Domäne in der Domänenzuordnung angezeigt wird.
Aktiv	Aktivieren Sie das Kontrollkästchen, um die Domäne zur Verwendung verfügbar zu machen. Sie müssen diese Option auswählen, damit diese Domäne in der Domänenzuordnung angezeigt wird.
Beschreibung	Geben Sie eine Beschreibung für die Domäne ein.

Jeder Domänendatensatz kann auch mehrere zugehörige Datensätze haben:

- Unternehmen
- Enthält Domänen
- Enthalten in

Nächste Maßnahme
Um die Domänenhierarchie zu ändern, wechseln Sie zur zugehörigen Liste „Enthält Domänen“ und wählen Sie die Domänendatensätze aus, die die untergeordneten (enthaltenen) Domänen der Beziehung „Enthält“ sind.

Legen Sie eine Domäne als Standard fest

Eine Domäne wurde zur Standarddomäne gemacht, der das System automatisch Aufgaben- und Benutzerdatensätze zuweist, die noch keiner Domäne zugewiesen sind.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Hinweis: Wenn Sie keine Standarddomäne festlegen, werden neue Aufgaben und Benutzerdatensätze in der globalen Domäne platziert.

Prozedur

1. Navigieren zu **Alle** > **Domänenadministrator** > **Domänen**an.
2. Öffnen Sie die Domäne, die Sie als Standarddomäne festlegen möchten, z. B. Main.
3. Konfigurieren Sie das Formularlayout so, dass das Feld **Standard** hinzugefügt wird.
4. Aktivieren Sie das Kontrollkästchen **Default (Standard)**.
5. Klicken Sie auf **Aktualisieren**.

Verwalten Sie die Domäne manuell für bestimmte Datensätze

Standardmäßig weist das System automatisch eine Domäne basierend auf dem Unternehmensdatensatz des Benutzers zu. In einigen Fällen möchten

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Domänenadministratoren jedoch manuell verwalten, zu welcher Domäne ein bestimmter Datensatz gehört.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Im Feld **Verwaltete Domäne** können Domänenadministratoren manuell eine Domäne für den Benutzer-, Gruppen-, Abteilungs-, Standort- oder CI-Datensatz auswählen, anstatt die automatisch vom Unternehmensdatensatz zugewiesene Domäne zu verwenden. Das Feld **„Verwaltete Domäne** " ist für diese Datensatztypen verfügbar.

- Benutzerdatensätze
- Gruppendatensätze
- Abteilungsdatensätze
- Standortdatensätze
- CI-Datensätze

Prozedur
1. Navigieren Sie zu dem Datensatz, den Sie manuell verwalten möchten.
2. Aktivieren Sie das Kontrollkästchen **Verwaltete** Domäne.
3. **Wählen** Sie im Feld Domäne die Domäne für den Datensatz aus.
4. Klicken Sie auf **Aktualisieren**.

   Durch Deaktivieren des Kontrollkästchens **Verwaltete Domäne** wird das Feld **Domäne** ausgeblendet, und der Datensatz verwendet den Domänenwert aus dem Unternehmen des Datensatzes.

Zugehörige Informationen

Empfohlene Domain Separation-Verfahren für Service Provider

Domänengetrennte Tabellen

Mit der Funktion „Domain Separated Tables" (Domänengetrennte Tabellen) können Sie auf einen Blick sehen, welche Tabellen in Ihrer Instanz domänengetrennt sind.

Übersicht

Verwenden Sie die Funktion „Domänengetrennte Tabellen", um zu sehen, welche Tabellen domänengetrennt sind. Beginnen Sie mit der Eingabe von „Domäne" im Filter **Alle**, um im linken Navigationsbereich auf Domänengetrennte **Tabellen** zuzugreifen.

Sie können diese Ansicht filtern, um Spaltennamen anzuzeigen oder zu entfernen und nach bestimmten Eigenschaften oder Attributen zu suchen, die in Ihren Tabellen enthalten sind. Es gibt zwei Tabellentypen, die in der Liste angezeigt werden:

- Tabellen, die eine explizite **Spalte** *sys_domain* enthalten, wobei der Spaltenname den Wert *sys_domain* in der Liste anzeigt.
- Tabellen, die das Attribut *domain_master* verwenden, um Domain Separation von einem referenzierten Datensatz abzuleiten, wobei die Spalte **Attribute** den Wert *domain_master=ref-field-value* enthält.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie im Menü „Spaltenname“ die Option „Übereinstimmungen anzeigen“ oder „Herausfiltern“ verwenden, können Sie diese beiden Tabellentypen anzeigen.

Domänenüberschreibungsbetrachter

Mit dem Domänenüberschreibungs-Viewer können Sie alle Ihre Prozessüberschreibungen gleichzeitig für die gesamte Instanz anzeigen und verwalten.

Übersicht

Anstatt eine aufwändige Suche nach Überschreibungen in Ihren Skripts zu erstellen, können Sie sie mit dem Domänenüberschreibungs-Viewer schnell finden. Beginnen Sie mit der Eingabe von „Domäne“ im Filter **Alle**, um im linken Navigationsbereich auf den **Domänenüberschreibungs-Viewer** zuzugreifen.

Die Tabellenauswahl im Domänenüberschreibungs-Viewer zeigt eine Liste nur der Tabellen an, die Datensatzüberschreibungen enthalten, zusammen mit der Anzahl der Überschreibungen in dieser Tabelle. Nachdem Sie eine Tabelle ausgewählt haben, wird eine Liste aller übergeordneten Datensätze mit Überschreibungen zurückgegeben. Sie können schnell alle **übergeordneten Datensätze**, die **Domäne** des übergeordneten Datensatzes und die **Anzahl** der Überschreibungen für jeden Datensatz anzeigen.

Wenn Sie Überschreibungen anzeigen **auswählen**, wird eine neue Registerkarte geladen, auf der alle Überschreibungen, einschließlich des übergeordneten Datensatzes, in der Standardlistenansicht angezeigt werden. Wählen Sie eine Tabelle aus der Dropdown-Liste aus, um alle Datensätze und Überschreibungen anzuzeigen. Wählen Sie für einen Datensatz die Option Überschreibungen anzeigen aus, um alle **datensatzspezifischen** Überschreibungen anzuzeigen.

Hinweis: Nur Tabellen mit Überschreibungen sind aufgelistet.

Weitere Informationen finden Sie unter Domänengetrennte Eigenschaftsüberschreibungen erstellen .

Aktivieren oder deaktivieren Sie eine Domäne

Wenn Sie eine Domäne aktivieren oder deaktivieren, wird der Aktivierungsstatus auf Unternehmen innerhalb der Domäne kaskadiert.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie einen Unternehmensdatensatz aktivieren, aktiviert Domain Separation automatisch die zugehörige Domäne des Unternehmens. Wenn Sie beispielsweise das Unternehmen ACME aktivieren, aktivieren Sie auch die Domäne TOP/ACME.

Prozedur

1. Navigieren Sie zum Domänendatensatz.
2. Deaktivieren oder aktivieren Sie das Kontrollkästchen **Aktiv**.
3. Klicken Sie auf **Aktualisieren**.

Warnung: Löschen Sie keine Domänen. Deaktivieren Sie Domänen, die Sie nicht mehr benötigen, anstatt sie zu löschen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fügen Sie einer Tabelle ein Domänenfeld hinzu

Als Administrator trennen Sie eine benutzerdefinierte Tabelle von der Domäne, indem Sie ihr ein Feld „sys_domain“ hinzufügen.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Hinweis:

Fügen Sie Basissystemtabellen keine Domänen hinzu.

Prozedur

1. Navigieren Sie zur Listenansicht der Tabelle.
   Beispiel: Typ <table name>`.list` im Navigationsfilter.
2. Klicken Sie mit der rechten Maustaste auf den Listenheader, und wählen Sie **Konfigurieren** > **Listenlayout**an.
3. Geben Sie im Abschnitt **Neues Feld erstellen**`sys_domain` als **Name** und `Domänen-ID` als **Typ**ein.
4. Klicken Sie auf **Hinzufügen**.
5. Klicken Sie auf **Speichern**.

Hinweis:

Bei jeder anderen Methode zum Erstellen eines Felds wird dem Spaltennamen das Präfix **u_ hinzugefügt**. Beim Feld Domäne erstellt das System das Feld jedoch automatisch ohne das Präfix **u_**. Sie können die folgenden Funktionen als Verknüpfung verwenden: Wenn Sie ein **sys_domain**-Feld erstellen, nennen Sie es **sys_domain**, und lassen Sie den Feldtyp unverändert. Das System legt den Feldtyp automatisch auf Domänen- **ID** und die Feldbezeichnung auf **Domäne**fest, wodurch Sie einige Klicks sparen.

Das Hinzufügen von Domänen zu Basissystemtabellen erfordert übermäßig gründliche Tests, Updates und das Hinzufügen neuer Logik. Außerdem ist der Quellcode in vielen Fällen für den Kunden nicht zugänglich.

Zeigen Sie Domänenbeziehungen an

Die Domänenzuordnung bietet Domänenadministratoren eine schreibgeschützte Darstellung der aktiven Domänen in der Instanz und ihrer Beziehung zueinander.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Für alle Domänenzuordnungen muss eine Domäne als primäre Domäne festgelegt sein. Darüber hinaus muss jede Domäne in der Domänenzuordnung die folgenden Kriterien erfüllen:

- Das Feld „ **Übergeordnet** “ muss ausgefüllt werden (die primäre Domäne ist die einzige Ausnahme).
- Das Kontrollkästchen **Aktiv** muss aktiviert sein.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Domänenzuordnung zeichnet keine Domänenbeziehungen für Domänen, die die Zuordnungskriterien nicht erfüllen.

Prozedur

1. Navigieren zu **Alle** > **Domänenadministrator** > **Domänenzuordnung**an.
2. Klicken Sie auf das Plussymbol (**+**) oder das Minussymbol (**–**) in den Domänenheadern, um Subdomänen ein- oder auszublenden.

Wählen Sie eine primäre Domäne aus

Die primäre Domäne gibt die Domäne der obersten Ebene in der Domänenzuordnung an.

Vorbereitungen
Erforderliche Rolle: admin

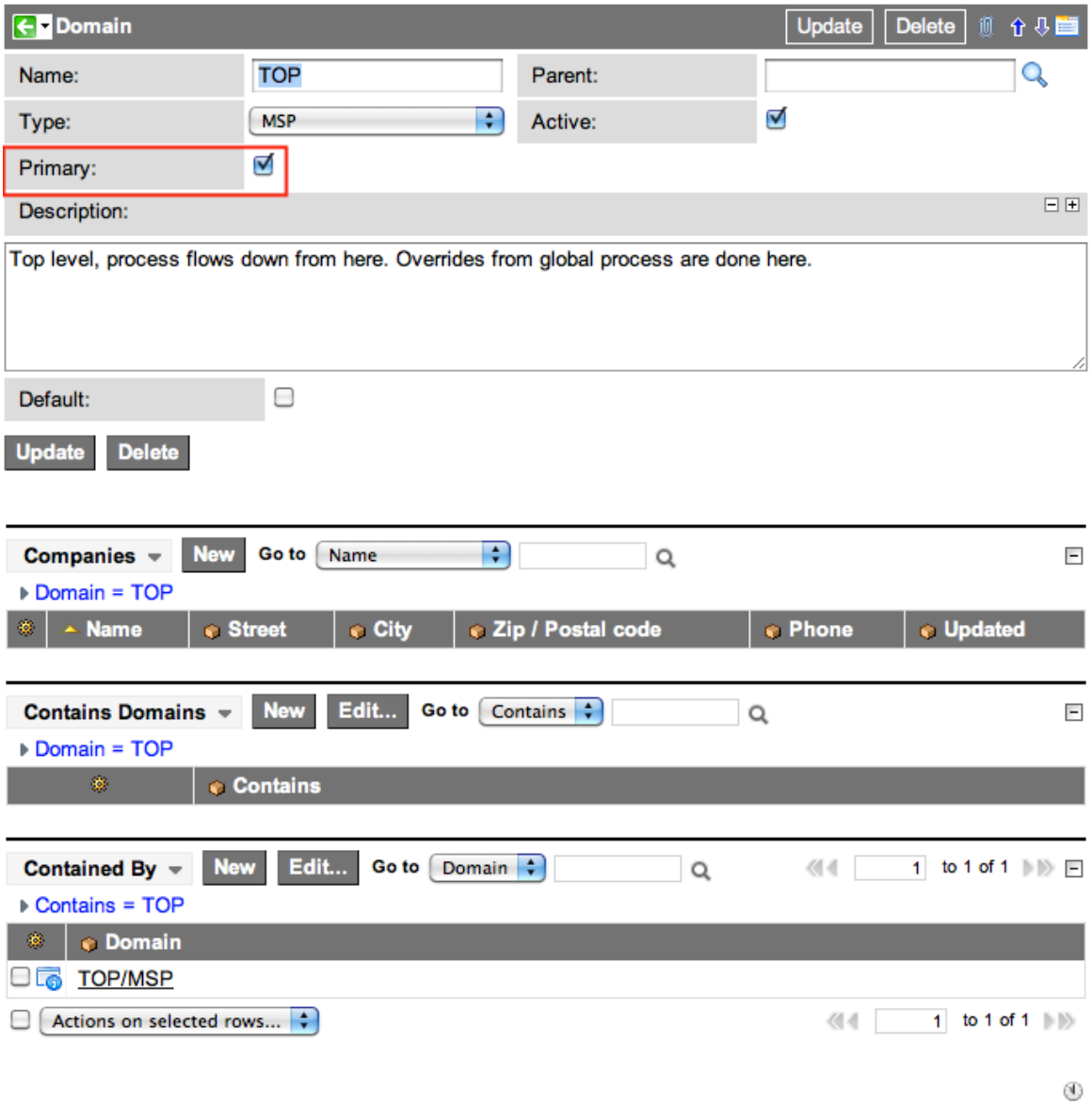
Warum und wann dieser Vorgang ausgeführt wird
Die primäre Domäne darf keine übergeordnete Domäne haben und muss mindestens eine untergeordnete Domäne haben. Es kann jeweils nur eine primäre Domäne geben. Wenn Sie eine andere Domäne als primäre Domäne auswählen, überschreibt diese die vorherige primäre Domäne.

Prozedur

1. Navigieren zu **Alle** > **Domänenadministrator** > **Domänen**an.
2. Wählen Sie die Domäne aus, die die primäre Domäne sein soll, z. B. TOP.
3. Aktivieren Sie die **Checkbox Primär**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Aktualisieren**.



Automatische Übersetzung

Erstellt „Enthält“-Beziehungen zwischen Domänen

Erstellen Sie eine „enthält“-Beziehung zwischen Domänen, um die Domänenhierarchie zu ändern.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

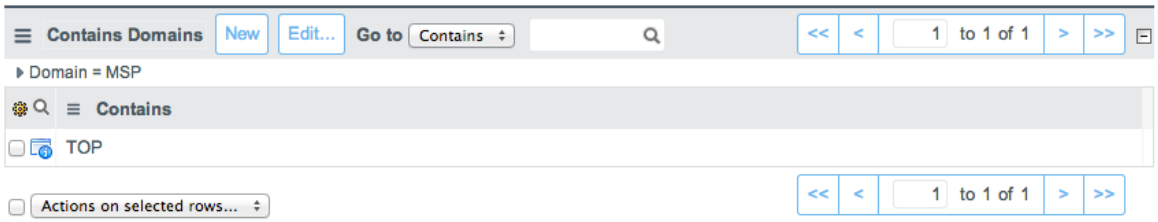
Domänen in einer Beziehung, die enthält, erben die Einstellungen der enthaltenen Domäne. Die enthaltende Domäne ermöglicht Benutzern das Anzeigen von Daten in der enthaltenen Domäne sowie in allen untergeordneten Elementen. Prozesse sind von einer Contains-Beziehung nicht betroffen.

Prozedur

1. Navigieren Sie zur Domänentabelle.
2. Wählen Sie den Domänendatensatz aus, der die übergeordnete Domäne (Container-Domäne) der neuen enthält-Beziehung ist.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Schalten Sie den Domänenbereich um, um bei Bedarf zwischen Sitzungsbereich und Datensatzbereich zu wechseln.
4. Klicken Sie in der zugehörigen Liste Enthält Domänen auf **Bearbeiten**.
5. Wählen Sie die Domänendatensätze aus, die die untergeordneten (enthaltenen) Domänen der Beziehung „enthält“ sind.
   Standardmäßig werden nur untergeordnete Domänen angezeigt, wenn die Domänenauswahl auf Global festgelegt ist. Schalten Sie den Domänenbereich um, um alle Domänen anzuzeigen.
6. Klicken Sie auf **Speichern**und dann auf **Aktualisieren**.



Zugehörige Informationen

Empfohlene Domain Separation-Verfahren für Service Provider

Domänenbereich erweitern

Wenn ein Benutzer in der globalen Domäne eine Tabelle mit einer Spalte **„sys_overrides“ anzeigt**, sieht er standardmäßig nur Datensätze aus der globalen Domäne. Wenn ein Administrator in der globalen Domäne eine Prozesstabelle anzeigt, sieht er nur Datensätze, die sich in dieser Prozesstabelle befinden.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Ändern Sie die Eigenschaft *glide.sys.restrict_global_domain_processes* in **true**.
2. Um Datensätze aus allen Domänen anzuzeigen, klicken Sie unter „Zugehörige Links“ auf **Domänenbereich erweitern**.
3. Um zum Anzeigen von Datensätzen nur aus der globalen Domäne zurückzukehren, klicken Sie auf **Domänenbereich reduzieren**.

Fügen Sie einer Liste mit Domänen mit Sichtbarkeit Domänen hinzu

Das Hinzufügen einer Sichtbarkeitsdomäne ermöglicht es einem Benutzer oder einer Gruppe, Datensätze aus einer anderen Domäne anzuzeigen und potenziell zu bearbeiten, unabhängig von der normalen Domänenmitgliedschaft des Benutzers oder der Gruppe.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Das Zuweisen von Sichtbarkeitsdomänen an alle Mitglieder einer Gruppe wird gegenüber der Erteilung an einzelne Benutzer bevorzugt.

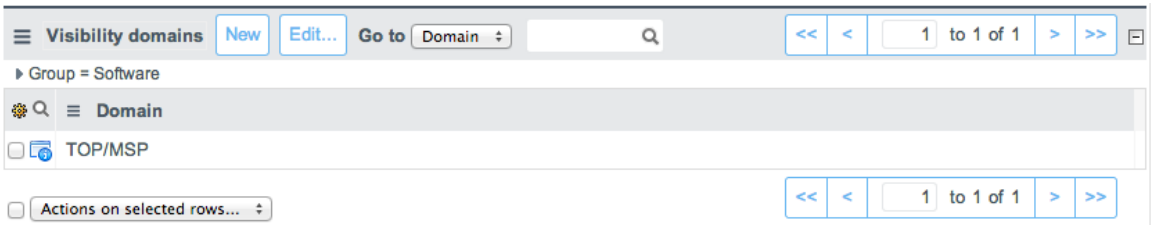
Hinweis: Durch das Hinzufügen einer Sichtbarkeitsdomäne werden die Anforderungen für die Zugriffssteuerungsregel einer Tabelle oder eines Datensatzes nicht geändert.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie zur Gruppentabelle.
2. Wählen Sie die Gruppe aus, für die Sie Sichtbarkeitsdomänen bereitstellen möchten.
3. Fügen Sie dem Formular die zugehörige Liste „ **Sichtbarkeitsdomänen“ hinzu**.
4. Klicken Sie in der zugehörigen Liste **Sichtbarkeitsdomänen** auf **Bearbeiten**.
5. Wählen Sie die Domänendatensätze aus, die für die Gruppe oder Domäne angezeigt werden sollen.
6. Klicken Sie auf **Speichern**und dann auf **Aktualisieren**.



Gewähren Sie einem einzelnen Benutzer Domänen mit Sichtbarkeit

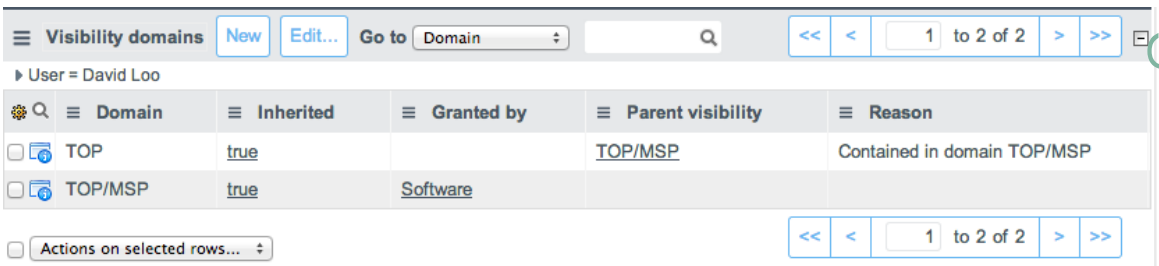
Es ist zwar möglich, im Benutzerformular Sichtbarkeitsdomänen für bestimmte Benutzer hinzuzufügen, am besten jedoch nur über Gruppen. Dies steuert Berechtigungen und Zugriffe, falls Mitarbeiter die Abteilung wechseln oder das Unternehmen verlassen.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Anwenderadministration** > **Anwender**an.
2. Wählen Sie den Benutzer aus, dem Sie Sichtbarkeitsdomänen bereitstellen möchten.
3. Fügen Sie dem Formular die zugehörige Liste „ **Sichtbarkeitsdomänen“ hinzu**.
4. Klicken Sie in der zugehörigen Liste „Sichtbarkeitsdomänen“ auf **Bearbeiten**.
5. Wählen Sie die Domänen aus, deren Datensätze der Benutzer sehen soll.
6. Klicken Sie auf **Speichern**und dann auf **Aktualisieren**.



Die eingebettete Liste der Transparenzdomäne enthält die folgenden Felder.

Feld	Beschreibung
Domäne	Domäne, die für die Gruppe oder den Benutzer sichtbar ist.
Geerbt	Die Domäne wird von der Domänentransparenz oder einer übergeordneten Domäne geerbt.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Gewährt von	Name der Gruppe, die die Domänensichtbarkeit gewährt hat.
Übergeordnete Sichtbarkeit	Name der übergeordneten Domäne, der für die Gruppierung von Datensätzen verwendet wird. Wenn der übergeordnete Datensatz gelöscht wird, werden auch alle Datensätze mit demselben übergeordneten Element gelöscht.

Erstellen Sie eine domänenspezifische Auswahlliste

Administratoren können Auswahllisten so konfigurieren, dass sie Einträge enthalten, die für eine bestimmte Domäne spezifisch sind.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Wählen Sie die Domäne aus der Domänenauswahl aus, wobei die Auswahlmöglichkeit hinzugefügt werden soll.
2. Klicken Sie mit der rechten Maustaste auf das Auswahlfeld, das Sie anpassen möchten, und wählen Sie Auswahlmöglichkeiten **konfigurieren**aus.
3. Auswahlmöglichkeiten aktualisieren oder hinzufügen.
4. Verschieben Sie Changes über den normalen Change-Prozess, z. B. als Update Sets.

> **Hinweis:** Administratoren sollten sicherstellen, dass die Auswahlmöglichkeiten für alle Domänen eindeutig sind, um administrative Verwirrung in der globalen Domäne zu vermeiden.

Wenn ein Administrator eine neue Auswahl aus der globalen Domäne hinzufügt, sehen Benutzer aus Domänen, die in der Hierarchie niedriger sind, die neue Auswahl am Ende ihrer aktuellen Auswahllisten. Wenn die neue Auswahl auf globaler Ebene nicht aktiv ist, steht sie den Domänenbenutzern über Auswahlmöglichkeiten **konfigurieren** zur Verfügung, wird jedoch nicht als aktive Auswahl angezeigt.

Erweiterte Verwaltung mit Domänentrennung

Administratoren können Informationen zur Domänentrennung anzeigen, potenzielle Probleme identifizieren und Konfigurationseinstellungen ändern.

Sie können die folgenden erweiterten Verwaltungsaufgaben für Domänen ausführen:

- Verwenden Sie Domänenauswahlmenüs
- Zeigen Sie Domänenbeziehungen an

Verwenden Sie Domänenauswahlmenüs

Die Instanz bietet die Domänenauswahl über zwei Menüformate.

- Domänenauswahl: Stellt eine einfache Dropdown-Liste der verfügbaren Domänen bereit.
- Domänenreferenz-Auswahl: aktiviert ein Referenzfeld, das Filter und eine AutoVervollständigen-Typeahead-Eingabefunktion bietet. Verwenden Sie dieses Format für längere Listen.

Die Platzierung dieser Auswahlmöglichkeiten und das Verfahren zum Ein- oder Ausblenden unterscheiden sich je nach Anwenderoberflächenversion.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktivieren Sie Domänenauswahlmenüs in Core-UI

Durch Anzeigen der Domänenauswahl in Core-UI wird die Domänenauswahl standardmäßig aktiviert. Nachdem Sie die Domänenauswahl aktiviert haben, können Sie eine Systemeigenschaft hinzufügen, um die Domänenreferenzauswahl zu aktivieren.

Vorbereitungen

Hinweis: Die Domain Separation (Plugin com.snc.pa.domain_support) ist erforderlich, um die Domänenreferenzauswahl zu aktivieren.

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Klicken Sie auf das Zahnradsymbol im Header.
2. Klicken Sie auf der Registerkarte Allgemein auf den Schalter **Domänenauswahl in Header** anzeigen.
   Die Domänenauswahl wird im Header Core-UI angezeigt.
3. Wahlweise: Aktivieren Sie die Domänenreferenzauswahl.

   Hinweis: Durch Aktivieren der Domänenreferenzauswahl wird die globale Option aus der Liste entfernt. Um zu Ihrer Stammdomäne zurückzukehren, klicken Sie auf den Zurück-Pfeil neben dem Referenzfeld. Administratorbenutzer können auf den Zurück-Pfeil klicken, um zur globalen Domäne zurückzukehren.

   a. Geben Sie `sys_properties.list` im Anwendungsnavigator ein.

   b. Falls noch nicht vorhanden, fügen Sie die Eigenschaft `glide.ui.domain_reference_picker.enabled` hinzu, und legen Sie den Wert auf **true**fest.

   c. Aktualisieren Sie den Browser.
   Die Auswahl der Domänenreferenz wird im Header Core-UI angezeigt.

Beschränken Sie den Zugriff auf die Domänenauswahl

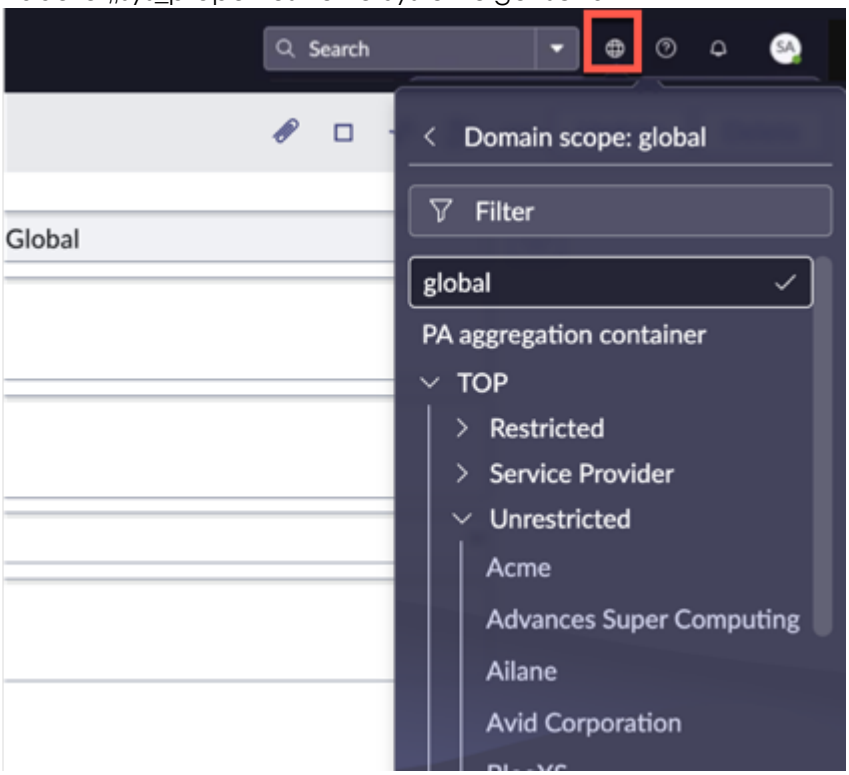
Verwenden Sie eine Systemeigenschaft, um den Zugriff auf die Domänenauswahl in Core-UI und Next Experienceeinzuschränken.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Standardmäßig können Benutzer mit der Rolle „ITIL“ und Rollen, die die Rolle „ITIL“ enthalten (z. B. Administratoren), auf die Domänenauswahl in Next Experiencezugreifen. Sie können anderen Rollen Zugriff gewähren, indem Sie sie der Eigenschaft hinzufügen, oder Rollen durch Entfernen einschränken. Es wird empfohlen, die Rolle nur auf Administratoren zu beschränken.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Administratoren können Benutzern Zugriff gewähren, indem sie in der Tabelle „sys_properties“ eine Systemeigenschaft erstellen.



Prozedur

1. Öffnen Sie die Tabelle „Systemeigenschaften“ [sys_properties].
2. Fügen Sie diese Eigenschaft hinzu: `glide.ui.Polaris.domain_picker.role`
3. Konfigurieren Sie den Eigenschaftswert als kommagetrennte Liste der Rollen: **admin, itil**. Weitere Informationen finden Sie unter Next Experience-Auswahlmöglichkeiten konfigurieren

Eigenschaften der Anwendung zur Domänentrennung

Das Plugin „Domain Separation“ verfügt über zwei neue Tabellen, um Service Providern mehr Flexibilität bei der Anpassung ihrer Anwendungen zu geben, die Domain Separation verwenden. Diese Tabellen sind die Tabelle „Systemanwendungseigenschaft“ [sys_application_property] und die Tabelle „Wert der Systemanwendungseigenschaft“ [sys_application_property_value].

Neue Tabellen bieten mehr Optionen

Bei Anwendungen des Service Providers (SP) können bestimmte Aktionen je nach Domäne variieren. Die Tabelle „Systemeigenschaften“ [sys_properties ServiceNow® des Basissystems [] ist jedoch nicht domänengetrennt und erfüllt daher nicht die Anforderungen für Anwendungen, die Domain Separation verwenden.

Jeder SP-Kunde möchte seine Anwendungen möglicherweise anders anpassen. Zuvor wurden Funktionen, die angepasst werden konnten, nur als ein globaler Wert definiert. Anwendungsentwickler benötigen eine flexiblere Tabelle. Jetzt können Sie Ihre Anwendung ändern, ohne jedes Mal Code erstellen zu müssen, wenn Sie Funktionen hinzufügen oder ändern möchten.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wie Überschreibungen in den neuen Tabellen funktionieren

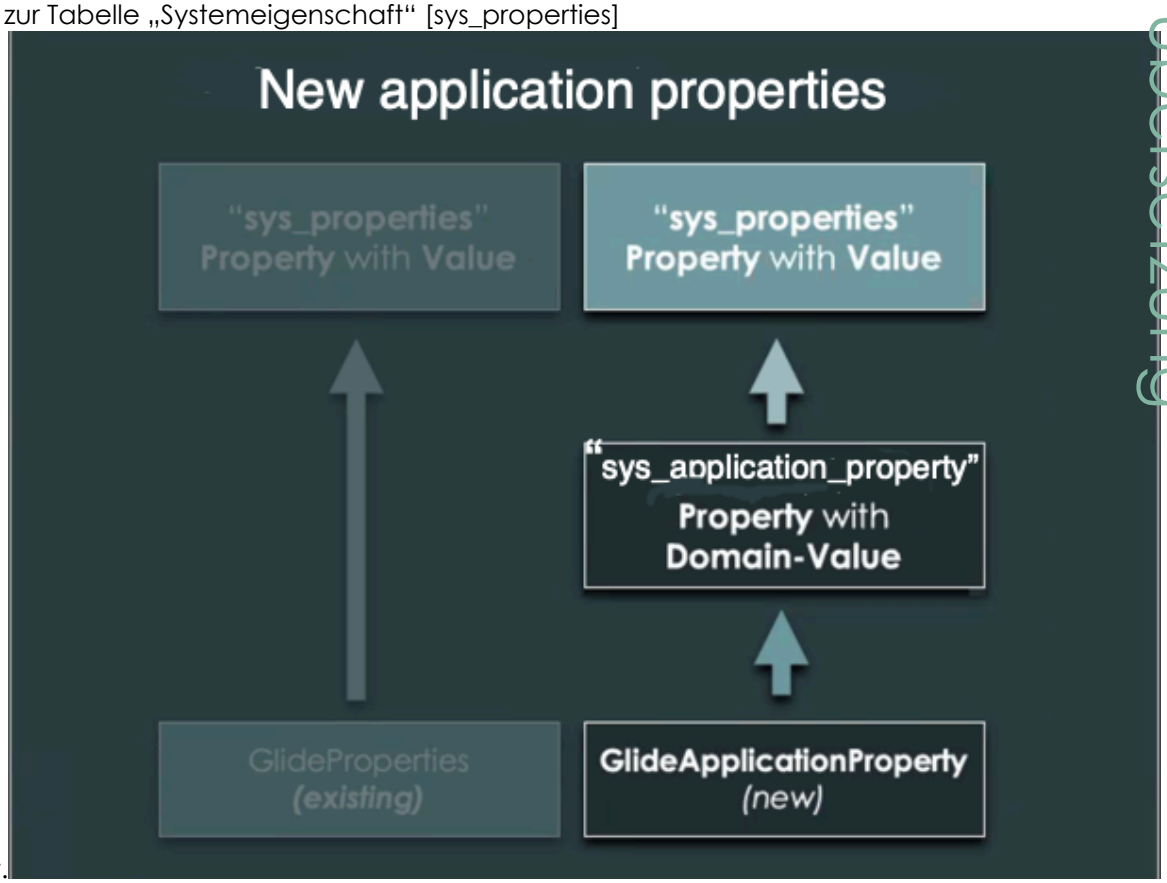
Entwickler verwenden normalerweise die Tabelle ServiceNow -Systemeigenschaft [sys_properties], um verschiedene Funktionen in Anwendungen zu erstellen. Wenn Sie eine Anwendung so entwickeln möchten, dass sie sich in verschiedenen Domänen unterschiedlich verhält, müssen Sie sie selbst anpassen.

Im Paris-Release vereinfacht die neue Tabelle für Anwendungseigenschaften [sys_application_property] diese Anpassung. Anstatt für einen Wert direkt zur Tabelle „Systemeigenschaft" zu wechseln, wechselt die Tabelle mit den Anwendungseigenschaften zuerst zur Tabelle „Systemanwendung". Diese neue Tabelle speichert jetzt die Logik, die Sie zum Konfigurieren Ihrer Anwendung benötigen. Wenn in der neuen Tabelle eine Eigenschaft gefunden wird, wird dieser Inhalt verwendet. Wenn in dieser Tabelle keine Informationen vorhanden sind, werden sie in die Tabelle mit den Basissystemeigenschaften verschoben.

Wenn Sie die Unterstützung für Domain Separation konfigurieren, können Sie dieser neuen Tabelle mit Anwendungseigenschaften Domänenlogik hinzufügen. Diese Tabelle kann Eigenschaften enthalten, die in der Tabelle „Systemeigenschaften" nicht vorhanden sind. Oder Sie können der Konfigurationstabelle Eigenschaften hinzufügen, die jede in der Tabelle „Systemeigenschaften" ausgewählte Eigenschaft überschreiben können.

Angenommen, Sie möchten eine Anwendung mit der Funktion Erster Tag der Woche konfigurieren. Manchmal kann es nützlich sein, dass der erste Tag der Woche Sonntag ist. In anderen Fällen möchten Sie möglicherweise, dass der erste Tag der Woche Montag ist. In der Basissystemtabelle gibt es möglicherweise nur eine einzige Tag-1-Option, und zwar Sonntag. Mit der neuen Tabelle können Sie eine weitere Eigenschaft speichern, wodurch der Tag 1 zu „Sonntag" und die Domäne „Montag" zu einer untergeordneten Domäne wird.

Diese Abbildung zeigt, wie das System Eigenschaften aus der Tabelle „Anwendungseigenschaften" bezieht, bevor es zur Tabelle „Systemeigenschaft" [sys_properties] wechselt.

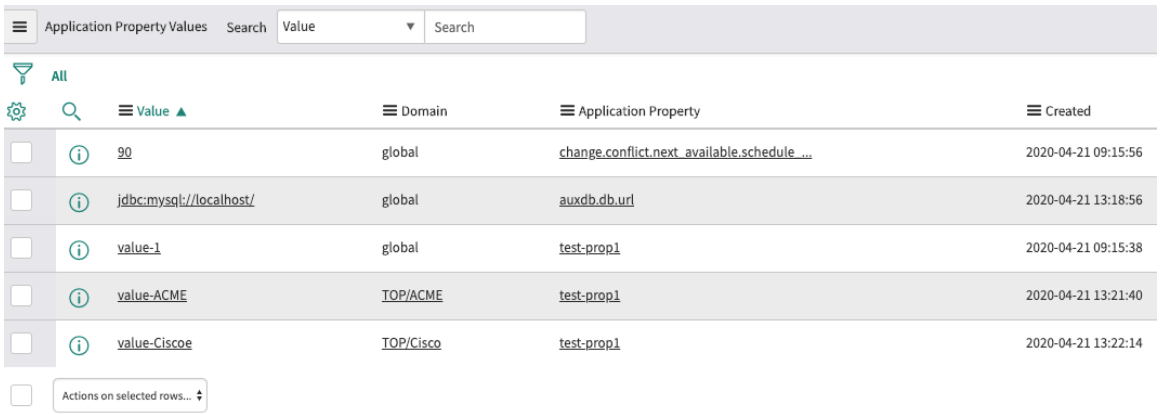


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Funktionsweise von bereichsbezogenen Apps in der neuen Tabelle

Die neue Tabelle „Anwendungseigenschaften“ wird von bereichsbezogenen Anwendungen unterstützt. Der Name der Anwendungseigenschaft ist, ähnlich wie der Name der Systemeigenschaft, eindeutig. Dies bedeutet, dass ihm der Bereichsname vorangestellt wird, wenn er nicht global ist. Der Umfang einer Anwendung wirkt sich auf Ihre Konfiguration aus. Der Umfang kann bestimmen, welcher Tag 1 als Sonntag und welcher als Montag definiert wird. Sie können dieselbe Eigenschaft verwenden, sie jedoch so anpassen, dass „Tag 1, Sonntag“ die übergeordnete Domäne und „Tag 1, Montag“ die untergeordnete Domäne ist. In der neuen Tabelle gibt es sowohl eine Domänenspalte als auch eine Bereichsspalte, sodass Sie diese Eigenschaften für jede Spalte festlegen können.

Sie können die Ansicht Domänenbereich erweitern in der Tabelle „sys_application_property_value“ verwenden, um alle Überschreibungen anzuzeigen (siehe folgende Abbildung).



Hinweis:

Wenn diese Tabellen nicht verfügbar sind, vergewissern Sie sich, dass das Plugin „Domain Extension Installer“ (com.glide.domain.msp_extensions.installer) aktiviert ist.

Neue Anwendungseigenschaftentabellen

Die neue Tabelle „Systemanwendungseigenschaft“ [sys_application_property] enthält diese Felder:

- Name
- Beschreibung
- Typ (Auswahl aus Zeichenfolge, true | false, Ganzzahl, Zeitzone, Farbe usw.)
- default_value
- Eigenschaft (Referenz zu sys_properties)
- „usage_notes“
- „read_roles“
- write_roles
- Eindeutiger Schlüssel: (Name)

Die neue Tabelle „Eigenschaftswert der Systemanwendung“ [sys_application_property_value] enthält diese Felder:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sys_application_property (Referenz zu sys_application_property)
- sys_domain
- sys_overrides
- Wert
- Eindeutiger Schlüssel: (sys_application_property, sys_domain)

Neue APIs

Die neuen APIs werden auch in bereichsbezogenen Apps unterstützt. Domänengetrennte Anwendungseigenschaften haben unterschiedliche APIs. Die GlideApplicationProperty-API verfügt über zwei neue skriptfähige Methoden, die sowohl in globalen als auch in bereichsbezogenen Anwendungen verfügbar sind. Unter GlideApplicationProperty – Scoped, Global erfahren Sie mehr über diese neuen APIs.

Zugehörige Informationen

Empfohlene Domain Separation-Verfahren für Service Provider

Domänenmigrationstool

Verwenden Sie das Domänenmigrationstool, um einen Kunden aus einer domänengetrennten Umgebung in eine eigene dedizierte Instanz zu migrieren.

Plugin „Domain Migration Tool“

Das Plugin „Domain Migration Tool“ (com.glide.domain.migration_tool) vereinfacht die Aufgabe, einen Kunden aus einer domänengetrennten Umgebung in eine flexiblere dedizierte Instanz zu migrieren. Kunden möchten möglicherweise zu einer separaten Instanz migrieren, um die Fähigkeiten von Now Platform besser nutzen zu können. Obwohl das Plugin „Domain Separation“ installiert ist, sind die Eigenschaften für die Daten- und Prozesstrennung deaktiviert.

Hinweis: Sie müssen eine geklonte Instanz anfordern und die Aktivierung des Plugins „Domain Migration Tool“ anfordern, bevor Sie es verwenden können.

Das Domain Migration Tool wird nur ausgeführt, wenn Daten- und Prozesstrennung in der domänengetrennten Instanz aktiviert sind:

- Die Dateneigenschaft *glide.sys.domain.partitioning* muss auf **true**festgelegt werden.
- Die Prozesseigenschaft *glide.sys.domain.delegated_administration* muss auf **true**festgelegt werden.

Funktionsweise des Migrationstools

- Ein Großteil des Migrationsprozesses wird automatisiert, insbesondere die Bereinigung von Daten.
- Migriert die domänengetrennte Instanz zu einer neuen dedizierten Instanz.
- Löscht Daten aus der dedizierten Instanz.

  Hinweis: Das Tool löscht keine Daten, die global, in der Zieldomäne oder in zusätzlichen Datendomänen (falls angegeben) sind.

- Reduziert Prozessdaten oder löscht Prozessdaten, wenn dies nicht möglich ist
- Behält Prozessdatensätze bei, die für die Zieldomäne sichtbar sind

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Aktualisiert die Spezialtabellen „sys_choice“, „sys_ui_list“ und „sys_ui_related_list“.
- Bereinigt Datensätze, die von Domain Separation-Plugins hinzugefügt wurden:
  - Business-Regeln
  - UI-Aktionen
  - Geplante Aufgaben
  - Installations-Exits
  - Navigationsmodule
- Deaktiviert Domain Separation und entfernt Domänen aus der geklonten Instanz:
  - Legt diese Eigenschaften in der geklonten Instanz auf „ **false** “ fest:
    - *glide.sys.domain.partitioning*
    - *glide.sys.domain.delegated_administration*
    - *glide.sys.domain.enabled*
  - Löscht alle Domänen mit Ausnahme der Zieldomäne und aller zusätzlichen angegebenen Datendomänen.
- Aktualisiert das Feld „ **Status** “ in der Tabelle „domain_migration_tool_status“.

Individueller Status der Tabellen

Status	Beschreibung
Ausstehend	Standardstatus von domänengetrennten Tabellen während der Migration. Die Migration der Tabellen ist geplant, die Migration wurde jedoch noch nicht gestartet.
Fehler	Fehler auf Tabellenebene. Wenn der Migrationsprozess mit Fehlern abgeschlossen wird, gibt dieser Status an, welche Tabellen Fehler aufweisen.
Wird ausgeführt	Der Status der Tabelle, die derzeit migriert wird. Nur eine Tabelle kann diesen Status haben und wird derzeit migriert.
Erfolgreich	Der Status der Tabellen, die erfolgreich migriert wurden.
Erfolgreich beendet	Der Migrationsprozess wird ohne Fehler abgeschlossen.
Mit Fehlern abgeschlossen	Der Migrationsprozess wird mit Fehlern abgeschlossen.

- Protokolliert Fortschritt und Status in „syslog_domain“.

  Die Quelle ist **MigrationTool** für alle Protokolleinträge, die der Migration zugeordnet sind.
  - Protokolliert jede Datentabelle und wie viele Datentabellen verbleiben
  - Protokolliert jede Prozesstabelle und die Datensätze welcher Domäne derzeit deaktiviert oder gelöscht werden

Was das Migrationstool nicht kann

- Klonen Sie die Instanz
- Erstellen Sie eine weitere domänengetrennte Instanz

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Migrieren Sie Datensätze (Daten oder Prozess), wenn Daten- oder Prozesstrennungseigenschaften deaktiviert sind, bevor Sie das Tool ausführen
- Ändern Sie beliebige Daten in der Quellinstanz
- Globale Daten, Daten in der Zieldomäne oder in zusätzlichen Datendomänen (falls angegeben) löschen

Was Sie nach dem Ausführen des Tools tun müssen

Das Domain Migration Tool automatisiert die Entfernung von Daten außerhalb der gewünschten Domänen (Zieldomäne, zusätzliche Datendomänen und globale Domäne). Sie müssen alle verbleibenden Konfigurationen bewerten, um sicherzustellen, dass sie für Ihre dedizierte Instanz geeignet sind und funktionieren. Wenn Sie beispielsweise eine Geschäftsregel hatten, die das Feld „Domäne“ auf Datensätze festlegt, können Sie diese Geschäftsregel deaktivieren, da sie keinen Zweck mehr erfüllt.

Migrieren Sie eine domänengetrennte Instanz zu einer dedizierten Instanz

Verschieben Sie einen Kunden aus einer domänengetrennten Umgebung in eine eigene dedizierte Instanzumgebung.

Vorbereitungen

Erforderliche Rolle: security_admin und admin

Prozedur

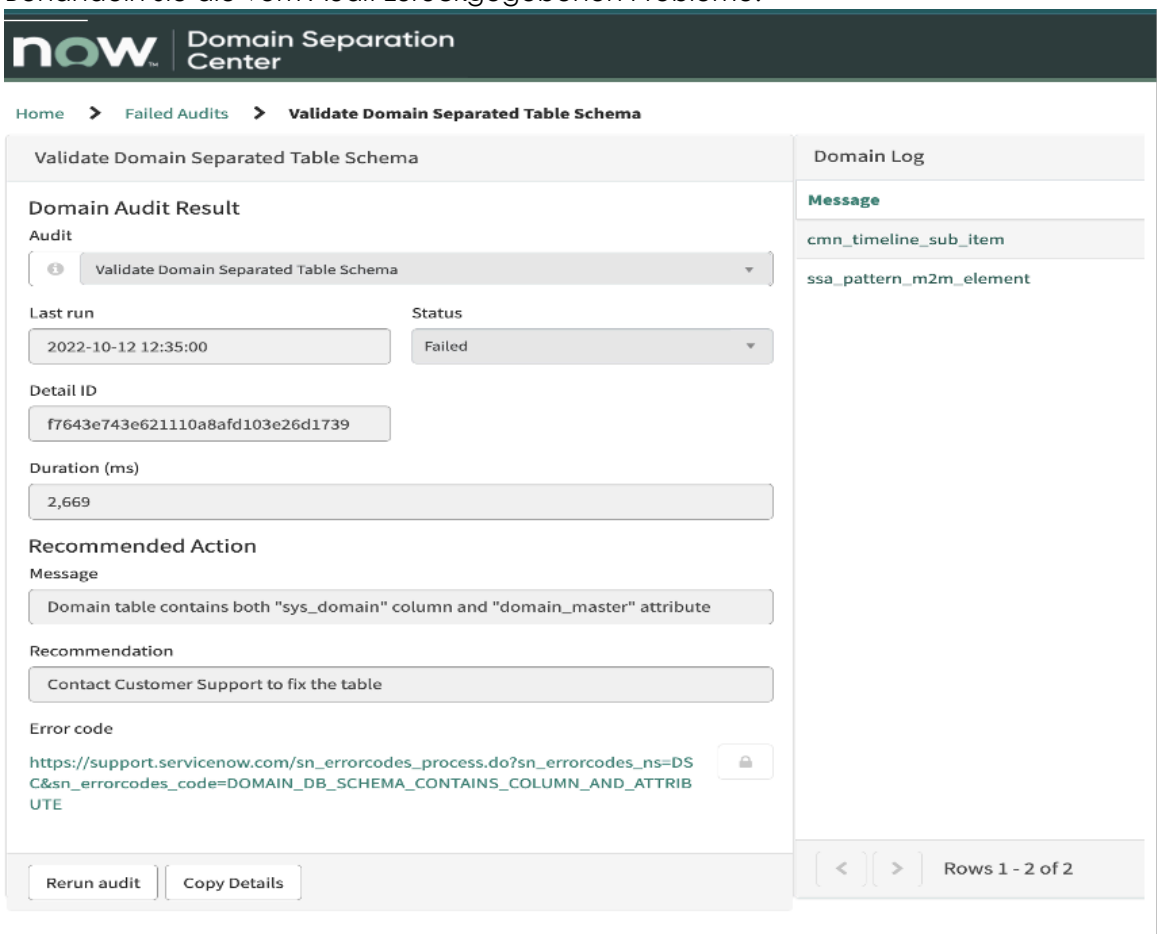
1. Erhöhen Sie die Berechtigungen auf die Rolle security_admin.
   Details siehe Auf eine privilegierte Rolle hochstufen.
2. Navigieren zu **Alle** > **Domänenadministrator** > **Domänenmigrationstool**an.
   Greifen Sie auch mit **„domain_migration_tool_status.list“**auf zu.
3. Klicken Sie auf **Neu**.
4. Füllen Sie das Formular aus.

Feld	Beschreibung
Zieldomäne	Geben Sie die Domäne an, die für den Prozess und die Daten verwendet wird, die Sie migrieren möchten. Nur die Zieldomäne wird beibehalten, nicht ihre untergeordneten Elemente, sofern dies nicht im Feld **„Zusätzliche Datendomänen“** angegeben ist.
Zusätzliche Datendomänen	Geben Sie optional zusätzliche Datendomänen an, die Sie migrieren möchten. Wenn Sie die Zieldomäne und alle zugehörigen untergeordneten Elemente migrieren möchten, müssen Sie alle untergeordneten Elemente angeben.

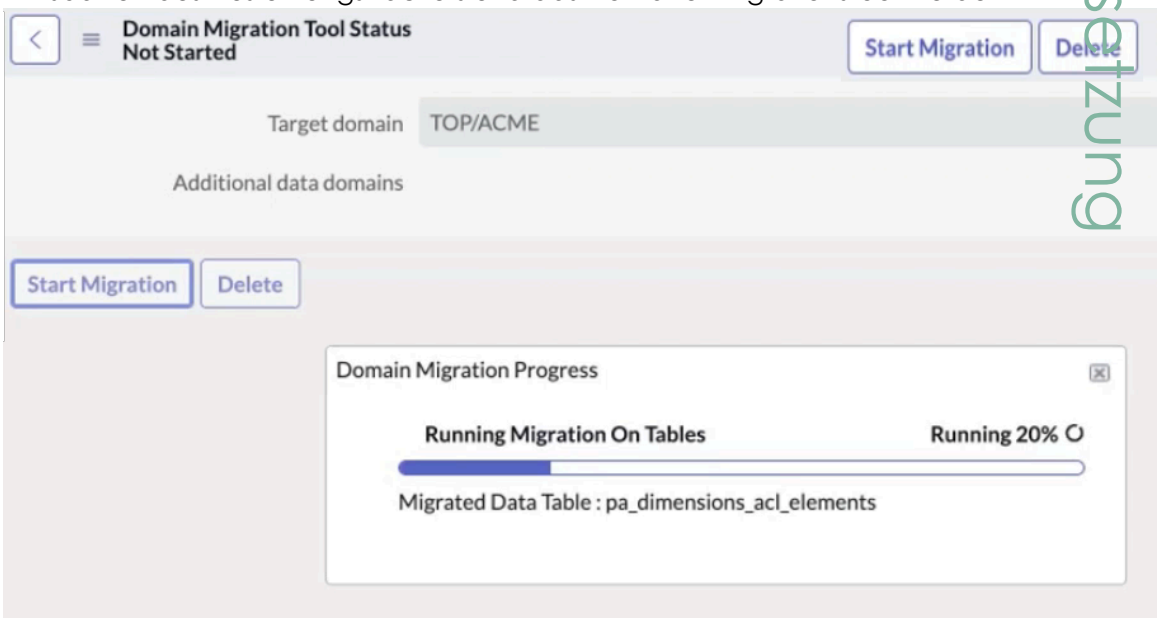
5. Wählen Sie **Absenden**.
6. Öffnen Sie das gerade übermittelte Formular.
7. Navigieren zu **Alle** > **Domain Separation Center** > **Audits konfigurieren** .
   Weitere Informationen finden Sie unter Domain Separation Center.
8. Setzen Sie den Audit des **Validate Domain Separated Table Schema** (Domänengetrenntes Tabellenschema validieren) auf **Aktiv**, und weisen Sie einen Zeitplan zu.
   Dies ist ein vorsorglicher Domänen-Audit, um das Schema für die Integrität von domänengetrennten Tabellen vorab zu überprüfen. Auf diese Weise können Sie Fehler beheben, bevor Sie die Migration ausführen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Führen Sie den **Audit-Zeitplan aus**, der das Schema enthält.
   Details siehe Audits sofort ausführen.
10. Behandeln Sie die vom Audit zurückgegebenen Probleme.



11. Wählen **Sie Migration starten aus**.
    - Der Fortschrittsbalken des Ausführungstrackers und das Domänenmigrationstool werden ausgelöst.



    - Die aktuell verarbeitete Migrationstabelle wird zusammen mit dem Gesamtprozentsatz der erfolgreich migrierten Tabellen angezeigt.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die Tabelle, in der alle domänengetrennten Tabellen mit dem Migrationsstatus, der Gesamtzahl der Datensätze in jeder Tabelle und der Anzahl der migrierten Datensätze aufgezeichnet werden.
- Die Anzahl der Tabellen, bei denen die Migration fehlgeschlagen ist, wird ebenfalls aufgezeichnet.
- Der **Status** wird aktualisiert, wenn das Tool seine Funktionen ausführt.
- Die Domänenmigration wird weiterhin im Hintergrund ausgeführt, wenn Sie den Fortschrittsbalken schließen. Greifen Sie auf die Tabelle „ `sys_execution_tracker` " zu, und suchen Sie in „Tabellen“ nach „ **Laufende Migration** “, um den im Hintergrund ausgeführten Migrationsprozess zu überprüfen.

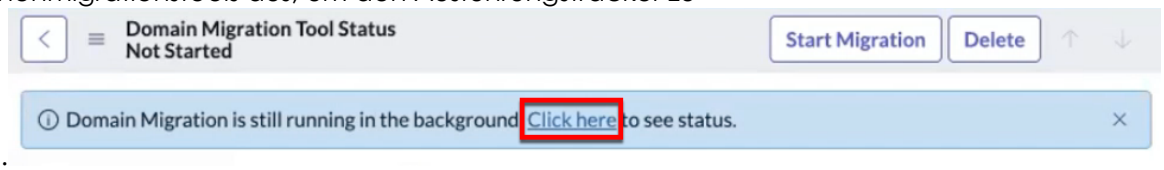
Der Status des Domänenmigrationstools zeigt die folgenden Felder an:

Statusfelder des Domänenmigrationstools

Feld	Beschreibung
Status	Zeigt den Migrationsstatus an. ◦ **Datentabellen werden migriert...**: Status „In Bearbeitung“. ◦ **Migration erfolgreich**: Der aktualisierte Status nach einer erfolgreichen Migration. ◦ **In einer der domänengetrennten Tabellen wurde eine falsche Konfiguration beobachtet**: Gibt einen Fehler bei der Datenmigration an. Ein Schemafehler wurde gefunden, die Migration wird nicht gestartet. Führen Sie das Audit **„Domänengetrenntes Tabellenschema validieren“ aus**. Das Audit schlägt fehl und zeigt die Tabellen an, die nicht dem Schemastandard entsprechen. ◦ **Abgeschlossen mit Fehlern in Revisit-Tabellen**: Die Anzahl der Tabellen für die Schemamigration wird aufgelistet. Suchen Sie die Fehler in Anzahl der Revisit-Tabellen, und beheben Sie Schemaprobleme. ◦ **Domänenmigration für Tabellen fehlgeschlagen...**: Nicht-Zieldatensätze müssen manuell aus fehlgeschlagenen Tabellen gelöscht werden. ◦ **Erfolgreich abgeschlossen**: Wenn alle Tabellen migriert wurden.
Zieldomäne	Die ausgewählte Zieldomäne für die Migration.
Zusätzliche Datendomänen	Wird ausgefüllt, wenn mehrere Migrationsdomänen ausgewählt wurden.
Anzahl der erneut verarbeiteten Tabellen	Dieses Feld wird nur ausgefüllt, wenn eine Tabelle nicht migriert werden kann. Wenn keine Fehler vorliegen, ist diese Anzahl Null. In diesem Fall werden die Tabellen überarbeitet, um die Migration erneut zu versuchen. Wenn keine Fehler auftreten, müssen Sie die Tabellen nicht erneut überprüfen oder die Migration erneut versuchen.
Aktuell verarbeitete Tabelle	Zeigt den Namen der Tabelle an, die derzeit migriert wird. Nach der erfolgreichen Migration ist dieses Feld leer.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

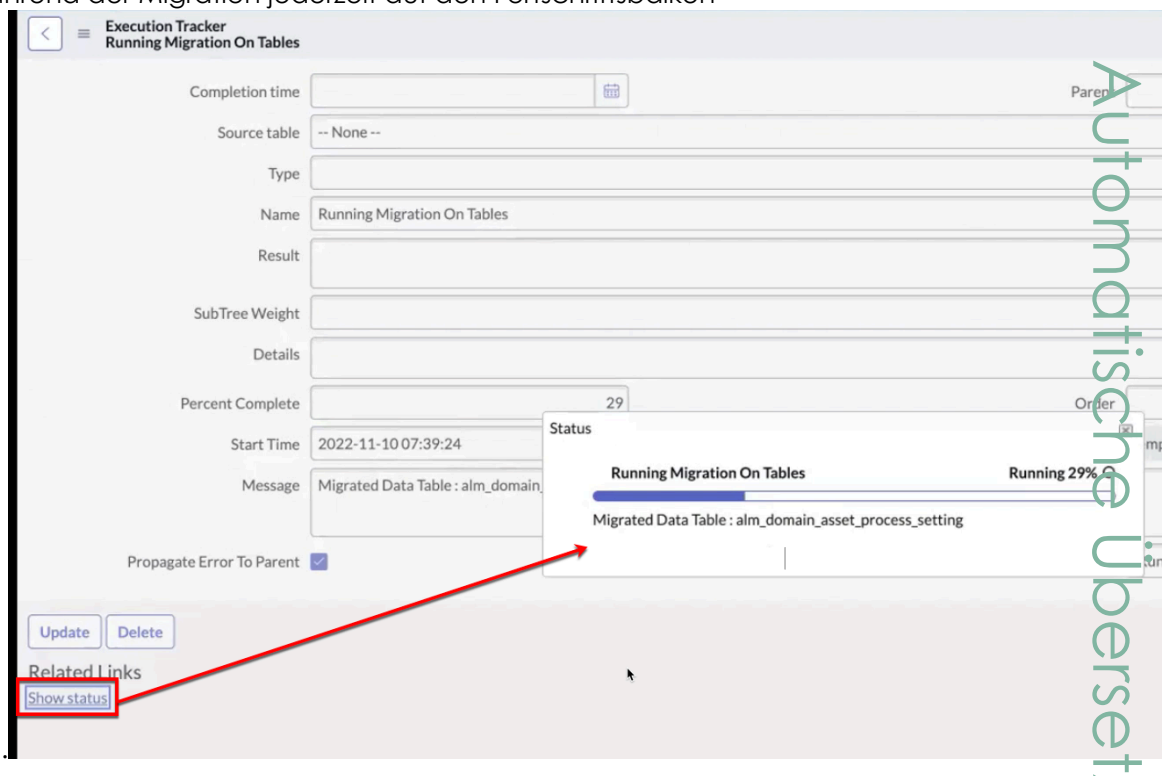
12. Wählen Sie den Link **Hier klicken** auf der Statusseite des Domänenmigrationstools aus, um den Ausführungstracker zu



öffnen.

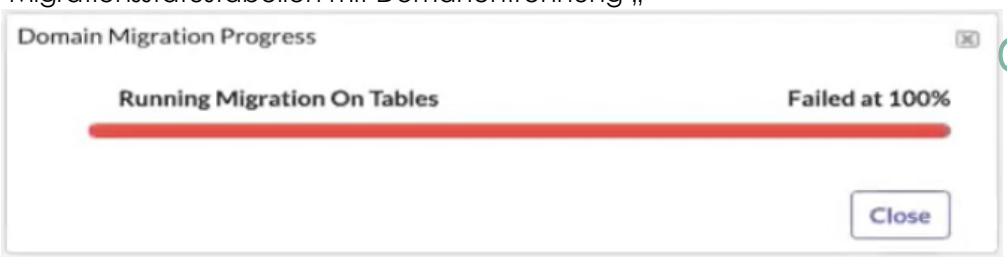
Sie können auch auf die Tabelle „ *sys_execution_tracker* "zugreifen und nach „ **Laufende Migration für Tabellen** “ suchen, um den im Hintergrund ausgeführten Migrationsprozess zu überprüfen.

13. Wählen Sie im Abschnitt „Zugehörige Links“ die Option **Status** anzeigen aus, um während der Migration jederzeit auf den Fortschrittsbalken



zuzugreifen.

Falls eine Tabelle die Schemaprüfung nicht bestanden hat, lautet der Gesamtstatus der Migrationsstatustabellen mit Domänentrennung „

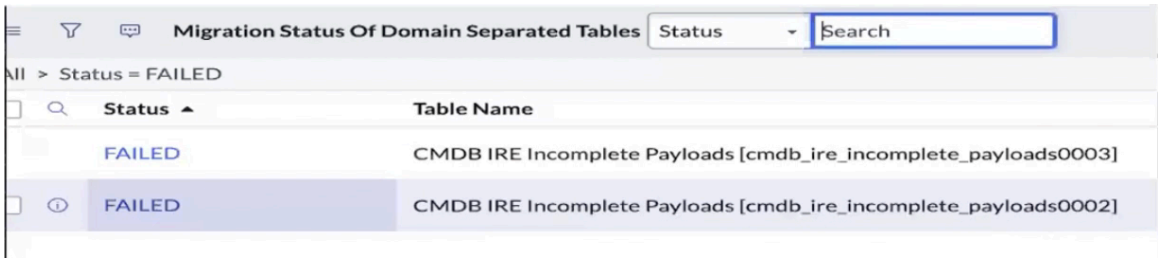


Fehlgeschlagen“.

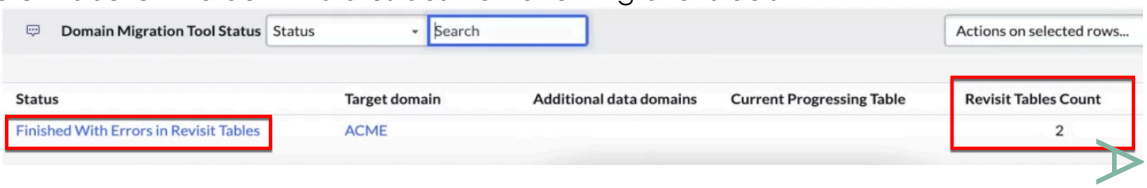
Für jede entsprechende Tabelle sind **fehlgeschlagene** Einträge vorhanden.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Der Rest der Migration wird fortgesetzt, und eine Zusammenfassung aller fehlgeschlagenen Tabellen und die Gesamtzahl der Anzahl der **überarbeiteten Tabellen** werden im Status des Domänenmigrationstools ausgefüllt.



Der **Status** lautet **„Erfolgreich** abgeschlossen“, wenn die Migration abgeschlossen ist.



Prozessverwaltung

Mit der Prozessverwaltung können Administratoren domänenspezifische Richtlinien festlegen.

Die Richtlinien, die niedriger in der Domänenhierarchie platziert sind, überschreiben Richtlinien, die höher in der Domänenhierarchie platziert sind. In einer Domäne können Administratoren domänenspezifische Versionen dieser globalen Richtlinien und Einstellungen festlegen:

- Client-Skripts
- Systemrichtlinien
- Anwendungs- und Modulnamen
- Anwendungsrollen
- Modulfilter

⚠ **Warnung:** Alle Benutzer mit der Administratorrolle haben speziellen Zugriff auf alle Features, Funktionen und Daten des Systems, da Administratoren ACL-Regeln überschreiben und alle Rollenprüfungen übergeben können. Gewähren Sie diese Berechtigung mit Bedacht.

Wenn Benutzer über die **Administratorrolle** verfügen, stehen ihnen alle Richtlinien in der Instanz unabhängig von der zugewiesenen Domäne zur Verfügung. Sie können eine bestimmte Domäne eingeben, und dann sind nur Richtlinien in dieser Domäne oder höher sichtbar und werden während einer relevanten Transaktion verarbeitet. Wenn ein Administrator eine Richtlinie ändert, die sich in einer höheren Domäne oder der globalen Domäne befindet, erstellt das System automatisch einen neuen Datensatz für die

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aktuelle Domäne dieses Administrators. Der ursprüngliche Richtlinien-, Anwendungs- oder Moduldatensatz wird dadurch nicht geändert. Dieser neue Datensatz überschreibt den ursprünglichen.

Um Änderungen an einer Richtlinie in einer Domäne auf niedrigerer Ebene vorzunehmen, wechseln Sie in diese Domäne und ändern Sie die Richtlinie. Bei diesem Ansatz wird der Richtliniendatensatz in Ihrer Domäne erstellt, der den ursprünglichen Richtliniendatensatz auf höherer Ebene überschreibt.

Ändern Sie nicht die Richtlinie einer höheren Ebene und ändern Sie dann das Feld **Domäne** in dieser Richtlinie. Bei diesem Ansatz wird kein Richtliniendatensatz in Ihrer Domäne auf niedrigerer Ebene erstellt, und der Richtliniendatensatz für die Domäne auf höherer Ebene wird auch nicht gespeichert.

Das Feld **sys_overrides** gibt an, dass eine Richtlinie, eine Anwendung oder ein Modul auf einer niedrigeren Ebene in der Hierarchie einen Datensatz auf einer höheren Ebene überschreibt. Dieses Feld wird vom System automatisch festgelegt, wenn ein Administrator versucht, eine Richtlinie, eine Anwendung oder ein Modul zu ändern, die/das zu einer anderen, in der Hierarchie höherstehenden Domäne gehört.

Anstatt den Datensatz der höheren Ebene zu ändern, wird die versuchte Aktualisierung in eine Einfügung geändert, und das Feld **sys_overrides** wird so festgelegt, dass es die Richtlinie, die Anwendung oder das Modul der höheren Ebene angibt, die bzw. das überschrieben wird. Wenn später die Datensätze für eine relevante Transaktion geladen werden, wird anstelle des Originals die übergeordnete domänenspezifische Richtlinie, Anwendung oder das übergeordnete Modul verwendet.

Domänen für die Prozessadministration

Standardmäßig verwendet die Prozessadministration immer die Domäne des Datensatzes, um zu bestimmen, welche Richtlinien angewendet werden.

Die Domäne des Datensatzes hat Vorrang vor der Domäne des Benutzers. Wenn in der Domäne des Datensatzes keine Richtlinien vorhanden sind, sucht die delegierte Administration nach Richtlinien in der nächsthöheren Ebene der Domänenhierarchie. Die Suche nach Domänenrichtlinien wird in der Domänenhierarchie fortgesetzt, bis die globale Domäne erreicht wird. Wenn es in der Domänenhierarchie keine Domänenrichtlinien weiter unten gibt, verwendet die Prozessverwaltung die Richtlinien für die globale Domäne.

Zum Beispiel ist Fred Luddy ein Benutzer in der Acme-Domäne, der Datensätze in den untergeordneten Domänen der untergeordneten Domänen Acme: Atlanta, Acme: San Diego und Acme: NY anzeigen kann. Wenn dieser Benutzer einen Datensatz in der Domäne „Acme: San Diego“ öffnet, sucht die Prozessverwaltung zuerst nach Richtlinien in der Domäne „Acme: San Diego“. Wenn auf dieser Ebene der Domänenhierarchie keine Richtlinien vorhanden sind, sucht die Prozessverwaltung nach Richtlinien aus der Acme-Domäne. Wenn in der Acme-Domäne keine Richtlinien vorhanden sind, verwendet die Prozessverwaltung die globalen Domänenrichtlinien, da sich in der Domänenhierarchie keine anderen Domänen höher befinden.

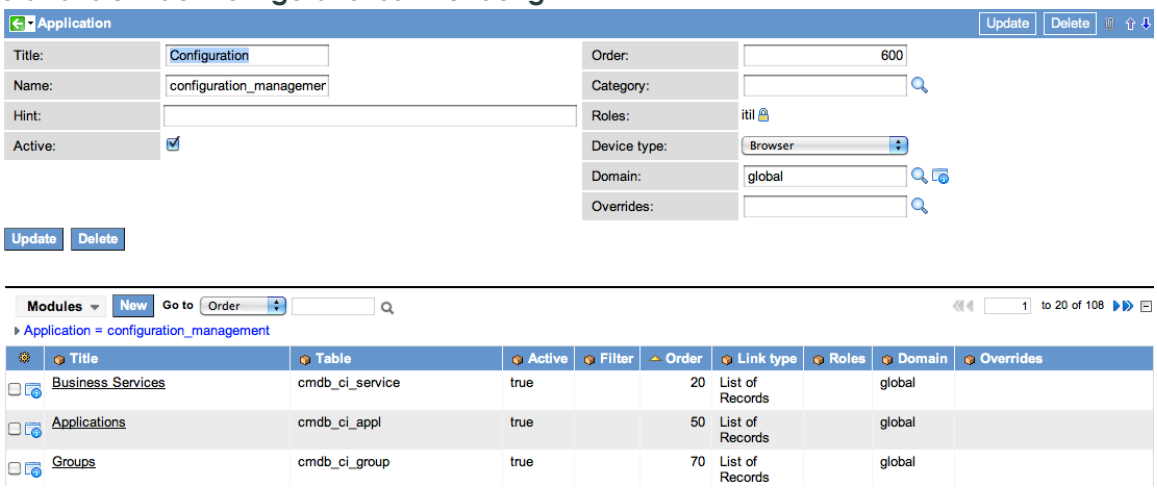
Beispiel für die Prozessverwaltung mit domänenspezifischen Anwendungen

Das folgende Beispiel veranschaulicht die Prozessverwaltung mit domänenspezifischen Anwendungen und Modulen.

Als Administrator der Ozeanischen Domäne beschließt David Loo, die Konfigurationsanwendung anzupassen. Zunächst geht David auf die im Anwendungsmodul Konfiguration verfügbaren Module ein.

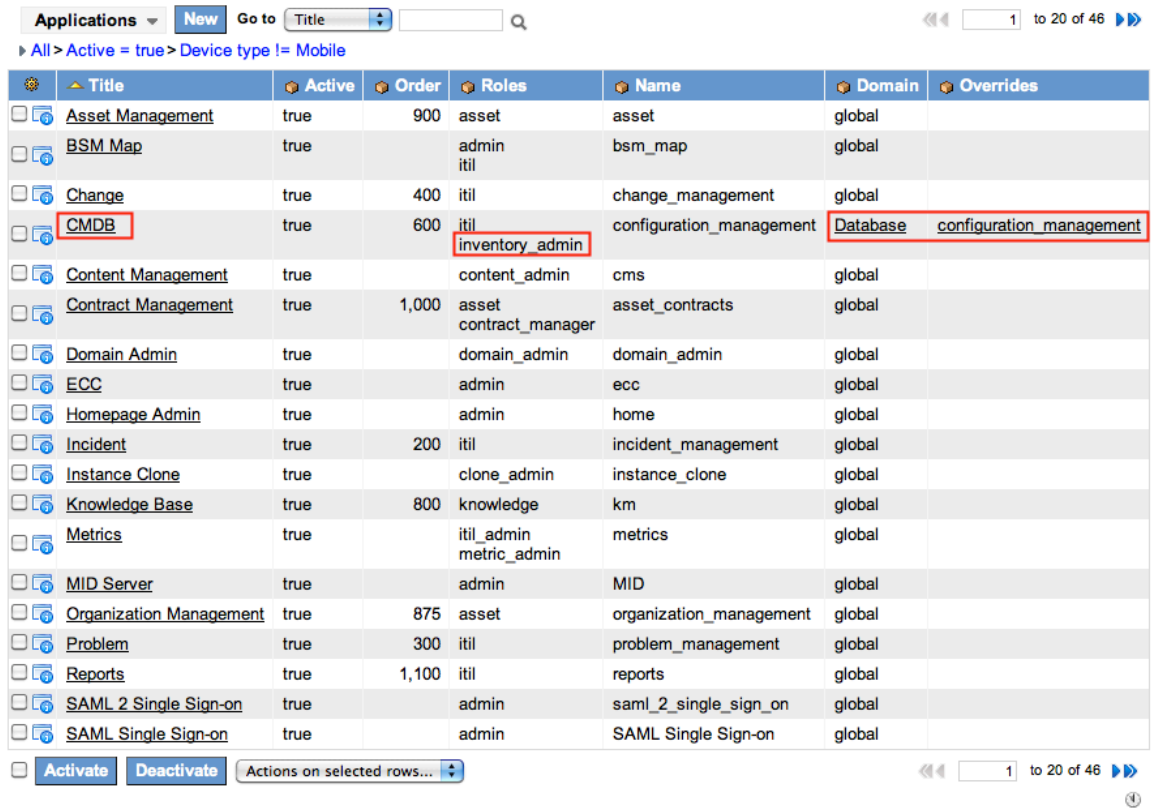
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Startansicht der Konfigurationsanwendung



David beschließt, die Konfigurationsanwendung in CMDB umzubenennen und zuzulassen, dass die Rolle inventory_admin die Anwendung sehen kann.

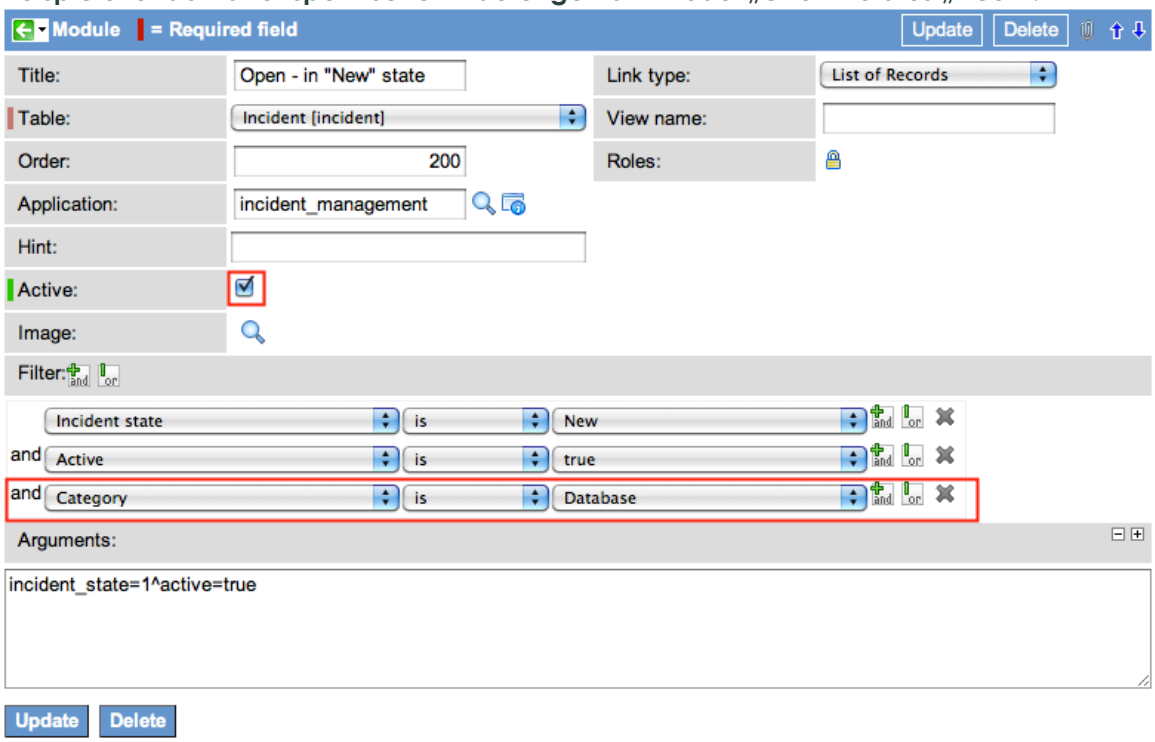
Beispiele für domänenspezifische Changes an der Konfigurationsanwendung



Als nächstes beschließt David, die Incident-Anwendung zu ändern, indem er das Modul **Open - in „New“ State** aktiviert und ein neues Filterelement hinzufügt, um offene Incidents in der Kategorie „Oceanic“ anzuzeigen.

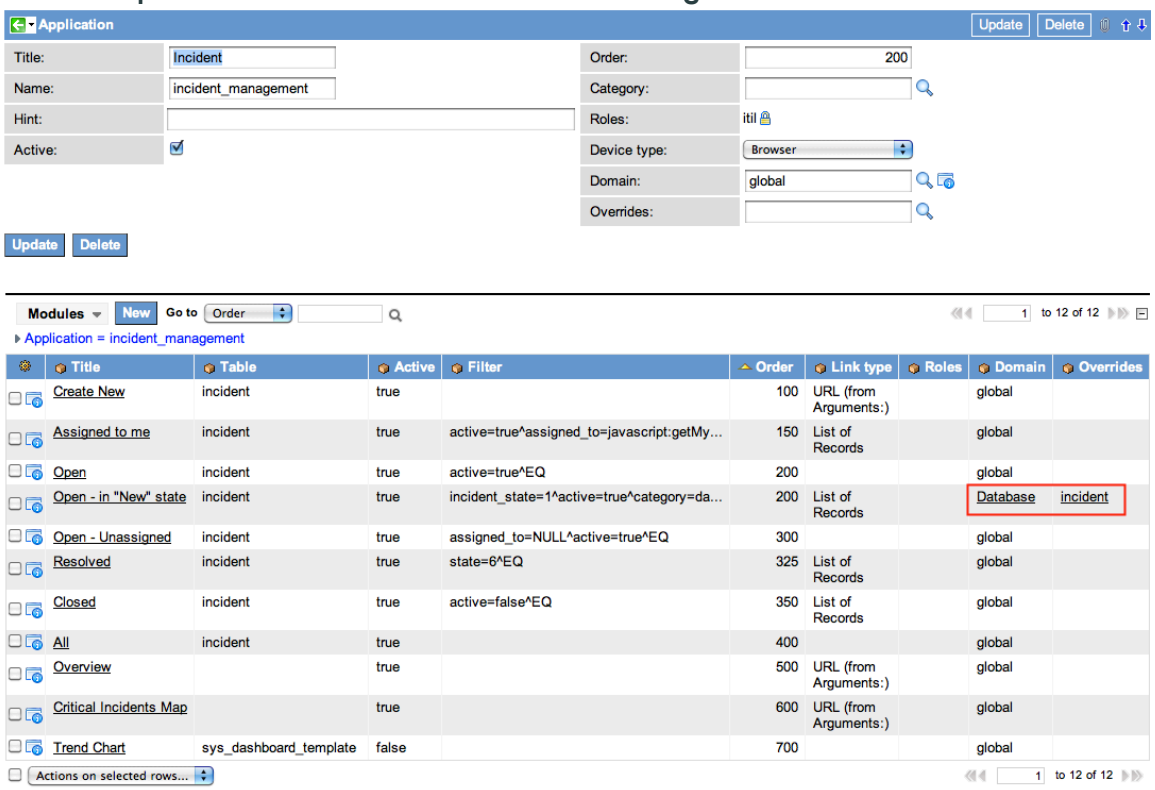
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiele für domänenspezifische Änderungen am Modul „Offen – Status „Neu““.



Dadurch wird ein neuer Moduleintrag in der Anwendung erstellt, anstatt das vorhandene Modul in der globalen Domäne zu überschreiben.

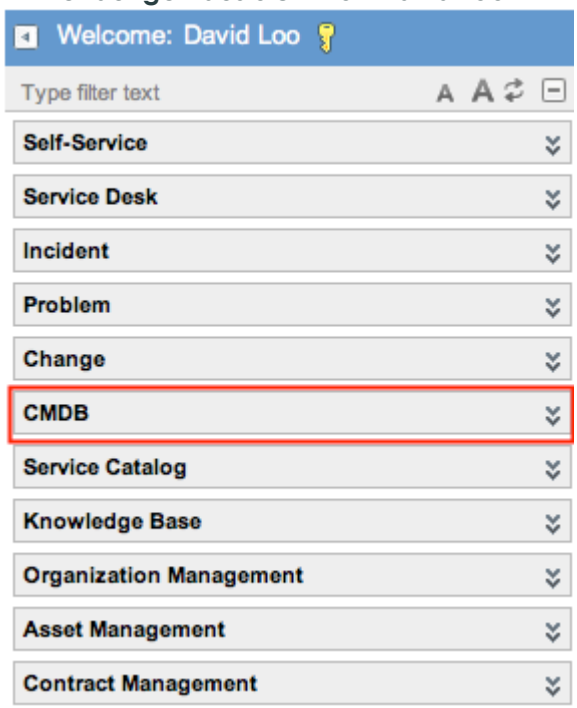
Domänenspezifische Ansicht der Incident-Anwendung



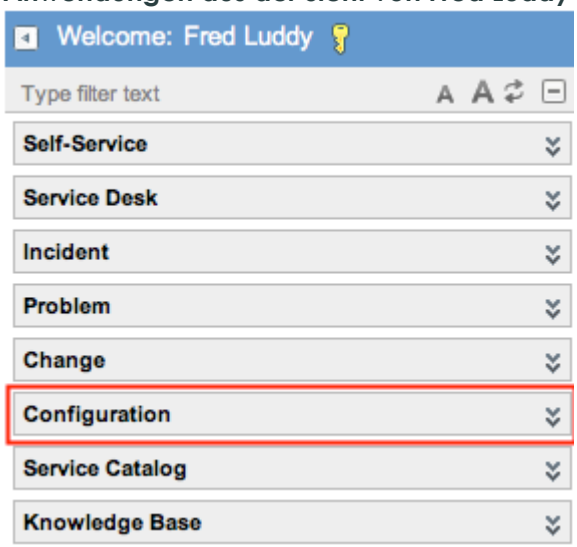
Wenn sich ein anderer Administrator aus einer anderen Domäne (z. B. Fred Luddy) anmeldet und auf die Konfigurationsanwendung zuschaut, werden die Einstellungen aus der globalen Domäne angezeigt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungen aus Sicht von David Loo



Anwendungen aus der Sicht von Fred Luddy



Aktiviert die ausführliche Domänenprotokollierung und Debug-Nachrichten

Domänenprotokoll- und Debug-Nachrichten ermöglichen Ihnen die Behebung von Domänenkonfigurationsfehlern.

Vorbereitungen

Erforderliche Rolle: admin
Stellen Sie sicher, dass Sie die aktuelle Instanz sind, um eine optimale Leistung zu erzielen.

Prozedur

1. Navigieren Sie im Domain Separation Center zu **Domänenadministrator**.
2. Klicken Sie **auf Domänencenter konfigurieren**.
3. Aktivieren Sie für **Ausführliche Domänenprotokollierung aktivieren**das Kontrollkästchen **Ja**.
4. Klicken Sie auf **Aktualisieren**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie eine Echtzeit-Domänennachricht an

Sie können Domänennachrichten in Echtzeit in den Systemprotokollen anzeigen.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Ausführliche Domänenprotokollierung aktivieren: Navigieren Sie zu **Alle** > **Domänenadministrator** > **Domain Separation Center** > **Domänencenter konfigurieren** > **Aktiviert detaillierte Domänenprotokollierung** > **Ja** (oder legen Sie die Eigenschaft „`glide.sys.domain.verbose`“ auf „ **True**“ fest).
2. Navigieren zu **Systemdiagnostik** > **Sitzung debuggen** > **Alle aktivieren**an.
   Da es sich um eine Echtzeitüberprüfung handelt, muss die Debug-Sitzung nicht vor der Überprüfung der Protokolldateien ausgeführt werden.
3. Navigieren Sie zur Sitzungs-Debug-Konsole, um die detaillierten Systemdomänenprotokolle anzuzeigen.
4. Suchen Sie nach der Textabfrage gegen Tabelle.

   Diese Abfrage findet Protokollnachrichten in diesem Format:

```
08:36:43.974: [Domain Paths] Query against table incident restricted by
 domain values [Database Atlanta[db53580b0a0a0a6501aa37c294a2ba6b],
Database[287ee6fea9fe198100ada7950d0b1b73],
Database San Diego[db53a9290a0a0a650091abebccf833c6], global, NY
 DB[5f74727dc0a8010e01efe33a251993f9]]
```

   In diesem Beispiel hat der Benutzer, der die Incident-Tabelle angezeigt hat, nur Datensätze gesehen, die den DB-Domänen Database Atlanta, Database, San Diego, Global und NY DB entsprechen.

Zeigen Sie eine historische Domänennachricht an

Zeigen Sie historische Domänennachrichten in der Protokolldatei an, um Probleme mit der Domänentrennung zu beheben.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Ausführliche Domänenprotokollierung aktivieren: Navigieren Sie zu **Alle** > **Domänenadministrator** > **Domain Separation Center** > **Domänencenter konfigurieren** > **Aktiviert detaillierte Domänenprotokollierung** > **Ja** (oder legen Sie die Eigenschaft „`glide.sys.domain.verbose`“ auf „ **True**“ fest).
2. Navigieren zu **Systemdiagnostik** > **Sitzung debuggen** > **Alle aktivieren**an.
3. Lassen Sie die Debug-Sitzung für einen Zeitraum, z. B. einen Tag, laufen, bevor Sie die Protokolldateien überprüfen.
4. Navigieren zu **Systemprotokolle** > **Dienstprogramme** > **Knotenprotokolldatei-Download**an.
5. Öffnen Sie den Datensatz für den Tag, den Sie anzeigen möchten.
   Protokolldateien verwenden das Benennungsformat „ `localhost_log“.`<yyyy-mm-dd> .txt .
6. Klicken Sie auf den zugehörigen Link Protokoll **herunterladen**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Öffnen Sie die heruntergeladene Protokolldatei in einem Texteditor, und suchen Sie nach Protokollnachrichten im folgenden Format:

   Abfrage des durch Domänenwerte eingeschränkten Tabellen-Incidents `[global, Software[8a4dde73c6112278017a6a4baf547aa7]]`

   In diesem Beispiel hat ein Benutzer nur Datensätze aus der Incident-Tabelle gesehen, die mit den Domänen „Global“ und „Software“ übereinstimmen.

Behandeln Sie Domain Separation-Fehler

Wenn Probleme mit der Domänentrennung auftreten, überprüfen Sie diese Liste der Lösungen.

Fehler oder Symptom	Lösung
Eine Domänen-sys_id verweist auf eine nicht vorhandene Domäne	Dieser Fehler tritt auf, wenn ein Datensatz, z. B. ein Benutzer- oder Aufgabendatensatz, einen `sys_domain-` Spaltenwert hat, dessen `sys_id` in der aktuellen Domänentabelle nicht vorhanden ist. Die `sys_id` der Domäne wurde möglicherweise versehentlich gelöscht oder verweist auf eine vorherige Domänentabelle, wenn Sie die Domänentabelle geändert haben. Um den Fehler zu beheben, öffnen Sie eine Liste für die Tabelle, die den Fehler enthält, und filtern Sie nach dem ungültigen Wert für „`sys_domain`“. Geben Sie dann den richtigen Wert `für sys_domain` entweder manuell ein, oder entfernen Sie ihn. **Hinweis:** Jede Tabelle, die auf die Domänentabelle verweist, kann ungültige Domänen `-sys_ids enthalten`. Ungültige Domänen-IDs können beispielsweise in den Tabellen „Anwendersichtbarkeitsdomäne “ `[sys_user_visibility]`, „Gruppensichtbarkeitsdomäne “ `[sys_user_group_visibility]` und „Enthaltene Domäne “ `[domain_contains] auftreten`.
Ein Domänenpfad oder eine Domänennummer-sys_id verweist auf die falsche Domäne	Dieser Fehler tritt auf, wenn eine Domänennummern- oder Domänenpfadabfrage nicht mit dem tatsächlichen Domänennamen synchronisiert ist. Dieser Fehler kann bei Domänennummern auftreten, wenn das Hinzufügen von Domänen eine Neunummerierung erfordert oder während der Konvertierung von Domänennummern in Domänenpfade. Um den Fehler zu beheben, überprüfen Sie die Ergebnisse in Domain Separation Center. Wenn der Fehler weiterhin besteht, können Sie den Wert für die Spalten „ `sys_domain_path`“ oder „`sys_domain_number` “ manuell bearbeiten, um auf die richtige Domäne zu verweisen.
Die Struktur der Domänenstruktur ist beschädigt	Dieser Fehler tritt auf, wenn eine Reihe von Domänen-enthält-Beziehungen eine Endlosschleife zwischen Domänen erstellen. Um den Fehler zu beheben, öffnen Sie eine Liste für die Domänentabelle, und bearbeiten Sie die Domäne, die Werte enthält, manuell, um keine Schleife zu bilden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

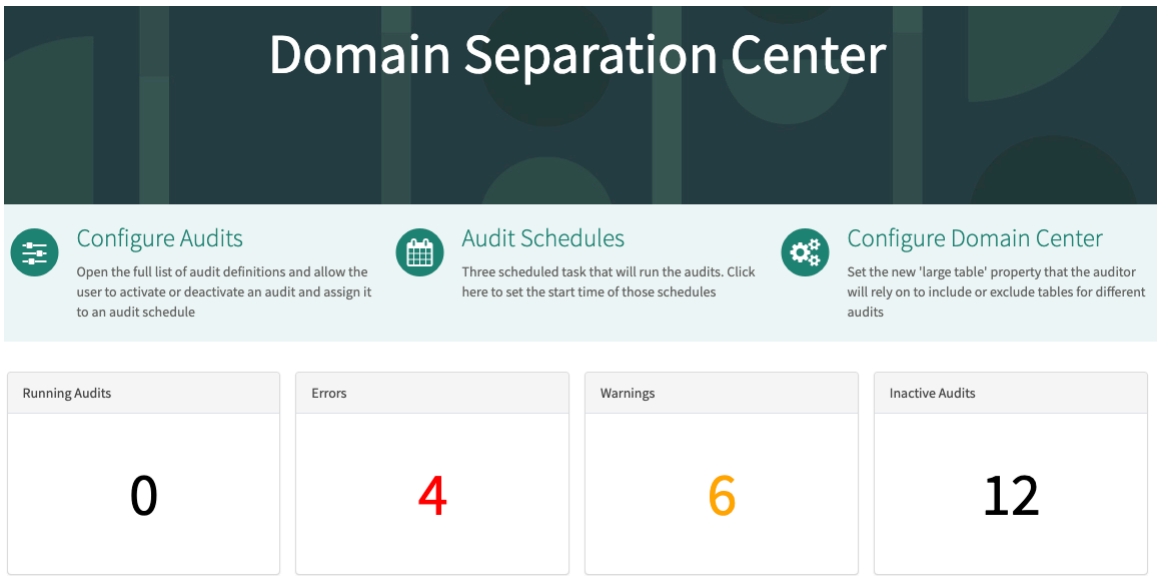
Domain Separation Center

Prüfen Sie Ihre Domänen regelmäßig, um Probleme aufzudecken.

Übersicht

Das Domain Separation Center ist ein Dashboard, in dem Sie Audits für alle in Ihrer Tabelle „domain_audit_definition“ gespeicherten Domänen planen und konfigurieren können. Mit dem Dashboard können Sie Audit-Ergebnisse überprüfen und sich eingehender mit Domänenfehlern und -warnungen befassen. Sie finden das Dashboard des Domain Separation Center unter<ServiceNow-instance-name> `/domaincenter`.

Das Domain Separation Center bietet viele Audits. Sie können keine eigenen erstellen. Sie können jedoch konfigurieren, wie häufig sie ausgeführt werden. Audits werden für alle in der Tabelle „domain_audit_definition“ gespeicherten Domänen ausgeführt.



Konfigurieren Sie Audits

Sie können konfigurieren, ob ein Audit aktiv ist und wie häufig es ausgeführt wird.

1. Wählen Sie im Domain Separation Center **Audits konfigurieren aus**.

   Die Seite **Audits konfigurieren** wird angezeigt.

2. Konfigurieren Sie jedes Audit, das aktiv sein soll. Audits sind standardmäßig deaktiviert.
   a. Wählen Sie einen Audit aus.
   b. Wählen Sie das Feld **Aktiv** aus, um den Audit zu aktivieren.
   c. Geben Sie im Feld **Häufigkeit** an, wie häufig der Audit ausgeführt wird.

      Das Domain Separation Center führt alle mit der gleichen Häufigkeit gekennzeichneten Audits gleichzeitig aus. Wählen Sie nicht **Täglich** für Audits aus, die für große Tabellen ausgeführt werden.

   d. Wiederholen Sie diese Schritte für jedes Audit, das Sie aktivieren möchten.
3. Wählen Sie **Speichern**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeitpläne für Audit

Konfigurieren Sie einen oder mehrere Audits für die tägliche, wöchentliche oder monatliche Ausführung. Der Zeitplaner gibt an, an welchen Tagen und zu welchen Zeiten diese Audits ausgeführt werden sollen. Alle Audits mit der gleichen Planungshäufigkeit werden nacheinander zu dem von Ihnen konfigurierten Zeitpunkt ausgeführt.

1. Wählen Sie im Domain Separation Center **Audit-Zeitpläne**aus.

   Die Seite „ **Audit-Zeitplan** “ wird angezeigt.

2. Konfigurieren Sie die Audit-Zeitpläne.
   a. Wählen Sie einen Zeitplannamen aus.
   b. Geben Sie die Uhrzeit für die Ausführung des Audits an.

      Zeiteinheiten werden im 24-Stunden-Format gemessen, d. h. 14 Uhr ist 14 Uhr.

   c. Wählen Sie bei wöchentlichen Zeitplänen den Wochentag aus, an dem das Audit ausgeführt werden soll, wobei 1 Sonntag ist.
   d. Wählen Sie bei monatlichen Zeitplänen den Tag des Monats aus, für den das Audit ausgeführt werden soll.
   e. Wiederholen Sie den Vorgang für die anderen Zeitpläne.
3. Wählen **Sie Speichern** aus, um die Konfigurationsänderungen zu speichern.
4. Wählen Sie **Jetzt** ausführen aus, um alle geplanten Audits mit der oben im rechten Bereich angezeigten Häufigkeit auszuführen. Wenn der Fenstertitel beispielsweise **Domänen-Audit-Zeitplan - Täglich**lautet, werden alle täglich ausgeführten Audits ausgeführt.

Um den Status eines laufenden Audits anzuzeigen, wählen Sie im Domain Separation Center die Zahl im Feld **Audits** wird ausgeführt aus.

Audits sofort ausführen

Audits werden in der Regel wie geplant ausgeführt. Sie können jedoch alle Audits auf Befehl ausführen.

1. Wählen Sie im Domain Separation Center **Audit-Zeitpläne**aus.

   Die Seite „ **Audit-Zeitplan** “ wird angezeigt.

2. Wählen Sie den Namen des Audit-Zeitplans aus, den Sie ausführen möchten, z. B. täglich, wöchentlich oder monatlich.
3. Wählen Sie **Jetzt ausführen**.

Um den Status eines laufenden Audits anzuzeigen, wählen Sie im Domain Separation Center die Zahl im Feld **Audits** wird ausgeführt aus.

Konfigurieren Sie das Domain Separation Center

1. Wählen Sie im Domain Separation Center **Domänencenter konfigurieren**aus.
2. Wählen Sie auf der Seite **„Domänencenter konfigurieren“** für **Aktiviert detaillierte Domänenprotokollierung**die Option **Ja** aus, um detaillierte Protokolle zu speichern, die bei der Diagnose von domänenbezogenen Problemen helfen. Eine detaillierte Protokollierung kann zu Leistungsproblemen führen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Protokolle beziehen sich auf serverseitige Protokolle in der Tabelle „syslog_domain“. Informationen zum Anzeigen der Protokolle finden Sie unter Audits mit Warnungen und Fehlern anzeigen.

3. Wählen Sie im Slushbucket alle Ihre großen Tabellen aus, und verschieben Sie sie in die Spalte **Ausgewählt**.

   Tägliche Audits sollten nicht für große Tabellen ausgeführt werden. Ausgegraute Tabellennamen in der Spalte **Ausgewählt** sind groß und können nicht in die Spalte **Verfügbar** verschoben werden.

4. Wählen Sie **Aktualisieren**.

Zeigen Sie Audits mit Warnungen und Fehlern an

Im Dashboard enthalten **Fehler** und **Warnungen** detaillierte Informationen zu Audits, bei denen Probleme aufgetreten sind. Protokolle im Zusammenhang mit Domain Separation befinden sich auf Ihrem Server in der Tabelle „syslog_domain“.

1. Wählen Sie im Domain Separation Center die Zahl im Feld **Fehler** oder **Warnungen** aus.

   Die Seite „ **Fehler** “ bzw. „ **Warnungen** “ wird angezeigt.

2. Wählen Sie einen der Audits in der Liste aus.

   Auf der Seite werden detaillierte Informationen zu Problemen mit dem ausgewählten Audit angezeigt. Die Nachrichten in den **Audit-Ergebnisdetails** beziehen sich auf Werte in der Tabelle „syslog_domain“ für Tabellen-Audits, die Fehler oder Warnungen aufgedeckt haben.

3. So zeigen Sie die Protokolle auf dem Server an, die Informationen zu Warnungs- oder Fehler-Audits enthalten:
   a. Kopieren Sie den Wert für die **Detail-ID** im linken Bereich einer Warnung oder eines Fehlers.
   b. Geben Sie im Filternavigator von Hl *syslog_domain.do*ein.

      Die Seite „Domänenprotokoll“ wird angezeigt.

   c. Geben Sie im Feld **Quellensuche**= ein<Detail-ID> (kein Leerzeichen nach dem Gleichheitszeichen), z. B. =f6a00fd29a85b300a9503a81b9169678.

      Auf der Seite „Domänenprotokoll“ werden nur die Protokolle angezeigt, die sich auf das Audit mit der von Ihnen angegebenen Detail-ID beziehen. Jede Zeile in der Tabelle gibt einen anderen Datensatz an, in dem beim Audit Probleme gefunden wurden. Beachten Sie, dass das Feld **Nachricht** auf dieser Seite mit den Werten in der Spalte **Nachricht** des Domänen-Servicecenters übereinstimmt. Das Format der Nachricht entspricht dem Audit-Typ.

4. Wählen Sie Folgendes aus:
   - **Audit**erneut ausführen – Führen Sie ein Audit erneut aus, um zu sehen, ob weiterhin eine Warnung oder ein Fehler auftritt.
   - **Audit deaktivieren** – Deaktiviert einen Audit.
   - **Details**kopieren – Audit-Details in die Zwischenablage kopieren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie laufende und ausstehende Audits an

Aktive Audits werden regelmäßig ausgeführt oder werden zur Ausführung nach Zeitplan in die Warteschlange gestellt. Sie können ihren Status anzeigen, während sie ausgeführt werden.

1. Wählen Sie die Zahl im Feld „ **Laufende Audits** “ aus, um Audits anzuzeigen, die derzeit ausgeführt werden oder deren Ausführung aussteht.

   Die Seite „ **Laufende Audits** “ wird angezeigt.

2. Wählen Sie ein Audit aus, um weitere Informationen darüber zu erhalten.

Zeigen Sie inaktive Audits an

1. Wählen Sie die Zahl im Feld **Inaktive Audits** aus.

   Auf der Seite **Inaktive Audits** werden alle derzeit deaktivierten Audits angezeigt.

2. Wählen Sie einen der Audits aus, um weitere Informationen darüber anzuzeigen.
3. Aktivieren Sie zum Aktivieren eines Audits das Kontrollkästchen **Aktiv**, und geben Sie im Feld **Häufigkeit** an, wie häufig das Audit ausgeführt wird.
4. Wählen Sie **Aktualisieren**.

Konfigurieren Sie das Domain Separation Center

Geben Sie an, welche Tabellen in Domänen groß sind und ob Sie eine detaillierte Protokollierung wünschen.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können Audits so planen, dass sie täglich, wöchentlich oder monatlich ausgeführt werden. Audits, die für große Tabellen ausgeführt werden, können viel Zeit in Anspruch nehmen. Vermeiden Sie daher die tägliche Ausführung von Audits für große Tabellen. Das Starten eines neuen Audits mit einem Audit, dessen Ausführung länger als einen Tag dauert, kann negative Auswirkungen haben.

Eine detaillierte Protokollierung kann bessere Einblicke in Probleme bieten, die bei Audits gefunden wurden, kann jedoch auch zu Leistungsproblemen führen.

Prozedur

1. Wählen Sie im Domain Separation Center **Domänencenter konfigurieren**aus.
   Die Seite „Domänencenter konfigurieren“ wird angezeigt.
2. Wählen Sie **Ja** für **Aktiviert detaillierte Domänenprotokollierung**aus, um detaillierte Protokolle zu speichern, die bei der Diagnose von domänenbezogenen Problemen helfen. Diese Protokolle beziehen sich auf serverseitige Protokolle in der Tabelle „Domänenprotokoll“ [syslog_domain]. Informationen zum Anzeigen der Protokolle finden Sie im Abschnitt Audits mit Warnungen und Fehlern anzeigen.
3. Verschieben Sie in der Liste alle Ihre großen Tabellen in die Spalte **Ausgewählt**.
   Tägliche Audits sollten nicht für große Tabellen ausgeführt werden. Ausgegraute Tabellennamen in der Spalte **Ausgewählt** sind groß und können nicht in die Spalte **Verfügbar** verschoben werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie **Aktualisieren**.
5. Wenn Sie große Tabellen haben, die niemals geprüft werden sollen, legen Sie die Systemeigenschaft *com.glide.domain.audit.big_tables.additional* auf eine durch Kommas getrennte Liste dieser Tabellennamen fest.

Konfigurieren Sie Audits

Konfigurieren Sie, ob ein Audit aktiv ist und wie häufig es ausgeführt wird.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Klicken Sie im Domain Separation Center auf **Audits konfigurieren**.
   T wird angezeigt.
2. Konfigurieren Sie auf der Seite „Audits konfigurieren“ alle Audits, die aktiv sein sollen. Audits sind standardmäßig deaktiviert.
   a. Klicken Sie auf einen Audit.
   b. Klicken Sie auf das Kontrollkästchen **Aktiv**, um das Audit zu aktivieren.
   c. Geben Sie im Feld **Häufigkeit** an, wie häufig der Audit ausgeführt wird.
      Das Domain Separation Center führt alle mit der gleichen Häufigkeit gekennzeichneten Audits gleichzeitig aus. Wählen Sie nicht **Täglich** für Audits aus, die für große Tabellen ausgeführt werden.
   d. Wiederholen Sie die Schritte a bis c für jeden Audit, den Sie aktivieren möchten.
3. Klicken Sie auf **Speichern**.

Planen Sie Audits

Geben Sie die Uhrzeit und den Tag für die Ausführung der Audits an.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Sie haben mindestens eine Audit-Ausführung täglich, wöchentlich oder monatlich konfiguriert. Der Zeitplaner gibt an, an welchen Tagen und zu welchen Zeiten diese Audits ausgeführt werden sollen. Alle Audits mit derselben Planungshäufigkeit werden ab dem von Ihnen konfigurierten Zeitpunkt nacheinander ausgeführt.

Prozedur

1. Klicken Sie im Domain Separation Center auf **Audit-Zeitpläne**.
   Die Seite „Audit-Zeitplan“ wird angezeigt.
2. Konfigurieren Sie die Audit-Zeitpläne.
   a. Klicken Sie auf einen Zeitplannamen.
   b. Geben Sie die Uhrzeit für die Ausführung des Audits an.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für die Zeiteinheiten wird das 24-Stunden-Format verwendet (d. h. 14 ist 14 Uhr).

c. Wählen Sie bei wöchentlichen Zeitplänen den Wochentag aus, an dem das Audit ausgeführt werden soll, wobei 1 Sonntag ist.

d. Wählen Sie bei monatlichen Zeitplänen den Tag des Monats aus, für den das Audit ausgeführt werden soll.

e. Wiederholen Sie den Vorgang für die anderen Zeitpläne.

3. Klicken Sie auf **Speichern**, um die Konfigurationsänderungen zu speichern.
4. Wahlweise: Klicken Sie auf **Jetzt** ausführen, um alle geplanten Audits mit der im oberen rechten Bereich angezeigten Häufigkeit auszuführen.
   Beispiel: Wenn der **Bereichstitel Domänen-Audit-Zeitplan – Täglich**lautet, werden von **'Jetzt** ausführen' sofort alle Audits ausgeführt, für die eine tägliche Ausführung geplant ist.

Nächste Maßnahme
Um den Status eines laufenden Audits anzuzeigen, klicken Sie im Domain Separation Center auf die Zahl im Feld **Audits** werden ausgeführt.

Audits sofort ausführen

Audits werden in der Regel wie geplant ausgeführt. Sie können jedoch alle Audits auf Befehl ausführen.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können einzelne Audits nicht manuell ausführen. Sie können jedoch alle Audits ausführen, die mit der gleichen Zeitplanhäufigkeit konfiguriert sind. Sie können beispielsweise alle Audits ausführen, die für eine tägliche Ausführung konfiguriert sind.

Prozedur

1. Klicken Sie im Domain Separation Center auf **Audit-Zeitpläne**.
2. Klicken Sie auf den Namen des Audit-Zeitplans, den Sie ausführen möchten (z. B. täglich, wöchentlich oder monatlich).
3. Klicken Sie auf **Jetzt ausführen**.

Nächste Maßnahme
Um den Status eines laufenden Audits anzuzeigen, klicken Sie im Domain Separation Center auf die Zahl im Feld **Audits** werden ausgeführt.

Audits mit Warnungen und Fehlern anzeigen

Das Domain Separation Center enthält Details zu Audit-Fehlern und -Warnungen.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Im Dashboard des Domain Separation Center enthalten **Fehler** und **Warnungen** detaillierte Informationen zu Audits, bei denen Probleme aufgetreten sind. Protokolle im Zusammenhang mit Domain Separation befinden sich auf Ihrem Server in der Tabelle „syslog_domain“. Fehler

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

sind Probleme, die sofortige Aufmerksamkeit erfordern. Warnungen führen nicht zu Fehlern, stellen jedoch Best Practices dar, z. B., den Domänennamen nicht zu lang zu machen.

Prozedur

1. Klicken Sie im Domain Separation Center auf die Zahl im Feld **Fehler** oder **Warnungen**.
   Die Seite „ **Fehler** “ oder „ **Warnungen** “ wird angezeigt.
2. Klicken Sie auf einen der Audits in der Liste.
   Auf der Seite werden detaillierte Informationen zu Problemen mit dem ausgewählten Audit angezeigt. Die Nachrichten in den **Audit-Ergebnisdetails** beziehen sich auf Werte in der Tabelle „syslog_domain“ auf dem Server für Tabellen-Audits, die Fehler oder Warnungen aufgedeckt haben.
3. So zeigen Sie die Protokolle auf dem Server an, die Informationen zu Warnungs- oder Fehler-Audits enthalten:

   a. Kopieren Sie den Wert für die **Detail-ID** im linken Bereich einer Warnung oder eines Fehlers.

   b. Geben Sie in der Instanz, auf der das Domain Separation Center ausgeführt wird, im **Filternavigator** *syslog_domain.list* ein.
   Die Seite „Domänenprotokoll“ wird angezeigt.

   c. Geben Sie im Suchfeld der Spalte **Quelle** = ein<Detail-ID> (kein Leerzeichen nach dem Gleichheitszeichen), z. B. `=f6a00fd29a85b300a9503a81b9169678`.
   Auf der Seite „Domänenprotokoll“ werden nur die Protokolle angezeigt, die sich auf das Audit mit der von Ihnen angegebenen Detail-ID beziehen. Jede Zeile in der Tabelle gibt einen anderen Datensatz an, in dem beim Audit Probleme gefunden wurden. Beachten Sie, dass das Feld **Nachricht** auf dieser Seite mit den Werten in der Spalte **Nachricht** des Domain Service Center übereinstimmt. Die in der Nachricht enthaltenen Informationen entsprechen dem Audit-Typ.

4. Wahlweise: Wählen Sie eine der folgenden Optionen aus:
   - **Audit** erneut ausführen – Führen Sie ein Audit erneut aus, um zu sehen, ob weiterhin eine Warnung oder ein Fehler auftritt.
   - **Audit deaktivieren – Deaktiviert** einen Audit.
   - **Details** kopieren – Audit-Details in die Zwischenablage kopieren.

Zeigen Sie laufende und ausstehende Ergebnisse an

Sie können laufende und ausstehende Audits anzeigen, um deren Status anzuzeigen.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Aktive Audits werden regelmäßig ausgeführt oder werden zur Ausführung nach Zeitplan in die Warteschlange gestellt. Sie können ihren Status anzeigen, während sie ausgeführt werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Klicken Sie auf die Zahl im Feld **Audits** werden ausgeführt, um Audits anzuzeigen, die derzeit ausgeführt werden oder deren Ausführung aussteht.
   Die Seite „Laufende Audits“ wird angezeigt.
2. Klicken Sie auf ein laufendes oder ausstehendes Audit, um Informationen darüber anzuzeigen.

Zeigen Sie inaktive Audits an

Sie können alle inaktiven Audits an zentraler Stelle anzeigen und optional aktivieren.

Vorbereitungen

Erforderliche Rolle: admin

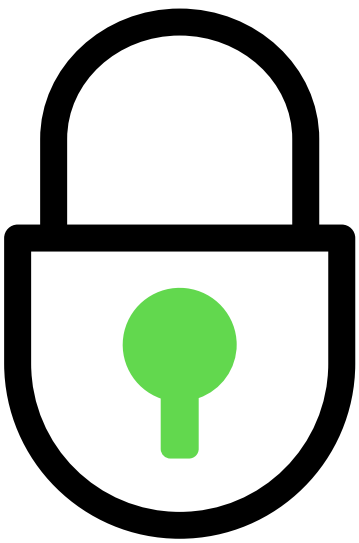
Prozedur

1. Klicken Sie auf die Zahl im Feld **Inaktive Audits**.
   Auf der Seite Inaktive Audits werden alle derzeit deaktivierten Audits angezeigt.
2. Klicken Sie auf einen der Audits, um weitere Informationen darüber anzuzeigen.
3. Wahlweise: Aktivieren Sie ein Audit, indem Sie auf das Kontrollkästchen **Aktiv** klicken und im Feld **Häufigkeit** angeben, wie häufig das Audit ausgeführt wird.
4. Klicken Sie auf **Aktualisieren**.

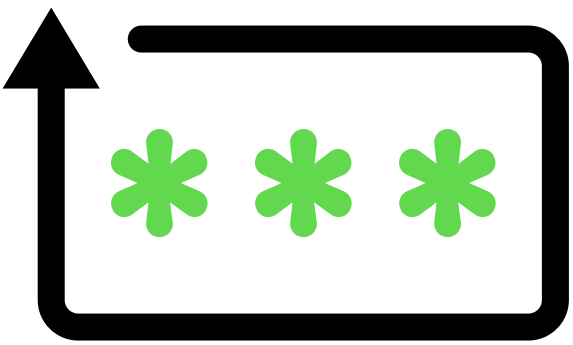
Authentifizierung

ServiceNow® Die Authentifizierung von validiert die Identität eines Benutzers, der auf eine -Instanz zugreift, und autorisiert den Benutzer dann für Funktionen, die der Rolle oder Jobfunktion des Benutzers entsprechen.

Erste Schritte



Single Sign-on (SSO) für mehrere Anbieter

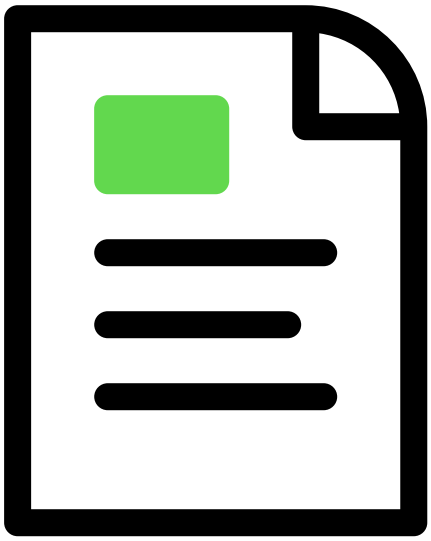


OAuth eingehend und ausgehend

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendername und Passwort, die bei Identitätsanbietern konfiguriert sind, für die ein übereinstimmender Anwenderaccount in der Datenbank vorhanden ist.

Die OAuth-basierte Authentifizierung validiert die Identität des Clients, der versucht, mithilfe eines Authentifizierungsprotokolls eine Vertrauensstellung im System herzustellen.



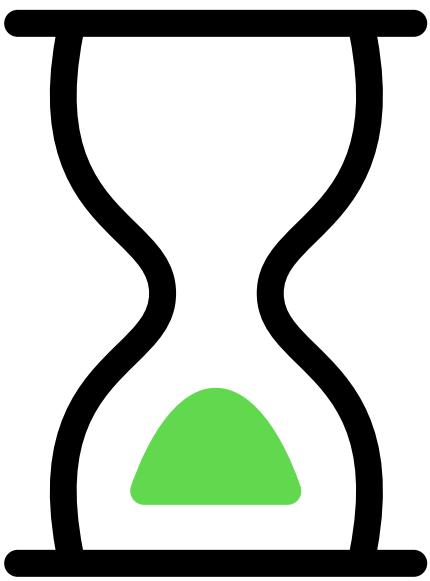
API-Zugriffsrichtlinie

Die API-Zugriffsrichtlinie definiert die Berechtigungen und den Zugriff auf eine API, die durch eine Richtlinie gesteuert werden können.



Digest-Token-Authentifizierung

Der Anwendername und das Geheimnis in der Tabelle führen einen anwenderspezifischen Hash-Vorgang aus, z. B. SHA1, SHA 256 oder MD5. Dieser Wert muss als Teil des URL-Suffixes angehängt werden, das für den Abfrageparameter funktioniert.



Zeitlich begrenzte Authentifizierung



Multifaktor-Authentifizierung (MFA)

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie die linkbasierte Authentifizierung auf der

ServiceNow

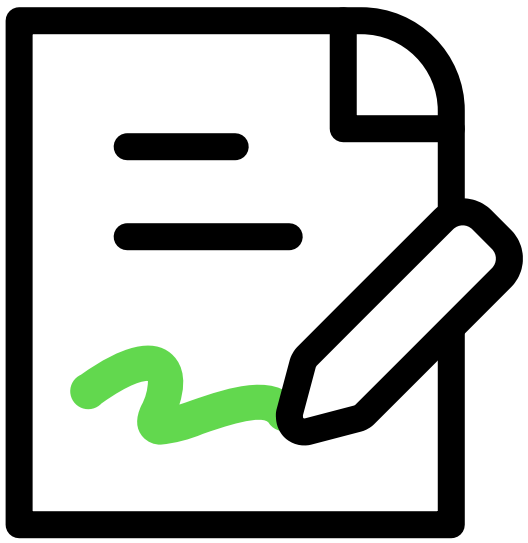
von ServiceNow zu interagieren. Der konfigurierte Link kann per E-Mail oder SMS für den Benutzer freigegeben werden, und der Benutzer kann diese Links verwenden, um sich bei der Instanz anzumelden.

Mit MFA können Sie eine zweite Authentifizierungsebene bereitstellen, die die Verwendung von Passcodes aus einer Authentifizierungs-App, einem Hardwareschlüssel, einem biometrischen Authentifikator, SMS oder E-Mail umfasst.



Zertifikatbasierte Authentifizierung

Eindeutige Zertifikate mit PEM-Verschlüsselung, die Anwendern anstelle von Anwendername und Passwort für die zertifikatsbasierte Authentifizierung zugeordnet sind.

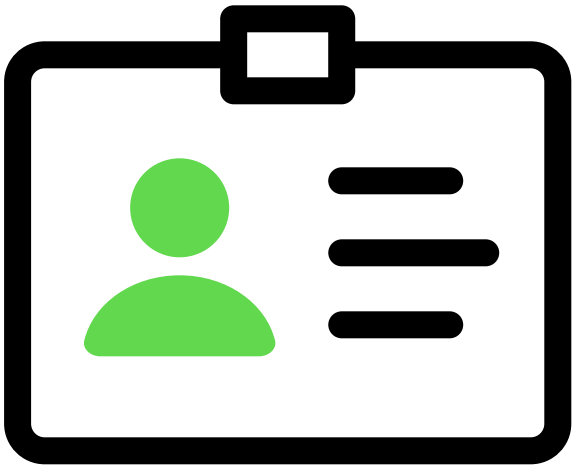


Selbstregistrierung

Verwenden Sie die Selbstregistrierung externer Anwender, um das Onboarding einer großen Anzahl externer Anwender für Ihre Instanz durchzuführen.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



LDAP

Integrieren Sie mit einem LDAP-Verzeichnis (Leighted Directory Access Protocol), um den Benutzeranmeldungsprozess zu optimieren

Sie können verschiedene Methoden verwenden, um Benutzer zu authentifizieren. Die Anmeldeinformationen der Anwender werden für jede Methode mit anderen gespeicherten Anmeldeinformationen abgeglichen.

Hinweis:

- Das SSO-Plugin Okta ist veraltet.
- Weitere Informationen zu den Sicherheitseigenschaften, die sich auf die Autorisierungsverarbeitung auswirken, finden Sie unter Zugriffssteuerung in den Härtungseinstellungen für die Instanzsicherheit.
- Sie können die SAML- und Digest-Authentifizierung über die Anwendung „Mehrere Anbieter – SSO“ verwenden.

Adaptive Authentifizierung

Verwenden Sie das Richtlinien-Framework für die adaptive Authentifizierung, um kontextbezogene Authentifizierungskontrollen für die richtigen Anwender zur richtigen Zeit zu erzwingen. Die adaptive Authentifizierung verwendet Authentifizierungsrichtlinien, um Authentifizierungsanforderungen auszuwerten und dann den Zugriff auf Ihre Instanz basierend auf den angegebenen Richtlinienbedingungen zu verweigern oder zuzulassen.

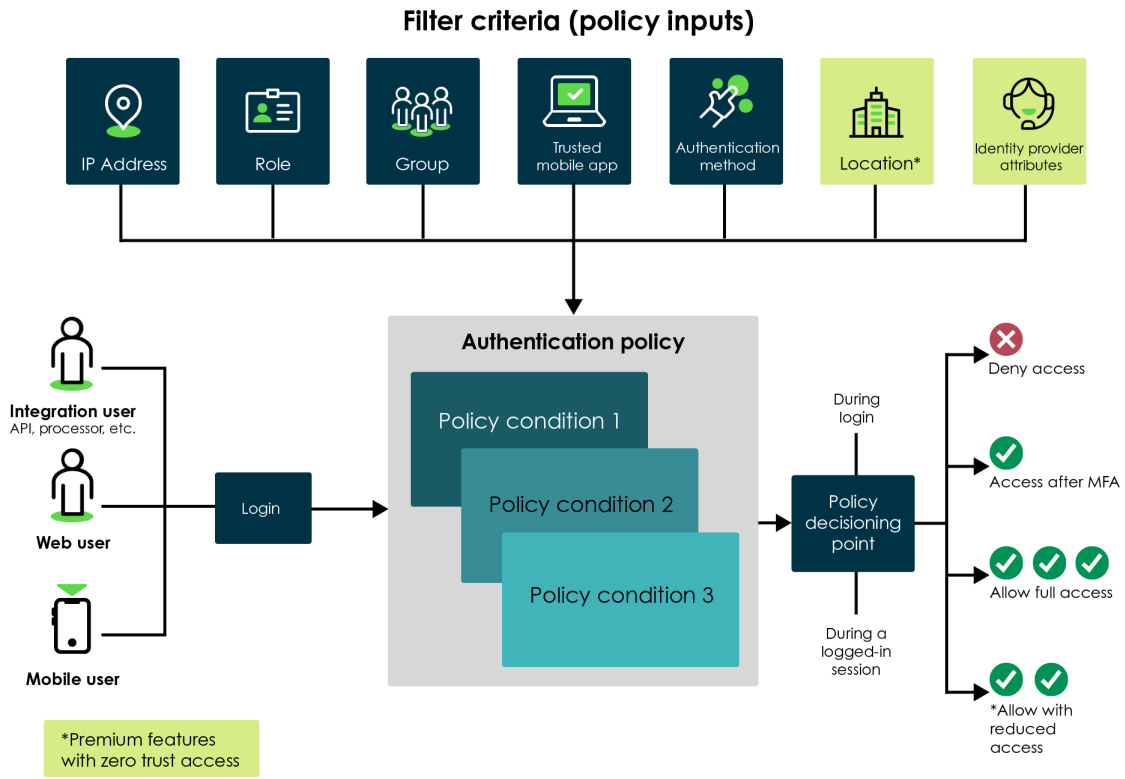
Verwenden Sie Richtlinien und Kontexte für adaptive Authentifizierung, um den Zugriff auf Ihre Instanz für Anwender und APIs basierend auf Kriterien wie IP-Adresse, Anwenderrolle und Anwendergruppe zu beschränken. Sie können die integrierten Authentifizierungsrichtlinien entsprechend Ihren Sicherheitsanforderungen konfigurieren.

Beispielsweise kann ein Administrator *`Allow Access Policy`* so konfigurieren, dass sich nur Benutzer innerhalb eines vertrauenswürdigen IP-Adressbereichs und Mitglieder

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

einer bestimmten Rolle anmelden können. Bei Zuweisung zu *Post-authentication context*verweigert die Zugriffsrichtlinie den Zugriff von nicht vertrauenswürdigen IP-Adressen.

Um eine anwenderdefinierte Nachricht in der Sprache Ihrer Instanz festzulegen, müssen Sie in „sys_ui_message.list“ ein Schlüssel-Wert-Paar hinzufügen und den `Datensatz „sys_ui_message“` aktualisieren. Wenn Sie sich mit einem falschen Passwort anmelden, wird die anwenderdefinierte Nachricht in der bevorzugten Sprache angezeigt.



Komponenten der adaptiven Authentifizierung

Authentifizierungsrichtlinien

Authentifizierungsrichtlinien werten Authentifizierungsanforderungen basierend auf den angegebenen Richtlinienbedingungen aus und erlauben oder verweigern den Zugriff, abhängig von der Ausgabe der Bewertung der Richtlinienbedingungen. Beispielsweise ist der -Zugriff nur zulässig, wenn alle in der **Allow-Zugriffsrichtlinie angegebenen Richtlinienbedingungen** als true ausgewertet werden.

Authentifizierungsrichtlinien verwenden Informationen, die durch Filterkriterien für den Vergleich mit den Bedingungen der Richtlinie bereitgestellt werden, um zu bestimmen, ob Zugriff auf die Instanz gewährt werden soll. Beispielsweise geben Filterkriterien die IP-Adresse eines Benutzers an, und eine Richtlinienbedingung bestimmt, ob sich diese Adresse innerhalb des spezifischen Bereichs befindet, bevor Zugriff gewährt wird. Weitere Informationen zu Authentifizierungsrichtlinien finden Sie unter Authentifizierungsrichtlinien.

Kontexte der Authentifizierungsrichtlinie

Kontexte der Authentifizierungsrichtlinie definieren, wie und wann Richtlinien während des Anmeldevorgangs erzwungen werden. Der Kontext der Vorauthentifizierung wird ausgeführt, bevor dem Anwender ein

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anmeldebildschirm angezeigt wird. Der Kontext nach der Authentifizierung wird ausgeführt, nachdem der Benutzer seine Anmeldeinformationen eingegeben hat. Um eine Richtlinie verwenden zu können, muss sie einem Richtlinienkontext zugewiesen werden. Einzelheiten zu diesen Kontexten finden Sie unter Kontexte der Authentifizierungsrichtlinie.

Filterkriterien

Filterkriterien (auch als Richtlinieneingaben bezeichnet) werden als Eingaben für Richtlinienbedingungen verwendet. Richtlinienbedingungen verwenden diese Eingaben, um die Anforderungen von Authentifizierungsanforderungen zu überprüfen und zu erfüllen. Diese Eingaben enthalten Informationen wie Anwenderrolle, IP-Bereich und Identitätsanbieter. Weitere Informationen zu Filterkriterien finden Sie unter Filterkriterien.

Authentifizierungseigenschaften

Verwenden Sie Authentifizierungseigenschaften, um zu steuern, ob die adaptive Authentifizierung in Ihrer Instanz aktiv ist. Sie können auch -Eigenschaften verwenden, um das Debugging zu aktivieren und die Messaging-Benutzer zu definieren, die angezeigt werden, wenn der Zugriff blockiert wird. Einzelheiten zu diesen Eigenschaften finden Sie unter Konfigurieren Sie die Eigenschaften der adaptiven Authentifizierung.

REST API-Zugriffsrichtlinien

Sie können die Filterkriterien des adaptiven Authentifizierungs-Frameworks verwenden, um den Zugriff auf eingehende ServiceNow REST APIs einzuschränken. Weitere Informationen finden Sie unter REST API-Zugriffsrichtlinien.

Domänentrennung und adaptive Authentifizierung

Die adaptive Authentifizierung wird in domänengetrennten Instanzen auf der Bedingungsebene der Authentifizierungsrichtlinie unterstützt. Richtlinienbedingungen wirken sich auf die Domäne im Datensatzfeld „ **Domäne** “ [sys_domain] aus. Richtlinienbedingungen in der globalen Domäne wirken sich auf alle Domänen aus.

Adaptive Authentifizierungsereignisse

Sie können die Tabelle mit den adaptiven Authentifizierungsereignissen verwenden, um mehr über die Ereignisse zu erfahren, die speziell für die adaptive Authentifizierungsfunktion aufgetreten sind. Weitere Informationen finden Sie unter Adaptive Authentifizierungsereignisse.

Aktivieren Sie die adaptive Authentifizierung

Wenn Sie die Administratorrolle innehaben, können Sie das Plugin „ Adaptive Authentifizierung “ (com.snc.adaptive_authentication) für die adaptive Authentifizierung aktivieren.

Vorbereitungen

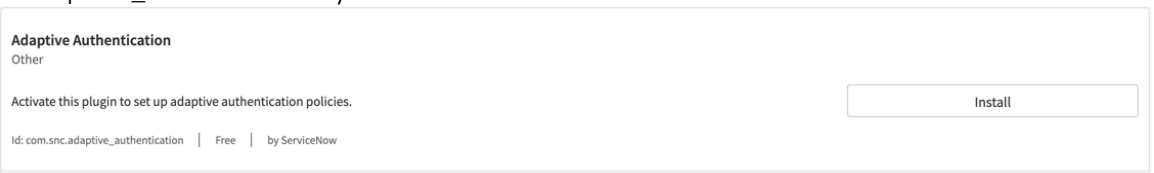
Erforderliche Rolle: admin.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie das Plugin „ **Adaptive Authentifizierung** “ (com.snc.adaptive_authentication) mithilfe der Filterkriterien und der Suchleiste.



   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.

3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: `Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.`

   Nach Abschluss der Installation wird eine Meldung angezeigt.

Nächste Maßnahme

Konfigurieren Sie Ihre Authentifizierungsrichtlinien, um kontextbezogene Authentifizierungskontrollen in Ihrer Instanz zu erzwingen.

Sobald Ihre Richtlinien konfiguriert sind. Aktivieren Sie die adaptive Authentifizierung mithilfe der **Richtlinie** „Authentifizierungsrichtlinie aktivieren“. Einzelheiten zu den Eigenschaften der adaptiven Authentifizierung finden Sie unter Konfigurieren Sie die Eigenschaften der adaptiven Authentifizierung.

Filterkriterien

Filterkriterien (auch als Richtlinieneingaben bezeichnet) werden als Eingaben für Richtlinienbedingungen verwendet, um die Anforderungen einer Authentifizierungsanforderung zu überprüfen und zu erfüllen.

Verwenden Sie Filterkriterien, um Informationsauthentifizierungsrichtlinien wie IP-Adresse, Rollen oder Gruppen eines Anwenders anzugeben. Fügen Sie diese Kriterien im Abschnitt **„Richtlinienbedingungen** “ Ihrer Richtlinien hinzu.

Es gibt sieben Arten von Filterkriterien, die bei der adaptiven Authentifizierung verwendet werden. Ihre Authentifizierungsrichtlinien können eines oder mehrere dieser Kriterien verwenden, um Authentifizierungsanforderungen auszuwerten.

Filterkriterientypen

Typ	Beschreibung
IP-Filterkriterien	Verwenden Sie IP-Filterkriterien, um Benutzer basierend auf den IP-Adressen der Benutzer zu filtern. Sowohl IPv4 als auch IPv6 werden unterstützt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Filterkriterientypen (Fortsetzung)

Typ	Beschreibung
Rollenfilterkriterien	Verwenden Sie Rollenfilterkriterien, um Benutzer basierend auf ihren Rollen zu filtern.
Gruppenfilterkriterien	Verwenden Sie Gruppenfilterkriterien, um Benutzer basierend auf der Benutzergruppe zu filtern, zu der der Benutzer gehört.
Standortfilterkriterien	Verwenden Sie Standortfilterkriterien, um Anwender anhand des Anwenderstandorts zu filtern.
Filterkriterien für Identitätsanbieterattribut	Verwenden Sie die Attribute des Identitätsanbieters, die von der SAML-Antwort vom IdP empfangen werden, als Filterkriterien für die Authentifizierung.

Generische Kriterien

Zusätzlich zu den zuvor aufgeführten Typen gibt es vier generische Filterkriterien. Diese Kriterien werden nicht in Ihrem Filternavigator angezeigt, Sie können sie jedoch auswählen, während Sie Ihren Authentifizierungsrichtlinien Richtlinieneingaben hinzufügen.

Generische Filterkriterientypen

Typ	Beschreibung
Authentifizierungsschema	Verwenden Sie, um basierend auf dem Authentifizierungsschema des Anwenders zu filtern. Dieses Kriterium ist ein Auswahltyp mit zwei Optionen: • Anwendername und Passwort, die eine lokale Anmeldung kennzeichnen • SSO – eine auf Multi-SSO (SAML, OIDC oder Digest) basierende Anmeldung. **Hinweis:** Diese Filterkriterien sind nur verfügbar, wenn das Plugin „ **Integration – Single Sign-on-Installationsprogramm für mehrere Anbieter**“ [com.snc.integration.sso.multi.installer] installiert ist.
Identitätsanbieter	Verwenden Sie, um basierend auf dem Identitätsanbieter des Benutzers zu filtern. Verwenden Sie zusammen mit den Kriterien des Authentifizierungsschemas, um eine granulare Kontrolle über den Anmeldevorgang zu erhalten. Dieses Kriterium bezieht sich auf die Tabelle „ **Identitätsanbieter** “ [sso_properties]. **Hinweis:** Diese Filterkriterien sind nur verfügbar, wenn das Plugin „ **Integration – Single Sign-on-Installationsprogramm für mehrere Anbieter**“ [com.snc.integration.sso.multi.installer] installiert ist.
Rollenbasierte MFA	Verwenden Sie, um basierend auf der rollenbasierten MFA-Funktion zu filtern. Dieses Kriterium ist ein boolesches Filterkriterium, das angibt, ob die rollenbasierte MFA für den Anwender aktiviert ist.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Generische Filterkriterientypen (Fortsetzung)

Typ	Beschreibung
Anwenderbasierte MFA	Verwenden Sie, um basierend auf der anwenderbasierten MFA-Funktion zu filtern. Dieses Kriterium ist ein boolesches Filterkriterium, das angibt, ob anwenderbasierte MFA für den Anwender aktiviert ist.
Vertrauenswürdige mobile App	Vertrauenswürdiger Filter für mobile Apps zum Aktivieren des Instanzzugriffs über die mobile App.

IP-Filter

Verwenden Sie IP-Filterkriterien, um die Benutzer basierend auf den IP-Adressen der Benutzer zu filtern. Sowohl IPv4 als auch IPv6 werden unterstützt.

Mit IP-Filterkriterien können Sie Benutzer basierend auf den IP-Adressen der Benutzer filtern. Sie können eine Authentifizierungsrichtlinie konfigurieren, um den Zugriff auf eine bestimmte Adresse oder einen bestimmten Adressbereich zuzulassen oder zu verweigern.

Erstellen Sie IP-Filterkriterien

Mit IP-Filterkriterien können Sie Benutzer basierend auf den IP-Adressen der Benutzer filtern. Sie können eine Authentifizierungsrichtlinie konfigurieren, um den Zugriff auf eine bestimmte Adresse oder einen bestimmten Adressbereich zuzulassen oder zu verweigern.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

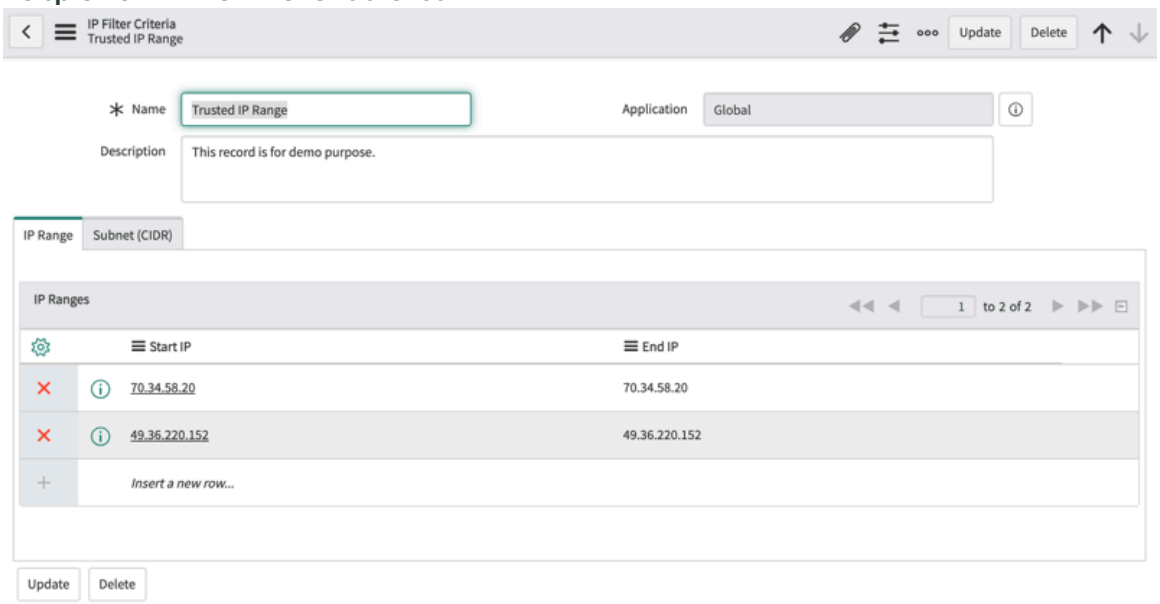
1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Filterkriterien** > **IP-Filterkriterien**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular aus.

Formular „IP-Filterkriterien“.

Feld	Beschreibung
Name	Name zur Identifizierung des IP-Netzwerks.
Beschreibung	Kurze Beschreibung des IP-Netzwerks.
Anwendung	Umfang der Anwendung.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

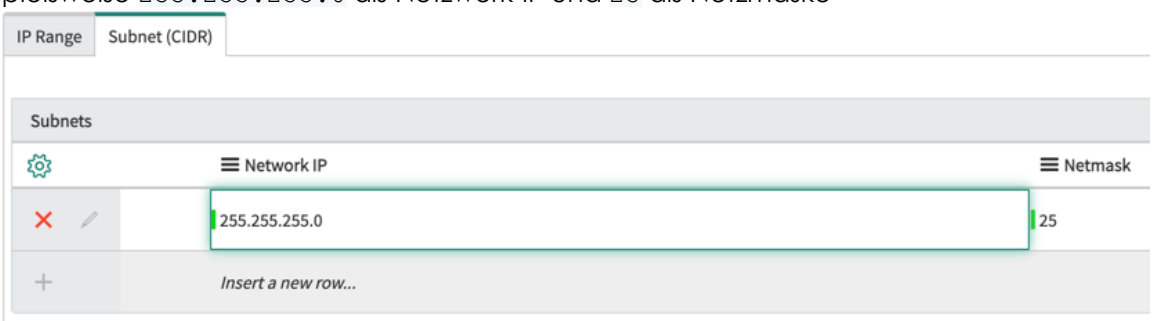
Beispiel für IP-Filterkriteriendatensatz



4. Klicken Sie mit der rechten Maustaste in den Header Kopfzeile des Formulars, und wählen Sie **Speichern** aus.
5. Doppelklicken Sie auf der Registerkarte **IP** -Bereich auf **Neue Zeile einfügen**.
   Sie können eine einzelne IP-Adresse oder mehrere IP-Adressbereiche eingeben. Geben Sie für einen Bereich von IP-Adressen beispielsweise `192.0.2.0` in der Spalte **Start-IP** und `192.0.2.255` in der Spalte **End-IP** ein.

   Hinweis: Stellen Sie bei einzelnen IP-Adressen sicher, dass Sie dieselbe IP-Adresse in die Spalten **Start IP** address (Start-IP-Adresse) und **End IP** (End-IP-Adresse) eingeben. Wenn Sie eine IP-Adresse in die Spalte „ **Start IP** “ (Start-IP) eingeben, lassen Sie die Spalte „ **End IP** “ leer, und speichern Sie dann den Datensatz. Die Spalte „ **End-IP** “ wird automatisch mit derselben **Start-IP** -Adresse gefüllt.

6. Doppelklicken Sie auf der Registerkarte **Subnetz (CIDR)** auf **Neue Zeile einfügen**.
   Geben Sie die Netzwerk-IP-Adresse und die Netzmaske im CIDR-Format (Classless Inter-Domain Routing) ein. Geben Sie beispielsweise `255.255.255.0` als Netzwerk-IP und `25` als Netzmaske ein.



Rollenfilter

Verwenden Sie Rollenfilterkriterien, um Benutzer basierend auf ihren Rollen zu filtern.

Mit Rollenfilterkriterien können Sie Benutzer basierend auf den Rollen filtern. Sie können eine Authentifizierungsrichtlinie konfigurieren, um den Zugriff auf eine Liste von Anwenderrollen zuzulassen oder zu verweigern.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie Rollenfilterkriterien

Mit Rollenfilterkriterien können Sie Benutzer basierend auf den Rollen filtern. Sie können eine Authentifizierungsrichtlinie konfigurieren, um den Zugriff auf eine Liste von Anwenderrollen zuzulassen oder zu verweigern.

Vorbereitungen

Erforderliche Rolle: admin

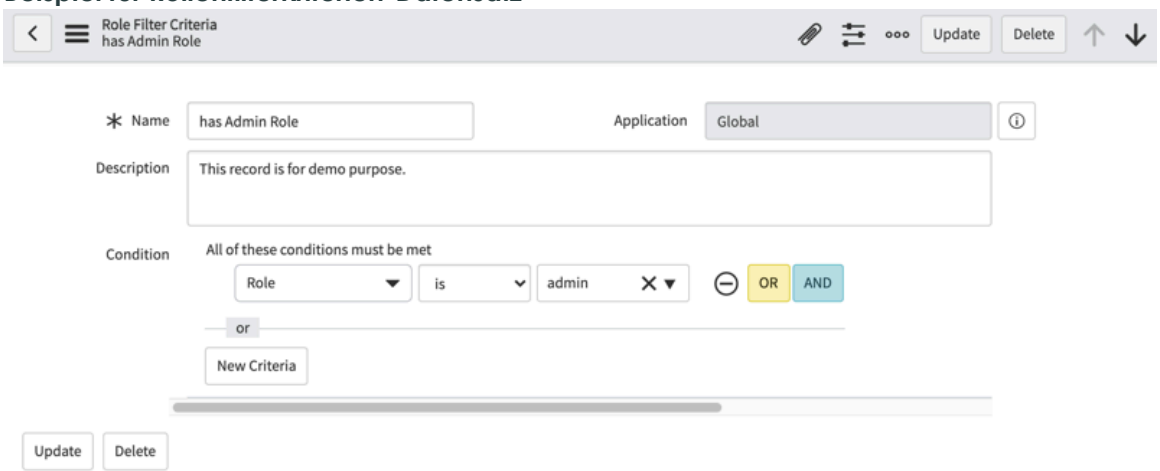
Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Filterkriterien** > **Rollen-Filterkriterien**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular aus.

Formular „Rollenfilterkriterien“.

Feld	Beschreibung
Name	Name zur Identifizierung der Rolle.
Anwendung	Umfang der Anwendung.
Beschreibung	Kurze Beschreibung der Rolle.

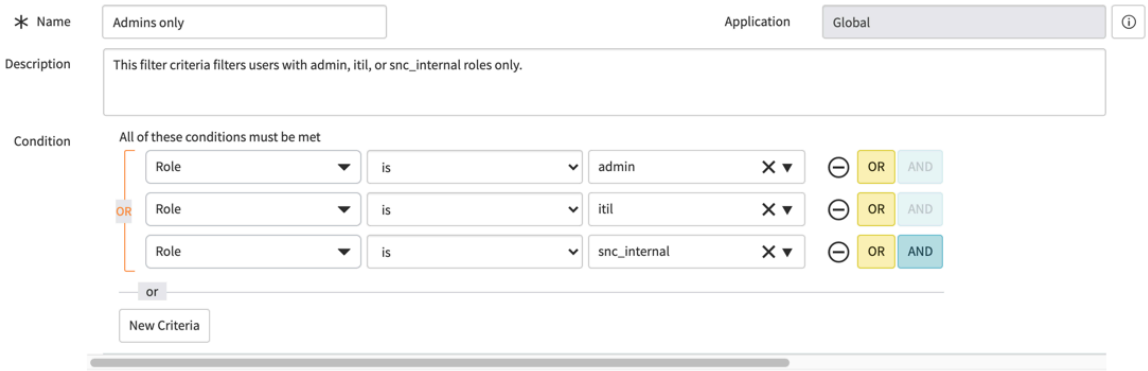
Beispiel für Rollenfilterkriterien-Datensatz



4. Doppelklicken Sie unter **Rollen für Kriterien**auf **Neue Zeile einfügen**.
5. Erstellen Sie mit dem Bedingungsgenerator eine Bedingung für eine bestimmte Rolle. Sie können beispielsweise eine Bedingung erstellen, die nur Benutzer mit den Rollen „admin“, „itil“ oder „snc_internal“ zulässt. Weitere Informationen zum Bedingungsgenerator finden Sie unter Bedingungsanweisungen mit dem Bedingungsgenerator erstellen .

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Derzeit wird Dot-Walking in den Rollenfilterkriterien nicht unterstützt.



Gruppenfilter

Verwenden Sie Gruppenfilterkriterien, um Benutzer basierend auf der Benutzergruppe zu filtern, zu der der Benutzer gehört.

Gruppenfilterkriterien gewähren oder verweigern den Benutzerzugriff basierend auf der Benutzergruppe, zu der der Benutzer gehört.

Erstellen Sie Gruppenfilterkriterien

Gruppenfilterkriterien gewähren oder verweigern den Benutzerzugriff basierend auf der Benutzergruppe, zu der der Benutzer gehört.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

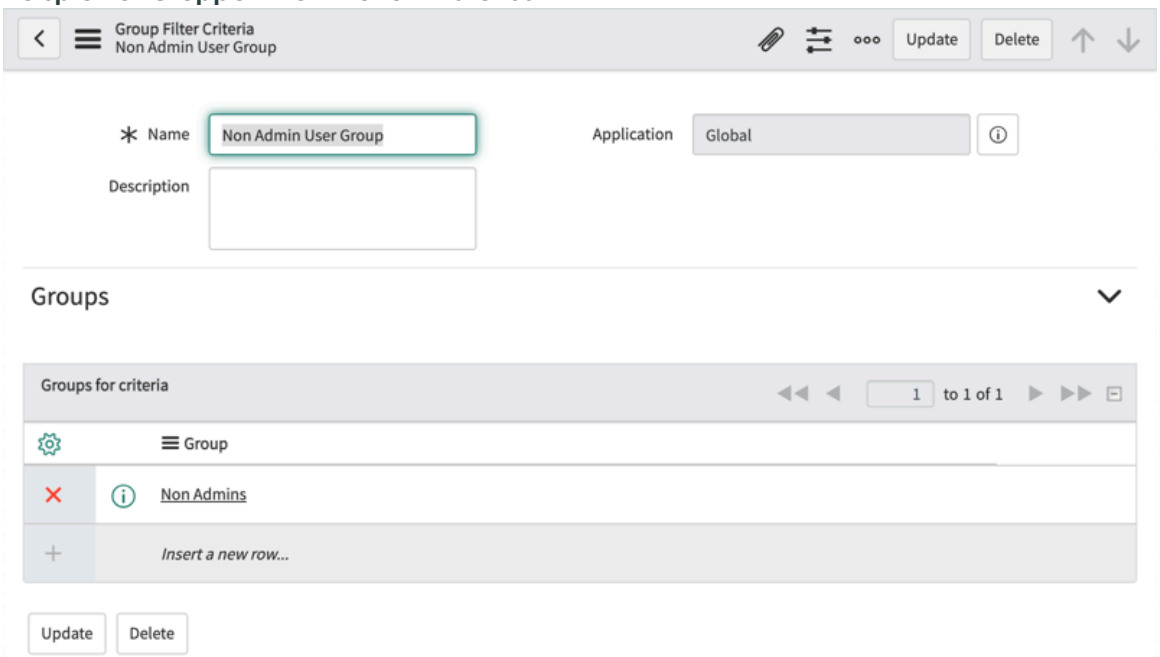
1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Filterkriterien** > **Gruppenfilterkriterien**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular aus.

Gruppenfilterkriterien

Feld	Beschreibung
Name	Name zur Identifizierung der Gruppe.
Beschreibung	Kurze Beschreibung der Gruppe.
Anwendung	Umfang der Anwendung.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für Gruppenfilterkriterien-Datensatz



4. Doppelklicken Sie auf der Registerkarte **Gruppen für Kriterien** auf **Neue Zeile einfügen**.
5. Klicken Sie auf das Suchsymbol , suchen Sie und wählen Sie eine Benutzergruppe aus.
6. Klicken Sie auf das Speichern-Symbol – .

Standortfilter

Standortfilterkriterien können als Filtereingabe für Benutzer basierend auf dem Benutzerstandort verwendet werden.

Der Standortfilter ist ein Filterkriterium, das Administratoren beim Erstellen der Authentifizierungsrichtlinien basierend auf dem physischen Standort des Geräts verwenden können.

Hinweis:

- Die Standortfilterkriterien sind ein kostenpflichtiges Plugin und erfordern eine Lizenz.
- Die Instanz muss sich auf ADCv2 befinden. Wenn sich die Instanz nicht auf ADCv2 befindet, sind keine Informationen zum Anwenderstandort verfügbar.

Mit den Standortfilterkriterien können Sie:

- Agieren Sie als Richtlinieneingabe-Akt, damit Richtlinienbedingungen überprüft und die Anforderungen für die Authentifizierung erfüllt werden.
- Bieten Sie die Möglichkeit, Richtlinien für adaptive Authentifizierung basierend auf dem **Land**zu erstellen.
- Erlauben Sie den Instanzzugriff auf eine bestimmte Geografie oder verweigern Sie ihn.
- Verwenden Sie die auf dem geografischen Standort basierende Vor- oder Nachauthentifizierungsrichtlinie für Folgendes:

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Verhindern Sie den Zugriff aus sanktionierten Ländern, außerhalb einer Region mit strengem Datenschutz, nach Ermessen des Unternehmens.
- Erlauben Sie den Zugriff auf Bereiche nur innerhalb der geltenden Datenschutzregion und innerhalb des Ermessens des Unternehmens.
- Konfigurieren Sie die länderbasierte Allow-Liste für die Authentifizierung.

Anwendungsfälle

Im Folgenden finden Sie einige Anwendungsfälle für die Verwendung von Standortfilterkriterien für die adaptive Authentifizierung:

- Blockieren Sie den Zugriff auf die Instanz aus einem Land.
- Erlauben Sie den Zugriff auf die Instanz nur aus einem bestimmten Land.
- Erzwingen Sie die Step-up-Authentifizierung oder MFA für die Anmeldung basierend auf dem Land.
- Reduzieren oder beschränken Sie die Rollen für den Anwender basierend auf dem Land.
- Standortfilterkriterien können für MFA, Zero Trust Access (ZTA), Kontext vor der Authentifizierung und Kontext nach der Authentifizierung verwendet werden.

Standortidentifizierung

Die Ortungsdienste zum Identifizieren des Standorts des Benutzers werden von einem Drittanbieterservice – MaxMind – bereitgestellt.

Der Standort des Benutzers wird über das VPN anhand des Headers „x-forwarded-for“ identifiziert. Wenn vom Service kein Header ausgefüllt wird, wird nur die VPN-IP (Standort) als Anwenderstandort angezeigt.

Hinweis: Wenn nach der Konfiguration des Standortfilters falsche Standorte angezeigt werden, lesen Sie zur Problembehandlung den KB-Artikel .

Aktivieren Sie den standortbasierten Zugriff

Aktivieren Sie **Zero Trust – Standortbasierter Zugriff** (`com.snc.zero_trust_location_access`), damit Administratoren Richtlinien für adaptive Authentifizierung basierend auf dem Standort des Anwenders konfigurieren können.

Vorbereitungen

Erforderliche Rolle: admin

- Abhängiges Plugin: Adaptive Authentifizierung
- Plugin-Typ: Kostenpflichtig und erfordert Lizenz.
- Die Instanz muss sich auf ADCv2 befinden. Wenn sich die Instanz nicht auf ADCv2 befindet, sind keine Informationen zum Anwenderstandort verfügbar.

Prozedur

1. Navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie das Plugin „ **Zero Trust – Standortbasierter Zugriff** “ (`com.snc.zero_trust_location_access`) mithilfe der Filterkriterien und der Suchleiste.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.

3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: `Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.`

   Nach Abschluss der Installation wird eine Meldung angezeigt.

Erstellen Sie Standortfilterkriterien

Verwenden Sie Standortfilterkriterien, um die Eingabe für die Anwenderauthentifizierung basierend auf dem Anwenderstandort zu filtern.

Vorbereitungen

Erforderliche Rolle: admin

Erforderliches Plugin: **Zero Trust – standortbasierter Zugriff** (`com.snc.zero_trust_location_access`).

Eigenschaft: Aktivieren Sie die Eigenschaft „Adaptive Authentifizierung“.

Hinweis: Administratoren können die Richtlinie nur basierend auf Standortfiltern erstellen, wenn der Standort für die aktuelle Benutzersitzung verfügbar ist.

Prozedur

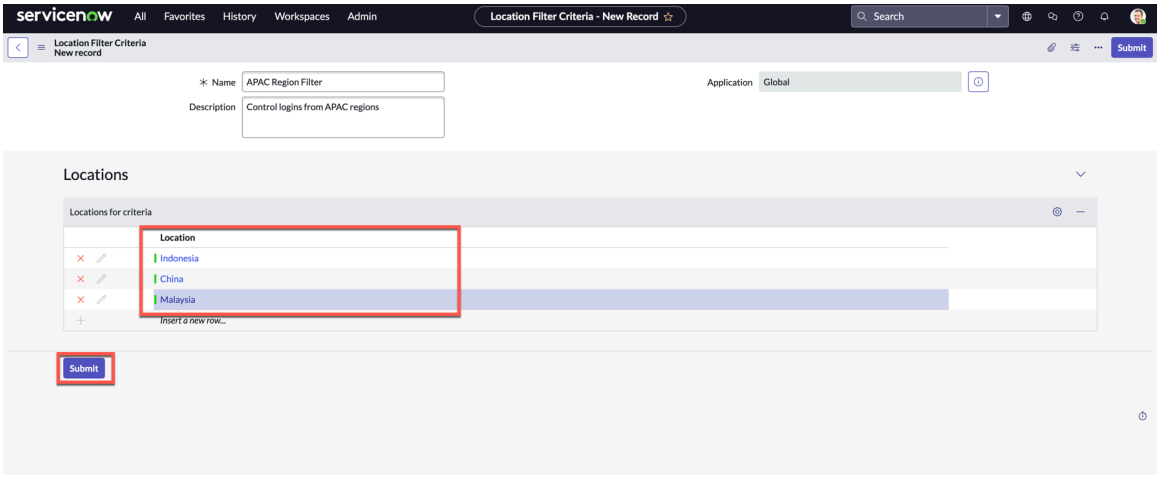
1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Filterkriterien** > **Standortfilterkriterien**an.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular aus.

Formular „Standortfilterkriterien“.

Feld	Beschreibung
Name	Name zur Identifizierung der Kriterien.
Beschreibung	Kurze Beschreibung der Kriterien.
Anwendung	Umfang der Anwendung.

4. Doppelklicken Sie im Abschnitt **Standorte** auf der Registerkarte Standorte für Kriterien auf **Neue Zeile einfügen**.
5. Geben Sie die Standorte an.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Wählen Sie **Absenden**.

Lernprogramm: Verwenden Sie Standortfilterkriterien

Beschreibt Schritte zur Verwendung von Standortfilterkriterien in der Authentifizierungsrichtlinie und zur Beschränkung des Zugriffs auf die Benutzer basierend auf dem Standort.

Vorbereitungen

Erforderliche Rolle: admin

Erforderliches Plugin: **Zero Trust – standortbasierter Zugriff** (`com.snc.zero_trust_location_access`).

Eigenschaft: Aktivieren Sie die Eigenschaft „Adaptive Authentifizierung“.

Hinweis: Administratoren können die Richtlinie nur basierend auf Standortfiltern erstellen, wenn der Standort für die aktuelle Benutzersitzung verfügbar ist.

Im folgenden Verfahren wird beschrieben, wie Sie die Standortfilterkriterien in einer Authentifizierungsrichtlinie erstellen und verwenden.

Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Filterkriterien** > **Standortfilter**an.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular aus.

Formular „Standortfilterkriterien“.

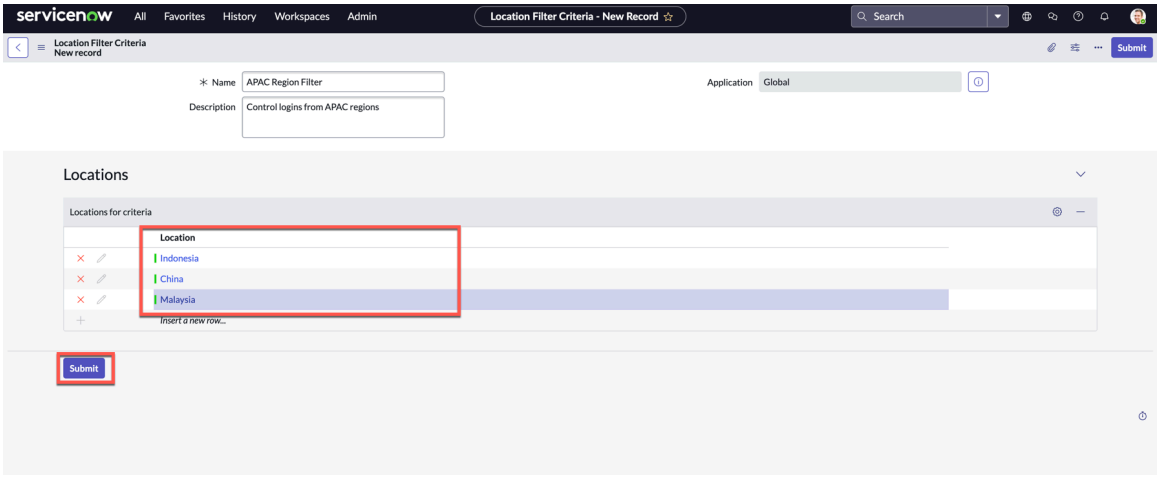
Feld	Beschreibung
Name	Name zur Identifizierung der Kriterien.
Beschreibung	Kurze Beschreibung der Kriterien.
Anwendung	Umfang der Anwendung.

4. Doppelklicken Sie im Abschnitt **Standorte** auf der Registerkarte Standorte für Kriterien auf **Neue Zeile einfügen**.
5. Geben Sie die Standorte an.

   Verwenden Sie beispielsweise einige APAC-Regionen, um die Anmeldungen der Benutzer aus APAC zu steuern.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Basierend auf den im Beispiel festgelegten Kriterien können Sie Anmeldungen aus `Incident`, `China`und `Malaiisch` für Ihre Instanz steuern.

6. Wählen Sie **Absenden**.
7. Verwenden Sie die Filterkriterien, die im Authentifizierungskontext (Pre, Post, MFA) und im Sitzungszugriff erstellt wurden.

   Weitere Informationen zur Konfiguration basierend auf Authentifizierungskontext und Sitzungszugriff finden Sie unter:

   - Standortfilter im Kontext vor der Authentifizierung
   - Standortfilter im Kontext nach der Authentifizierung
   - Standortfilter im MFA-Kontext
   - Standortfilter für Sitzungszugriff

   Sie können die Eigenschafts-ID – Fehlermeldung, die dem Anwender angezeigt wird, wenn die Anmeldung aufgrund eines Fehlers bei der Authentifizierungsrichtlinie fehlschlägt (`glide.auth.policy.ui.error.message`) verwenden, um die Fehlermeldung anzupassen.

Standortfilter im Kontext vor der Authentifizierung verwenden

Verwenden Sie die im Kontext vor der Authentifizierung erstellten Standortfilterkriterien.

Vorbereitungen

Erforderliche Rolle: admin

Erforderliches Plugin: **Zero Trust – standortbasierter Zugriff** (`com.snc.zero_trust_location_access`).

Erstellen Sie einen Standortfilter mit den Ländern, die den Zugriff auf die Anwender basierend auf dem Standort einschränken möchten. Weitere Informationen finden Sie unter Erstellen Sie Standortfilterkriterien.

Prozedur

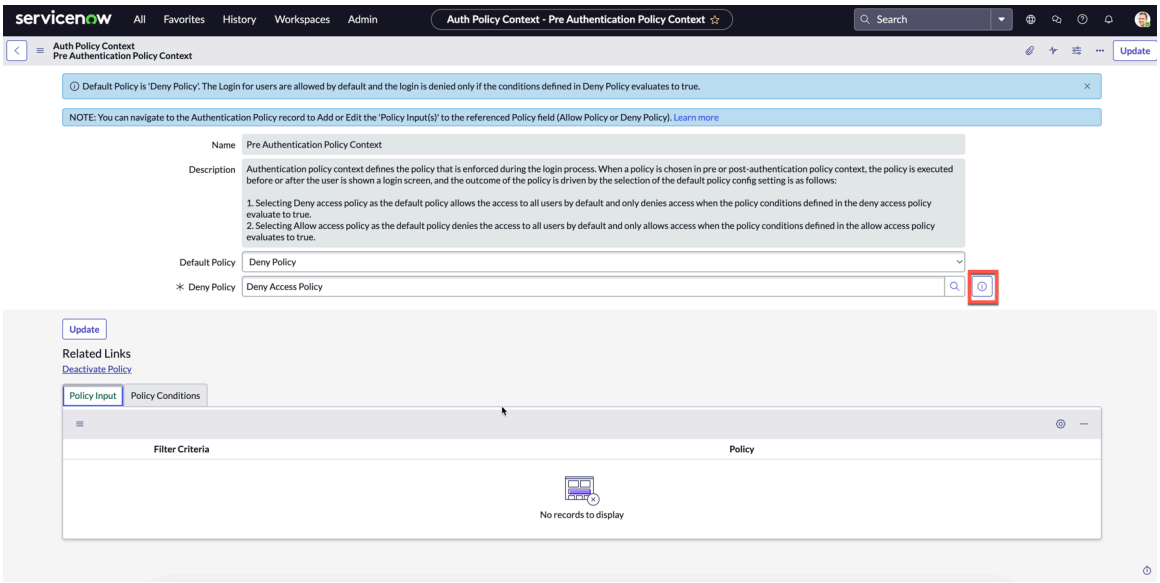
1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Kontext der Authentifizierungsrichtlinie** > **Kontext vor der Authentifizierung**an.

   Wenn eine Richtlinie im Richtlinienkontext vor der Authentifizierung ausgewählt wird:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn Sie die Zugriffsverweigerungsrichtlinie als Standardrichtlinie auswählen, wird standardmäßig der Zugriff für alle Anwender gewährt und nur dann verweigert, wenn die in der Zugriffsverweigerungsrichtlinie definierten Richtlinienbedingungen als „wahr“ ausgewertet werden.
- Wenn Sie die Richtlinie „Zugriff zulassen“ als Standardrichtlinie auswählen, wird standardmäßig allen Anwendern der Zugriff verweigert und nur dann gewährt, wenn die in der Richtlinie „Zugriff zulassen“ definierten Richtlinienbedingungen als „wahr“ ausgewertet werden.

Das Beispiel zeigt, wie Sie die Anmeldungen von den angegebenen Standorten einschränken können. Sie können Zugriff verweigern und die zugehörige Richtlinie Zugriff verweigern als Richtlinie vor der Authentifizierung auswählen und die Richtlinieneingaben und -bedingungen angeben.



2. Wählen Sie das Informationssymbol, um den Datensatz **„Richtlinie verweigern“** zu öffnen.

> **Hinweis:** Das in dieser Aufgabe beschriebene Beispiel ist **Deny Policy**(Richtlinie verweigern). Sie können auch die **Zulassungsrichtlinie** verwenden und die Bedingungen entsprechend festlegen, um die Anmeldungen zu steuern.

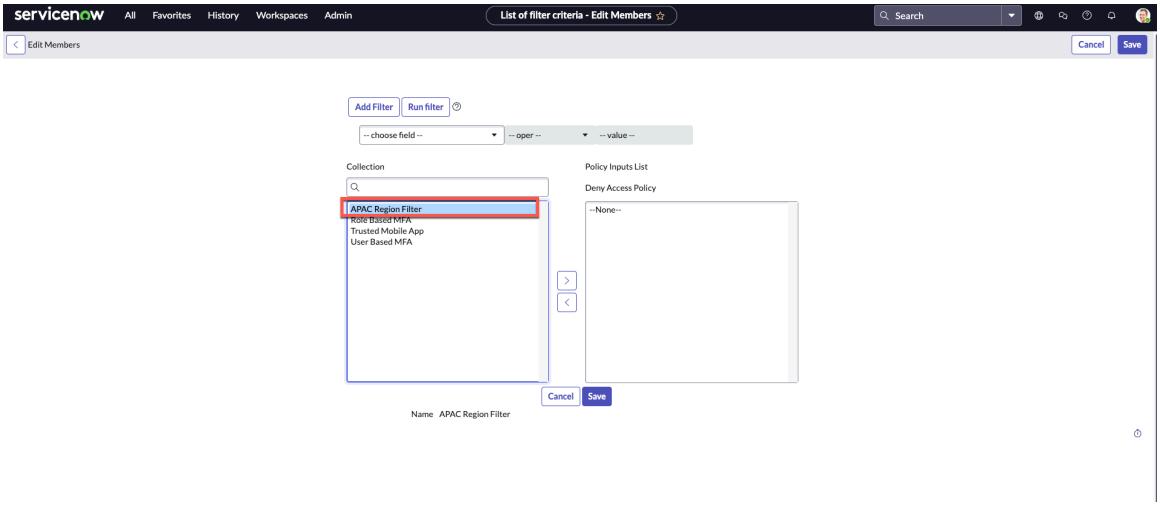
3. Wählen Sie in der Richtlinie „Zugriff verweigern“ im Abschnitt „Richtlinieneingaben“ **Neu**.



4. Fügen Sie die Eingabe Standortfilter hinzu, und **speichern Sie**.

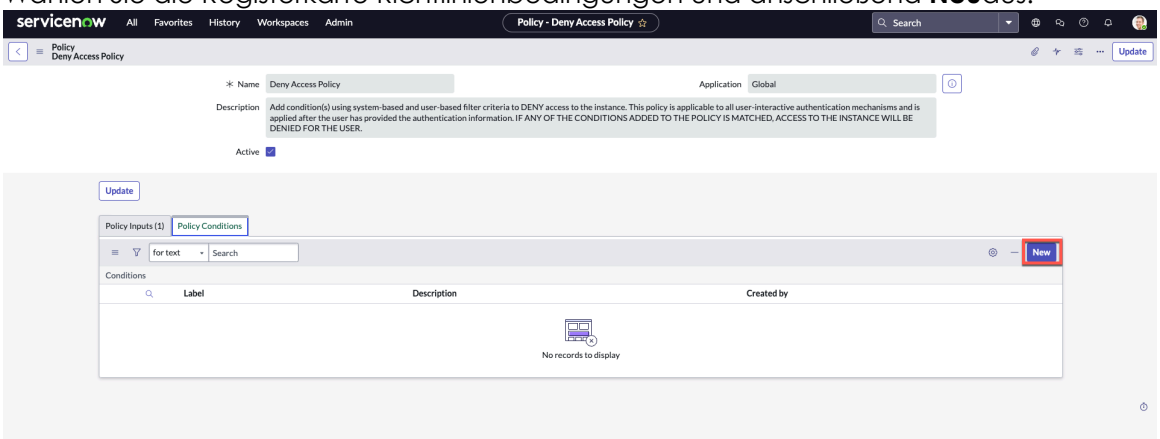
Beispiel: APAC-Region.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

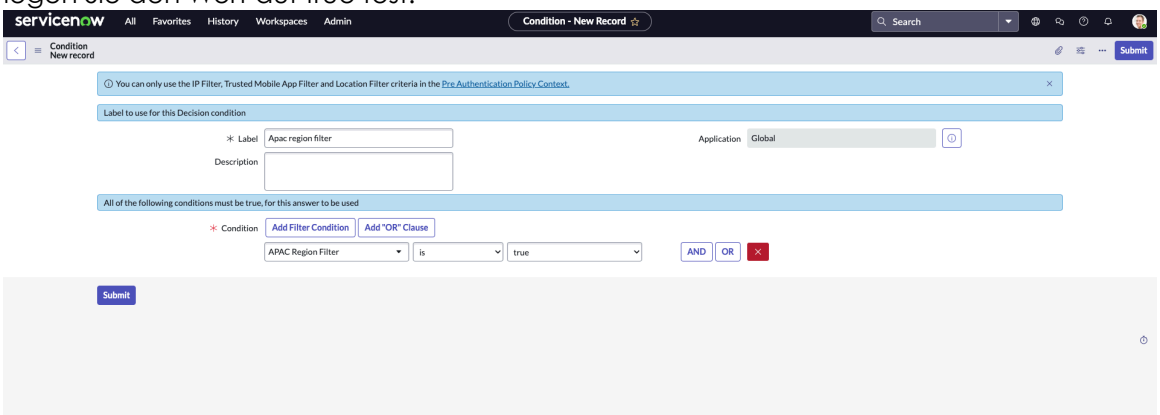


Der Filter wird als **Richtlinieneingaben**hinzugefügt.

5. Wählen Sie die Registerkarte Richtlinienbedingungen und anschließend **Neu**aus.



6. Geben Sie auf der Seite „Bedingungen“ die Bezeichnung und die Bedingungen an, und legen Sie den Wert auf true fest.



Hinweis:

- In diesem Beispiel bedeutet die Auswahl von true als Bedingung, dass sich der Anwender, der sich aus den konfigurierten Regionen anmeldet, nicht bei der Instanz anmelden kann.
- Wenn die Bedingung auf „false“ festgelegt ist, können sich nur Anwender aus konfigurierten Regionen bei der Instanz anmelden. Die anderen Anwender können sich nicht bei der Instanz anmelden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Wählen Sie **Absenden**.
   Anwendern, die den Instanzlink auswählen und sich aus den konfigurierten Ländern anmelden, wird eine Fehlermeldung über die Zugriffsverweigerung angezeigt (Fehlermeldung, die von ihren Administratoren auf der Seite mit den Richtlinieneigenschaften konfiguriert wurde).

Standortfilter nach Authentifizierungskontext verwenden

Verwenden Sie die im Post-Authentifizierungskontext erstellten Standortfilterkriterien.

Vorbereitungen

Erforderliche Rolle: admin

Erforderliches Plugin: **Zero Trust – standortbasierter Zugriff** (`com.snc.zero_trust_location_access`).

Erstellen Sie einen Standortfilter mit den Ländern, die den Zugriff auf die Anwender basierend auf dem Standort einschränken möchten. Weitere Informationen finden Sie unter Erstellen Sie Standortfilterkriterien.

Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Kontext der Authentifizierungsrichtlinie** > **Kontext nach der Authentifizierung**an.

   Wenn eine Richtlinie im Richtlinienkontext nach der Authentifizierung ausgewählt wird:

   - Wenn Sie die Zugriffsverweigerungsrichtlinie als Standardrichtlinie auswählen, wird standardmäßig der Zugriff für alle Anwender gewährt und nur dann verweigert, wenn die in der Zugriffsverweigerungsrichtlinie definierten Richtlinienbedingungen als „wahr“ ausgewertet werden.
   - Wenn Sie die Richtlinie „Zugriff zulassen“ als Standardrichtlinie auswählen, wird standardmäßig allen Anwendern der Zugriff verweigert und nur dann gewährt, wenn die in der Richtlinie „Zugriff zulassen“ definierten Richtlinienbedingungen als „wahr“ ausgewertet werden.

   Das Beispiel zeigt, wie Sie einen `itil-` Benutzer mit einer Bedingung konfigurieren können, um nur vom angegebenen Standort (USA) auf die Instanz zuzugreifen. Und die `ITIL-` Benutzer können sich nicht aus anderen Ländern anmelden.

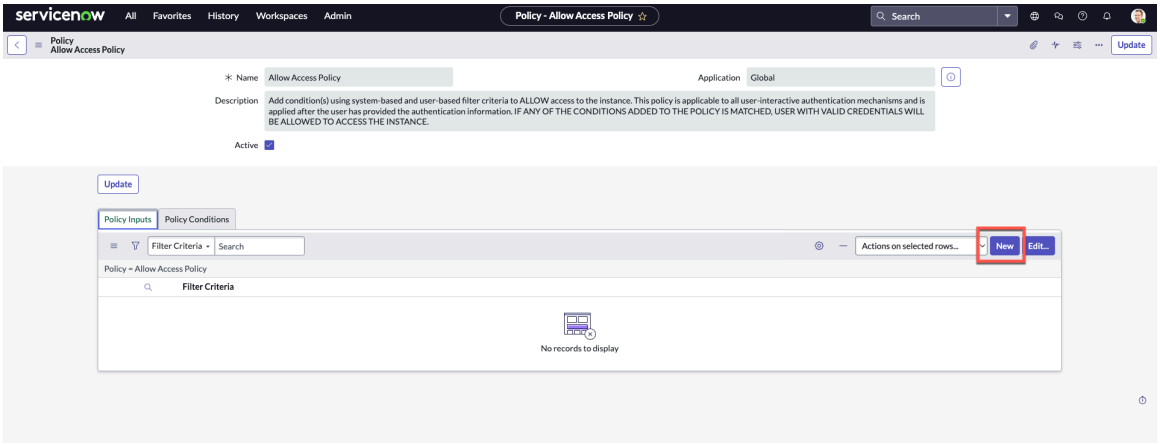
   Nachdem Benutzer ihre Anmeldeinformationen auf der Anmeldeseite angegeben haben. Sie können „Zugriff zulassen“ und die zugehörige Richtlinie (Zugriff zulassen) als Richtlinie nach der Authentifizierung auswählen und die Richtlinieneingaben und -bedingungen angeben.

2. Wählen Sie das Informationssymbol aus, um den Datensatz **„Allow Policy“** (Richtlinie zulassen) zu öffnen.

   Hinweis: Das in dieser Aufgabe beschriebene Beispiel ist **Zulassungsrichtlinie**. Sie können auch eine **Verweigerungsrichtlinie** verwenden und die Bedingungen entsprechend festlegen, um die Anmeldungen zu steuern.

3. Wählen Sie in der Richtlinie „Zugriff zulassen“ im Abschnitt „Richtlinieneingaben“ **Neu**.

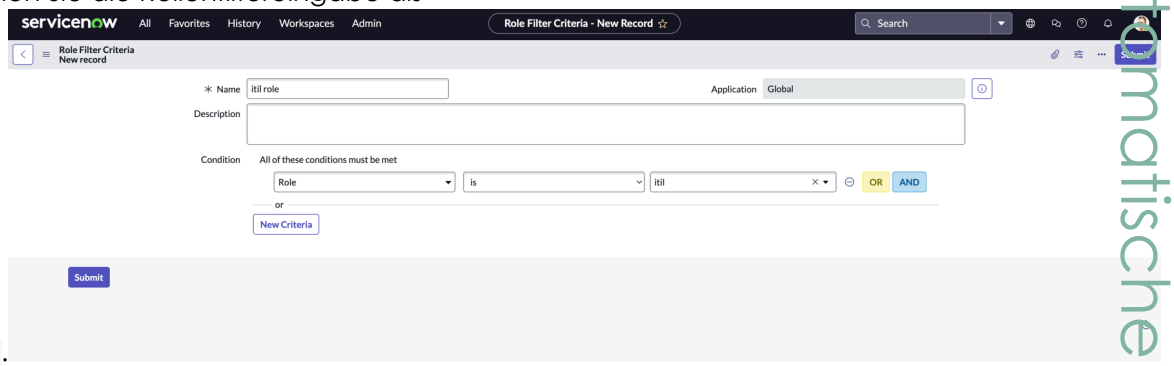
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Fügen Sie die Rollenfilterkriterien und Standortfilterkriterien hinzu.

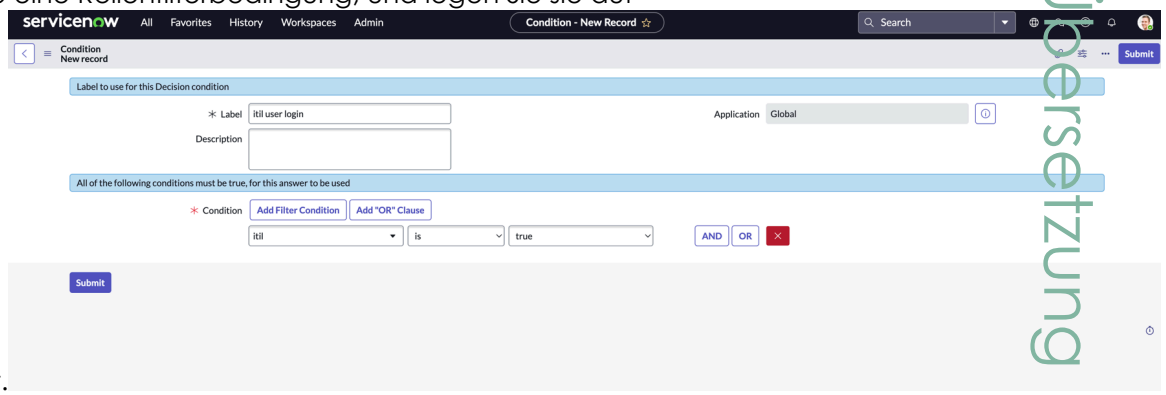
a. Hinzufügen von Rollenfilterkriterien:

- Erstellen Sie die Rollenfiltereingabe als



`itil`.

- Erstellen Sie eine Rollenfilterbedingung, und legen Sie sie auf



`„wahr“`fest.

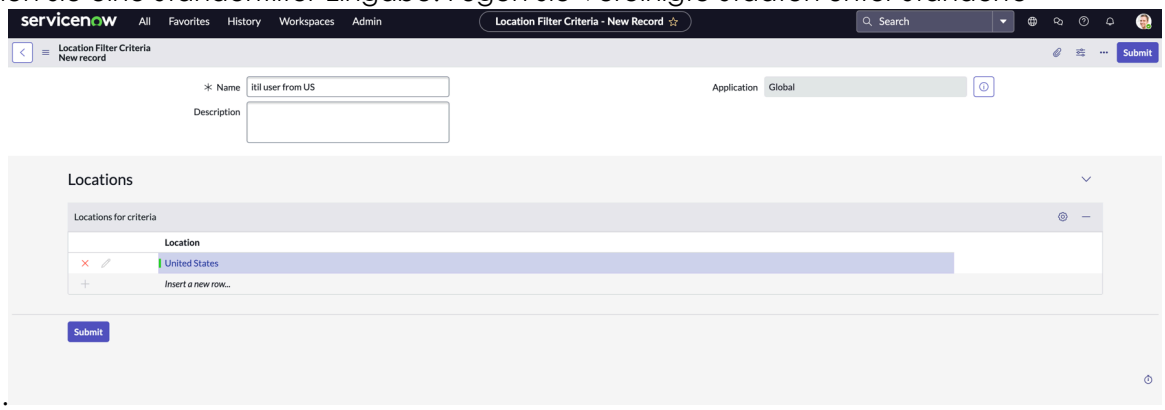
Weitere Informationen zum Erstellen von Rollenfilterkriterien finden Sie unter Erstellen Sie Rollenfilterkriterien.

b. Standortfilterkriterien werden hinzugefügt:

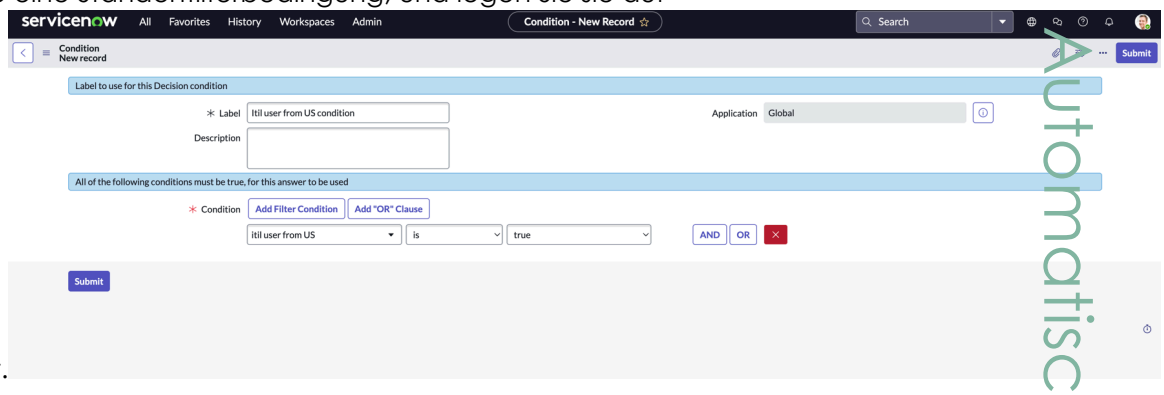
Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erstellen Sie eine Standortfilter-Eingabe. Fügen Sie Vereinigte Staaten unter Standorte hinzu.



- Erstellen Sie eine Standortfilterbedingung, und legen Sie sie auf „wahr“ fest.

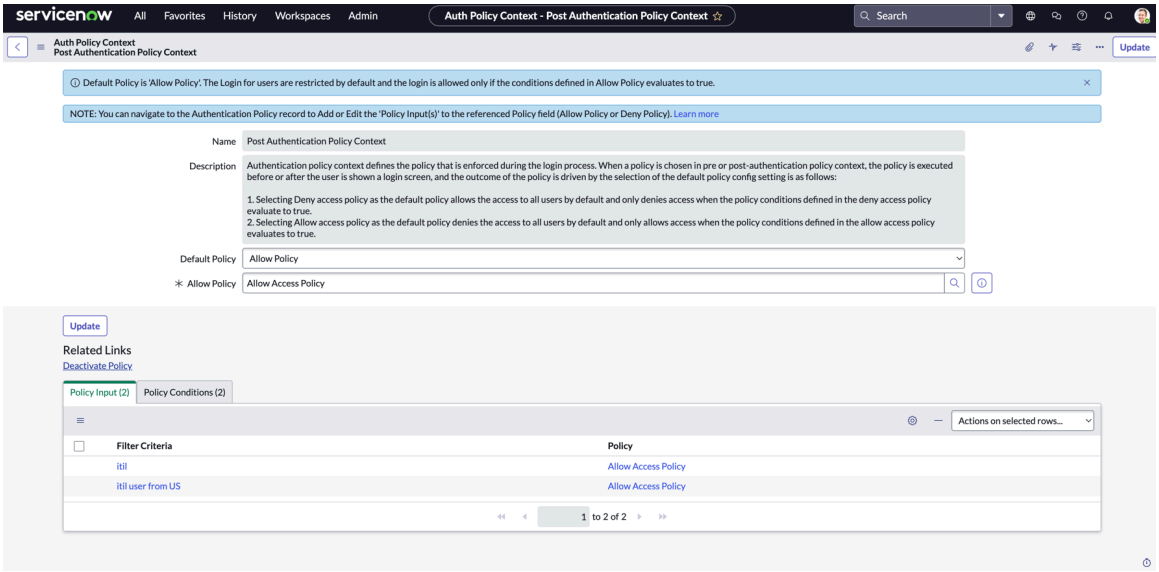


Weitere Informationen zum Erstellen von Rollenfilterkriterien finden Sie unter Erstellen Sie Standortfilterkriterien.

Die Richtlinie „Zugriff zulassen“ zeigt die Richtlinieneingaben und -bedingungen, die in den vorherigen Schritten erstellt wurden:

- Richtlinieneingaben: itil, itil user aus den USA
- Richtlinienbedingungen: itil-Benutzeranmeldung, itil-Benutzer aus US-Bedingung.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:

- In diesem Beispiel bedeutet die Auswahl von true als Bedingung, dass sich die `itil`- Benutzer, die sich aus dem konfigurierten Land (US) anmelden, bei der Instanz anmelden können.
- Wenn die Bedingung auf „false“ festgelegt ist, können sich die `itil`- Benutzer aus dem konfigurierten Land (USA) nicht bei der Instanz anmelden, und die anderen Benutzer können sich nicht bei der Instanz anmelden.

5. Wählen Sie **Absenden** oder **Aktualisieren** aus, um den Kontext nach der Authentifizierung zu aktualisieren.
   Wenn ITIL-Benutzer den `Instanzlink` auswählen, ihre Anmeldeinformationen angeben und sich dann außerhalb des konfigurierten Landes (USA) anmelden, wird eine Fehlermeldung über die Zugriffsverweigerung angezeigt (Fehlermeldung, die von ihren Administratoren auf der Seite mit den Richtlinieneigenschaften konfiguriert wurde).

Standortfilter im MFA-Kontext verwenden

Verwenden Sie die im MFA-Kontext erstellten Standortfilterkriterien.

Vorbereitungen

Erforderliche Rolle: admin

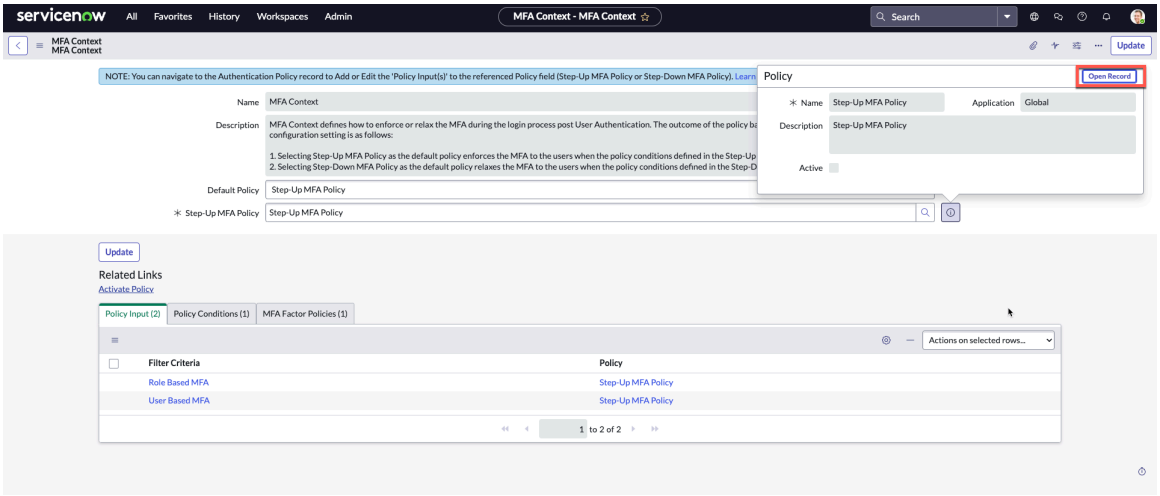
Erforderliches Plugin: **Zero Trust – standortbasierter Zugriff** (`com.snc.zero_trust_location_access`).

Im folgenden Verfahren wird beschrieben, wie Sie einen Standortfilter mit den Ländern erstellen, für die Sie MFA als zweiten Faktor für die Authentifizierung der Anwender basierend auf dem Standort konfigurieren möchten.

Prozedur

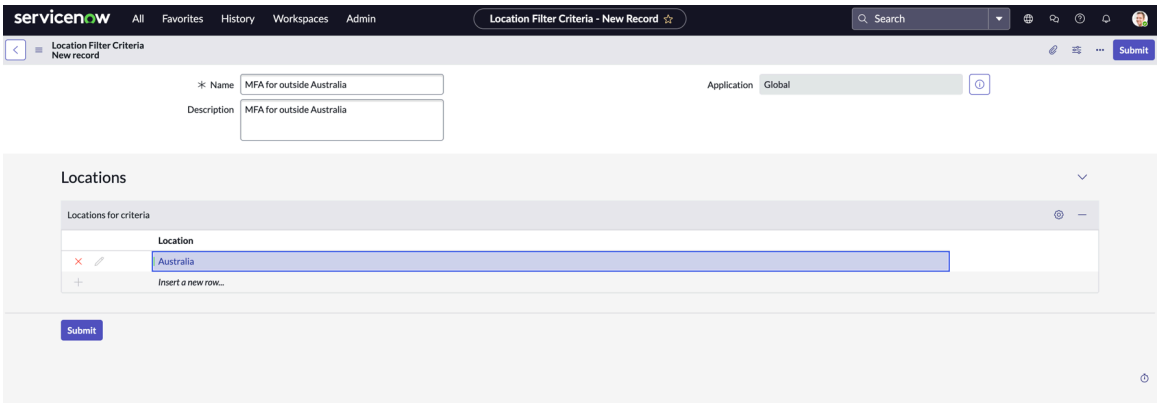
1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Kontext der Authentifizierungsrichtlinie** > **MFA-Kontext**an.
2. Wählen Sie auf der Seite „ **MFA-Kontext** “ das Symbol für **Step-Up-MFA-Richtlinieninformationen**, und öffnen Sie den Datensatz.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

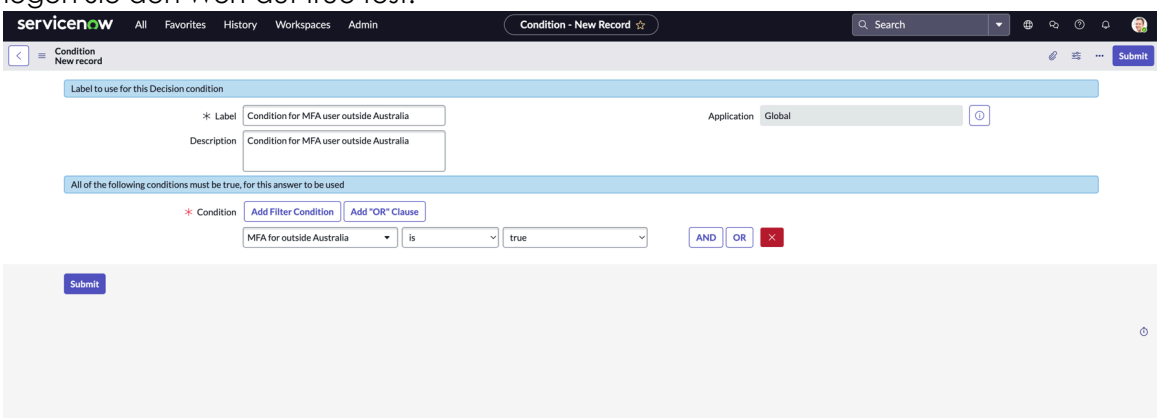


3. Wählen Sie auf der Seite „Step-Up-MFA-Richtlinie“ unter der Registerkarte Richtlinieneingaben die Option **Neu**aus.
4. Fügen Sie die Eingabe Standortfilter hinzu, und übermitteln Sie den Vorgang **absenden**.

   Beispielsweise möchten Sie MFA für Benutzer anzeigen, die sich bei der Instanz außerhalb Australiens anmelden.



5. Wählen Sie auf der Seite „Step-Up-MFA-Richtlinie“ die Registerkarte Richtlinienbedingungen und anschließend **Neu**aus.
6. Geben Sie auf der Seite „Bedingungen“ die Bezeichnung und die Bedingungen an, und legen Sie den Wert auf true fest.



7. Wählen Sie **Absenden**.
8. Aktivieren Sie auf der Seite „Step-Up MFA Policy“ (Step-Up-MFA-Richtlinie) die MFA-Richtlinie, wenn sie **deaktiviert**ist.
9. Wählen Sie **Aktualisieren** aus, um die Konfiguration zu aktualisieren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benutzer außerhalb des konfigurierten Landes (Australien), die den Instanzlink auswählen und ihre Anmeldeinformationen angeben wird mit dem MFA-Bildschirm angezeigt, um die Anmeldeinformationen für den zweiten Faktor für die Anmeldung bei der Instanz bereitzustellen.

Verwenden Sie Standortfilter für Sitzungszugriff

Verwenden Sie die in Sitzungszugriff erstellten Standortfilterkriterien, um die Rollen basierend auf dem Standort des Anwenders zu reduzieren.

Vorbereitungen

Erforderliche Rolle: admin

Erforderliches Plugin: **Zero Trust – standortbasierter Zugriff** (`com.snc.zero_trust_location_access`).

Das folgende Verfahren beschreibt, wie Sie einen Standortfilter mit den Ländern erstellen, die Sie entfernen oder für die Sie basierend auf dem Standort Rollen für Anwender beschränken möchten.

Prozedur

1. Navigieren zu **Alle** > **Zero Trust-Zugriff** > **Konfigurationen der Sitzungszugriffsrolle**an.
2. Um eine Konfiguration für eine Sitzungszugriffsrolle zu erstellen, wählen Sie **Neu**aus.
3. Füllen Sie im Formular die folgenden Felder aus:

Konfiguration der Sitzungszugriffsrolle

Feld	Beschreibung
Name	Name der Konfiguration
Beschreibung	Kurze Beschreibung der Konfiguration.
Richtlinie	Wählen Sie die Zugriffsrichtlinie. Verwenden Sie das Suchsymbol, um die Liste der Richtlinien anzuzeigen. **Hinweis:** Sie müssen die Standortfiltereingabe und -bedingungen hinzufügen, indem Sie den Richtliniendatensatz öffnen.
Aktion	**Rollen entfernen** oder **Auf Rollen beschränken**. ◦ **Rollen entfernen**: Wenn sich der konfigurierte Anwender angemeldet hat, wird die Liste der in der Rollen- oder Gruppenliste bereitgestellten Rollen für die angemeldete Sitzung entfernt. ◦ **Auf Rollen beschränken**: Wenn sich der konfigurierte Anwender anmeldet, werden nur die ausgewählten Rollen für den Anwender bereitgestellt und alle anderen Rollen werden für die angemeldete Sitzung entfernt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Rollenliste	Wählen Sie die Rolle aus der Rollenliste aus.
Gruppenliste	Wählen Sie die Rolle aus der Gruppenliste aus.

4. Auswählen, **Absenden**.

   Die Anmeldung für Benutzer erfolgt basierend auf den konfigurierten Ländern wie folgt:

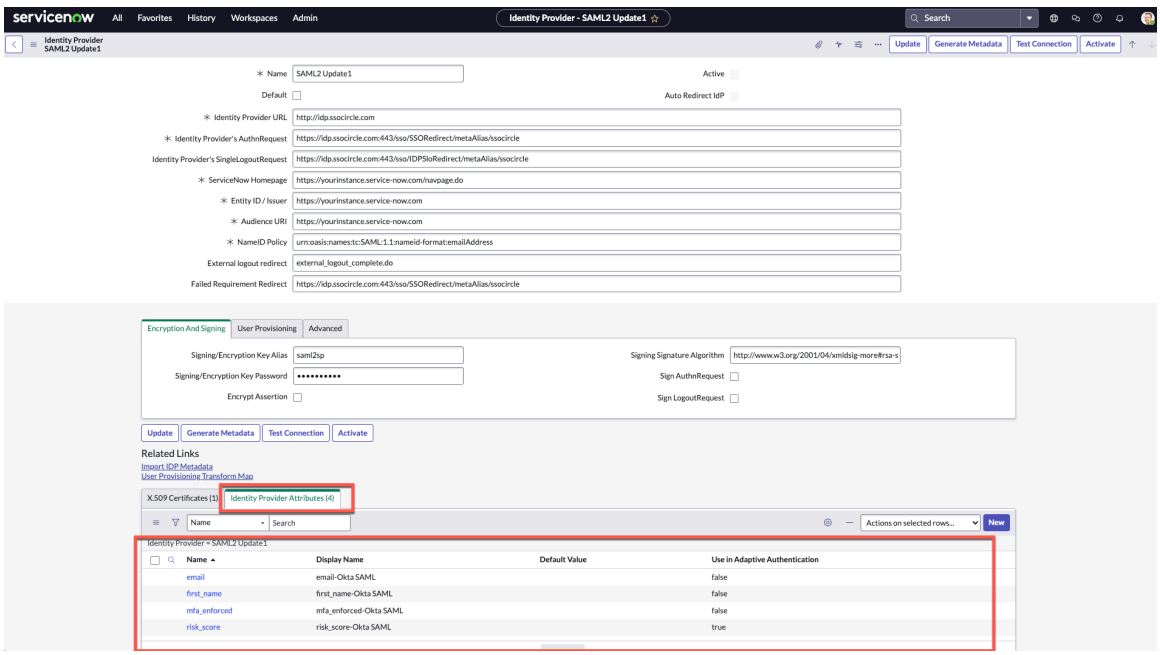
   - Wenn **Rollen entfernen festgelegt**ist, werden die Anwender aus den konfigurierten Ländern im Standortfilter mit den für die Sitzung konfigurierten Rollen entfernt.
   - Wenn **Auf Rollen beschränken**, haben die Benutzer aus den konfigurierten Ländern im Standortfilter nur die Rollen, die für die Sitzung konfiguriert sind.

   Weitere Informationen zum Entfernen oder Einschränken von Rollen für eine Sitzung finden Sie unter Lernprogramm: Verwenden Sie Zero Trust-Zugriff.

Attributfilter für Identitätsanbieter

Verwenden Sie die Attribute des Identitätsanbieters, die von der SAML-Antwort (Security Assertion Markup Language) vom Identitätsanbieter (IdP) empfangen werden, als Filterkriterien für die Authentifizierung.

Um alle Attribute von einem IdP über die SAML-Antwort abzurufen, sollten Sie eine Testverbindung mit dem IdP herstellen. Nach einer erfolgreichen Testverbindung werden die Attribute auf einer neuen Registerkarte auf der Konfigurationsseite des Identitätsanbieters hinzugefügt.



Sie können auch Attribute hinzufügen, indem Sie im Abschnitt „Identitätsanbieter-Attribute“ **Neu** auswählen und diese Attribute für die adaptive Authentifizierung verwenden, indem Sie die Option auf `true festlegen`.

Die **Attribute des Identitätsanbieters** werden mit den folgenden Details angezeigt:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Standortfilterkriterien“.

Feld	Beschreibung
Name	Attributname, der vom Identitätsanbieter bereitgestellt wird.
Anzeigename	Anzeigename ist der detaillierte Name, der für die Filterkriterien verwendet wird. **Hinweis:** Sie können einen lesbaren Namen als Anzeigenamen angeben. In einigen Fällen ist der vom Identitätsanbieter bereitgestellte Anzeigename lang und nicht lesbar.
Standardwert	Der Standardwert wird für die Bewertung von Filterkriterien verwendet, falls das Attribut in der SAML-Antwort fehlt.
In adaptiver Authentifizierung verwenden	Option zur Verwendung des Attributs in der adaptiven Authentifizierung.

Hinweis: Bei Attributen, die aus Azure IdP ausgefüllt werden, sind Name und Anzeigename aufgrund der Namenslänge des Attributs auf Zeichen beschränkt.

Sie können auch neue Attribute hinzufügen, indem Sie im Abschnitt **Attribute des IdentitätsanbietersNeu** auswählen.

Wenn „In adaptiver Authentifizierung verwenden“ auf „true“ festgelegt ist, wird das ausgewählte Attribut als Filterkriterium in den generischen Filterkriterien hinzugefügt. Beispiel: **„risk_score“** auf „ `true`“ festgelegt. Auf der Seite „Generische Filterkriterien“ wurde ein neuer Filter erstellt.

Verwenden Sie das Identitätsanbieterattribut als Filterkriterium

Verwenden Sie das IDP-Attribut (Identity Provider) aus der SAML-Antwort (Security Assertion Markup Language) als Filterkriterium für die Authentifizierungsrichtlinie.

Vorbereitungen

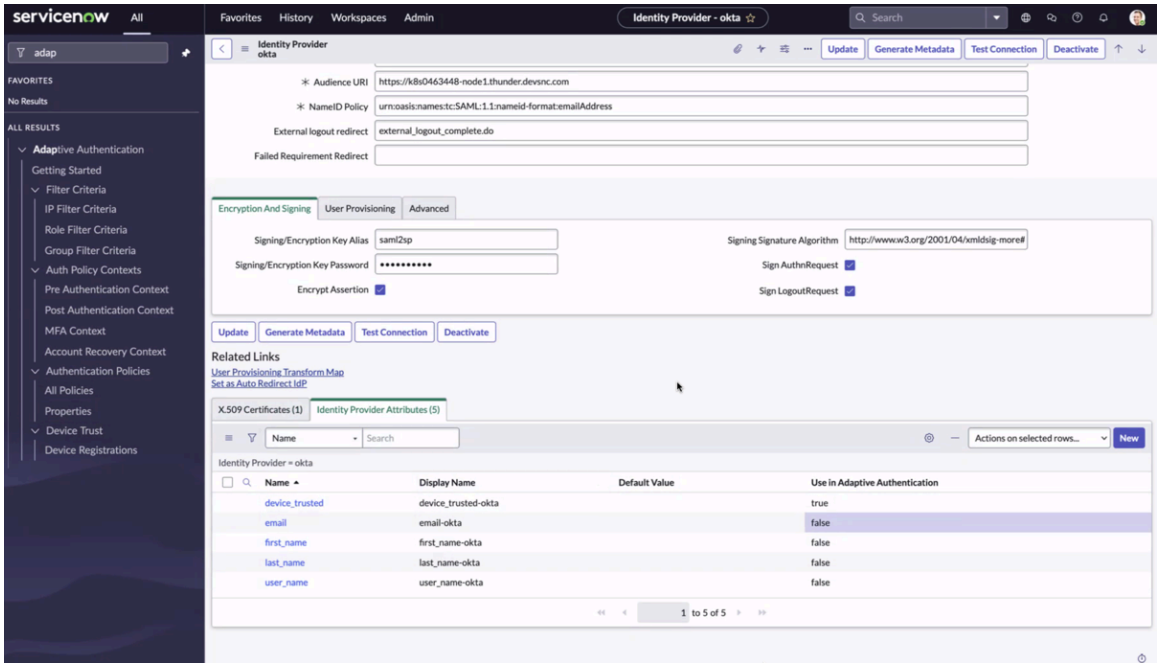
Erforderliche Rolle: admin

Sie können eine Sitzungszugriffsrichtlinie erstellen, indem Sie den Richtlinienkontext (Vorauthentifizierung, Nachauthentifizierung, Multifaktor-Authentifizierung) und Filterkriterien (Rolle, Gruppe, IP, Standort) mit Richtlinieneingaben und -bedingungen verwenden.

Das folgende Verfahren zeigt Schritte zum Konfigurieren des IdP-Attributs aus der SAML-Antwort als Richtlinieneingabe zur Steuerung der Authentifizierung im Kontext nach der Authentifizierung, im **Kontext**der **Multifaktor-Authentifizierung (MFA)**und im **Zero Trust – Richtlinienbasierter Sitzungszugriff**.

Die Okta-IDP-Attribute werden im folgenden Screenshot angezeigt. Sie müssen „Verwenden“ in der adaptiven Authentifizierung auf „wahr“ festlegen, um sie in den Richtlinien „Kontext nach der **Authentifizierung**“, **„MFA-Kontext“ (Multifaktor-Authentifizierung)**und **„Zero Trust – Richtlinienbasierter Sitzungszugriff“** zu verwenden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis: Richtlinien im Sitzungszugriff auf Basis von Nachautorisierung, MFA, Zero Trust – Richtlinie werden ausgeführt, nachdem die Anwender die Anmeldeinformationen eingegeben oder die SSO-Antwort eingegeben haben.

Prozedur

1. Verwendung des IDP-Attributs im Richtlinienkontext nach der Authentifizierung.
   Beispiel: Konfiguration, um Anmeldungen über die Okta IDP-Attribute zu ermöglichen, wenn das Gerät vertrauenswürdig ist.

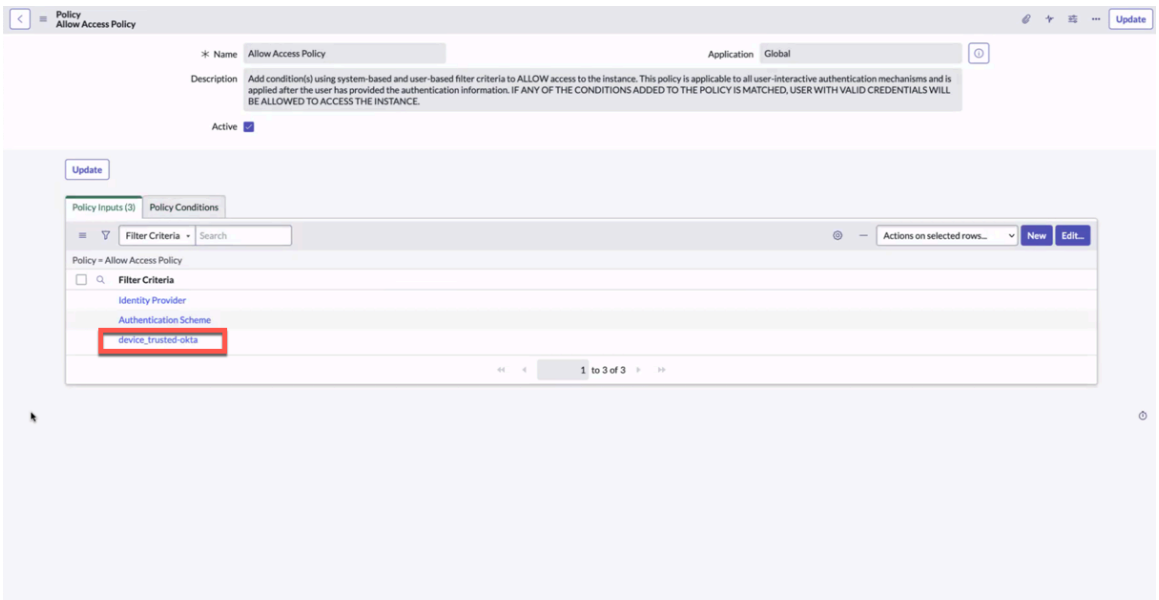
   a. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Kontexte der Authentifizierungsrichtlinie** > **Richtlinienkontext nach der Authentifizierung.**an.

   b. Wählen **Sie Allow Policy** (Richtlinie zulassen), und öffnen Sie den Richtliniendatensatz.

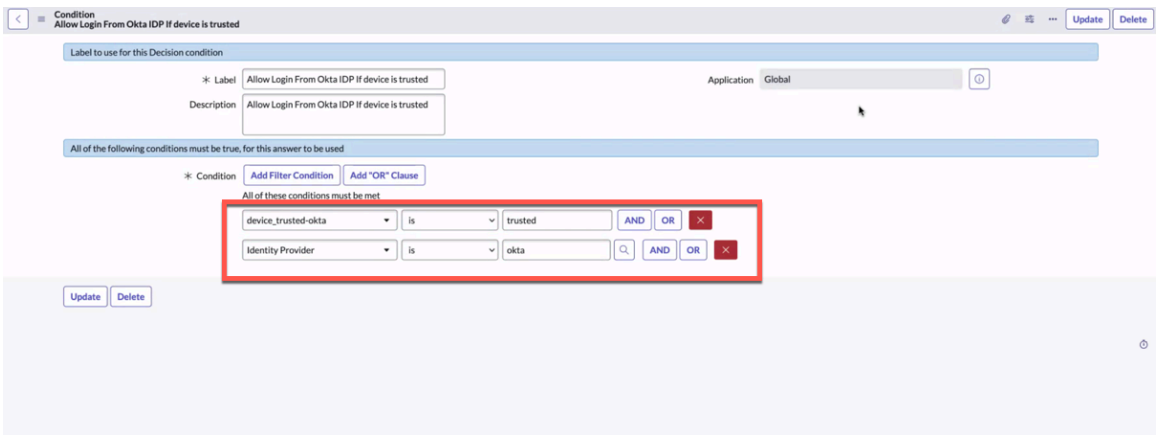
   c. Erstellen Sie in der Richtlinieneingabe die Richtlinieneingabe und die Richtlinienbedingung.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Richtlinieneingabe**: Fügen Sie **device_trusted-okta hinzu**.



- **Richtlinienbedingungen**: **„device_trusted-okta“** ist `vertrauenswürdig` und der **Identitätsanbieter** ist „ `okta`“.



Basierend auf dieser Konfiguration wird der Benutzer gegenüber der Instanz authentifiziert, wenn er von Okta (IdP) als vertrauenswürdig eingestuft wird.

Weitere Informationen zum Erstellen des Kontexts nach der Authentifizierung mit Richtlinie und Bedingung finden Sie unter Kontext nach der Authentifizierung.

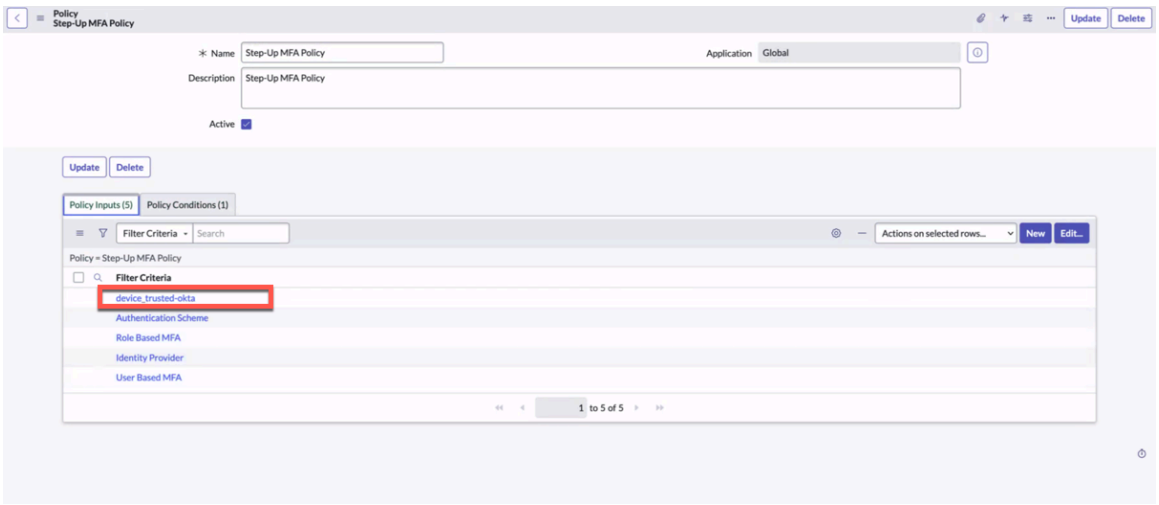
2. Verwendung des IDP-Attributs im MFA-Richtlinienkontext.
   Beispiel: Konfiguration, um MFA über die Okta IDP-Attribute zu aktivieren, wenn das Gerät nicht vertrauenswürdig ist.

   a. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Kontexte der Authentifizierungsrichtlinie** > **Richtlinienkontext der MFA-Authentifizierung.**an.

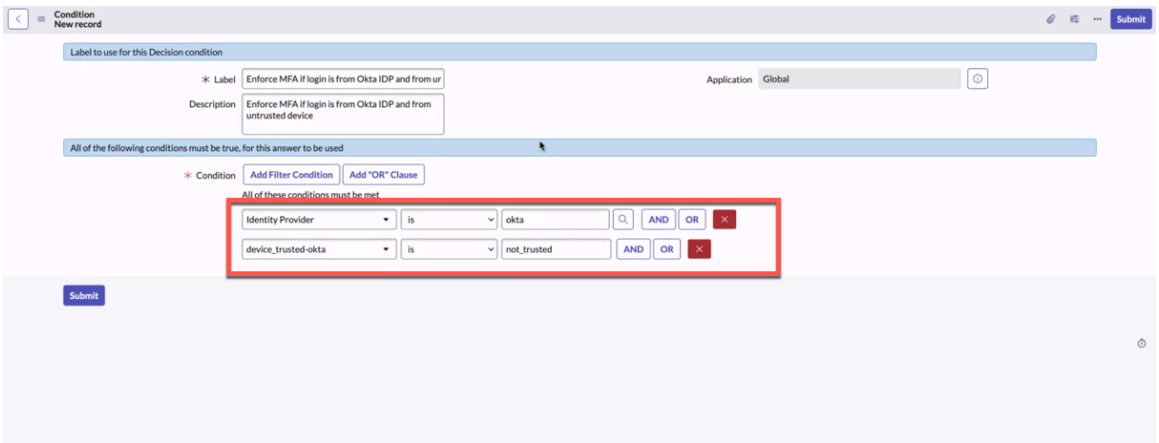
   b. Erstellen Sie in der Richtlinieneingabe die Richtlinieneingabe und die Richtlinienbedingung.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Richtlinieneingabe**: Fügen Sie **device_trusted-okta hinzu**.



- **Richtlinienbedingungen**: **„device_trusted-okta“** ist „`not_trusted`“ und der **Identitätsanbieter** ist „ `okta`“.



Wenn das Gerät von Okta (IdP) nicht vertrauenswürdig ist, wird dem Anwender basierend auf dieser Konfiguration eine zweite Faktorauthentifizierung angezeigt, um sich bei der Instanz anzumelden.

Weitere Informationen zum Erstellen des MFA-Kontexts mit Richtlinie und Bedingung finden Sie unter MFA-Kontext (Multifaktor-Authentifizierung)..

3. Verwendung des IDP-Attributs in Zero Trust – richtlinienbasierter Sitzungszugriff.
   Beispiel: Konfiguration zum Reduzieren der Berechtigung der Rolle „ `itil` “ aus Okta-IDP-Attributen, wenn das Gerät nicht vertrauenswürdig ist.

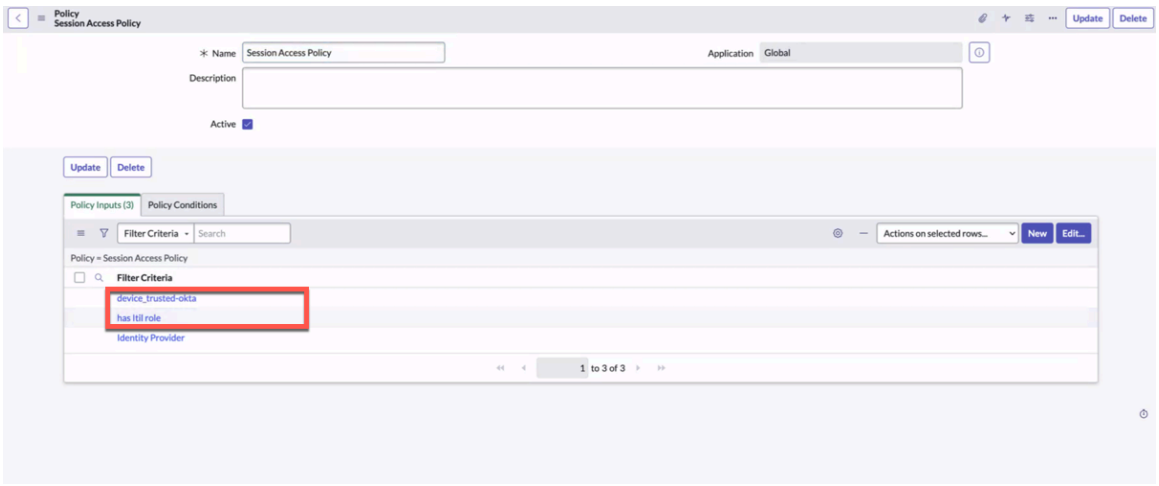
   a. Navigieren zu **Alle** > **Zero Trust-Zugriff** > **Konfigurationen der Sitzungszugriffsrolle**an.

   b. Erstellen Sie eine Konfiguration der Sitzungszugriffsrolle.

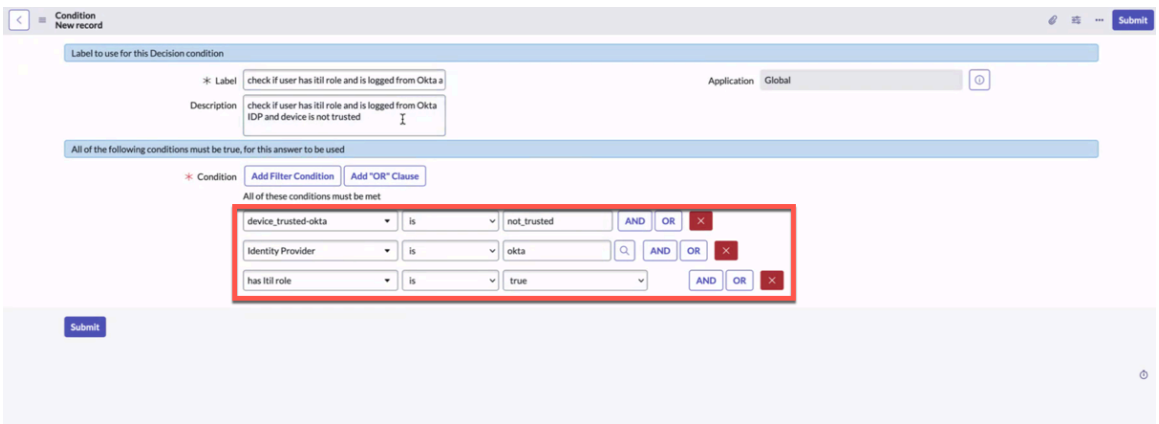
   c. Erstellen Sie in der Richtlinieneingabe die Richtlinieneingabe und die Richtlinienbedingung.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Richtlinieneingabe**: **Fügt device_trusted-okta hinzu** und **hat die Rolle itil**.



- **Richtlinienbedingungen**: **„device_trusted-okta“** ist „`not_trusted`“, „ **Identitätsanbieter** “ ist „ `okta`“ und **„hat Rolle itil“** ist „ `wahr`“.



Basierend auf dieser Konfiguration werden die Berechtigungen des Benutzers für die angemeldete Sitzung reduziert, wenn der Benutzer `itil` ein Gerät verwendet, dem nicht vom Okta-Server (IdP) vertraut wird.

Weitere Informationen zum Erstellen von Zero Trust -Richtlinienbasiertem Sitzungszugriff mit Richtlinie und Bedingung finden Sie unter Zero Trust-Zugriff.

Kontexte der Authentifizierungsrichtlinie

Verwenden Sie Kontexte für Authentifizierungsrichtlinien, um zu bestimmen, wie und wann Ihre Instanz Authentifizierungsrichtlinien erzwingt.

Authentifizierungskontexte definieren, wie und wann eine Richtlinie während des Anmeldevorgangs erzwungen wird. Weisen Sie einem Richtlinienkontext eine Richtlinie zu, um Eingaben und Bedingungen dafür zu definieren, wie Ihre Instanz die Authentifizierung behandelt.

Kontext vor der Authentifizierung

Richtlinien im Vorautorisierungskontext werden ausgeführt, wenn ein Benutzer zum ersten Mal auf die Instanz zugreift, bevor ein Anmeldebildschirm angezeigt wird. Sie können den Vorautorisierungskontext verwenden, um den Zugriff zuzulassen oder zu verweigern, bevor Ihre Benutzer basierend auf der von Ihnen ausgewählten Richtlinie zur Eingabe von

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anmeldeinformationen aufgefordert werden. Da diese Richtlinien ausgewertet werden, bevor ein Benutzer Informationen eingibt, können sie keine Kriterien wie Rollen oder Gruppen eines Benutzers berücksichtigen.

Weitere Informationen zu diesem Kontext finden Sie unter Kontext vor der Authentifizierung.

Kontext nach der Authentifizierung

Richtlinien im Kontext nach der Autorisierung werden ausgeführt, nachdem die Anwender ihre Anmeldeinformationen eingegeben oder die SSO-Antwort eingegeben haben. Ihre Instanz von gewährt oder verweigert den Zugriff basierend auf der von Ihnen ausgewählten Richtlinie. Da sich Ihre Benutzer über ihre Anmeldeinformationen identifiziert haben, kann die Richtlinie anhand von Benutzerinformationen bestimmen, ob Zugriff gewährt wird.

Weitere Informationen zu diesem Kontext finden Sie unter Kontext nach der Authentifizierung.

MFA-Kontext (Multifaktor-Authentifizierung).

Dem MFA-Kontext zugewiesene Richtlinien definieren, ob MFA während des Anmeldevorgangs erzwungen werden soll. Ob Ihre Instanz MFA erzwingt, hängt von der Konfiguration der Richtlinien in diesem Kontext ab. Weitere Informationen zu diesem Kontext finden Sie unter MFA-Kontext (Multifaktor-Authentifizierung)..

Kontext der Accountwiederherstellung

Administratoren können die Accountwiederherstellung (Account Recovery, ACR) konfigurieren, um Wiederherstellungsaktivitäten durchzuführen, z. B. um SSO-Fehlkonfigurationen oder abgelaufene Zertifikate zu beheben. Um die Accountwiederherstellung zu verwenden, müssen Sie mindestens einen Administratoraccount als Accountwiederherstellungsbenutzer registrieren. Single Sign-on kann in Ihrer Instanz erst aktiviert werden, wenn mindestens ein Account konfiguriert ist. Weitere Informationen zum Kontext, der festgelegt werden kann, finden Sie unter Kontext der Accountwiederherstellung.

Kontext der Sitzungsvalidierung

Der Sitzungsvalidierungskontext kann mit dem Richtlinien-Framework für die adaptive Authentifizierung verwendet werden. Das -Framework verwendet Authentifizierungsrichtlinien, um Authentifizierungsanforderungen (Sitzung) auszuwerten und dann den Zugriff basierend auf Richtlinienbedingungen zu verweigern oder zuzulassen. Weitere Informationen finden Sie unter Sitzungsvalidierungskontext.

Standardrichtlinie

Innerhalb des Richtlinienkontexts können Sie im Feld **Standardrichtlinie** eine Standardrichtlinie definieren. Dieser Standard definiert, wie Ihre -Instanz auf das Ergebnis Ihrer Richtlinie reagiert. Die verfügbaren Standardrichtlinienoptionen hängen davon ab, welchen Kontext Sie verwenden. Details zu diesen Optionen finden Sie in den Dokumenten, die diese einzelnen Kontexte beschreiben.

Kontext vor der Authentifizierung

Der Richtlinienkontext vor der Authentifizierung definiert, wie und wann eine Richtlinie während des Anmeldevorgangs erzwungen wird. Die in diesem Kontext verwendete Richtlinie wird ausgeführt, bevor Ihre Benutzer einen Anmeldebildschirm sehen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kontextdatensatz der Vorauthentifizierung

Richtlinien im Vorautorisierungskontext werden ausgeführt, wenn ein Benutzer zum ersten Mal auf die Instanz zugreift, bevor ein Anmeldebildschirm angezeigt wird.

Sie können den Vorauthentifizierungskontext verwenden, um den Zugriff zuzulassen oder zu verweigern, bevor Ihre Benutzer basierend auf der von Ihnen ausgewählten Richtlinie zur Eingabe von Anmeldeinformationen aufgefordert werden. Da diese Richtlinien ausgewertet werden, bevor ein Benutzer Informationen eingibt, können sie keine Kriterien wie Rollen oder Gruppen eines Benutzers berücksichtigen.

Verwenden Sie die Felder im Datensatz für den Richtlinienkontext vor der Authentifizierung, um zu definieren, wie Ihre Instanz Ihre Richtlinie verwendet.

Formular für den Kontext der Vorauthentifizierung

Feld	Beschreibung
Name	Name des Richtlinienkontexts Dieses Feld ist statisch und kann nicht geändert werden.
Beschreibung	Beschreibung des Kontexts
Standardrichtlinie	Definiert das Standardverhalten dieses Kontexts bei der Auswertung der Richtlinie. Wählen Sie unter den folgenden Optionen aus. Zulassungsrichtlinie Verweigert standardmäßig allen Anwendern den Zugriff und lässt den Zugriff nur zu, wenn die Bedingungen der im Feld Zulassungsrichtlinie ausgewählten **Richtlinie** als „wahr“ ausgewertet werden. Verweigerungsrichtlinie Ermöglicht standardmäßig allen Anwendern den Zugriff und verweigert den Zugriff nur, wenn die Bedingungen der im Feld Verweigerungsrichtlinie ausgewählten **Richtlinie** als „wahr“ ausgewertet werden.
Zulassungsrichtlinie	Die für diesen Kontext verwendete Richtlinie verwendet. Dieses Feld wird nur angezeigt, wenn das Feld **Standardrichtlinie** auf **Zulassungsrichtlinie**festgelegt ist.
Verweigerungsrichtlinie	Die für diesen Kontext verwendete Richtlinie verwendet. Dieses Feld wird nur angezeigt, wenn das Feld **Standardrichtlinie** auf **Verweigerungsrichtlinie**festgelegt ist.

Hinweis:

Sie können im Richtlinienkontext vor der Authentifizierung nur die Kriterien „IP-Filter“, „Trusted Mobile App-Filter“ und „Standortfilter“ verwenden.

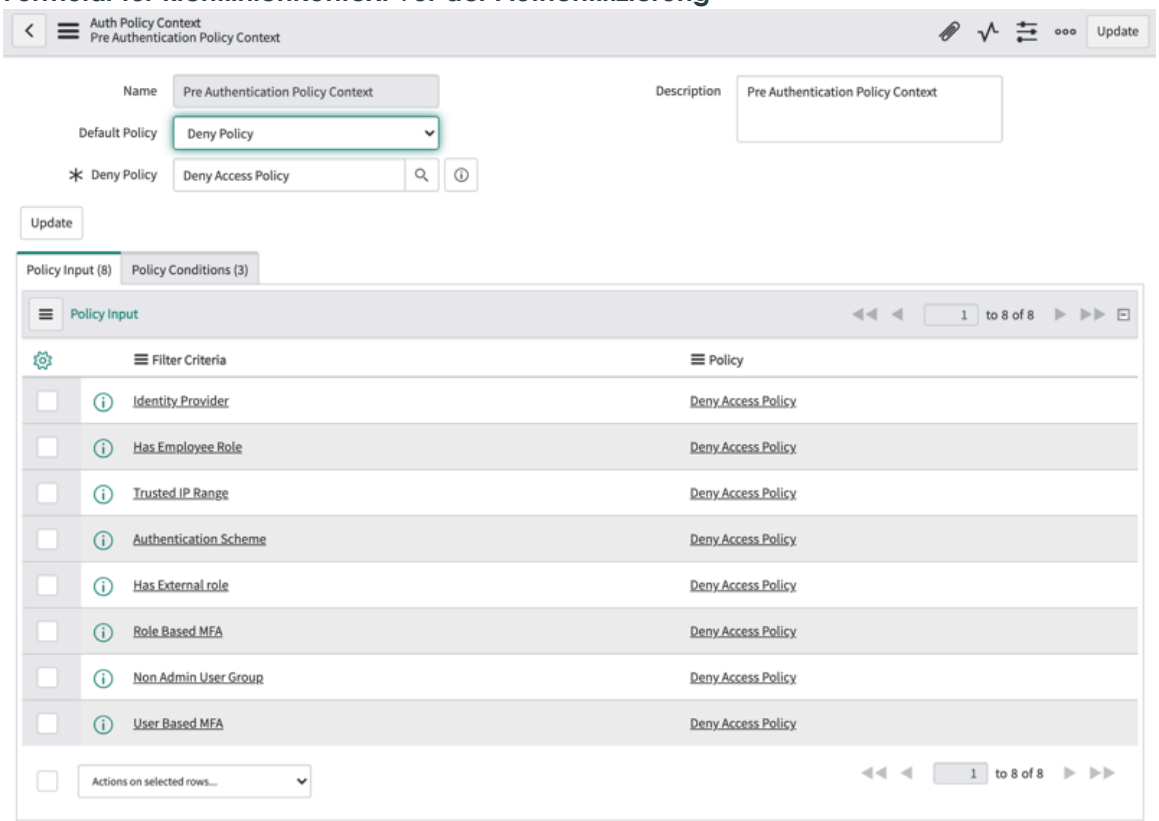
Richtlinieneingaben und -bedingungen

Die Registerkarten **Richtlinieneingabe** und **Richtlinienbedingungen** zeigen die Eingaben und Bedingungen der Richtlinie an, die im Feld **Zulassungsrichtlinie** oder **Verweigerungsrichtlinie** ausgewählt ist. Diese Registerkarten dienen als Referenz, können jedoch nicht zum Ändern der Richtlinieneingaben oder -bedingungen verwendet werden. Um Ihre Richtlinie zu ändern, navigieren Sie zu der Richtlinie, indem Sie das Referenzsymbol ( ) neben dem Feld **Zulassungsrichtlinie** oder **Verweigerungsrichtlinie** verwenden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieses Beispiel zeigt einen Richtlinienkontextdatensatz für die Vorauthentifizierung, der so konfiguriert ist, dass der Zugriff standardmäßig verweigert wird. Der Kontext verwendet eine Richtlinie namens **Zugriffsverweigerungsrichtlinie**. Diese Richtlinie verfügt über eine Reihe von Eingaben und Bedingungen, die auf den Registerkarten **Richtlinieneingabe** und **Richtlinienbedingung** angezeigt werden.

Formular für Richtlinienkontext vor der Authentifizierung



Kontext nach der Authentifizierung

Der Richtlinienkontext nach der Authentifizierung definiert, wie und wann eine Richtlinie während des Anmeldevorgangs erzwungen wird. Die in diesem Kontext verwendete Richtlinie wird ausgeführt, nachdem den Anwendern ein Anmeldebildschirm angezeigt wurde.

Kontextdatensatz nach der Authentifizierung

Richtlinien im Kontext nach der Autorisierung werden ausgeführt, nachdem die Anwender ihre Anmeldeinformationen eingegeben oder die SSO-Antwort eingegeben haben. Ihre Instanz von gewährt oder verweigert den Zugriff basierend auf der von Ihnen ausgewählten Richtlinie. Da sich Ihre Benutzer über ihre Anmeldeinformationen identifiziert haben, kann die Richtlinie anhand von Benutzerinformationen wie Rolle oder Gruppe bestimmen, ob Zugriff gewährt wird.

Verwenden Sie die Felder im Datensatz für den Richtlinienkontext nach der Authentifizierung, um zu definieren, wie Ihre Instanz Ihre Richtlinie verwendet.

Formular für den Kontext der Nachauthentifizierung

Feld	Beschreibung
Name	Name des Richtlinienkontexts Dieses Feld ist statisch und kann nicht geändert werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular für den Kontext der Nachauthentifizierung (Fortsetzung)

Feld	Beschreibung
Beschreibung	Beschreibung des Kontexts
Standardrichtlinie	Definiert das Standardverhalten dieses Kontexts bei der Auswertung der Richtlinie. Wählen Sie unter den folgenden Optionen aus. Zulassungsrichtlinie Verweigert standardmäßig allen Anwendern den Zugriff und lässt den Zugriff nur zu, wenn die Bedingungen der im Feld Zulassungsrichtlinie ausgewählten **Richtlinie** als „wahr“ ausgewertet werden. Verweigerungsrichtlinie Ermöglicht standardmäßig allen Anwendern den Zugriff und verweigert den Zugriff nur, wenn die Bedingungen der im Feld Verweigerungsrichtlinie ausgewählten **Richtlinie** als „wahr“ ausgewertet werden.
Zulassungsrichtlinie	Die für diesen Kontext verwendete Richtlinie verwendet. Dieses Feld wird nur angezeigt, wenn das Feld **Standardrichtlinie** auf **Zulassungsrichtlinie**festgelegt ist.
Verweigerungsrichtlinie	Die für diesen Kontext verwendete Richtlinie verwendet. Dieses Feld wird nur angezeigt, wenn das Feld **Standardrichtlinie** auf **Verweigerungsrichtlinie**festgelegt ist.

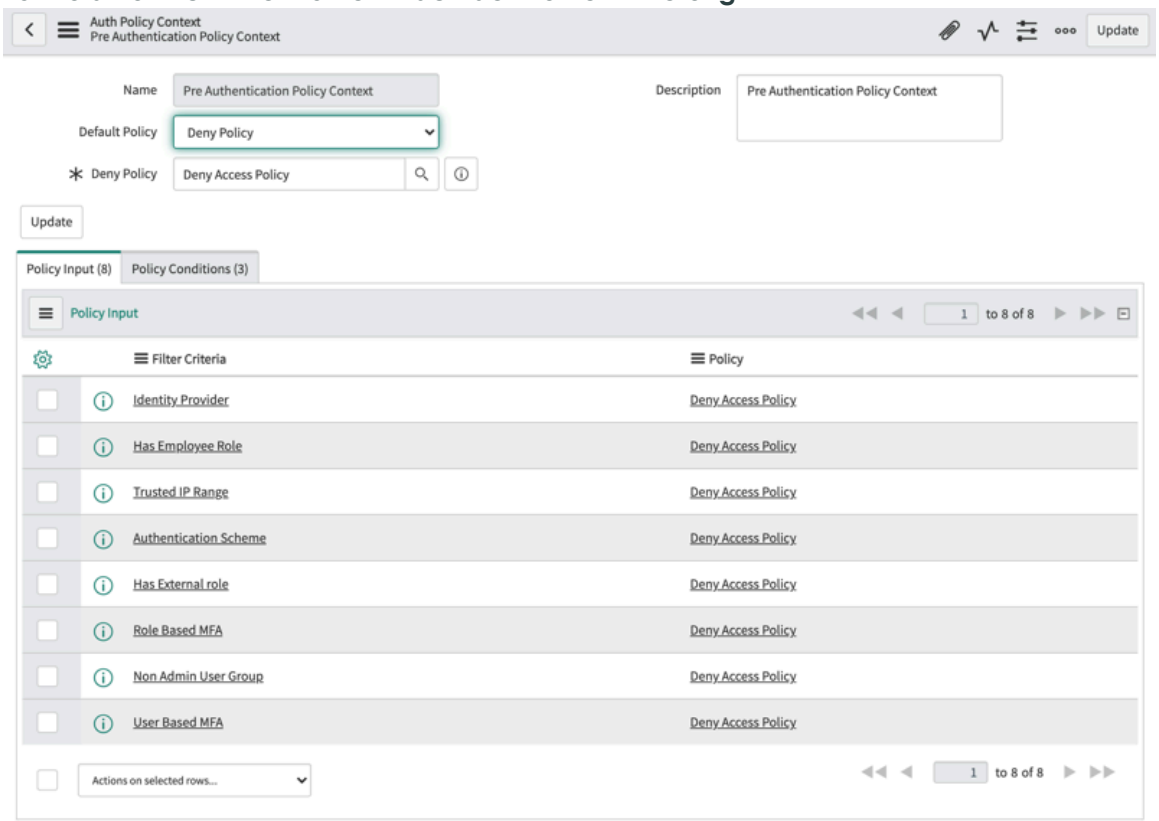
Richtlinieneingaben und -bedingungen

Die Registerkarten **Richtlinieneingabe** und **Richtlinienbedingungen** zeigen die Eingaben und Bedingungen der Richtlinie an, die im Feld **Zulassungsrichtlinie** oder **Verweigerungsrichtlinie** ausgewählt ist. Diese Registerkarten dienen als Referenz, können jedoch nicht zum Ändern der Richtlinieneingaben oder -bedingungen verwendet werden. Um Ihre Richtlinieneinstellungen zu ändern, navigieren Sie über das Referenzsymbol (ⓘ) neben dem Feld **Zulassungsrichtlinie** oder **Verweigerungsrichtlinie zur Richtlinie**.

Dieses Beispiel zeigt einen Richtlinienkontextdatensatz nach der Authentifizierung, der so konfiguriert ist, dass der Zugriff standardmäßig verweigert wird. Der Kontext verwendet eine Richtlinie namens **Zugriffsverweigerungsrichtlinie**. Diese Richtlinie verfügt über eine Reihe von Eingaben und Bedingungen, die auf den Registerkarten **Richtlinieneingabe** und **Richtlinienbedingung** angezeigt werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular für Richtlinienkontext nach der Authentifizierung



MFA-Kontext (Multifaktor-Authentifizierung).

Der MFA-Richtlinienkontext (Multifaktor-Authentifizierung) verwendet eine Richtlinie, um zu definieren, wie und wann MFA während des Anmeldevorgangs erzwungen wird.

MFA-Kontextdatensatz

Der MFA-Richtlinienkontext (Multifaktor-Authentifizierung) definiert, ob Ihre Anwender bei der Anmeldung eine zweite Form der Authentifizierung angeben müssen. Dieser Kontext verweigert nicht den Zugriff auf Ihre Instanz als Richtlinien nach der Authentifizierung und Vorauthentifizierung. Die Richtlinie, die Sie in diesem Kontext auswählen, hat Vorrang vor anwender- oder rollenbasierten Konfigurationen für die Multifaktor-Authentifizierung.

Um auf den MFA-Kontext zuzugreifen, navigieren Sie zu **Alle** > **Multi-Faktor-Authentifizierung** > **MFA-Kontext**an.

Verwenden Sie die Felder im Datensatz für den Richtlinienkontext nach der Authentifizierung, um zu definieren, wie Ihre Instanz Ihre Richtlinie verwendet.

Hinweis:

- Wenn die Standardrichtlinie **Step-Up-MFA-Richtlinie**ist, wird Anwendern Multifaktor-Authentifizierung angezeigt, wenn die in der **Step-Up-MFA-** Richtlinie konfigurierte Richtlinie als „wahr“ ausgewertet wird. Richtlinie hat Vorrang vor der anwender- oder rollenbasierten Konfiguration.
- MFA mit SSO-Anmeldung ist nur verfügbar, wenn die Eigenschaft „ `glide.authenticate.mfa.with.multisso.enabled`“ auf „wahr“ festgelegt ist.
- Sie können zum Datensatz „Authentifizierungsrichtlinie“ navigieren, um dem referenzierten Richtlinienfeld (**Step-Up-MFA-Richtlinie** oder **Step-Down-MFA-Richtlinie**) die Richtlinieneingabe(n) hinzuzufügen oder zu bearbeiten.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MFA-Kontextformular

Feld	Beschreibung
Name	Name des Richtlinienkontexts Dieses Feld ist statisch und kann nicht geändert werden.
Beschreibung	Beschreibung des Kontexts
Standardrichtlinie	Definiert das Standardverhalten dieses Kontexts bei der Auswertung der Richtlinie. Wählen Sie unter den folgenden Optionen aus. Step-Up-MFA-Richtlinie Erzwingt MFA für Anwender, wenn die im Feld **Step-Up-MFA-Richtlinie** definierten Richtlinienbedingungen als „wahr“ ausgewertet werden. Step-Down-MFA-Richtlinie Erzwingt MFA standardmäßig. MFA wird nicht nur erzwungen, wenn die im Feld **Step-Down-MFA-Richtlinie** definierten Richtlinienbedingungen als „wahr“ ausgewertet werden.
Step-Up-MFA-Richtlinie	Die für diesen Kontext verwendete Richtlinie verwendet. Dieses Feld wird nur angezeigt, wenn das Feld **Standardrichtlinie** auf **Step-Up MFA Policy**(Step-Up-MFA-Richtlinie) festgelegt ist.
Step-Down-MFA-Richtlinie	Die für diesen Kontext verwendete Richtlinie verwendet. Dieses Feld wird nur angezeigt, wenn das Feld **Standardrichtlinie** auf **Step-Down-MFA-Richtlinie**festgelegt ist.

Richtlinieneingaben und -bedingungen

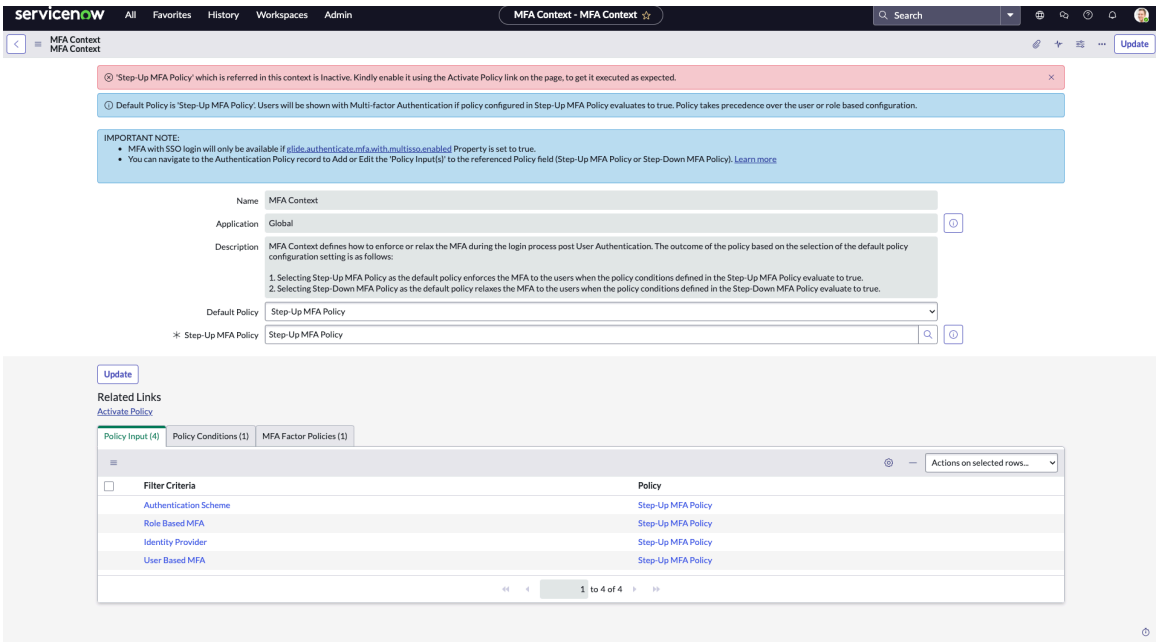
Die Registerkarten **Richtlinieneingabe** und **Richtlinienbedingungen** zeigen die Eingaben und Bedingungen der Richtlinie an, die im Feld **Step-Up-MFA-Richtlinie** oder **Step-Down-MFA-Richtlinie** ausgewählt ist. Diese Registerkarten dienen als Referenz, können jedoch nicht zum Ändern der Richtlinieneingaben oder -bedingungen verwendet werden. Um Ihre Richtlinieneinstellungen zu ändern, navigieren Sie zu der Richtlinie, indem Sie das Referenzsymbol (ⓘ) neben dem Feld **Step-Up-MFA-Richtlinie** oder **Step-Down-MFA-Richtlinie** verwenden.

Hinweis: Richtlinienbedingungen können hier erstellt werden. Als bewährte Methode wird jedoch empfohlen, neue Richtlinienbedingungen über die Richtlinienseite hinzuzufügen.

Dieses Beispiel zeigt einen MFA-Kontextdatensatz, der mit einer Step-up-MFA-Richtlinie konfiguriert wurde. Diese Standardrichtlinie bedeutet, dass MFA nur erzwungen wird, wenn die in der Richtlinie definierten Bedingungen als „wahr“ ausgewertet werden. Der Kontext verwendet eine Richtlinie namens **Step-Up MFA policy**(Step-Up-MFA-Richtlinie). Diese Richtlinie verfügt über eine Reihe von Eingaben und Bedingungen, die auf den Registerkarten **Richtlinieneingabe** und **Richtlinienbedingung** angezeigt werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular für MFA-Richtlinienkontext



Kontext der Accountwiederherstellung

Der Accountwiederherstellungskontext verwendet eine Richtlinie, um zu definieren, wie und wann die Accountwiederherstellung eingerichtet werden kann.

Administratoren können diesen Kontext und die zugehörige Richtlinie anzeigen und ändern, indem sie zu navigieren **Mehrfachanbieter-SSO** > **Accountwiederherstellung** > **Kontext der Accountwiederherstellung**an.

Hinweis: Standardmäßig lautet die Richtlinie **Zulassungsrichtlinie**. Die Anmeldung für Anwender ist standardmäßig eingeschränkt und wird nur zugelassen, wenn die in der Zulassungsrichtlinie definierten Bedingungen als „wahr “ ausgewertet werden.

Verwenden Sie die Felder im Datensatz des Accountwiederherstellungskontexts, um zu definieren, wie Ihre Instanz die Richtlinie verwendet.

Formular für den Accountwiederherstellungskontext

Feld	Beschreibung
Name	Name des Richtlinienkontexts Dieses Feld ist statisch und kann nicht geändert werden.
Beschreibung	Beschreibung des Kontexts
Standardrichtlinie	Definiert das Standardverhalten dieses Kontexts bei der Auswertung der Richtlinie. Wählen Sie unter den folgenden Optionen aus: • Zulassungsrichtlinie • Verweigerungsrichtlinie
Zulassungsrichtlinie	Dieses Feld wird nur angezeigt, wenn das Feld **Standardrichtlinie** auf **Zulassungsrichtlinie**festgelegt ist.
Verweigerungsrichtlinie	Dieses Feld wird nur angezeigt, wenn das Feld **Standardrichtlinie** auf **Verweigerungsrichtlinie**festgelegt ist.

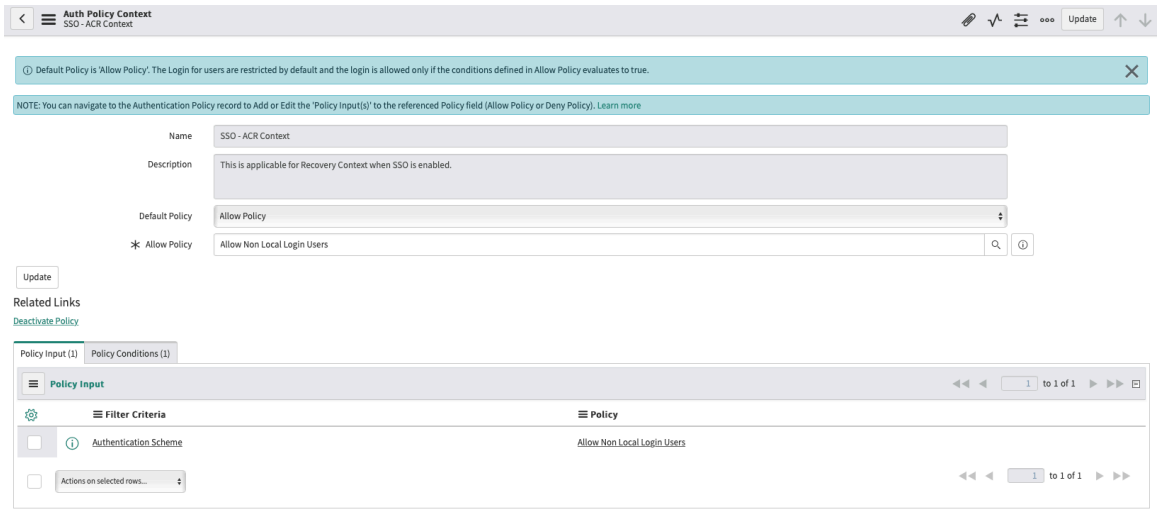
Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinieneingaben und -bedingungen

Die Registerkarten **Richtlinieneingabe** und **Richtlinienbedingungen** zeigen die Eingaben und Bedingungen der Richtlinie an, die im Feld **Zulassungsrichtlinie** oder **Verweigerungsrichtlinie** ausgewählt ist. Diese Registerkarten dienen als Referenz, können jedoch nicht zum Ändern der Richtlinieneingaben oder -bedingungen verwendet werden. Um Ihre Richtlinieneinstellungen zu ändern, navigieren Sie zu der Richtlinie, indem Sie auf das Symbol **Vorschau auf diesen Datensatz** neben dem Feld **Zulassungsrichtlinie** oder **Verweigerungsrichtlinie klicken**.

Hinweis: Richtlinienbedingungen können hier erstellt werden. Als bewährte Methode wird jedoch empfohlen, neue Richtlinienbedingungen über die Richtlinienseite hinzuzufügen.



Sitzungsvalidierungskontext

Verwenden Sie den Sitzungsvalidierungskontext als zusätzliche Schutzebene gegen Hijacking von Sitzungen oder Cookies.

Sie können den Sitzungsvalidierungskontext mit dem Richtlinien-Framework Adaptive Authentifizierung verwenden. Das -Framework verwendet Authentifizierungsrichtlinien, um Authentifizierungsanforderungen auszuwerten und dann den Zugriff basierend auf Richtlinieneingaben und -bedingungen zu verweigern oder zuzulassen.

Die Richtlinie für den Sitzungsvalidierungskontext kann in Verbindung mit der Nachauthentifizierungsrichtlinie verwendet werden, bei der ein Administrator IP-Beschränkungen für bestimmte oder alle Anwender während der angemeldeten Sitzung erzwingen kann.

Die Funktion „Sitzungsvalidierungskontext“ wertet die IP-Adressen basierend auf den von Ihnen festgelegten Bedingungen aus und ermöglicht den Zugriff auf die Instanz innerhalb einer Sitzung. Die Ergebnisse des Sitzungsvalidierungskontexts lauten wie folgt:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Verweigerungsrichtlinie: Wenn Sie die Zugriffsverweigerungsrichtlinie als Standardrichtlinie auswählen, können Benutzer die Sitzung standardmäßig fortsetzen. Die Sitzung wird nur beendet, wenn eine der in der Richtlinie „Zugriff verweigern“ definierten Bedingungen als „wahr“ ausgewertet wird.
- Zulassungsrichtlinie: Wenn Sie die Zulassungsrichtlinie als Standardrichtlinie auswählen, wird die Anwendersitzung sofort beendet, es sei denn, eine der in der Richtlinie für zulassen Zugriff definierten Bedingungen wird als true ausgewertet.

Hinweis:

- Der Sitzungsvalidierungskontext für eine Authentifizierungsrichtlinie ist standardmäßig auf **Zulassungsrichtlinie** festgelegt.
- Der Sitzungsvalidierungskontext wird durch die Allow-Richtlinie implementiert. Es wird nicht empfohlen, den Kontext auf das Ablehnen der Richtlinie festzulegen.

Der Sitzungsvalidierungskontext basiert auf dem folgenden Mechanismus:

- Erfasst die IP-Adresse des Anwenders bei der Sitzungserstellung aus der Anwenderanforderung und speichert sie in der Sitzung und Datenbank.
- Lehnt eine Anforderung ab, wenn sich die IP-Adresse von der in der Sitzung unterscheidet oder außerhalb der vom Kunden definierten gültigen IP-Bereiche liegt.

Hinweis: Der Sitzungsvalidierungskontext ist:

- Nur für authentifizierte Benutzer verfügbar.
- Gilt nicht für Gastbenutzersitzungen oder native mobile Apps.
- Optional und basierend auf der Anforderung, die konfiguriert werden kann.
- Wird nur für Anforderungen nach der Anmeldung ausgeführt.

Vorteile der Sitzungsvalidierung

Der Sitzungsvalidierungskontext bietet folgende Vorteile:

- Schränkt den Zugriff auf ServiceNow® ein, wenn Hijacker die Sitzungscookies eines Anwenders von einem Gerät auf ein anderes kopieren, um die Identität der Sitzung anzunehmen.
- Schränkt den Sitzungszugriff des Benutzers ein, wenn er ein unsicheres Netzwerk verwendet.
- Konfiguriert die verschiedenen Regeln und IP-Bereiche nach Anwendergruppe oder Rolle für Anwenderanmeldungen.

Kontextdatensatz für die Sitzungsvalidierung

Richtlinien im Sitzungsvalidierungskontext führen Anforderungen nach der Anmeldung aus.

Verwenden Sie die Felder im Richtlinienkontextdatensatz für die Sitzungsvalidierung, um zu definieren, wie Ihre Instanz Ihre Richtlinie verwendet.

Formular für den Kontext der Sitzungsvalidierung

Feld	Beschreibung
Name	Name des Richtlinienkontexts Dieses Feld ist statisch und kann nicht geändert werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular für den Kontext der Sitzungsvalidierung (Fortsetzung)

Feld	Beschreibung
Beschreibung	Beschreibung des Kontexts.
Standardrichtlinie	Definiert das Standardverhalten dieses Kontexts bei der Auswertung der Richtlinie. Wählen Sie unter den folgenden Optionen aus. Zulassungsrichtlinie Verweigert standardmäßig allen Anwendern den Zugriff und lässt den Zugriff nur zu, wenn die Bedingungen im **Feld** Zulassungsrichtlinie als „wahr“ ausgewertet werden. Verweigerungsrichtlinie Erlaubt standardmäßig allen Benutzern den Zugriff und verweigert den Zugriff nur, wenn die Bedingungen im Feld **Verweigerungsrichtlinie** als „wahr“ ausgewertet werden.
Zulassungsrichtlinie	Die für diesen Kontext verwendete Richtlinie. Dieses Feld wird nur angezeigt, wenn das Feld **Standardrichtlinie** auf **Zulassungsrichtlinie**festgelegt ist.
Verweigerungsrichtlinie	Die für diesen Kontext verwendete Richtlinie. Dieses Feld wird nur angezeigt, wenn das Feld **Standardrichtlinie** auf **Verweigerungsrichtlinie**festgelegt ist.

Sie können die **Sitzungsvalidierungsrichtlinie basierend auf der Richtlinieneingabe und den Richtlinienbedingungen** als Zulassungsrichtlinie oder Verweigerungsrichtlinie auswählen.

Hinweis:

Sie können nur die Filterkriterien IP, Rolle und Gruppe für die Richtlinie „Sitzungsvalidierung“ verwenden.

Richtlinieneingaben und -bedingungen

Die Registerkarten **Richtlinieneingabe** und **Richtlinienbedingungen** zeigen die Eingaben und Bedingungen der Richtlinie an, die im Feld **Zulassungsrichtlinie** oder **Verweigerungsrichtlinie** ausgewählt ist. Diese Registerkarten dienen als Referenz. Sie können jedoch nicht zum Ändern der Richtlinieneingaben oder -bedingungen verwendet werden. Um Ihre Richtlinie zu ändern, navigieren Sie zu der Richtlinie, indem Sie das Referenzsymbol (ⓘ) neben dem Feld **Zulassungsrichtlinie** oder **Verweigerungsrichtlinie** verwenden.

Aktivieren Sie den Validierungskontext der Sitzung

Verwenden Sie den Sitzungsvalidierungskontext, um den Zugriff auf ServiceNow® einzuschränken, wenn Hijacker die Sitzungscookies eines Anwenders von einem Gerät auf ein anderes kopieren, um die Identität der Sitzung anzunehmen, oder den Sitzungszugriff des Anwenders einschränken, wenn er ein unsicheres Netzwerk verwendet.

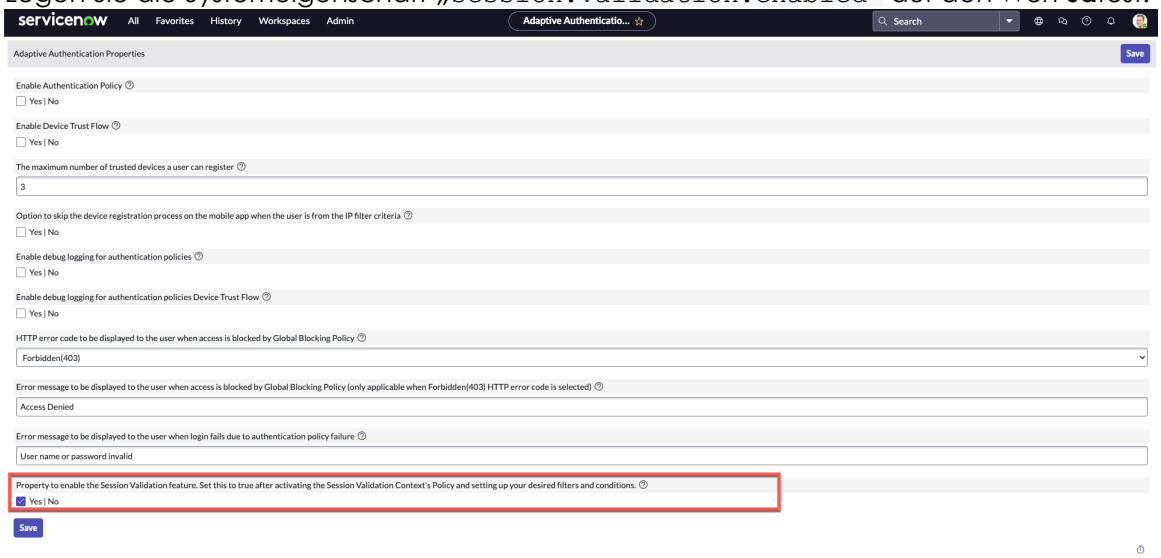
Vorbereitungen
Erforderliche Rolle: admin

Um die Sitzungsvalidierung zu verwenden, müssen Sie die folgenden Schritte ausführen:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Authentifizierungsrichtlinien** > **Alle Richtlinien**an.
2. Wählen Sie auf der Seite Richtlinien (`sys_authentication_policy_list.do`) die Richtlinie für die **Sitzungsvalidierung**aus.
3. Geben Sie die **Richtlinieneingaben** und **Richtlinienbedingungen an**.
4. Legen Sie die Bedingungen für die hinzugefügten Filter auf „ **true** “ oder „ **false** “ fest.
5. Aktivieren Sie das Kontrollkästchen **Aktiv**, um die Richtlinie zu aktivieren, nachdem Sie die Sitzungsvalidierungsrichtlinie mit Richtlinieneingaben und -bedingungen eingerichtet haben.
6. Aktivieren Sie für den standardmäßigen Identitätsanbieter in der Tabelle „ **sso_properties** “ das Kontrollkästchen AuthnRequest erzwingen, wenn für die Instanz SSO konfiguriert ist.
7. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Authentifizierungsrichtlinien** > **Eigenschaften**an.
8. Legen Sie die Systemeigenschaft `„session.validation.enabled“` auf den Wert **Ja**fest.



Ergebnisse

Die Funktion „Sitzungsvalidierung“ ist aktiviert. Sie können die Richtlinieneingaben und -bedingungen konfigurieren, damit die Richtlinie die Funktion verwenden kann. Weitere Informationen finden Sie unter Lernprogramm: Sitzungsvalidierung konfigurieren.

Lernprogramm: Sitzungsvalidierung konfigurieren

Konfigurieren Sie die Sitzungsvalidierung im Framework der adaptiven Authentifizierung, um eine zusätzliche Schutzebene für Hijacking von Sitzungen oder Cookies bereitzustellen.

Vorbereitungen

Erforderliche Rolle: admin

Erforderliches Plugin: **Adaptive Authentifizierung** (com.snc.adaptive_authentication)

Um die Sitzungsvalidierung zu konfigurieren, müssen Sie die folgenden Schritte ausführen:

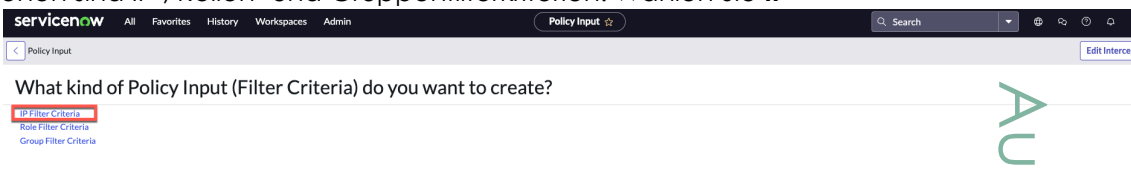
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Authentifizierungsrichtlinien** > **Alle Richtlinien**an.
2. Wählen Sie auf der Seite Richtlinien (`sys_authentication_policy_list.do`) die Richtlinie für die **Sitzungsvalidierung**aus.
3. Wählen Sie **Richtlinieneingaben aus**.

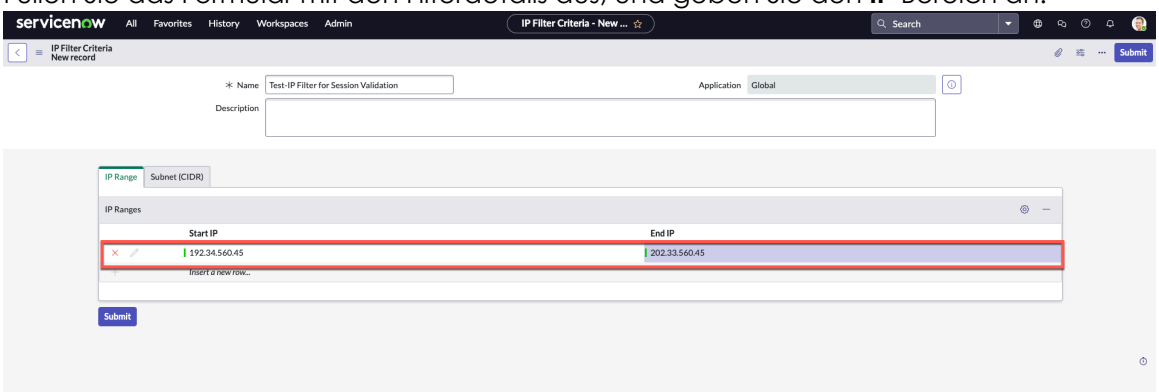
   a. Wählen Sie **Neu** oder **Bearbeiten aus**.

   b. Wählen Sie die Art der Richtlinieneingabe (Filterkriterien), die Sie erstellen möchten. Verfügbare Optionen sind IP-, Rollen- und Gruppenfilterkriterien. Wählen Sie **IP-**



   Filterkriterienaus.

   c. Füllen Sie das Formular mit den Filterdetails aus, und geben Sie den **IP**-Bereich an.



   Weitere Informationen zum Erstellen eines IP-Filters finden Sie unter Erstellen Sie IP-Filterkriterien.

   d. Wählen Sie **Absenden**.

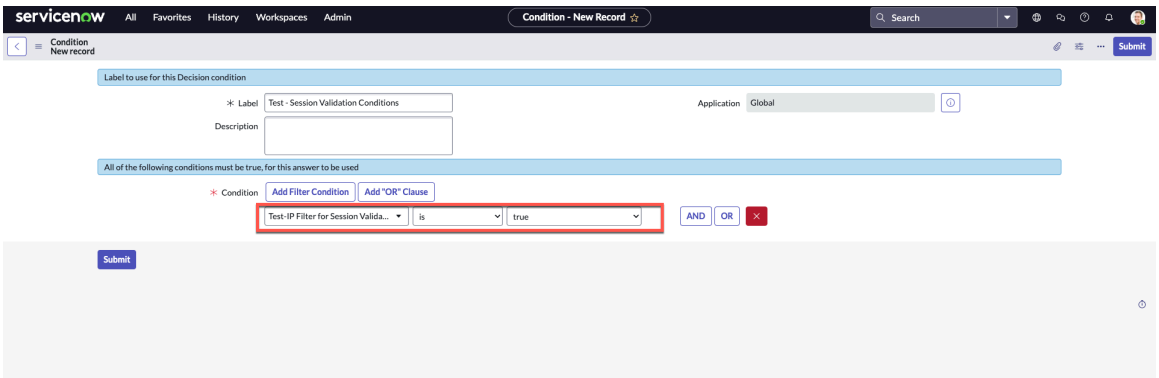
4. Wählen Sie auf der Seite „ **Richtlinien** für Sitzungsvalidierung“ die Option Richtlinienbedingungen aus.

   a. Wählen Sie **Neu**.

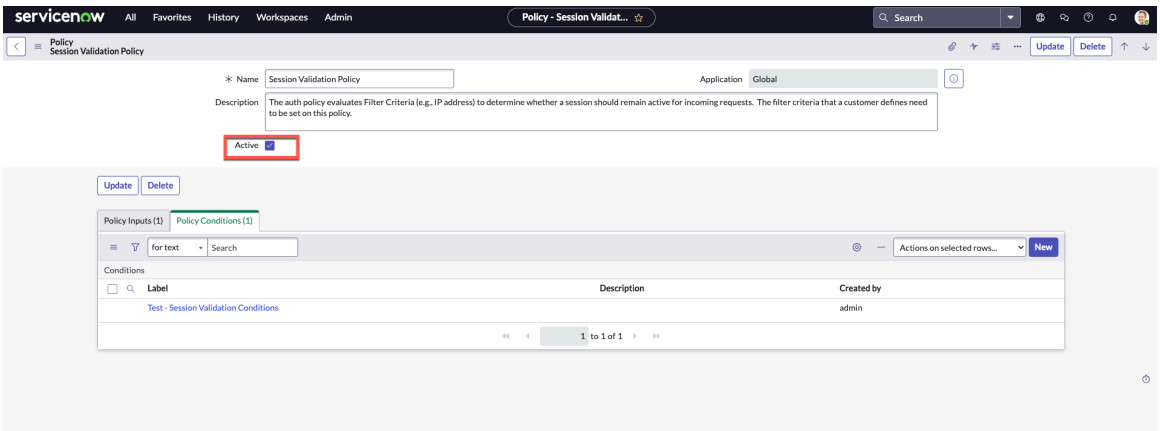
   b. Füllen Sie das Formular aus, und legen Sie die Bedingung für die Richtlinieneingabe fest.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

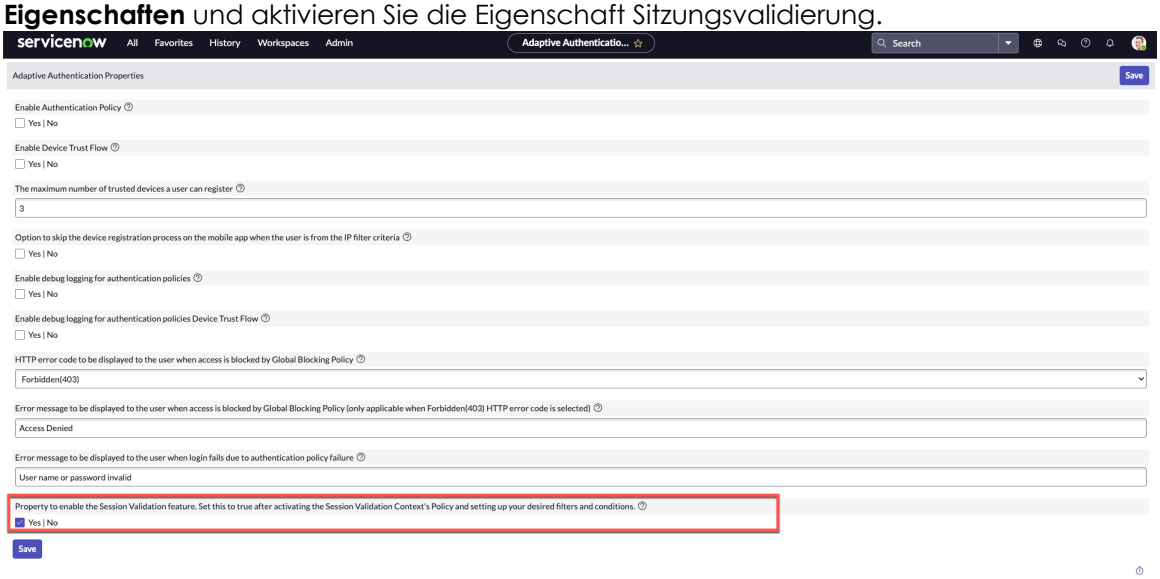
Hinweis: Sie können die Bedingungen je nach Konfiguration der Richtlinieneingabe auf „ `true` “ oder „ `false` “ festlegen. In diesem Beispiel ist sie auf `true`festgelegt. Wenn Sie die Bedingung in diesem Fall auf „true“ festlegen, kann sich nur der Benutzer mit der konfigurierten IP-Adresse anmelden.



5. Aktivieren Sie das Kontrollkästchen `Aktiv`, um die Richtlinie zu aktivieren, nachdem die Sitzungsvalidierungsrichtlinie mit Richtlinieneingaben und -bedingungen eingerichtet wurde.



6. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Authentifizierungsrichtlinien** > **Eigenschaften** und aktivieren Sie die Eigenschaft Sitzungsvalidierung.



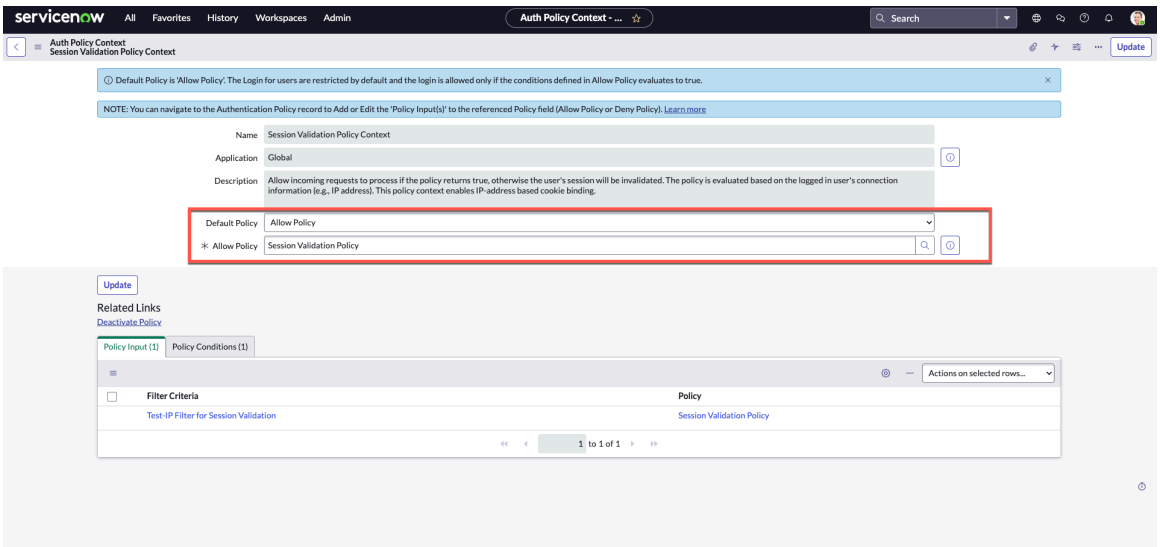
7. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Kontexte der Authentifizierungsrichtlinie** > **Sitzungsvalidierungskontext**an.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Legen Sie die Standardrichtlinie auf **Zulassungsrichtlinie** oder **Verweigerungsrichtlinie** fest, um den Sitzungsvalidierungskontext gemäß der Richtlinieneingabe und den Richtlinienbedingungen festzulegen.

   Hinweis: Standardmäßig gilt:

   - Der Kontext der Sitzungsvalidierung ist auf **Allow Policy**(Richtlinie zulassen) festgelegt.
   - Zulassungsrichtlinie ist als **Sitzungsvalidierungsrichtlinie**ausgewählt.



Ergebnisse

Die Konfiguration wertet die Anmeldesitzung basierend auf den folgenden Kriterien aus:

- Schränkt den Zugriff auf die Instanz ServiceNow® ein, wenn Hijacker die Sitzungscookies eines Anwenders von einem Gerät auf ein anderes kopieren, um die Identität einer Sitzung anzunehmen.
- Schränkt den Sitzungszugriff des Benutzers ein, wenn er ein unsicheres Netzwerk verwendet.

Authentifizierungsrichtlinien

Authentifizierungsrichtlinien werten Authentifizierungsanforderungen basierend auf den angegebenen Richtlinienbedingungen aus und erlauben oder verweigern den Zugriff, abhängig von der Ausgabe der Bewertung der Richtlinienbedingungen. Beispielsweise ist der -Zugriff nur zulässig, wenn alle in der **Allow-Zugriffsrichtlinie angegebenen Richtlinienbedingungen** als true ausgewertet werden.

Verwenden Sie die integrierten Authentifizierungsrichtlinien, oder erstellen Sie eine Authentifizierungsrichtlinie gemäß Ihren Sicherheitsanforderungen. Sie finden die Richtlinien in Ihrer Instanz, indem Sie zu navigieren **Adaptive Authentifizierung** > **Authentifizierungsrichtlinien** > **Alle Richtlinien**an.

Hinweis: Die Richtlinie „Zugriff zulassen“ oder die Richtlinie „Zugriff verweigern“ kann jederzeit ausgeführt werden, jedoch nicht beide.

Richtlinie	Beschreibung
Zugriffsrichtlinie zulassen	Lehnt standardmäßig alle Authentifizierungsanforderungen ab. Lässt nur die Authentifizierungsanforderungen

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie	Beschreibung
	zu, die den angegebenen Richtlinienbedingungen entsprechen.
Vorauthentifizierungsrichtlinie für Zugriffsgenehmigung	Vorauthentifizierungsrichtlinie für Zugriff zulassen.
Lassen Sie nicht lokale Anmeldeanwender zu	Wählen Sie diese Richtlinie, um nicht-lokale Anmeldeanwender zuzulassen. Wird im Kontext von SSO-Wiederherstellungs-Flows verwendet.
Zugriffsrichtlinie verweigern	Erlaubt standardmäßig die Authentifizierungsanforderungen. Lehnt nur die Authentifizierungsanforderungen ab, die den angegebenen Richtlinienbedingungen entsprechen.
Globale Sperrrichtlinie	Verweigert die Zugriffsanforderungen von Anwendern und APIs vor der Authentifizierung. Diese Richtlinie kann als Alternative zur IP-Adresszugriffssteuerungverwendet werden.
Richtlinie für die Sitzungsvalidierung	Die Authentifizierungsrichtlinie wertet Filterkriterien (z. B. IP-Adresse) aus, um zu bestimmen, ob eine Sitzung für eingehende Anforderungen aktiv bleiben soll. Sie müssen die Filterkriterien für diese Richtlinie festlegen.
Richtlinie zur Verweigerung der lokalen Anmeldung	Wählen Sie diese Richtlinie, um alle lokalen Anmeldungen zu blockieren. Wird im Kontext von SSO-Wiederherstellungs-Flows verwendet.
Step-down-MFA-Richtlinie	Wählen Sie die **Step-Down-MFA-Richtlinie** als Standardrichtlinie in Situationen aus, in der Anwender keine MFA-Authentifizierung benötigen. Wenn die in der Step-Up-MFA-Richtlinie definierten Richtlinienbedingungen als „true“ ausgewertet werden, müssen sich Benutzer nicht mit MFA anmelden.
Step-up-MFA-Richtlinie	Wählen Sie **Step-Up-MFA-Richtlinie** als Standardrichtlinie aus, um die MFA-Authentifizierung anzufordern, wenn die in der Step-Up-MFA-Richtlinie definierten Richtlinienbedingungen als „wahr“ ausgewertet werden.

Konfigurieren Sie eine Authentifizierungsrichtlinie

Konfigurieren Sie eine Authentifizierungsrichtlinie, um Eingaben und Bedingungen zu definieren, die zum Gewähren des Zugriffs auf eine Instanz oder zum Erzwingen der Multifaktor-Authentifizierung verwendet werden.

Vorbereitungen

Erforderliche Rolle: admin

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Authentifizierungsrichtlinien** > **Alle Richtlinien**an.

   Hinweis: Um Beispiele für abgeschlossene Richtlinien anzuzeigen, können Sie diese Richtlinien in Ihrer Instanz überprüfen:

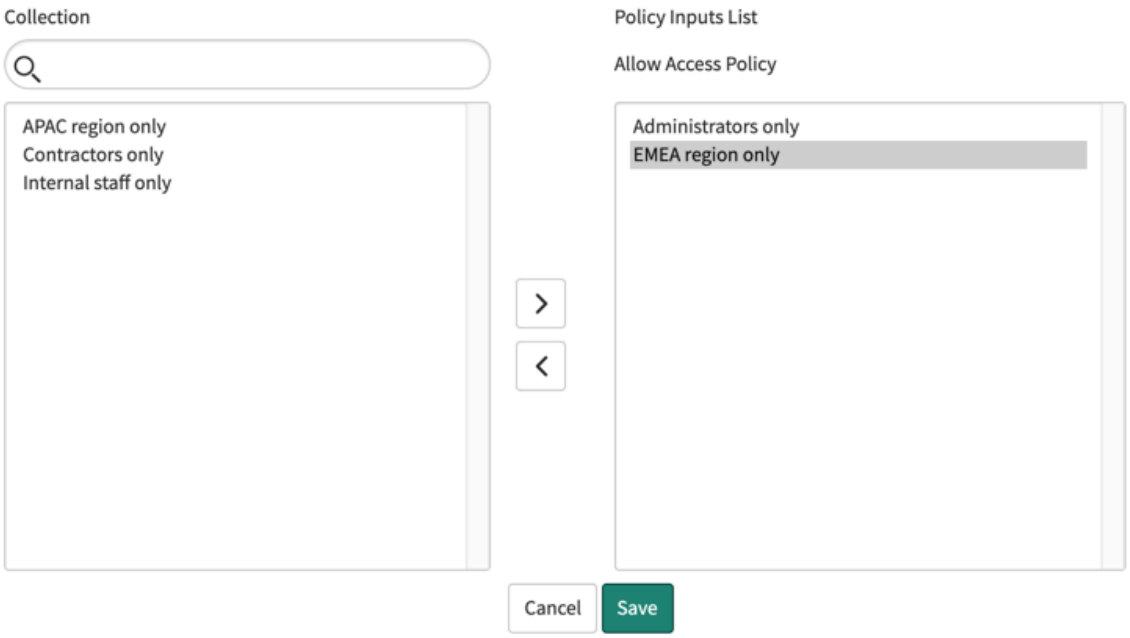
   - DEMO-RICHTLINIE: Lokale Anmeldung nur für Administratoren aus dem vertrauenswürdigen IP-Bereich zulassen
   - DEMO-RICHTLINIE: Lokale Anmeldung nur für Administratoren zulassen
   - DEMO-RICHTLINIE: Schränkt die auf Anwendernamen und Passwort basierende Authentifizierung für bestimmte Anwender ein

2. Klicken Sie auf die Schaltfläche **Neu**, um einen neuen Richtliniendatensatz zu erstellen.
3. Füllen Sie die Felder im Formular **Richtlinie** aus.

Formular „Richtlinie“.

Feld	Beschreibung
Name	Name Ihrer Richtlinie.
Anwendung	Die bereichsbezogene Anwendung für die Richtlinie. Dieses Feld wird automatisch mit der aktuellen Anwendung ausgefüllt.
Beschreibung	Beschreibung der Richtlinie
Aktiv	Gibt an, ob die Richtlinie aktiv ist.

4. Klicken Sie auf der Registerkarte **Richtlinieneingaben** auf **Bearbeiten**.
5. Wählen Sie ein oder mehrere Filterkriterien aus der Liste **Sammlung** aus, und verschieben Sie sie in die Liste Richtlinieneingaben der **ListeAllow Access Policy** (Zugriffsrichtlinie zulassen).



Hinweis: Informationen zum Erstellen eigener Filterkriterien für diesen Abschnitt finden Sie unter Filterkriterien.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie auf der Registerkarte **Richtlinienbedingungen** auf **Neu**.
7. Füllen Sie die Felder des Formulars aus.

Formular für Bedingungen

Feld	Beschreibung
Bezeichnung	Name zur Identifizierung der Bedingung.
Beschreibung	Beschreibung der Bedingung
Bedingung	Logische Kombination aus mehreren Richtlinieneingaben (Filterkriterien), die zur Auswertung von Authentifizierungsanforderungen verwendet wird. Sie können beispielsweise Bedingungen erstellen, die nur Auftragnehmer aus einer Liste vertrauenswürdiger IP-Adressen zulassen.

8. Wahlweise: Wiederholen Sie Schritt 7, um zusätzliche Richtlinienbedingungen zu erstellen.

> **Hinweis:** Wenn Sie mehrere Richtlinienbedingungen erstellen, hängt die endgültige Ausgabe der Zugriffsrichtlinie von der logischen ODER-Ausgabe aller Richtlinienbedingungen ab. Dies bedeutet, dass die Richtlinie als „true“ ausgewertet wird, wenn eine Ihrer Richtlinienbedingungen erfüllt ist.

9. Klicken Sie auf **Speichern**.

Fügen Sie einem Authentifizierungsrichtlinienkontext eine Authentifizierungsrichtlinie hinzu

Fügen Sie einem der Authentifizierungsrichtlinienkontexte eine Authentifizierungsrichtlinie hinzu. Der Authentifizierungskontext verwendet die Richtlinieneingaben und -bedingungen, um zu bestimmen, ob Benutzern Zugriff auf die Instanz gewährt wird oder ob MFA für Ihre Benutzer erzwungen wird.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Kontexte der Authentifizierungsrichtlinie**, und wählen Sie je nach Bedarf einen der Einträge aus.

   Kontext vor der Authentifizierung

   Verwenden Sie den Vorautorisierungskontext, um Ihre Richtlinie auszuwerten, bevor der Benutzer den Anmeldebildschirm sieht. Abhängig von dieser Auswertung wird Anwendern der Zugriff gewährt oder verweigert.

   Kontext nach der Authentifizierung

   Verwenden Sie den Kontext nach der Autorisierung, um Ihre Richtlinie auszuwerten, nachdem der Benutzer seine Anmeldeinformationen eingegeben hat. Abhängig von dieser Auswertung wird Anwendern der Zugriff gewährt oder verweigert. Da diese Auswertung erfolgt, nachdem die Instanz den Anwender identifiziert hat, können Richtlinien in diesem Kontext ihre Auswertung auf Grundlage von Anwenderdaten vornehmen, z. B. basierend auf ihrer Rolle oder Gruppe.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MFA-Kontext

Verwenden Sie den MFA-Kontext, um zu bestimmen, ob ein Anwender bei der Anmeldung die Multifaktor-Authentifizierung verwenden muss.

Sitzungsvalidierungskontext

Verwenden Sie den Sitzungsvalidierungskontext, um die IP-Adresse auszuwerten, die basierend auf den als Filter definierten Bedingungen festgelegt wird und den Zugriff auf die Instanz innerhalb einer Sitzung ermöglicht.

2. **Wählen Sie im Feld Standardrichtlinie** einen Wert aus.
   Der Wert in diesem Feld bestimmt, wie der Kontext das Ergebnis der Bedingungen Ihrer Richtlinie verwendet.

   Die verfügbaren Optionen in diesem Feld hängen vom ausgewählten Kontext ab. Einzelheiten zu diesen Kontexten finden Sie unter Kontexte der Authentifizierungsrichtlinie.

3. Weisen Sie dem Kontext eine Richtlinie zu.
   Der Name des Felds hängt davon ab, welchen Kontext Sie ausgewählt haben.

   Kontext vor und nach der Authentifizierung

   Diese Kontexte weisen je nach Auswahl im Feld **„Standardrichtlinie“ ein** Feld **„Verweigerungsrichtlinie“** oder **„Zulassungsrichtlinie“** auf.

   MFA-Kontext

   Dieser Kontext verfügt je nach Auswahl im Feld **„Standardrichtlinie“** über ein Feld **„Step-Up-MFA-Richtlinie“** oder „ **Step-Down-MFA-Richtlinie** “.

   Kontext der Sitzungsvalidierung

   Dieser Kontext verfügt je nach Auswahl im Feld **„Standardrichtlinie“** über ein Feld **„Zulassungsrichtlinie“** oder **„Verweigerungsrichtlinie** “.

4. Klicken Sie auf **Aktualisieren**.
   Nach dem Aktualisieren des Datensatzes können Sie die Eingaben und Bedingungen Ihrer Richtlinie auf den Registerkarten **Richtlinieneingabe** und **Richtlinienbedingungen** anzeigen.

Adaptive Authentifizierungsereignisse

Sie können die Ereignistabelle der adaptiven Authentifizierung verwenden, um mehr über die Ereignisse zu erfahren.

Im Folgenden sind einige der Protokolle aufgeführt, die in der Tabelle mit den Ereignissen der adaptiven Authentifizierung nachverfolgt werden können:

- `glide.adaptive.auth.log.success.event`: Um die `Erfolgsereignisse` für API-Anmeldungen nach der Authentifizierung zu kennen.
- `glide.adaptive.auth.log.mfa.relax.event`: Um die `mfa_relaxation-` Ereignisse für den MFA-Kontext zu kennen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Für `Vorauthentifizierungskontext`, REST API-Zugriffsrichtlinien vom Typ „`pre_auth` “: Standardmäßig werden Fehlerereignisse protokolliert. `Erfolgsereignissekönnen nicht` protokolliert werden.
- Für den Post-Auth-Kontext, REST-API-Zugriffsrichtlinien eines anderen Typs als „`pre_auth`“: Standardmäßig `Fehlerereignisse` oder protokolliert. Damit `Erfolgsereignisse` protokolliert werden, müssen Sie die Eigenschaft „`glide.adaptive.auth.log.success.event“ aktivieren`.
- Für MFA: Standardmäßig werden `MFA-Durchsetzungsereignisse` protokolliert.
- Damit MFA-Entspannungsereignisse protokolliert werden, müssen Sie die Eigenschaft „`glide.adaptive.auth.log.mfa.relax.event“ aktivieren`. Die`MFA-Entlastung` würde das gleiche Ereignis wie die `MFA-Erzwingung`protokollieren, wobei das `Ergebnisfeld` jedoch mit „ `Falsch`“ ausgefüllt ist.

Konfigurieren Sie die Eigenschaften der adaptiven Authentifizierung

Konfigurieren Sie nach der Aktivierung der adaptiven Authentifizierung die adaptiven Authentifizierungseigenschaften gemäß Ihren Sicherheitsanforderungen.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Authentifizierungsrichtlinien** > **Eigenschaften**an.
2. Konfigurieren Sie diese Eigenschaften:

Adaptive Authentifizierung – Eigenschaften

Eigenschaft	Beschreibung	Wert
Authentifizierungsrichtlinie aktivieren (glide.authenticate.auth.policy.enabled)	Option zum Aktivieren der Authentifizierungsrichtlinie.	Ja | Nein
Debug-Protokollierung für Authentifizierungsrichtlinien aktivieren (glide.authenticate.policy.debug)	Option zum Aktivieren der Debug-Protokollierung für die Authentifizierungsrichtlinien.	Ja | Nein
HTTP-Fehlercode, der dem Anwender angezeigt werden soll, wenn der Zugriff durch die globale Sperrrichtlinie blockiert wird (glide.authenticate.global.blocking_policy.error_code)	HTTP-Fehlercode, der während der Anmeldung angezeigt wird, wenn die globale Blockierungsrichtlinie eine Anwenderanmeldung blockiert.	Wählen Sie aus: ◦ Unzulässig (403) ◦ Nicht gefunden (404)
Fehlermeldung, die dem Anwender angezeigt werden soll, wenn der Zugriff durch die globale Blockierungsrichtlinie blockiert wird (nur anwendbar, wenn HTTP-Fehlercode „Forboten(403)“ ausgewählt ist) (glide.authenticate.global.blocking_policy.error_message)	Fehlermeldung, die angezeigt wird, wenn die globale Blockierungsrichtlinie den Zugriff blockiert.	Textfeld

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung	Wert
Flow für Gerätevertrauen aktivieren (glide.authenticate.preauth.allow.trusted.device)	Option zum Aktivieren des vertrauenswürdigen Geräte-Flows.	Ja | Nein
Maximale Anzahl der vertrauenswürdigen Geräte, die ein Anwender registrieren kann (glide.trusted.device.max.count)	Dies ist die maximale Anzahl vertrauenswürdiger Geräte, die ein Benutzer registrieren kann.	Textfeld
Flow „Geräteregistrierung für Gerätevertrauen“ überspringen, wenn der Anwender aus dem vertrauenswürdigen Netzwerk stammt (glide.authenticate.preauth.skip.user.registration)	Option zum Überspringen der Registrierung, wenn der Benutzer versucht, sich über das vertrauenswürdige Netzwerk zu registrieren	Ja | Nein
Eigenschaft zum Aktivieren der Sitzungsvalidierungsfunktion. Legen Sie diese Option auf „wahr“ fest, nachdem Sie die Richtlinie des Sitzungsvalidierungskontexts aktiviert und die gewünschten Filter und Bedingungen eingerichtet haben (session.validation.enabled).	Option zum Aktivieren der Sitzungsvalidierungsfunktion. Legen Sie diese Option auf „wahr“ fest, nachdem Sie die Richtlinie des Sitzungsvalidierungskontexts aktiviert und die gewünschten Filter und Bedingungen eingerichtet haben.	Ja | Nein

Lernprogramm: Konfigurieren Sie die adaptive Authentifizierung

Verwenden Sie diese Beispielschritte, um die adaptive Authentifizierung für eine -Instanz zu konfigurieren.

Zur Verwendung dieses Lernprogramms benötigen Sie eine Instanz mit aktivierter adaptiver Authentifizierung. Details zu diesem Vorgang finden Sie unter Aktivieren Sie die adaptive Authentifizierung.

Das Beispiel führt Sie durch die Erstellung einer neuen Richtlinie und deren Anwendung auf eine Instanz von. In diesem Tutorial werden Sie:

Erstellen Sie einen Filterkriteriendatensatz

Erstellen Sie einen Gruppenfilterkriterien-Datensatz, den Sie als Eingabe für Ihre Richtlinie verwenden können. Mit diesem Datensatz kann Ihre Richtlinie den Zugriff basierend auf der Gruppe eines Anwenders bestimmen. In diesen Schritten definieren Sie die Gruppe(n), anhand derer die Richtlinie den Zugriff bestimmt.

Erstellen Sie eine Richtlinie

Erstellen Sie eine Richtlinie, die bestimmt, ob ein Benutzer auf die Instanz zugreifen kann. Diese Richtlinie verwendet den von Ihnen erstellten Gruppenfilterkriterien-Datensatz als Eingabe. In diesen Schritten definieren Sie auch Richtlinienbedingungen, die definieren, wie die Richtlinie anhand der Richtlinieneingabe den Benutzerzugriff bestimmt.

Konfigurieren Sie einen Richtlinienkontext

Konfigurieren Sie den Richtlinienkontext nach der **Authentifizierung**, um Ihre neue Richtlinie zu verwenden. Bei entsprechender Konfiguration verweigert Ihre -Instanz Benutzern innerhalb der im Filterkriteriendatensatz definierten Gruppe den Zugriff.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie einen Filterkriteriendatensatz

Erfahren Sie, wie Sie einen Kriteriendatensatz erstellen, den Sie als Richtlinieneingabe für Ihre Richtlinie für adaptive Authentifizierung verwenden können.

Vorbereitungen

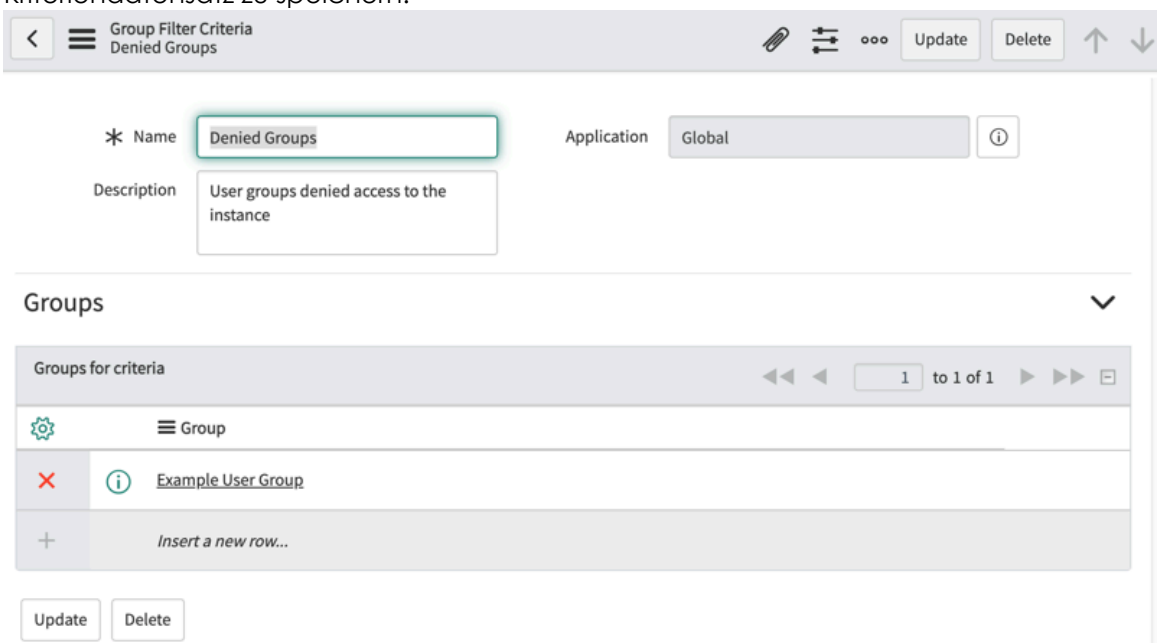
Erforderliche Rolle: admin

Um den Zugriff auf Ihre Instanz basierend auf Benutzergruppen zu verweigern, müssen Sie einen Datensatz mit Gruppenfilterkriterien erstellen. Dieser Datensatz definiert eine Anwendergruppe oder einen Satz von Anwendergruppen, denen Ihre Richtlinie den Zugriff gewähren oder verweigern kann. In diesem Beispiel erstellen Sie einen Gruppenfilterkriterien-Datensatz für eine einzelne Benutzergruppe.

Weitere Informationen zu -Benutzergruppen und ihrer Verwendung in Ihrer Instanz finden Sie unter Benutzerverwaltung erkunden .

Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Filterkriterien** > **Gruppenkriterien**an.
2. Klicken Sie auf **Neu**, um einen neuen Datensatz zu erstellen.
3. Geben Sie im Feld **Name** einen Namen für Ihren Datensatz ein.
   Beispiel: `Abgelehnte Gruppen`.
4. Geben Sie im Feld **Beschreibung** eine kurze Beschreibung ein.
   Beispiel: `Benutzergruppen, denen der Zugriff auf die Instanz verweigert`wurde.
5. Doppelklicken Sie in der Liste **Gruppen für Kriterien** auf **Neue Zeile einfügen...**.
6. Geben Sie den Namen einer Benutzergruppe ein, oder klicken Sie auf das Referenzsymbol ( ), um eine Gruppe aus einer Liste auszuwählen.
   Wenn Sie eine neue Benutzergruppe für Ihre Filterkriterien erstellen möchten, klicken Sie auf das Referenzsymbol ( ), und klicken Sie dann auf die Schaltfläche **Neu**. Weitere Informationen zum Erstellen von Benutzergruppen finden Sie unter Benutzergruppen erstellen .
7. Nachdem Sie Ihre Benutzergruppe hinzugefügt haben, klicken Sie auf **Absenden**, um Ihren Kriteriendatensatz zu speichern.



© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie eine Richtlinie

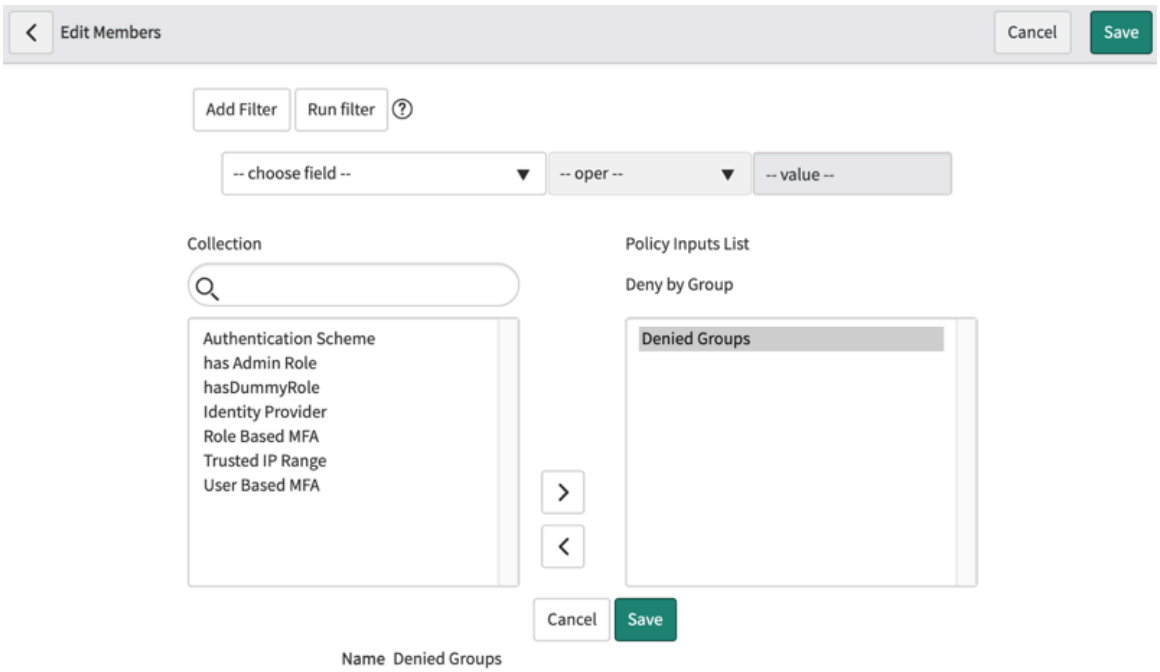
Erfahren Sie, wie Sie eine Richtlinie erstellen, um Anwendergruppen, die in Ihren Gruppenfilterkriterien definiert sind, den Zugriff zu verweigern.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

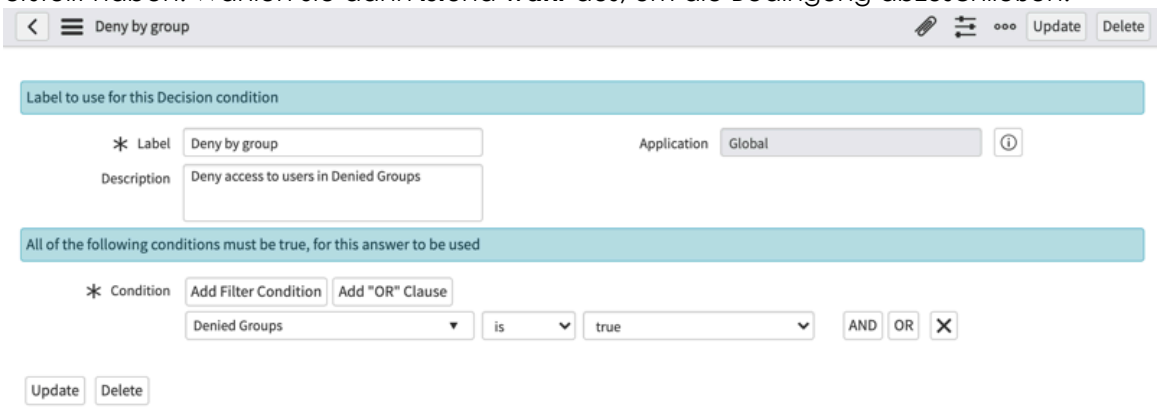
1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Authentifizierungsrichtlinien** > **Alle Richtlinien**an.
2. Klicken Sie in der Liste **Richtlinien** auf **Neu**.
3. Geben Sie im Feld **Name** einen Namen für Ihren Datensatz ein.
   Beispiel: `Nach Gruppe verweigern`.
4. Geben Sie im Feld **Beschreibung** eine kurze Beschreibung ein.
   Beispiel: `Benutzergruppen, denen der Zugriff auf die Instanz verweigert`wurde.
5. Klicken Sie mit der rechten Maustaste in den Header Kopfzeile des Formulars, und wählen Sie **Speichern** aus.
   Nach dem Speichern werden die Listen **Richtlinieneingaben** und **Richtlinienbedingungen** im Formular angezeigt.
6. Klicken Sie in der Liste **Richtlinieneingaben** auf **Bearbeiten**.
7. Fügen Sie im Listen-Sammlungsprogramm die in den vorherigen Schritten erstellten Filterkriterien zu Ihrer Richtlinie hinzu.



8. Klicken Sie auf **Speichern**.
   Die Instanz speichert die Richtlinieneingabe und zeigt den Richtliniendatensatz erneut an.
9. Klicken Sie in der Liste **Richtlinienbedingungen** auf **Neu**.
10. **Erstellen Sie** im Feld Bezeichnung eine Bezeichnung für diese Bedingung, z. B. `Ablehnen nach Gruppe`.
11. Geben Sie im Feld **Beschreibung** eine kurze Beschreibung ein.
    Beispiel: `Verweigern Sie Anwendern den Zugriff in Abgelehnte Gruppen`.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

12. Wählen Sie im Feld **Bedingung** die Filterkriterien aus, die Sie in den vorherigen Schritten erstellt haben. Wählen Sie dann **ist**und **wahr** aus, um die Bedingung abzuschließen.



13. Klicken Sie auf **Speichern**.

Konfigurieren Sie einen Richtlinienkontext

Konfigurieren Sie den Richtlinienkontext nach der Authentifizierung, um Ihre neue Richtlinie zu verwenden. Bei entsprechender Konfiguration verweigert Ihre -Instanz Benutzern innerhalb der im Filterkriteriendatensatz definierten Gruppe den Zugriff.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. **Adaptive Authentifizierung** > **Kontexte der Authentifizierungsrichtlinie** > **Kontext nach der Authentifizierung**an.
   Sie müssen den **Post-Authentifizierungskontext** verwenden, da die in diesem Tutorial verwendete Richtlinie bewerten muss, zu welcher Gruppe ein Anwender gehört. Diese Informationen sind erst verfügbar, nachdem die Anmeldeinformationen eingegeben wurden.
2. Wählen Sie im Feld **Standardrichtlinie** die Option `Verweigerungsrichtlinie`aus.
   Diese Auswahl gewährt Benutzern standardmäßig Zugriff und verweigert den Zugriff nur, wenn die Richtlinienbedingungen als „wahr“ ausgewertet werden.
3. **Wählen** Sie im Feld Verweigerungsrichtlinie die Richtlinie aus, die Sie in den vorherigen Schritten erstellt haben.
4. Klicken Sie auf **Aktualisieren**, um den Richtlinienkontextdatensatz zu speichern.

Adaptive Authentifizierung für vertrauenswürdige mobile Apps

Greifen Sie mit ServiceNow aus nicht vertrauenswürdigen Netzwerken auf Ihr [Now Mobile-Appzu.

Adaptive Authentifizierung für vertrauenswürdige mobile Apps

Mit der adaptiven Authentifizierung für vertrauenswürdige mobile Apps können Benutzer mit ServiceNow auf die Instanz Now Mobile-Appzugreifen. Die Instanz ist hinter einer vertrauenswürdigen IP-Netzwerkgrenze geschützt.

Im Folgenden finden Sie einige Szenarien, in denen Sie Zugriff auf die Instanz benötigen, während Sie sich außerhalb Ihres Netzwerks befinden.

Als -Mitarbeiter müssen Sie von außerhalb des Netzwerks auf Now Mobile-App und das Employee Service Center (Portal) zugreifen. Mit dem Filter für vertrauenswürdige mobile Apps

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

können Sie die eingehende Anforderung identifizieren, die von einer vertrauenswürdigen Now Mobile-App stammt, die mit einem Benutzerkonto verknüpft ist.

Als Administrator können Sie die Richtlinie konfigurieren. Mit der Richtlinie können Benutzer ihre Mobilgeräte registrieren und in einem vertrauenswürdigen Netzwerk auf die Instanz zugreifen.

Als Benutzer können Sie Ihr Mobilgerät registrieren, indem Sie den in der Instanz angezeigten QR scannen. Nach der Registrierung können Sie sich über Now Mobile-Appmit Ihren Anmeldeinformationen bei Ihrer Instanz anmelden.

Hinweis: Um das Mobilgerät zu registrieren, müssen Sie sich in einem vertrauenswürdigen Netzwerk befinden. Nach der Registrierung können Sie sich auch aus anderen Netzwerken bei der Instanz anmelden.

Funktionen

Als Administrator können Sie die folgenden Funktionen von verwenden:

- Konfigurieren Sie Richtlinien mithilfe von Filterkriterien für vertrauenswürdige Apps.
- Erstellen Sie Richtlinienbedingungen mit neuen Filterkriterien für vertrauenswürdige mobile Apps.
- Unterstützen Sie alle Anmeldemethoden in der vertrauenswürdigen mobilen App für die Anwender (lokale Anmeldung, SAML, OIDC und MFA).
- Widerrufen Sie ein vertrauenswürdiges Gerät.
- Fügen Sie Sicherheitsereignisse für alle Geräteregistrierungs- oder -widerrufaktionen hinzu. Die Ereignisse können verwendet werden, um den Benutzer zu benachrichtigen.
- Unterstützen Sie Sicherheitsereignisse bei Signaturfehlern, Fehlern bei der Cookie-Validierung, ungültigen Tokens, ungültigen Headern oder Abfrageparametern.
- Steuern Sie die maximale Anzahl registrierter Geräte.
- Verhindert die Registrierung neuer Geräte, es sei denn, der Benutzer entfernt ein vorhandenes gekoppeltes Gerät.
- Erfassen Sie, wann ein Gerät zuletzt verwendet wurde.

Aktivieren Sie die Trusted Mobile App

Aktivieren Sie die adaptive Authentifizierung mit Trusted Mobile-App mithilfe der Authentifizierungsrichtlinie und der Filterbedingungen.

Vorbereitungen

Stellen Sie sicher, dass das Plugin „Adaptive Authentifizierung“ (*com.snc.adaptive_authentication*) installiert ist.

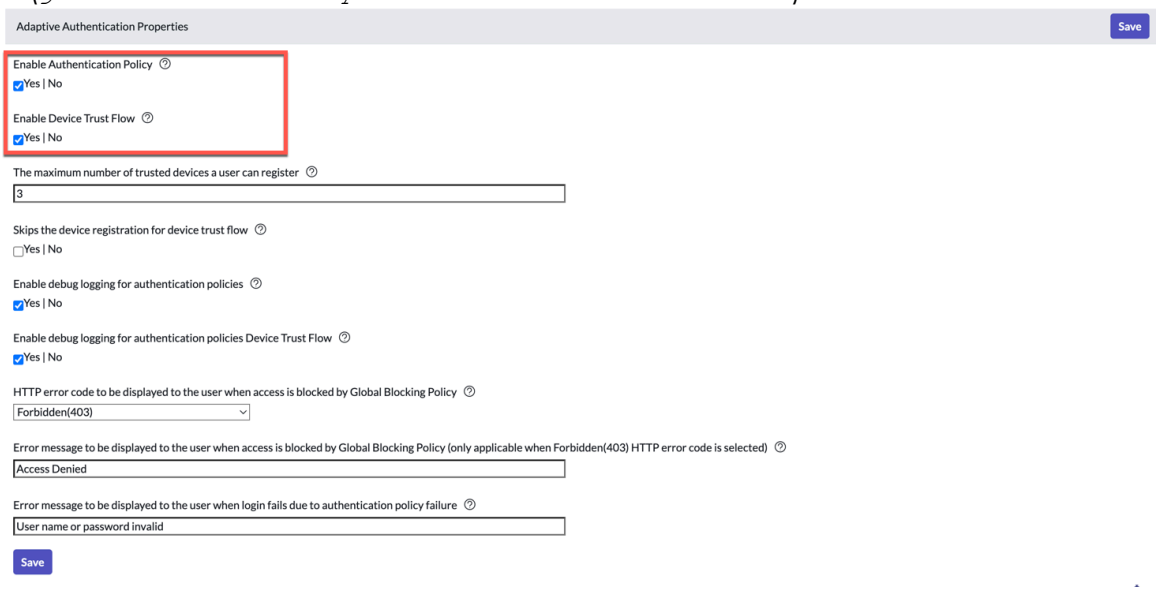
Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Authentifizierungsrichtlinien** > **Eigenschaften**an.
2. Aktivieren Sie auf der Seite „Eigenschaften der adaptiven Authentifizierung“ die folgenden Eigenschaften:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Authentifizierungsrichtlinie aktivieren (*glide.authenticate.auth.policy.enabled*)
- Flow für Gerätevertrauen aktivieren (*glide.authenticate.preauth.allow.trusted.device*)



Hinweis: Um die Flow-Eigenschaft für Gerätevertrauen zu deaktivieren, müssen Sie die Bedingungen mit dem Filter für vertrauenswürdige Mobilgeräte entfernen. Andernfalls wird eine Fehlermeldung angezeigt, in der Sie aufgefordert werden, die Bedingungen zu entfernen.

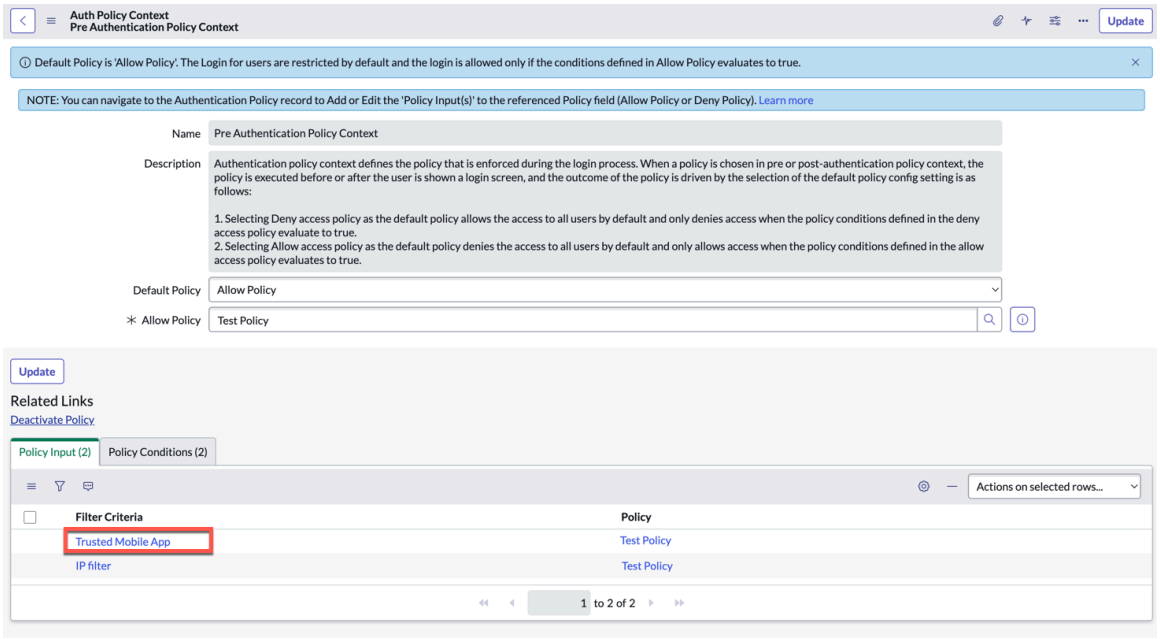
3. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Kontexte der Authentifizierungsrichtlinie** > **Kontext vor der Authentifizierung**an.
4. Definieren Sie die Bedingungen im Kontext vor der Authentifizierung. Weitere Informationen finden Sie unter Kontext vor der Authentifizierung.

Hinweis: Standardmäßig lautet die Richtlinienbedingung **Deny Policy**(Richtlinie verweigern). Sie können in **Zulassungsrichtlinie**ändern. Diese Richtlinien sind direkte Gegenteil.

- Mit der **Zulassungsrichtlinie**wird allen Benutzern standardmäßig der Zugriff verweigert und der Zugriff wird nur gewährt, wenn die Bedingungen der Richtlinie für den Zugriffszulassen auf „wahr“ gesetzt sind.
- Mit der **Verweigerungsrichtlinie**wird allen Benutzern standardmäßig der Zugriff gewährt, und der Zugriff wird nur verweigert, wenn die Bedingungen der Richtlinie für die Verweigerung des Zugriffs „wahr“ sind.

In der Richtlinieneingabe ist die Richtlinieneingabe **Trusted Mobile App** eine Richtlinieneingabe für die vertrauenswürdige mobile App.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

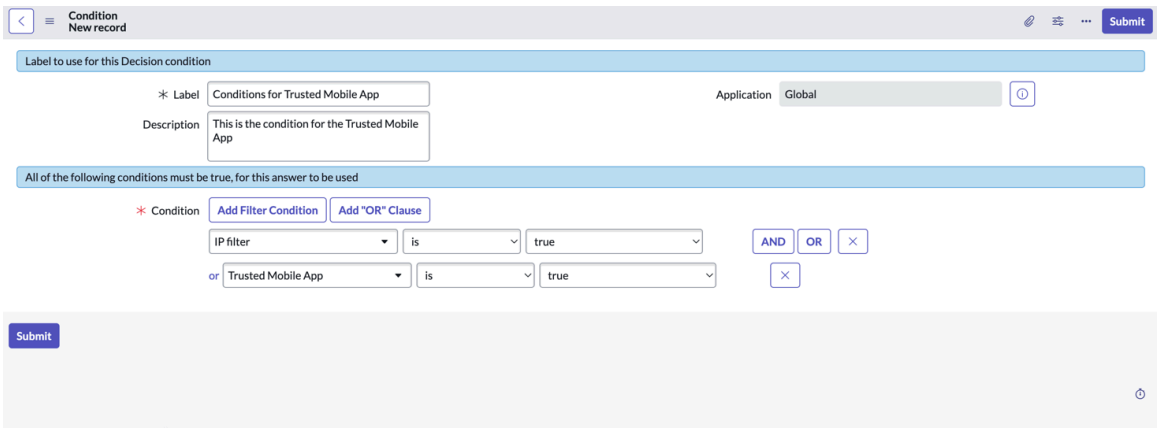


5. Erstellen Sie in den Richtlinienbedingungen die Bedingung, indem Sie auf **Neu**klicken.

6. Füllen Sie die Felder im Formular aus.

Formular „Filterbedingung“

Feld	Beschreibung
Bezeichnung	Name der Bedingung
Beschreibung	Beschreibung der Bedingung
Anwendung	Anwendungsbereich für diesen Datensatz
Bedingung	Bedingungen basierend auf AND und OR. Da die Authentifizierungsrichtlinie auf **Allow Policy**festgelegt ist, ist die Bedingung für Trusted Mobile App im Beispiel, das auf der Abbildung zu sehen ist, auf true festgelegt.



7. Klicken Sie auf **Absenden**.

Ergebnisse

Die Richtlinieneingabe und die Filterbedingungen werden für die Funktion „Vertrauenswürdiges Gerät“ erstellt. Benutzer können mit der Verwendung der Funktion

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

„Vertrauenswürdiges Gerät“ fortfahren, um von nicht vertrauenswürdigen Netzwerken aus auf die Instanz ServiceNow zuzugreifen, indem sie die Funktion Now Mobile-Appverwenden. Weitere Informationen finden Sie unter Registrieren Sie ein vertrauenswürdiges Gerät.

Registrieren Sie ein vertrauenswürdiges Gerät

Registrieren Sie ein vertrauenswürdiges Gerät, um außerhalb des Netzwerks auf die Instanz ServiceNow zuzugreifen.

Vorbereitungen

Sie müssen sich im vertrauenswürdigen Netzwerk befinden, um die vertrauenswürdige Geräteregistrierung durchzuführen.

Erforderliche Rolle: keine

Prozedur

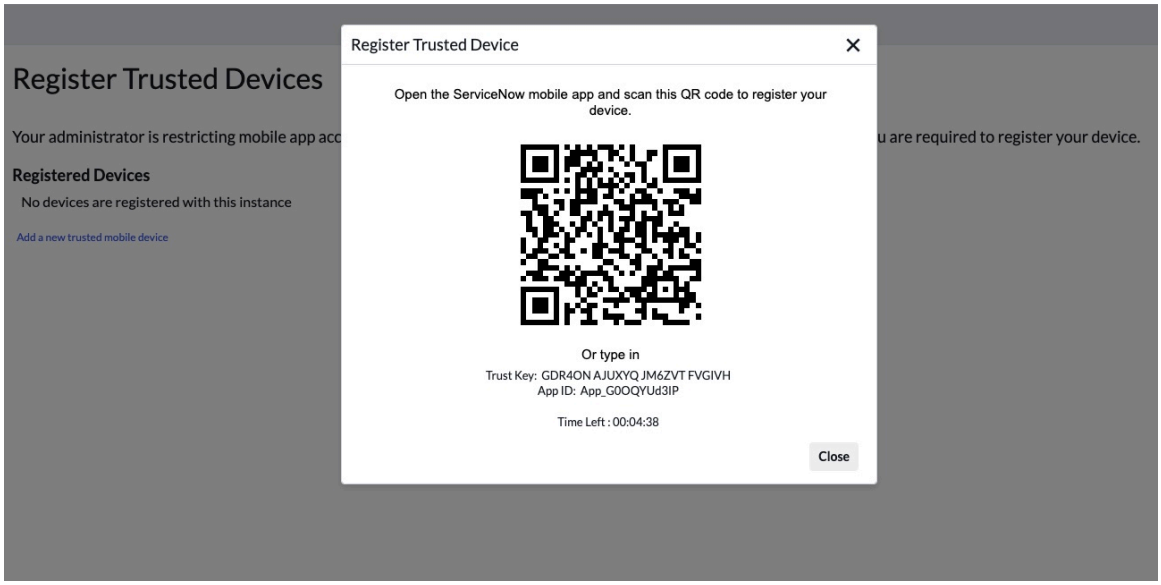
1. Navigieren Sie zu einer der folgenden Menüoptionen:
   - Navigieren Sie im Now Platformzu **Alle** > **Self-Service** > **Mein Profil**an.

     Hinweis: Sie können Ihr Profil auch aufrufen, indem Sie im Instanzheader auf Ihren Anwendernamen klicken.



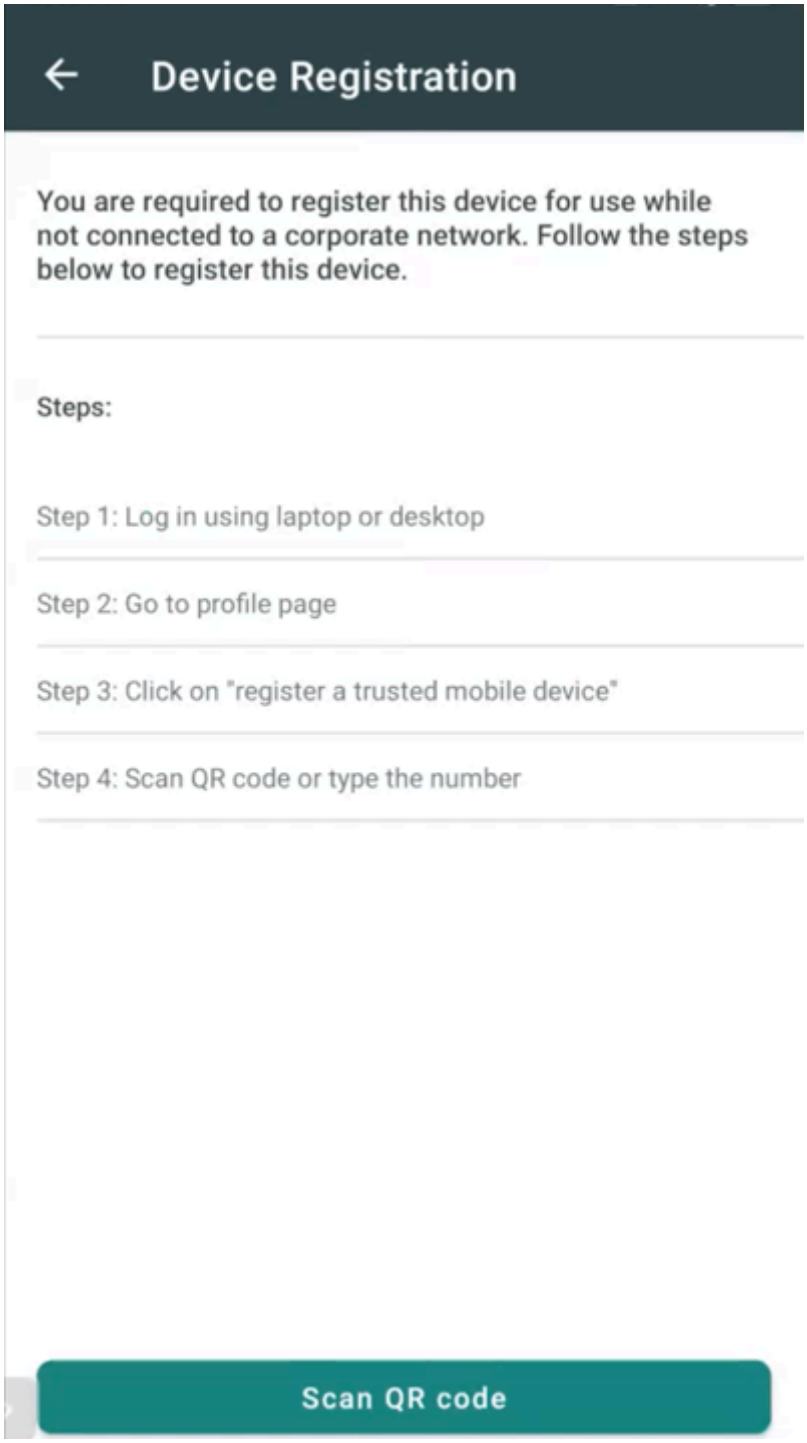
   - Klicken Sie unter Now Supportauf das Profil, und wählen Sie **Vertrauenswürdiges Gerät**aus.
2. Klicken Sie in Ihrem Anwenderprofil im Abschnitt „Zugehörige Links“ **auf Ein vertrauenswürdiges Mobilgerät registrieren**.
   Die Seite „Vertrauenswürdige Geräte registrieren“ wird angezeigt.
3. Registrieren Sie ein neues Gerät, indem Sie auf **Neues vertrauenswürdiges Mobilgerät hinzufügen**klicken.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Tippen Sie im Bildschirm „Geräteregistrierung“ in Ihrer mobilen App ServiceNow auf die Schaltfläche **QR-Code** scannen, und scannen Sie den QR-Code, der auf Ihrem Laptop oder Desktop-Computer angezeigt wird.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

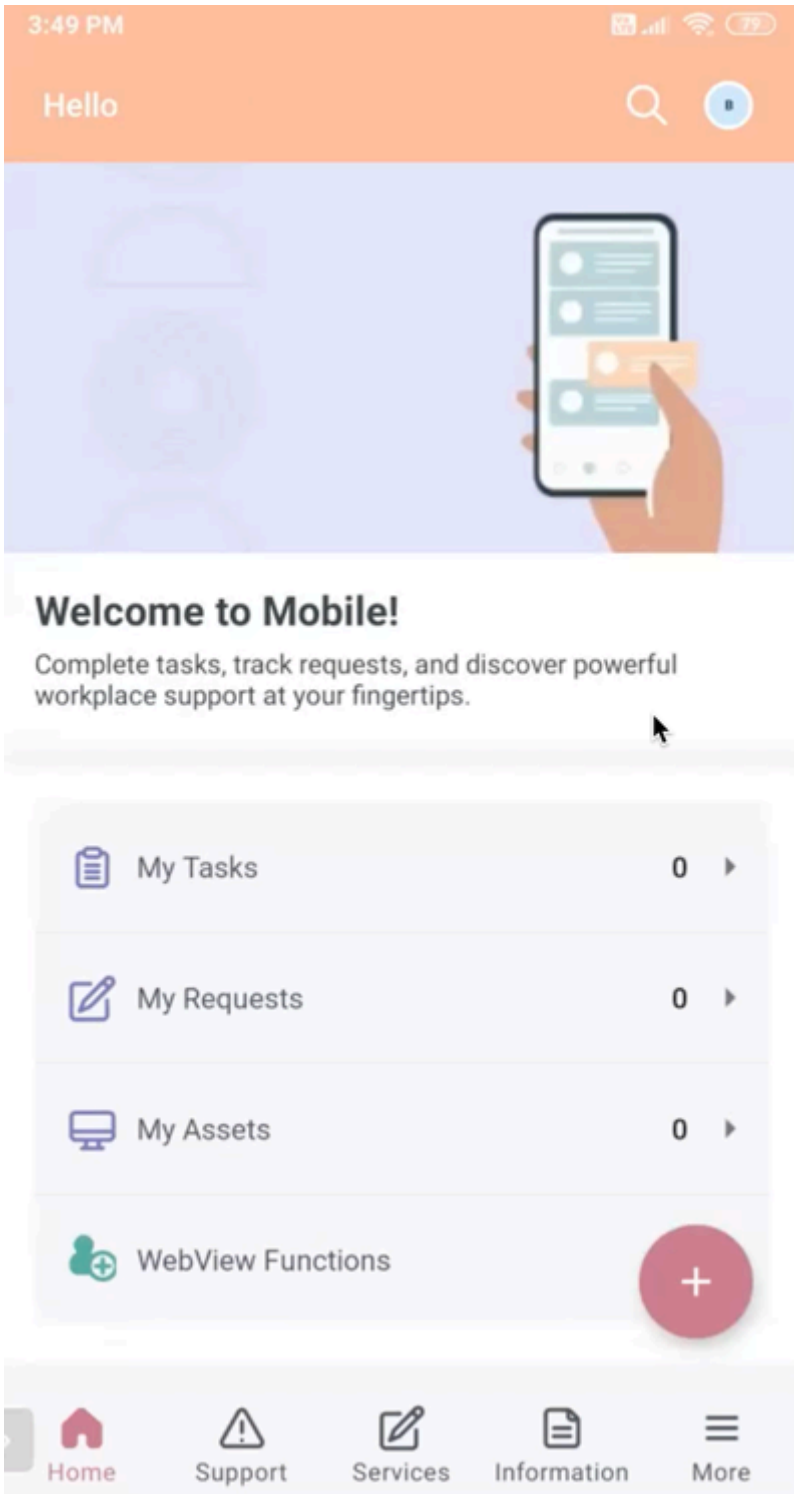


Der Registrierungsprozess wird abgeschlossen, und Sie werden zur Anmeldeseite aufgefordert, um sich zu authentifizieren.

5. Geben Sie Ihre Anmeldeinformationen an, und melden Sie sich bei Now Mobile-Appan.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der mobile Startbildschirm wird angezeigt.



Ergebnisse
Auf der Seite „Vertrauenswürdige Geräte registrieren“ auf Ihrem Laptop oder Desktop-PC wird das registrierte Gerät angezeigt. Sie können das verwenden, wenn Sie das registrierte Gerät von der Seite entfernen möchten.

Nächste Maßnahme
Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Gerätevertrauen** > **Geräteregistrierung** um alle Details des registrierten Geräts anzuzeigen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwalten Sie Ihr vertrauenswürdiges Gerät

Verwalten Sie Ihr vertrauenswürdiges Gerät über die Registrierungsseite für vertrauenswürdige Geräte.

Vorbereitungen

Erforderliche Rolle: keine

Prozedur

1. Navigieren Sie zu einer der folgenden Menüoptionen:
   - Navigieren Sie im Now Platformzu **Alle** > **Self-Service** > **Mein Profil**an.

     Hinweis: Sie können Ihr Profil auch aufrufen, indem Sie im Instanzheader auf Ihren Anwendernamen klicken.

   - Klicken Sie unter Now Supportauf das Profil, und wählen Sie **Vertrauenswürdiges Gerät**aus.
2. Klicken Sie in Ihrem Anwenderprofil im Abschnitt „Zugehörige Links“ auf **Trusted Device registrieren**.
   Die Seite „Vertrauenswürdige Geräte registrieren“ wird angezeigt.
3. Entfernen Sie auf der Seite „Vertrauenswürdige Geräte registrieren“ das Gerät, indem Sie auf das “ klicken.

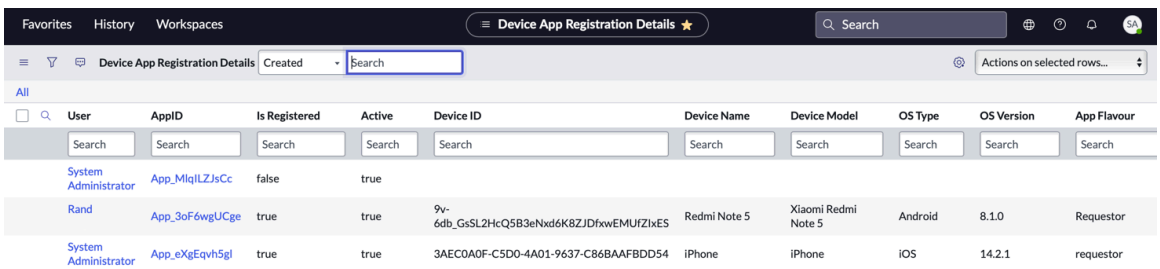
   Hinweis: Das gelöschte Mobilgerät muss erneut registriert werden, um auf die Instanz zugreifen zu können.

Registrierungsdetails von registrierten Geräten

Zeigen Sie die Details von Geräten an, die bei Ihrer Instanz ServiceNow registriert sind.

Um alle Details des bei der Instanz registrierten Geräts anzuzeigen, navigieren Sie zu **Alle** > **Adaptive Authentifizierung** > **Gerätevertrauen** > **Geräteregistrierung**an.

Verwenden Sie den Filter, um das Gerät zu identifizieren. Klicken Sie auf das Feld **AppID**, um mehr über das registrierte Gerät zu erfahren.

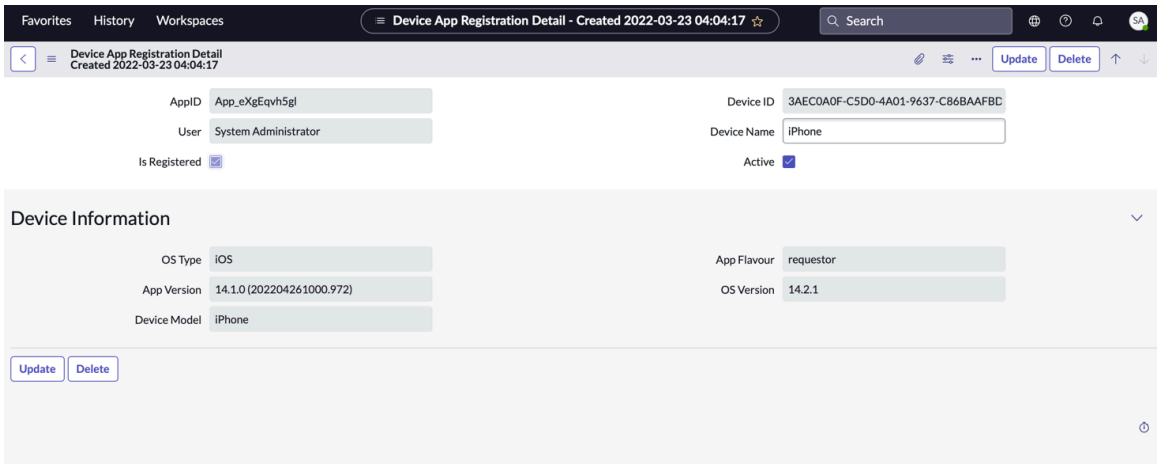


Die folgenden Details werden für das Gerät angezeigt:

- AppID
- Geräte-ID

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Anwender
- Gerätename
- Geräteinformationen wie:
  - BS-Typ
  - App-Variante
  - App-Version
  - BS-Version
  - Gerätemodell



Problembehandlung für vertrauenswürdige mobile App

Überprüfen Sie diese Problembehandlungsszenarien, um Probleme mit der vertrauenswürdigen mobilen App zu beheben.

In den folgenden Abschnitten werden einige Problembehandlungsszenarien und Möglichkeiten zur Problembehandlung beschrieben.

Zeitdifferenz zwischen Instanz und Mobilgerät (Uhrzeitversatz)

Wenn ein Taktversatz vorliegt, können Sie auf Ihrem Mobilgerät die Uhr für die Verwendung des vertrauenswürdigen Geräts anpassen oder zurücksetzen.

QR-Code-Ablauf in fünf Minuten

Der QR-Code für die Funktion „Vertrauenswürdiges Gerät“ läuft innerhalb von fünf Minuten ab. In diesem Fall können Sie auf klicken, um einen neuen QR-Code zu erhalten.

Hinweis: Der Ablauf des QR-Codes kann verlängert werden. Um den Ablauf des Codes zu verlängern, wenden Sie sich an Ihren Administrator.

Systemeigenschaft hat sich geändert

Wenn sich die Systemeigenschaft geändert hat, überprüfen Sie die Registrierung basierend auf der Systemeigenschaft für die gültigen Anmeldeinformationen, die für die Anmeldung verwendet werden können.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Maximale Anzahl registrierter Geräte

Wenn die maximale Anzahl von Geräteregistrierungen erreicht ist, entfernen Sie das vorhandene Gerät, oder wenden Sie sich an Ihren Administrator, um die maximale Geräteanzahl zu ändern.

API-Authentifizierung

Authentifizierungskonfigurationen für API.

Die API-basierte Authentifizierung in ServiceNow® validiert die Identität eines Benutzers, der auf eine -Instanz zugreift, und autorisiert den Benutzer dann für Funktionen, die der Rolle oder Jobfunktion des Benutzers entsprechen, während ein API-Aufruf an die Instanz ServiceNow® durchgeführt wird.

Nachstehend die Arten der API-Authentifizierung in ServiceNow®:

- Zertifikatbasierte Authentifizierung
- OAuth
- Tokenbasierte Authentifizierung

Zertifikatbasierte Authentifizierung

Mit der zertifikatsbasierten Authentifizierung können Sie eingehende API-Anforderungen mithilfe von Zertifikaten einer vertrauenswürdigen Zertifizierungsstelle gegenseitig authentifizieren.

Zertifikatbasierte Authentifizierung für eingehende Webservices

Authentifizieren Sie eingehende Anforderungen bei ServiceNow SOAP- und REST-APIs. Informationen zum Einrichten der gegenseitigen Authentifizierung für eingehende Webservices finden Sie unter Richten Sie die zertifikatbasierte Authentifizierung ein.

OAuth

Die OAuth-basierte Authentifizierung validiert die Identität des Clients, der versucht, mithilfe eines Authentifizierungsprotokolls eine Vertrauensstellung im System herzustellen.

OAuth 2.0 (Offene Autorisierung) ist das Branchenstandardprotokoll für die Autorisierung, das die Client-Entwicklerfreundlichkeit berücksichtigt und gleichzeitig spezifische Autorisierungs-Flows für Webanwendungen, Desktopanwendungen und Mobilgeräte bereitstellt.

Eingang

Erstellen Sie einen Endpunkt für externe Clients, die auf Ihre Instanz zugreifen möchten. Dadurch werden ein OAuth-Client-Anwendungsdatensatz sowie eine Client-ID und ein Clientgeheimnis generiert, die der Client für den Zugriff auf die eingeschränkten Ressourcen in der Instanz benötigt. Weitere Informationen finden Sie unter OAuth Eingehend.

Tokenbasierte Authentifizierung

Tokenbasierte Authentifizierung für die Konfiguration eingehender REST APIs mit API-Schlüssel oder HMAC.

Unterstützen Sie API-Token für REST API-Endpunkte, sodass ServiceNow® für die Anwenderauthentifizierung verwendet wird.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die tokenbasierte Authentifizierung für die Konfiguration eingehender REST APIs kann in der Instanz ServiceNow® mit dem API-Schlüssel oder dem HMAC-Tokendurchgeführt werden.

API-Schlüssel und HMAC-Authentifizierung für eingehende REST APIs

Unterstützen Sie API-Token für REST-API-Endpunkte, sodass der Anwendername und das Passwort des Anwenders ServiceNow® nicht in der Webhook-URL sichtbar sind.

Aktivieren Sie die auf API-Schlüsseln basierende Authentifizierung, um eingehende Webhook-URLs sicher zu authentifizieren.

Zur Verwendung des API-Schlüssels und der HMAC-Authentifizierung müssen Sie (Plugin: `com.glide.tokenbased_auth`) in der Instanz ServiceNow® installieren.

Warnung: Verwenden Sie die **POST** -Anforderung, wenn Sie vertrauliche Informationen an den Server übermitteln.

Die Installation des API-Schlüssels und der HMAC-Authentifizierung sind von den folgenden Plugins abhängig:

- REST API-Authentifizierungsbereich-Plugin (`com.glide.rest.auth.scope`)
- REST API Access Policy Plugin (`com.glide.rest.policy`)
- Authentifizierungsbereich (`com.glide.auth.scope`)

Vorteile

Der API-Schlüssel und die HMAC-Authentifizierung für eingehende REST APIs ermöglichen:

- Möglichkeit zur Angabe des API-Schlüssels oder HMAC-Tokens für die REST-API-Authentifizierung.
- Möglichkeit, ein Benutzeraccount mit dem API-Schlüssel oder HMAC-Token zu verknüpfen.
- Möglichkeit, ein Token als Abfrageparameter oder Header im REST-API-Aufruf anzugeben.
- Möglichkeit, den Authentifizierungsbereich mit API-Schlüssel- oder HMAC-Token-Konfigurationen zu verknüpfen, sodass API-Schlüssel nur zum Aufrufen von APIs verwendet werden können, die bestimmten Bereichen zugeordnet sind.
- Möglichkeit zum Zuordnen eines API-Schlüssels oder einer HMAC-Tokenkonfiguration zu einem Authentifizierungsprofil, das in API-Zugriffsrichtlinien verwendet werden kann.

API-Schlüssel und HMAC-Authentifizierung aktivieren

Sie können das Plugin „API Key and HMAC Authentication“ (`com.glide.tokenbased_auth`) in Ihrer -Instanz ServiceNow® aktivieren.

Vorbereitungen

Erforderliche Rolle: admin.

Prozedur

1. Navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie das Plugin „ API Key and HMAC Authentication “ (`com.glide.tokenbased_auth`) mithilfe der Filterkriterien und der Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: `Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.`

   Nach Abschluss der Installation wird eine Meldung angezeigt.

API-Schlüssel konfigurieren – Tokenbasierte Authentifizierung

Konfigurieren Sie einen API-Schlüssel, um die Authentifizierung für REST API-Endpunkte zu unterstützen.

Vorbereitungen

Erforderliche Rolle: admin

Erforderliches Plugin: API Key und HMAC-Authentifizierung (`com.glide.tokenbased_auth`)

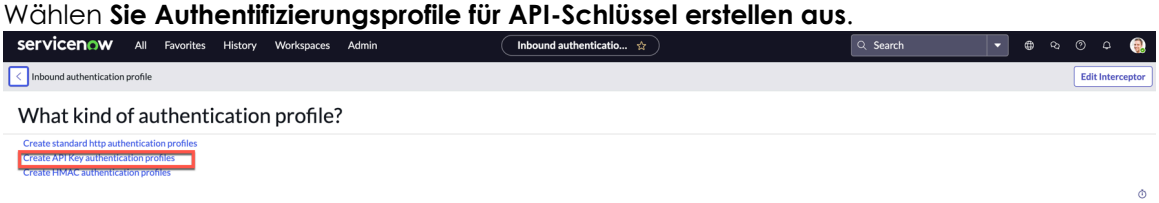
Prozedur

1. Erstellen Sie ein eingehendes Authentifizierungsprofil.

   a. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **Eingehende Authentifizierungsprofile**an.

   b. Wählen Sie **Neu**.
   Das System zeigt die Meldung `Welche Art von Authentifizierungsprofil?`

   c. Wählen **Sie Authentifizierungsprofile für API-Schlüssel erstellen aus**.



   d. Füllen Sie die Felder des Formulars aus.

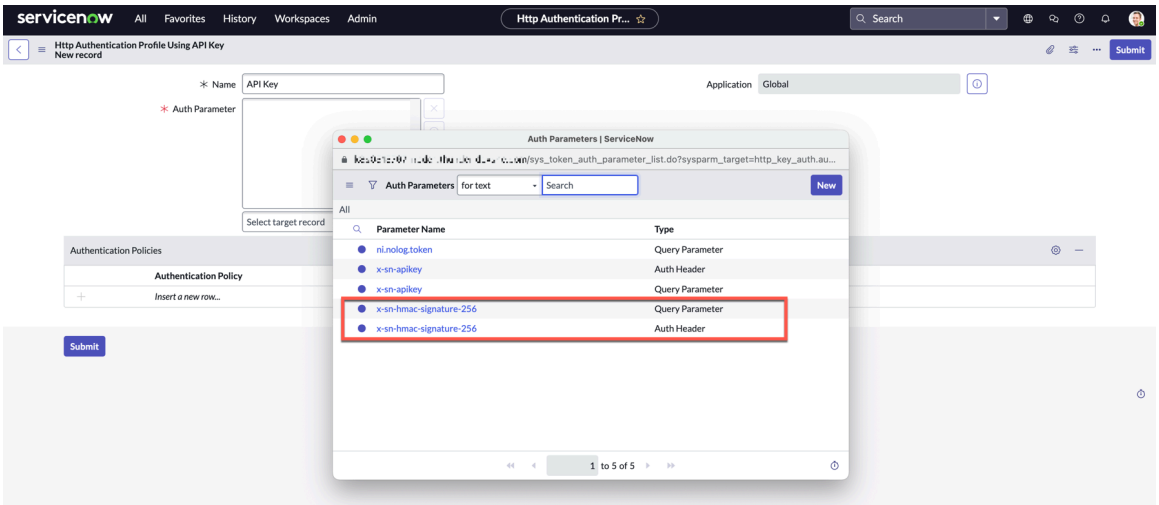
API-Schlüsselauthentifizierungsprofile

Feld	Beschreibung
Name	Name zur Identifizierung der Authentifizierungsrichtlinie.
Anwendung	Geltungsbereich der Authentifizierungsrichtlinie.
Auth-Parameter	Wählen Sie den Authentifizierungsparameter für die Authentifizierungsanforderung aus.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Sie können die Standardoptionen auswählen oder einen neuen Authentifizierungsparameter erstellen: ▪ x-sn-apikey: Auth-Header ▪ x-sn-apikey: Abfrageparameter-Header

Hinweis: Die ausgewählte Option muss im REST-Aufruf als Teil des Auth-Headers oder Abfrageparameters definiert werden.



e. Bestätigen Sie das Formular.

2. Erstellen Sie einen REST-API-Schlüssel.

a. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **REST-API-Schlüssel**an.

b. Wählen Sie **Neu**.

c. Füllen Sie im Formular die folgenden Felder aus:

API-Schlüssel

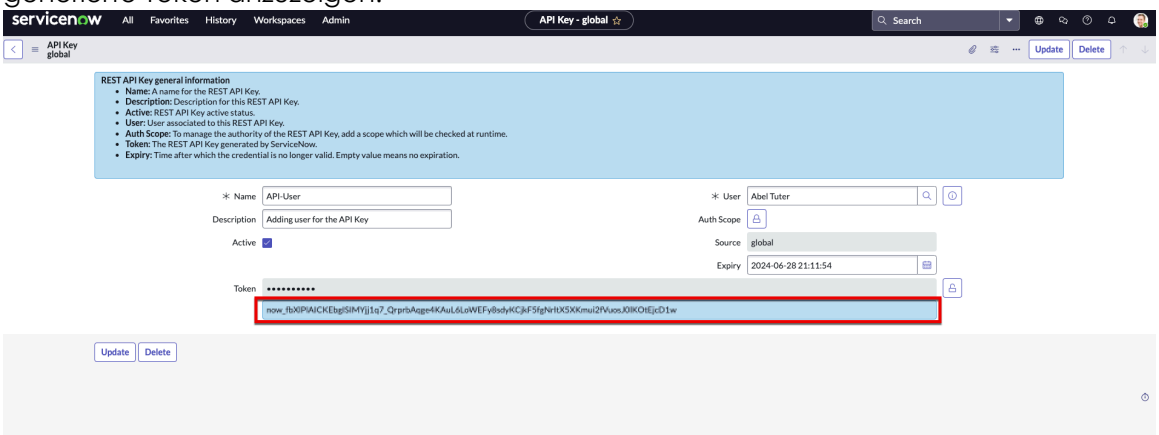
Feld	Beschreibung
Name	Name zur Identifizierung des REST API-Schlüssels
Beschreibung	Beschreibung für den REST API-Schlüssel.
Aktiv	Status des REST API-Schlüssels.
Anwender	Anwender, der dem REST API-Schlüssel zugeordnet ist. Verwenden Sie das Suchsymbol, um den Anwender auszuwählen.
Authentifizierungsbereich	Option zum Hinzufügen des Authentifizierungsbereichs, um die Berechtigung des REST-API-Schlüssels zu verwalten.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Token	Der von Now Platformgenerierte REST-API-Schlüssel. Kopieren Sie den Schlüssel, der als Teil des REST-API-Aufrufs innerhalb des Header- oder Abfrageparameters verwendet werden soll.
Ablauf	Zeitpunkt, nach dem die Anmeldeinformationen nicht mehr gültig sind. Ein leerer Wert bedeutet keinen Ablauf. **Hinweis:** Weitere Informationen zum Ablauf des Tokens finden Sie unter Token-Ablauf bereinigen.

d. Bestätigen Sie das Formular.

e. Öffnen Sie den erstellten Datensatz, um das von Now Platform für den Benutzer generierte Token anzuzeigen.



3. Erstellen Sie eine REST-API-Zugriffsrichtlinie.

a. Navigieren zu **Alle** > **System-Webservices** > **REST API-Zugriffsrichtlinien**an.

b. Wählen Sie **Neu**.

c. Füllen Sie die Felder des Formulars aus.

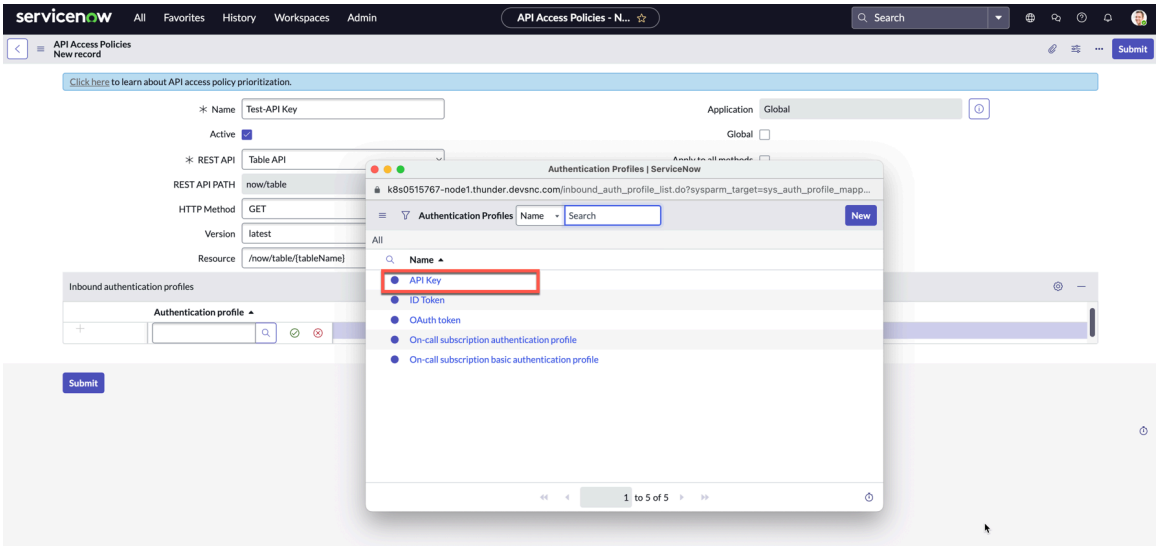
API-Zugriffsrichtlinien

Feld	Beschreibung
Name	Eindeutiger Name der API-Zugriffsrichtlinie.
Aktiv	Option zum Aktivieren der API-Zugriffsrichtlinie.
REST-API	Die REST API, auf die die Zugriffsrichtlinie angewendet wird. Beispiel: **Anhang-API**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
REST-API-PFAD	API-Pfad der REST API. Dieses Feld wird basierend auf der ausgewählten REST API automatisch ausgefüllt. Beispiel: **now/attachment**.
HTTP-Methode	Methode für die Interaktion mit der API. Dieses Feld wird basierend auf der ausgewählten REST API automatisch ausgefüllt.
Version	Version der API. Beispiel: **v1**. Dieses Feld wird basierend auf der ausgewählten REST API automatisch ausgefüllt. **Hinweis:** Wenn Sie eine Authentifizierungsrichtlinie für alle Versionen einer REST API erstellen möchten, müssen Sie für jede Version eine eigene Richtlinie erstellen.
Ressource	Untergeordnete Ressource der REST API. Dieses Feld wird basierend auf der ausgewählten REST API automatisch ausgefüllt. Beispiel: **/now/attachment**
Anwendung	Umfang der Anwendung.
Global	Aktivieren Sie dieses Feld, um die Authentifizierungsrichtlinie auf alle Methoden, Versionen und Ressourcen der API anzuwenden. **Hinweis:** Tokenbasierte Authentifizierung ist in der globalen REST-API-Richtlinie nicht zulässig.
Auf alle Methoden anwenden	Aktivieren Sie dieses Feld, um die Authentifizierungsrichtlinie für die API auf alle Methoden, Versionen und Ressourcen für die API anzuwenden.
Auf alle Ressourcen anwenden	Aktivieren Sie dieses Feld, um die Authentifizierungsrichtlinie für die API auf alle Versionen anzuwenden.
Auf alle Versionen anwenden	Aktivieren Sie dieses Feld, um die Authentifizierungsrichtlinie für die API auf alle Ressourcen anzuwenden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



d. Fügen Sie das erstellte API-Authentifizierungsprofil hinzu.

e. Bestätigen Sie das Formular.

Sie können den REST-API-Aufruf mit dem x-sn-apikey (Token) senden, der von Now Platform während der Erstellung des API-Schlüssels generiert wurde, je nach Konfiguration für die Authentifizierung im Header- oder Abfrageparameter.

> ⚠ **Warnung:** Verwenden Sie die **POST** -Anforderung, wenn Sie vertrauliche Informationen an den Server übermitteln.

HMAC konfigurieren – Tokenbasierte Authentifizierung

Konfigurieren Sie HMAC für die Unterstützung der Authentifizierung für REST API-Endpunkte.

Vorbereitungen

Erforderliche Rolle: admin

Erforderliches Plugin: API Key und HMAC-Authentifizierung (`com.glide.tokenbased_auth`)

Prozedur

1. Erstellen Sie eine HMAC-Konfiguration.

   a. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **HMAC-Konfiguration**an.

   b. Wählen Sie **Neu**.

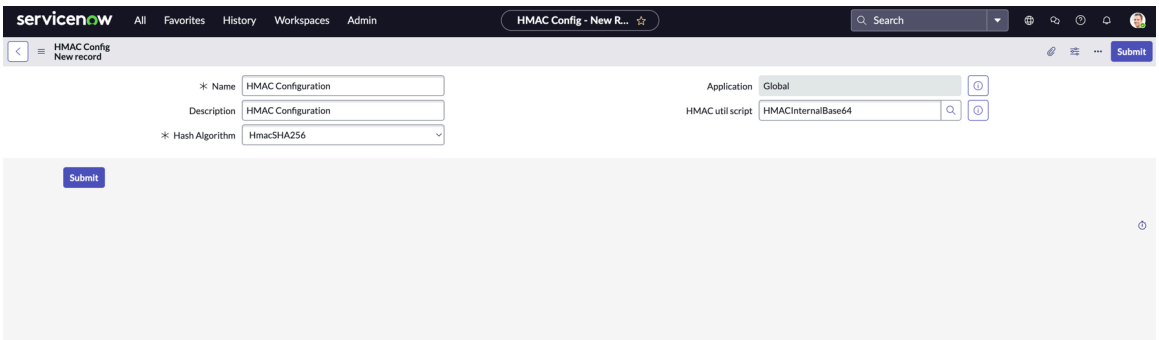
   > ℹ **Hinweis:** Sie können auch die **standardmäßige HMAC-SHA256-Base64-Codierung** verwenden, die bei der Installation des Plugins erstellt wird.

   c. Füllen Sie im Formular die folgenden Felder aus:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

HMAC-Konfiguration

Feld	Beschreibung
Name	Name für die HMAC-Konfiguration.
Anwendung	Umfang der Konfiguration.
Beschreibung	Detaillierte Beschreibung der Konfiguration.
Hash-Algorithmus	Wählen Sie den Hash-Algorithmus aus. Verfügbare Optionen: ▪ HmacSHA256 ▪ HmacSHA384 ▪ HmacSHA512
HMAC-Hilfsskript	Dienstprogrammskript für HMAC. **Hinweis:** Wenn Sie die HMAC-Authentifizierung mit Anforderungstext, Zeitstempel und Geheimnis ohne Schlüssel-ID validieren, gehen Sie wie folgt vor: ▪ Erstellen Sie eine anwenderdefinierte Skripteinbindung als HMAC-Hilfsskript ▪ Verwenden Sie dieses Skripteinbindungs-Dienstprogramm, um den übergebenen Zeitstempel und den Anforderungstext zu interpretieren. Für jedes in der Instanz ServiceNow® erstellte gemeinsame Geheimnis gibt es eine Schlüssel-ID. Sie müssen die Schlüssel-ID im HMAC-Authentifizierungsprofil als Standardschlüssel-ID konfigurieren.



d. Senden Sie den Datensatz ab.

Automatische Übersetzung

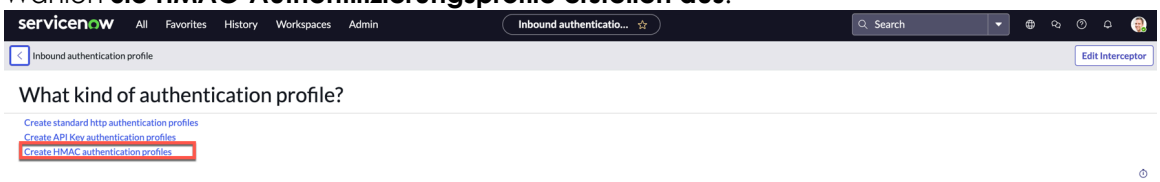
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Erstellen Sie ein eingehendes Authentifizierungsprofil.

a. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **Eingehende Authentifizierungsprofile**an.

b. Wählen Sie **Neu**.
Das System zeigt die Meldung `Welche Art von Authentifizierungsprofil?`

c. Wählen **Sie HMAC-Authentifizierungsprofile erstellen aus**.



d. Füllen Sie die Felder des Formulars aus.

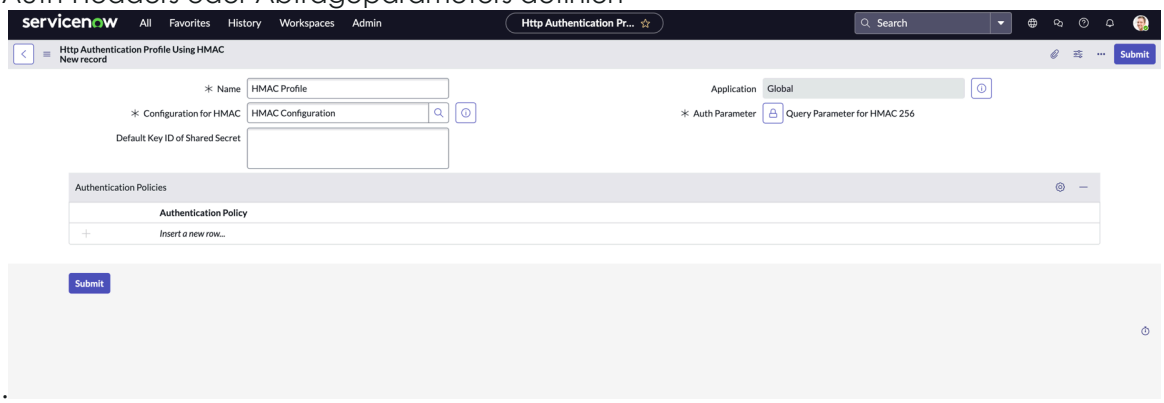
HMAC-Authentifizierungsprofile

Feld	Beschreibung
Name	Name zur Identifizierung der Authentifizierungsrichtlinie.
Anwendung	Geltungsbereich der Authentifizierungsrichtlinie.
Konfiguration für HMAC	Wählen Sie die erstellte HMAC-Konfiguration aus.
Auth-Parameter	Wählen Sie den Authentifizierungsparameter für die Authentifizierungsanforderung aus. Sie können die Standardoptionen auswählen oder einen neuen Authentifizierungsparameter erstellen: ▪ x-sn-hmac-signature-256: Auth-Header ▪ x-sn-hmac-signature-256: Abfrageparameter
Standardschlüssel-ID des gemeinsamen Geheimnisses	Die Tokeninformationen, die in diesem Feld für die Verwendung von HMAC aktualisiert werden können.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Die ausgewählte Option muss im REST-Aufruf als Teil des Auth-Headers oder Abfrageparameters definiert werden.



e. Bestätigen Sie das Formular.

3. Erstellen Sie ein HMAC-Geheimnis.

a. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **REST-API-HMAC-Geheimnis**an.

b. Wählen Sie **Neu**.

c. Füllen Sie im Formular die folgenden Felder aus:

REST-API-HMAC-Geheimnis

Feld	Beschreibung
Name	Name zur Identifizierung des REST API-HMAC-Geheimnisses.
Beschreibung	Beschreibung für das REST API-HMAC-Geheimnis.
Aktiv	Status des REST API-HMAC-Geheimnisses.
Anwender	Anwender, der dem REST API-HMAC-Geheimnis zugeordnet ist. Verwenden Sie das Suchsymbol, um den Anwender auszuwählen.
Schlüssel-ID	Schlüssel-ID, die als Teil des REST-Aufrufs gesendet werden muss. Die Schlüssel-ID wird nach dem Senden des Formulars generiert.
Gemeinsames Geheimnis	Gemeinsame Geheimnisse des Anwenders. Zum Beispiel das Passwort.
Quelle	Quelle des Datensatzes.
Ablauf	Zeitpunkt, nach dem die Anmeldeinformationen nicht mehr gültig sind. Ein leerer Wert bedeutet keinen Ablauf.

Automatische Übersetzung

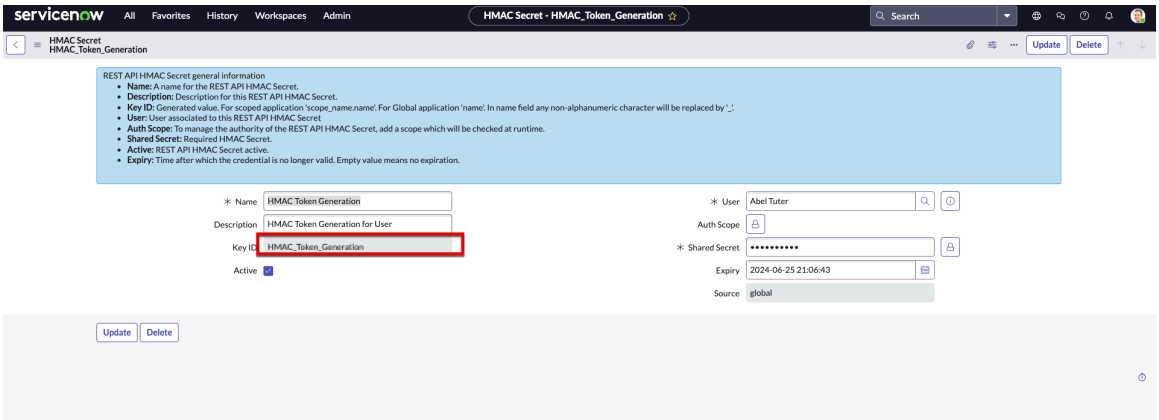
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Weitere Informationen zum Ablauf des Tokens finden Sie unter Token-Ablauf bereinigen.

d. Bestätigen Sie das Formular.

e. Öffnen Sie den erstellten Datensatz.

Suchen Sie die von Now Platform für den Anwender generierte Schlüssel-ID.



Hinweis: Sie können die Schlüssel-ID hinzufügen, die während der Schlüssel-ID in dem für HMAC erstellten Authentifizierungsprofil generiert wurde, wenn Sie den Auth- oder Query-Parameter für den API-Aufruf nicht angeben möchten.

4. Erstellen Sie eine REST-API-Zugriffsrichtlinie.

a. Navigieren zu **Alle** > **System-Webservices** > **REST API-Zugriffsrichtlinien**an.

b. Wählen Sie **Neu**.

c. Füllen Sie die Felder des Formulars aus.

API-Zugriffsrichtlinien

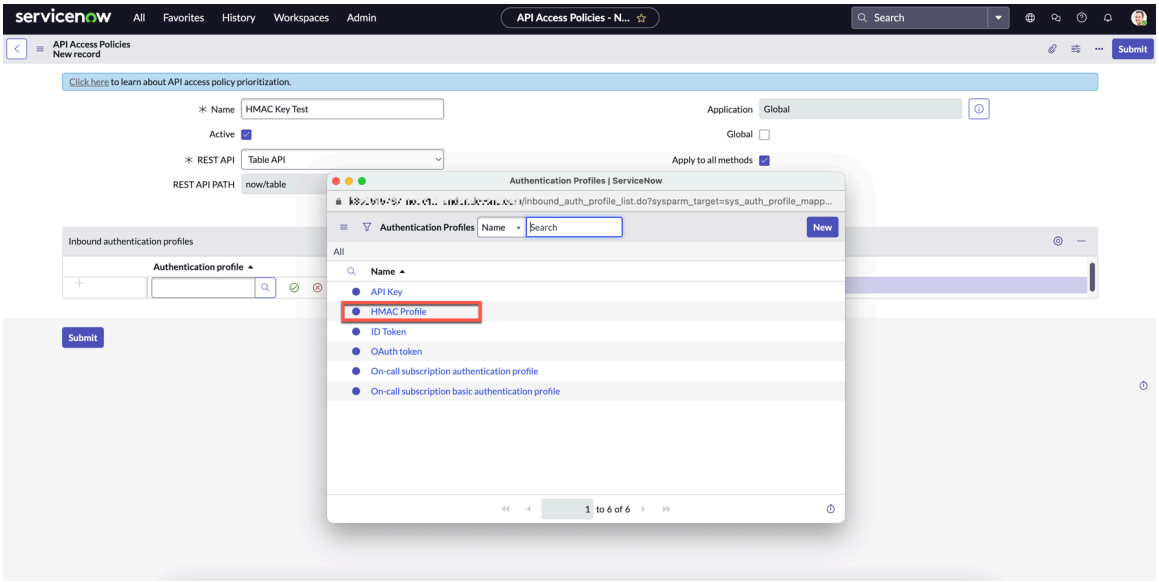
Feld	Beschreibung
Name	Eindeutiger Name der API-Zugriffsrichtlinie.
Aktiv	Option zum Aktivieren der API-Zugriffsrichtlinie.
REST-API	Die REST API, auf die die Zugriffsrichtlinie angewendet wird. Beispiel: **Anhang-API**.
REST-API-PFAD	API-Pfad der REST API. Dieses Feld wird basierend auf der ausgewählten REST API automatisch ausgefüllt. Beispiel: **now/attachment**.
HTTP-Methode	Methode für die Interaktion mit der API. Dieses Feld wird basierend auf der

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	ausgewählten REST API automatisch ausgefüllt.
Version	Version der API. Beispiel: **v1**. Dieses Feld wird basierend auf der ausgewählten REST API automatisch ausgefüllt. **Hinweis:** Wenn Sie eine Authentifizierungsrichtlinie für alle Versionen einer REST API erstellen möchten, müssen Sie für jede Version eine eigene Richtlinie erstellen.
Ressource	Untergeordnete Ressource der REST API. Dieses Feld wird basierend auf der ausgewählten REST API automatisch ausgefüllt. Beispiel: **/now/attachment**
Anwendung	Umfang der Anwendung.
Global	Aktivieren Sie dieses Feld, um die Authentifizierungsrichtlinie auf alle Methoden, Versionen und Ressourcen der API anzuwenden. **Hinweis:** Tokenbasierte Authentifizierung ist in der globalen REST-API-Richtlinie nicht zulässig.
Auf alle Methoden anwenden	Aktivieren Sie dieses Feld, um die Authentifizierungsrichtlinie für die API auf alle Methoden, Versionen und Ressourcen für die API anzuwenden.
Auf alle Ressourcen anwenden	Aktivieren Sie dieses Feld, um die Authentifizierungsrichtlinie für die API auf alle Versionen anzuwenden.
Auf alle Versionen anwenden	Aktivieren Sie dieses Feld, um die Authentifizierungsrichtlinie für die API auf alle Ressourcen anzuwenden.

d. Fügen Sie das erstellte API-Authentifizierungsprofil hinzu.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



e. Bestätigen Sie das Formular.
Sie können den REST-API-Aufruf wie folgt senden:

- Mit x-sn-hmac-signature-256, die von ServiceNow® während der Erstellung des API-Schlüssels im Header- oder Abfrageparameter basierend auf der Konfiguration für die Authentifizierung generiert wurde.
- Mit Voranforderungsskript und gemeinsamem Geheimnis, das als Teil der Anforderung angegeben ist.

> ⚠ **Warnung:** Verwenden Sie die **POST** -Anforderung, wenn Sie vertrauliche Informationen an den Server übermitteln.

Token-Ablauf bereinigen

Details zum Bereinigen des Tokenablaufs mithilfe verschiedener Systemeigenschaften.

Sobald der API-Schlüssel oder das HMAC-Geheimnis abläuft, werden die Details 7 Tage lang gespeichert. Eine geplante Aufgabe „`Abgelaufene Anmeldeinformationen für Token-Authentifizierung bereinigen`“ löscht anschließend die abgelaufenen API-Schlüssel oder HMAC-Geheimnisse. Sie können dieses Verhalten konfigurieren und die Löschung mithilfe der folgenden Eigenschaften steuern:

- **com.snc.platform.security.token.auth.cleanup**: Verwenden Sie diese Eigenschaft, wenn Sie abgelaufene API-Schlüssel und HMAC-Token löschen möchten. Standardmäßig `true`.
- **com.snc.platfrom.security.token.auth.days.expired.api_key.is.kept**: Legen Sie den Wert basierend auf Ihren Anforderungen fest, um die Anzahl der Tage zu bestimmen, für die das abgelaufene `API` -Token im System aufbewahrt werden soll. Standardmäßig 7.
- **com.snc.platfrom.security.token.auth.days.expired.hmac_key.is.kept**: Legen Sie den Wert basierend auf Ihren Anforderungen fest, um die Anzahl der Tage zu bestimmen, für die das abgelaufene `HMAC` -Token im System aufbewahrt werden soll. Standardmäßig 7.

Um zur Eigenschaft „Tokenablauf“ zu navigieren, geben Sie in der Navigationsleiste `sys.trigger.list` ein, und suchen Sie dann nach den folgenden Eigenschaften. Ändern Sie den Ablauf entsprechend Ihren Anforderungen.

API-Zugriffsrichtlinie

Die API-Zugriffsrichtlinie definiert die Berechtigungen und die Dauer des Zugriffs auf eine API.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit der API-Zugriffsrichtlinie können Sie den Zugriff auf eingehende ServiceNow® APIs basierend auf dem Authentifizierungstyp und den angegebenen Filterkriterien der Zugriffsrichtlinie einschränken.

Im Folgenden finden Sie die Unterstützung von drei Authentifizierungsrichtlinien für nicht interaktive Sitzungen:

- **REST API**: Der Administrator kann eine globale API-Authentifizierungsrichtlinie oder eine API-spezifische Authentifizierungsrichtlinie definieren.
- **SOAP-API**: Der Administrator kann eine globale API-Authentifizierungsrichtlinie oder eine API-spezifische Authentifizierungsrichtlinie definieren.
- **System-/Exportprozessor**: Der Administrator kann fünf Basissystem-Authentifizierungsprofile definieren, die verwendet werden können, um das Authentifizierungsprofil auf die API-Authentifizierungsrichtlinie oder die prozessorspezifische Authentifizierungsrichtlinie anzuwenden.

Hinweis: Wenn Sie eine globale Authentifizierungsrichtlinie hinzufügen, gilt die Richtlinie für alle REST APIs, SOAP APIs oder System-/Exportprozessoren.

Im Folgenden finden Sie die automatisch installierten Plugins für API-Richtlinien und Authentifizierungsbereich:

- com.glide.rest.policy
- com.glide.soap.policy
- com.glide.processor.policy
- com.glide.rest.auth.scope

Sie können die standardmäßige globale Blockierungsrichtlinie konfigurieren oder eine anwenderdefinierte API-Zugriffsrichtlinie gemäß Ihren Sicherheitsanforderungen erstellen. Und wenden Filterkriterien an, die Filterbedingungen oder Abfragen enthalten, die als Richtlinieneingaben für eine Authentifizierungsrichtlinie verwendet werden.

Die folgenden API-Zugriffsrichtlinien werden in ServiceNow®unterstützt:

- REST API-Zugriffsrichtlinien
- Zugriffsrichtlinien für SOAP-API

Informationen zu Richtlinien im Zusammenhang mit Exportprozessoren finden Sie unter Zugriffsrichtlinie für System-/Exportprozessoren.

REST API-Zugriffsrichtlinien

Mit REST-API-Zugriffsrichtlinien können Sie den Zugriff auf eingehende REST-APIs basierend auf dem Authentifizierungstyp und den angegebenen Filterkriterien der Zugriffsrichtlinie einschränken.

Eine REST API, auch bekannt als RESTful API, ist eine Art von Anwendungsprogrammierschnittstelle (API), die den Richtlinien des REST-Architekturstils entspricht. REST APIs bieten ein hohes Maß an Flexibilität und sind daher im gesamten Web verbreitet.

Filterkriterien enthalten Filterbedingungen oder Abfragen, die als Richtlinieneingaben für eine Authentifizierungsrichtlinie verwendet werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können die standardmäßige globale Blockierungsrichtlinie konfigurieren oder eine anwenderdefinierte API-Zugriffsrichtlinie gemäß Ihren Sicherheitsanforderungen erstellen. Sie können beispielsweise eine anwenderdefinierte API-Zugriffsrichtlinie erstellen, die nur den Authentifizierungstyp OAuth 2.0 aus einem angegebenen Bereich von IP-Adressen zulässt. Authentifizierungsanforderungen anderer Authentifizierungstypen und Zugriffsanforderungen von anderen IP-Adressen als den angegebenen IP-Adressen werden abgelehnt.

Aktivieren Sie die REST-API-Zugriffsrichtlinie

Sie können das Plugin „ REST API Access Policy“ (com.glide.rest.policy) aktivieren, wenn Sie die Administratorrolle innehaben. Die Anwendung enthält Demodaten und installiert zugehörige ServiceNow® Store-Anwendungen und Plugins, sofern sie nicht bereits installiert sind.

Vorbereitungen
Erforderliche Rolle: admin.

Warum und wann dieser Vorgang ausgeführt wird
Die folgenden Elemente werden mit der REST-API-Zugriffsrichtlinieinstalliert:

- Plugins: com.gilde.auth.profile, com.snc.adaptive_authentication, com.snc.platform.security.oauth
- Tabellen: sys_api_access_policy, sys_auth_profile_mapping, auth_policy_mapping, inbound_auth_profile, std_http_auth.

Weitere Informationen finden Sie unter Adaptive Authentifizierung.

Prozedur

1. Navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie das Plugin „ REST API Access Policy“ (com.glide.rest.policy) mithilfe der Filterkriterien und der Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: `Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.`

   Nach Abschluss der Installation wird eine Meldung angezeigt.

Erstellen Sie ein Authentifizierungsprofil

Erstellen Sie ein Authentifizierungsprofil, und fügen Sie dem Profil eine oder mehrere Authentifizierungsrichtlinien hinzu. Sie können auch die standardmäßig verfügbaren Authentifizierungsprofile für **ID-Token** und **OAuth-Token** konfigurieren.

Vorbereitungen
Erforderliche Rolle: admin

Hinweis: Sie können Authentifizierungsrichtlinien, IP-Bereiche, rollenbasierte, anwenderbasierte usw. mit gegenseitiger Authentifizierung und anwenderdefinierter Authentifizierung anwenden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **Eingehende Authentifizierungsprofile**an.
2. Wählen Sie **Neu**.
   Das System zeigt die Nachricht an. `Welche Art von Authentifizierungsprofil?`
3. Wählen **Sie Standard-HTTP-Authentifizierungsprofile erstellen aus**.
4. Füllen Sie die Felder des Formulars aus.

Formular „Standardauthentifizierungsprofil“.

Feld	Beschreibung
Name	Name zur Identifizierung der Authentifizierungsrichtlinie.
Beschreibung	Beschreibung der Authentifizierungsrichtlinie.
Aktiv	Option zum Aktivieren der Authentifizierungsrichtlinie.
Anwendung	Geltungsbereich der Authentifizierungsrichtlinie.
Typ	Typ der verfügbaren Authentifizierung. Sie können **Basisauthentifizierung**, **ID-Token**, **Zertifikatbasierte Authentifizierung**oder **OAuth**auswählen.
OAuth-Entität	OAuth-Entitätsprofil. Dieses Feld wird nur angezeigt, wenn **ID-Token** oder **OAuth** als **Typ**ausgewählt wird.

5. Doppelklicken Sie auf **Neue Zeile einfügen**.
6. Wählen Sie eine Authentifizierungsrichtlinie aus der Liste aus, und wählen Sie das Speichern-Symbol .

Hinweis: Wählen Sie nicht die Option „Zugriffsrichtlinie zulassen“ oder „Zugriffsrichtlinie verweigern“ aus. Diese Richtlinien sind nur für Anwenderanmeldungen vorgesehen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können eine oder mehrere Authentifizierungsrichtlinien für ein Authentifizierungsprofil hinzufügen.

Hinweis:

Header authentifizieren [WWW-Authenticate].

Wenn die REST-API-Zugriffsrichtlinie aktiv ist, wird das zuletzt zugeordnete Authentifizierungsprofil im Authentifizierungsheader zurückgegeben. Wenn der Server alle Authentifizierungsschemata zurückgeben soll, verwenden Sie die Eigenschaft `glide.security.response.authenticate.header.auth_profile.first_scheme_only`, und legen Sie sie auf **false**fest. Die Antwort wird mit mehreren Headern zurückgegeben. Beispiel:

```
< WWW-Authenticate: BEARER realm="Service-now"
< WWW-Authenticate: BASIC realm="Service-now"
```

Erstellen Sie eine REST-API-Zugriffsrichtlinie

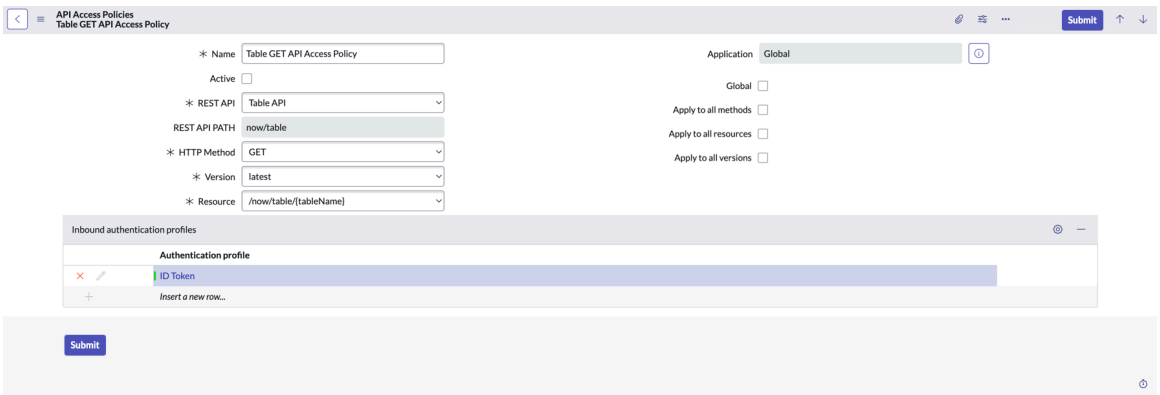
Erstellen Sie eine API-Zugriffsrichtlinie, und ordnen Sie ein Authentifizierungsprofil zu, um den Authentifizierungstyp für eine REST API einzuschränken. Sie können beispielsweise eine API-Zugriffsrichtlinie erstellen, die nur die ID-Token-Authentifizierung für eine REST API zulässt.

Vorbereitungen

- Erforderliche Rolle: admin
- Stellen Sie sicher, dass ein Authentifizierungsprofil erstellt wird. Weitere Informationen finden Sie unter Authentifizierungsprofile erstellen.

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **REST API-Zugriffsrichtlinien**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.



API-Zugriffsrichtlinien

Feld	Beschreibung
Name	Eindeutiger Name der API-Zugriffsrichtlinie.
Aktiv	Option zum Aktivieren der API-Zugriffsrichtlinie.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
REST-API	Die REST API, auf die die Zugriffsrichtlinie angewendet wird. Beispiel: **Anhang-API**.
REST-API-PFAD	API-Pfad der REST API. Dieses Feld wird basierend auf der ausgewählten REST API automatisch ausgefüllt. Beispiel: **now/attachment**.
HTTP-Methode	Methode für die Interaktion mit der API. Dieses Feld wird basierend auf der ausgewählten REST API automatisch ausgefüllt.
Version	Version der API. Beispiel: **v1**. Dieses Feld wird basierend auf der ausgewählten REST API automatisch ausgefüllt. **Hinweis:** Wenn Sie eine Authentifizierungsrichtlinie für alle Versionen einer REST API erstellen möchten, müssen Sie für jede Version eine eigene Richtlinie erstellen.
Ressource	Untergeordnete Ressource der REST API. Dieses Feld wird basierend auf der ausgewählten REST API automatisch ausgefüllt. Beispiel: **/now/attachment**
Anwendung	Umfang der Anwendung.
Global	Aktivieren Sie diese Option, um die Authentifizierungsrichtlinie auf alle Methoden, Versionen und Ressourcen der API anzuwenden.
Auf alle Methoden anwenden	Aktivieren Sie diese Option, um die Authentifizierungsrichtlinie für die API auf alle Methoden, Versionen und Ressourcen für die API anzuwenden.
Auf alle Ressourcen anwenden	Aktivieren Sie diese Option, um die Authentifizierungsrichtlinie für die API auf alle Versionen anzuwenden.
Auf alle Versionen anwenden	Aktivieren Sie diese Option, um die Authentifizierungsrichtlinie für die API auf alle Ressourcen anzuwenden.

Hinweis: Weitere Informationen zur Priorisierung von API-Zugriffsrichtlinien finden Sie unter Priorisierung von API-Zugriffsrichtlinien.

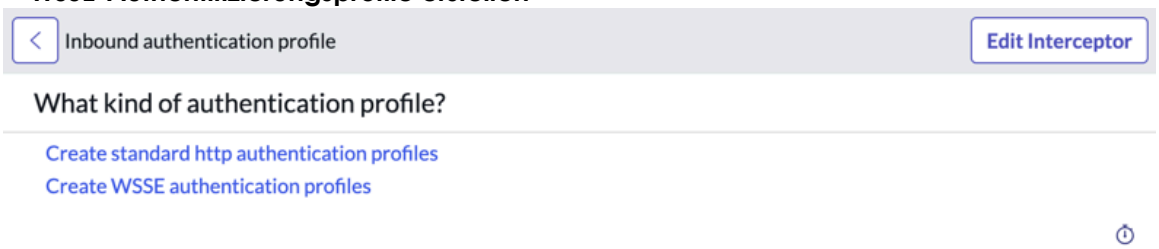
4. Doppelklicken Sie auf **Neue Zeile einfügen**.
5. Wählen Sie ein eingehendes Authentifizierungsprofil aus der Liste aus, und klicken Sie auf das Speichern-Symbol .
   Sie können beispielsweise Basisauthentifizierung, **ID-Token**, **zertifikatsbasierte**Authentifizierung, **OAuth**oder **WSSE-Authentifizierung hinzufügen**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie zum Hinzufügen eines oder mehrerer eingehender Authentifizierungsprofile auf **Neu**, um ein neues Profil zu erstellen.

b. Welche Art von Authentifizierungsprofilen auswählen?.

- **Standardmäßiges http-Authentifizierungsprofil erstellen**
- **WSSE-Authentifizierungsprofile erstellen**



c. Speichern Sie den Datensatz, nachdem Sie das Authentifizierungsprofil erstellt haben.

6. Klicken Sie auf **Absenden**, um die REST-API-Zugriffsrichtlinie zu übermitteln.

Priorisierung von API-Zugriffsrichtlinien

Erfahren Sie mehr über die Richtlinienpriorisierungslogik, wenn für Ihre Instanz ServiceNow® mehrere API-Zugriffsrichtlinien konfiguriert sind.

API-Zugriffsrichtlinien werden basierend auf dem Typ des REST-API-Richtliniensatzes in Ihrer Instanz ServiceNow® priorisiert.

Der Ansatz besteht darin, für jeden Teil der API unterschiedliche Gewichtungen zu definieren, z. B. Methode, Ressource und Version.

Die API-Richtlinie wird zuerst für nicht-globale und dann für globale priorisiert. Mit anderen Worten: Eine nicht globale Zugriffsrichtlinie überschreibt immer eine globale API-Zugriffsrichtlinie.

Die Priorisierungslogik lautet wie folgt:

Priorisierung

Felder	Priorität	Priorisierungslogik
Methode, Ressource und Version	1	Wenn die 3 Felder mit der Richtlinie übereinstimmen,

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Priorisierung (Fortsetzung)

Felder	Priorität	Priorisierungslogik
		hat diese Richtlinie die 1. Priorität.
Methode+Ressource	2	Wenn die beiden Felder mit der Richtlinie übereinstimmen, hat diese Richtlinie die 1. Priorität.
Ressource + Version	3	Wenn die Felder 2 zusammen mit dem Feld Auf **alle Methoden anwenden** mit der Richtlinie übereinstimmen, hat diese Richtlinie die 3. Priorität.
Ressource	4	Wenn das Feld zusammen mit dem Feld Auf **alle Methoden anwenden** mit der Richtlinie übereinstimmt, hat diese Richtlinie die 4. Priorität.
Methode + Version	5	Wenn die Felder 2 zusammen mit dem Feld Auf **alle Ressourcen anwenden** mit der Richtlinie übereinstimmen, hat diese Richtlinie die 5. Priorität.
Methode	6	Wenn das Feld zusammen mit dem Feld Auf **alle Ressourcen anwenden** mit der Richtlinie übereinstimmt, hat diese Richtlinie die 5. Priorität.
Version	7	Wenn das Feld zusammen mit den Feldern Auf **alle Methodenanwenden und Auf alle Versionen anwenden** mit der Richtlinie übereinstimmt, hat diese Richtlinie die 7. Priorität.
Global und Auf alle Methoden anwenden	8	Wenn in den Feldern „ **Global** “ der Wert „ `wahr` “ und **„Auf alle Methoden anwenden** “ der Wert „ `falsch` “ festgelegt ist, hat diese Richtlinie die 8. Priorität.
Global und Auf alle Methoden anwenden	9	Wenn in den Feldern „ **Global** “ der Wert „ `wahr` “ und **„Auf alle Methoden anwenden** “ der Wert „ `wahr` “ festgelegt ist, erhält diese Richtlinie die 9. Priorität.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

REST-API-Authentifizierungsbereich

Unterstützung des Authentifizierungsbereichs für die REST API.

Vor dem Release Xanadu ist jedes Zugriffstoken oder OIDC-Token mit dem Anwendungsbereich useraccount verknüpft, der vollständigen Zugriff auf die REST APIs des Benutzers hat. Ab Release Xanadu werden die OAuth-Token-Bereiche eingeführt, um Zugriff nur auf bestimmte REST APIs zu gewähren.

Wenn eine OAuth-Entität mit einem Authentifizierungsbereich verknüpft ist, wird das Token von dieser OAuth-Entität ausgegeben oder verwaltet und kann nur für den Zugriff auf die REST APIs verwendet werden (eine OAuth-Entität kann mit mehreren Authentifizierungsbereichen verknüpft sein). Für die neue OAuth-Entität ist der standardmäßige Auth-Bereich leer. Sie müssen den Auth-Bereich manuell mit der OAuth-Entität verknüpfen.

Hinweis:

- Nachdem der REST-API-Authentifizierungsbereich aktiviert und dem Authentifizierungsbereich für die REST-API hinzugefügt wurde, können alle vorhandenen OAuth-Token nicht mehr auf diese API zugreifen, es sei denn, der Administrator fügt diesen Authentifizierungsbereich der entsprechenden OAuth-Entität hinzu
- Der Administrator ist dafür verantwortlich, dass „oauth_entity“ nach dem über den richtigen Authentifizierungsbereich verfügt, um den Authentifizierungsbereich mit der REST-API zu verknüpfen.
- Von ServiceNow ausgegebene OAuth-Zugriffstoken unterstützen den Authentifizierungsbereich.
- OIDC-Token, das nicht von [] ausgestellt wurde, wird von ServiceNowServiceNow validiert.
- Das OIDC-Token hat seinen Bereich von IDP, wenn Sie ein ID-Token benötigen. Hier gilt der Authentifizierungsbereich für ServiceNow anstelle von Drittpartei (IdP).

Konfigurationen für den REST-API-Bereich

Führen Sie zum Konfigurieren des REST-API-Bereichs die folgenden Aufgaben aus:

- Erstellen Sie einen Authentifizierungsbereich
- Verknüpfen Sie den Authentifizierungsbereich mit der REST API
- Authentifizierungsbereich mit OAuth-Entität verknüpfen
- Führen Sie den OAuth-Flow aus, um das OAuth-Zugriffstoken zu erhalten
- Verwenden Sie das OAuth-Zugriffstoken, um den API-Aufruf durchzuführen

Aktivieren Sie den REST API-Authentifizierungsbereich

Sie können das Plugin „REST API Auth Scope“ (com.glide.rest.auth.scope) aktivieren, um die OAuth-Entität mit Authentifizierungsbereichen zu verknüpfen.

Vorbereitungen

Installieren Sie die folgenden Plugins:

- OAuth 2.0
- REST API-Anbieter

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Authentifizierungsbereich
- REST API-Bereich

Hinweis: Das Plugin *REST API Scope* wird als Teil des Release Tokyo] hinzugefügt.

Erforderliche Rolle: admin

Prozedur

1. Navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie das Plugin „REST-API-Authentifizierungsbereich“ (*com.glide.rest.auth.scope*) mithilfe der Filterkriterien und der Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: `Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.`

   Nach Abschluss der Installation wird eine Meldung angezeigt.

Eigenschaften und Tabellen des REST API-Authentifizierungsbereichs

Das Plugin „REST API Auth Scope“ (com.glide.rest.auth.scope) enthält die folgenden Systemeigenschaften, Tabellen und Skripts.

Eigenschaften des REST-API-Authentifizierungsbereichs

REST API-Authentifizierungsbereich fügt die folgenden Systemeigenschaften hinzu.

Eigenschaften

Name	Beschreibung
com.glide.rest.api.auth.scope.check.enable	Diese Eigenschaft wird verwendet, um die Umfangsprüfung der Authentifizierung auf Plattformebene zu deaktivieren. Bei Festlegung auf „falsch“ wird während der Laufzeit die Überprüfung des Authentifizierungsbereichs übersprungen, unabhängig davon, ob er mit der RETS-API verknüpft ist oder nicht. Standardmäßig ist diese Eigenschaft auf „true“ festgelegt. Diese Eigenschaft wird verwendet, wenn Sie zum vorherigen Release-Verhalten zurückkehren möchten.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften (Fortsetzung)

Name	Beschreibung
com.glide.oauth.token.scope.useraccount	Diese Eigenschaft wird nur verwendet, wenn der Authentifizierungsbereich *useraccount* gelöscht und vom Endanwender manuell wieder hinzugefügt wird. In diesem Fall wird die Sys-ID für *useraccount* geändert. Diese Eigenschaft muss auf die neue sys_id aktualisiert werden. Während der Laufzeit wird anstelle des Namens des Authentifizierungsbereichs die Sys-ID des Authentifizierungsbereichs verwendet.

REST API-Authentifizierungsbereichstabellen

REST API-Authentifizierungsbereich für die folgenden Tabellen.

Tabellen

Name	Beschreibung
Authentifizierungsbereich (sys_auth_scope)	Diese Tabelle definiert den Authentifizierungsbereich, der mit der REST-API und der OAuth-Entität verknüpft werden kann. Der Name des Authentifizierungsbereichs muss eindeutig sein und gilt global.
REST API-Authentifizierungsbereich (sys_api_access_scope)	Diese Tabelle verknüpft die REST-API mit dem Authentifizierungsbereich.

Konfigurieren Sie den REST-API-Authentifizierungsbereich

Verknüpfen Sie die OAuth-Entität mit einem Authentifizierungsbereich, um das Token für den Zugriff auf die REST APIs zu verwalten, die mit dem Authentifizierungsbereich verknüpft sind.

Vorbereitungen

Installieren Sie die folgenden Plugins:

- OAuth 2.0
- REST API-Anbieter
- Authentifizierungsbereich
- REST-API-Authentifizierungsbereich

Hinweis: Das Plugin *REST API Auth Scope* wird als Teil des Release Tokyo] hinzugefügt.

Erforderliche Rolle: admin

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **API-Authentifizierungsbereiche** > **REST-API-Authentifizierungsbereich**an.
   Die Seite „REST-API-Authentifizierungsbereiche“ wird angezeigt.
2. Klicken Sie auf **Neu**, um einen neuen REST-API-Authentifizierungsbereich zu konfigurieren.
3. Füllen Sie die Felder des Formulars aus.

REST-API-Authentifizierungsbereich

Name	Ein eindeutiger Name, der den REST-API-Authentifizierungsbereich identifiziert
Aktiv	Aktivieren Sie das Kontrollkästchen, um die Konfiguration zu aktivieren.
Anwendung	Schreibgeschützter Anwendungsbereich.
REST-API	Die REST API, auf die der Authentifizierungsbereich angewendet wird. Zum Beispiel die Tabellen-API.
Authentifizierungsbereich	Wählen Sie den Authentifizierungsbereich über das Suchsymbol aus.
REST-API-PFAD	API-Pfad der REST API. Dieses Feld wird basierend auf der ausgewählten REST API automatisch ausgefüllt. Beispiel: now/table.
HTTP-Methode	Methode für die Interaktion mit der API. Wählen Sie die Methode aus der Dropdown-Liste aus. Sie können das Feld „ **Authentifizierungsbereich auf alle HTTP-Methoden in dieser API anwenden** “ im Formular manuell deaktivieren, um die Methode auszuwählen.
REST API-Version	Version der API. Beispiel: v1. Dieses Feld wird basierend auf der ausgewählten REST API automatisch ausgefüllt. Sie können das Feld **„Authentifizierungsbereich auf alle Versionen in dieser API anwenden“** im Formular manuell deaktivieren, um die Version auszuwählen.
Ressource	Untergeordnete Ressource der REST API. Dieses Feld wird basierend auf der ausgewählten REST API automatisch ausgefüllt. Beispiel: /now/table. Sie können das Feld **„Authentifizierungsbereich auf alle Ressourcen in dieser API anwenden“** im Formular manuell deaktivieren, um die Ressourcen auszuwählen.

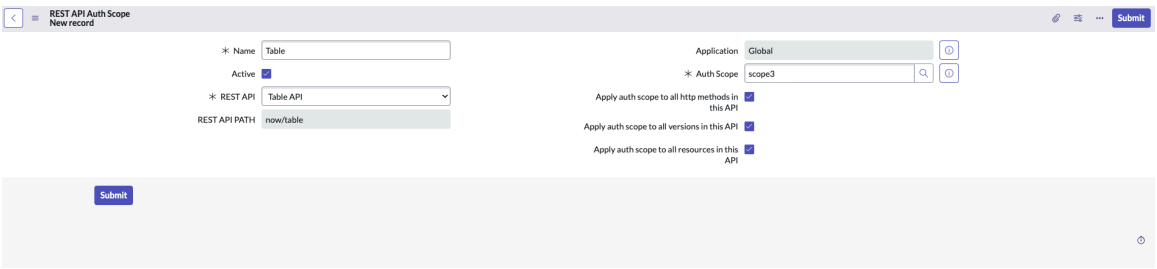
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Authentifizierungsbereich auf alle HTTP-Methoden in dieser API anwenden	Wenn diese Option aktiviert ist, wird der Authentifizierungsbereich auf alle HTTP-Methoden in der API angewendet.
Authentifizierungsbereich auf alle Versionen in dieser API anwenden	Wenn diese Option aktiviert ist, wird der Authentifizierungsbereich auf alle Versionen in der API angewendet.
Authentifizierungsbereich auf alle Ressourcen in dieser API anwenden	Wenn diese Option aktiviert ist, wird der Authentifizierungsbereich auf alle Ressourcen in der API angewendet

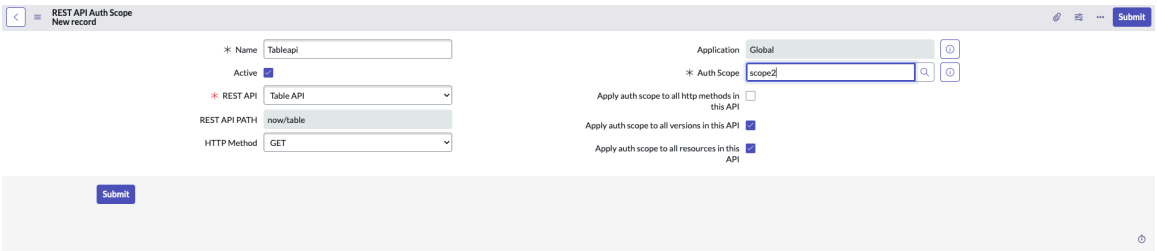
4. Klicken Sie auf **Absenden**.
   Basierend auf der ausgewählten REST API und dem ausgewählten Authentifizierungsbereich rufen die APIs Informationen ab, die für den Bereich spezifisch sind.

Example: Erwägen Sie die Erstellung von drei REST-API-Authentifizierungsbereichen für die Tabellen-API

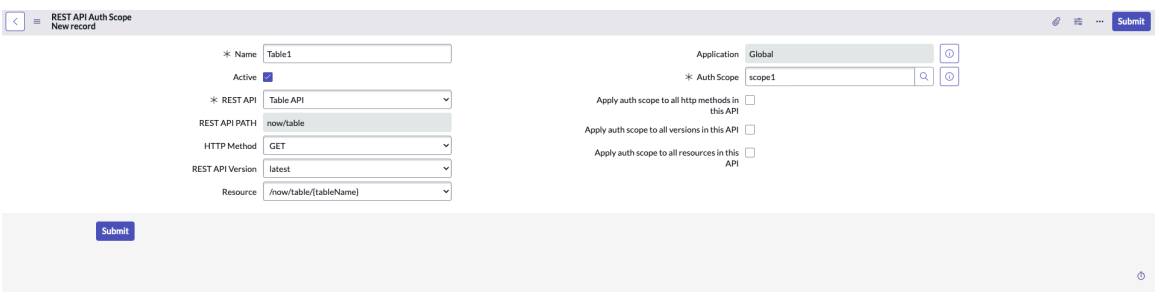
Der erste Authentifizierungsbereich wird der **Tabellen-API** zugeordnet, wobei alle HTTP-Methoden, -Versionen und -Ressourcen aktiviert sind.



Der zweite Authentifizierungsbereich wird der **Tabellen-API** zugeordnet, wobei alle Versionen und Ressourcen aktiviert sind. Sie wählen jedoch die HTTP-Methode, in diesem Beispiel die **GET-** Methode.



Der dritte Authentifizierungsbereich wird der **Tabellen-API** zugeordnet, ohne dass HTTP-Methoden, -Versionen und -Ressourcen aktiviert sind. Sie wählen die HTTP-Methode, Version und Ressource jedoch manuell aus. In diesem Beispiel ist die HTTP-Methode **GET**, die REST API-Version ist **aktuell**und die Ressource ist `/now/table/{tableName}`.



© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn alle diese Authentifizierungsbereiche erstellt wurden, können Sie die **GET** -Methode mit allen drei Bereichen verwenden. Für die Methoden **POST**, **PUT**, **DELETE**oder **PATCH** kann jedoch nur **scope3** verwendet werden.

Problembehandlung für den REST-API-Bereich

Aktionen zur Fehlerbehebung können zur Behebung allgemeiner Probleme beim Einrichten oder Ausführen des REST-API-Bereichs beitragen.

Problembehandlung

Problem	Aktion
Die REST-API ist mit dem Authentifizierungsbereich verknüpft. Zur Laufzeit findet jedoch auch bei Verwendung der Bearer-Token-Authentifizierung keine Überprüfung des Authentifizierungsbereichs statt.	• Stellen Sie sicher, dass der Datensatz „sys_api_access_policy“ aktiv ist. Die Laufzeit ignoriert inaktive Datensätze. • Überprüfen Sie, ob die Eigenschaft *com.glide.rest.api.auth.scope.check.enable* auf „falsch“ festgelegt ist. • Überprüfen Sie, ob das OAuth-Token den `Authentifizierungsbereich useraccount` hat.
Die REST API ist mit *auth_scope1*verknüpft, aber das Zugriffstoken mit *auth_scope2* kann auch darauf zugreifen.	• Überprüfen Sie, ob dieser Datensatz aktiv ist. • Suchen Sie nach diesem REST und prüfen Sie, ob andere Datensätze vorhanden sind, die dieselben APIs, aber unterschiedliche Anwendungsmethoden, Versionen oder Ressourcen aufweisen.
Die REST-API ist mit dem Authentifizierungsbereich verknüpft, zur Laufzeit findet jedoch keine Authentifizierungsbereichsprüfung für *basicAuth* und *mutualAuth*statt.	Dies wird erwartet, da der REST-API-Authentifizierungsbereich nur für das OAuth-Zugriffstoken oder OIDC-Token gilt. BasicAuth-, Sitzungscookies- und zertifikatsbasierte Authentifizierung werden nicht angewendet.
REST-API-Aufruf gibt bei Verwendung des OAuth-Zugriffstokens 403 zurück.	Überprüfen Sie, ob die Fehlermeldung „Erforderlicher API-Zugriffsbereich fehlt“ angezeigt wird. Wenn gefunden wird, schlägt die Überprüfung des Authentifizierungsbereichs für diese REST API fehl
`Vordefinierter Anwenderaccount wurde` gelöscht und kann nicht wiederhergestellt werden.	Exportieren `Sie useraccount` als `XML` aus der anderen Instanz, und importieren Sie es, oder erstellen Sie ein `useraccount`, und ändern Sie die Systemeigenschaft *glide.oauth.token.scope.useraccount* für den neu erstellten Datensatz sys_id.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Häufige Fragen

Im Folgenden finden Sie einige häufig gestellte Fragen, wenn Sie den REST-API-Authentifizierungsbereich verwenden:

Kann ein OAuth-Token mit mehreren Authentifizierungsbereichen verknüpft werden?

Ja, eine `oauth_entity` kann mit mehreren Authentifizierungsbereichen verknüpft werden. Jedes von dieser `oauth_entity` ausgegebene OAuth-Token hat dieselben Authentifizierungsbereiche.

Können verschiedene OAuth-Token mit unterschiedlichen Authentifizierungsbereichen auf dieselbe REST API zugreifen?

Ja, für dieselbe REST API können verschiedene Authentifizierungsbereiche darauf zugreifen. Solange ein Authentifizierungsbereich übereinstimmt, gibt der Authentifizierungsbereich die Ergebnisse zurück.

Kann ein OAuth-Zugriffstoken mit `dem Authentifizierungsbereich „useraccount“` auf alle REST APIs zugreifen?

Ja, der `Anwenderaccount` hat vollständigen Zugriff auf den Authentifizierungsbereich.

Kann der OAuth-Bereich des OAuth-Zugriffstokens dynamisch geändert werden?

Ja, die bereichsbezogene Authentifizierung ist nicht mit dem Zugriffstoken in der Tabelle `„oauth_credential“ hartcodiert`. Stattdessen wird der Authentifizierungsbereich während der Laufzeit von der verknüpften `oauth_entity abgerufen`.

Kann das OAuth-Token nach der Aktualisierung dieselben Authentifizierungsbereiche beibehalten?

Ja, der Authentifizierungsbereich ändert sich nach der Token-Aktualisierung nicht, es sei denn, `oauth_admin` ändert den mit `oauth_entity`verknüpften Authentifizierungsbereich.

Der vordefinierte Datensatz für den Anwenderaccount-Authentifizierungsbereich wurde gelöscht. Kann ein neuer `Authentifizierungsbereich mit dem Namen „useraccount“` erstellt werden?

Das Erstellen eines neuen Authentifizierungsbereichs mit demselben `Anwenderaccount` funktioniert nicht. Zur Laufzeit wird für die Überprüfung des Authentifizierungsbereichs die `sys_id` anstelle des Namens verwendet. Ändern Sie die Systemeigenschaft *`glide.oauth.token.scope.useraccount`* für den neu erstellten Datensatz „ `sys_id`“.

Wenn der Administrator den mit `oauth_entity`verknüpften Authentifizierungsbereich ändert, werden dann alle vorhandenen OAuth-Zugriffstoken geändert, die von dieser OAuth-Entität ausgestellt wurden?

Ja, der Authentifizierungsbereich ist nicht direkt mit dem OAuth-Zugriffstoken verknüpft, sondern wird während der Laufzeit von `„oauth_entity“ abgerufen`.

Können verschiedene OAuth-Zugriffstoken, die von derselben `oauth_entity` ausgegeben werden, unterschiedliche Authentifizierungsbereiche haben?

Nein, der gesamte Zugriff auf das Token wird von derselben `oauth_entity ausgegeben` und hat immer dieselben Authentifizierungsumfänge.

Kann ein Benutzer verschiedene Authentifizierungsbereiche für einen bestimmten Endpunkt definieren?

Nein, es gibt eine eindeutige Einschränkungsprüfung für einen bestimmten REST-API-Endpunkt. Für denselben REST API-Endpunkt können jedoch mehrere übereinstimmende Authentifizierungsbereiche vorhanden sein.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wird die Authentifizierungsbereichsprüfung auch für BasicAuth verwendet?

Nein, die Umfangsprüfung bezieht sich nur auf das OAuth-Zugriffstoken und das OIDC-Token. Sie wird nicht für *basicAuth* und *mutualAuth*angewendet.

Zugriffsrichtlinien für SOAP-API

Mit SOAP-API-Zugriffsrichtlinien können Sie den Zugriff auf eingehende SOAP-APIs basierend auf dem Authentifizierungstyp und den angegebenen Filterkriterien der Zugriffsrichtlinie einschränken.

Mit den SOAP-API-Zugriffsrichtlinien können Sie das eingehende Authentifizierungsprofil und die API-Zugriffsrichtlinien auf eingehende SOAP-APIs und geskriptete SOAP-APIs anwenden.

Sie können Zugriffsrichtlinien der ServiceNow API wie IP-Bereich und rollenbasierte Einschränkungen nutzen, um eingehende SOAP-API-Aufrufe basierend auf der Authentifizierung zuzulassen oder zu verhindern.

Als Administrator können Sie die folgenden Aktionen ausführen, um die Richtlinien anzuwenden.

- Aktivieren Sie die SOAP-API-Zugriffsrichtlinien- und Authentifizierungsprofil-Plugins. Weitere Informationen finden Sie unter Aktivieren Sie die SOAP-API-Zugriffsrichtlinie.
- Erstellen Sie SOAP-API-Zugriffsrichtlinien, und ordnen Sie diese Richtlinien einem Authentifizierungsprofil zu. Weitere Informationen finden Sie unter Erstellen Sie eine SOAP-API-Zugriffsrichtlinie und Erstellen Sie ein Authentifizierungsprofil.

  Hinweis: Die Richtlinien gelten für die SOAP-Tabellen-API oder die geskriptete SOAP-API. Neben dem Standard `-HTTP- und WSSE-Authentifizierungsprofil`

- Erstellen Sie Authentifizierungsrichtlinien wie IP-Bereich und rollenbasierte Einschränkungen, und ordnen Sie diese Richtlinie dem Authentifizierungsprofil zu. Weitere Informationen finden Sie unter Erstellen Sie eine API-Authentifizierungsrichtlinie.

Aktivieren Sie die SOAP-API-Zugriffsrichtlinie

Installieren Sie für die SOAP-API-Zugriffsrichtlinie das Plugin „SOAP API Access Policy“ (`com.glide.soap.policy`).

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Das folgende Element wird mit dem SOAP-API-Zugriffsrichtlinien-Plugin installiert: Prozessorzugriffsrichtlinie (`com.glide.processor.policy`)

Abhängiges Plugin: Authentifizierungsprofil (`com.glide.auth.profile`)

Prozedur

1. Navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie das Plugin „SOAP API Access Policy“ (`com.glide.soap.policy`) mithilfe der Filterkriterien und der Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.

3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: `Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.`

Nach Abschluss der Installation wird eine Meldung angezeigt.

Erstellen Sie ein Authentifizierungsprofil

Erstellen Sie ein Authentifizierungsprofil, und fügen Sie dem Profil eine oder mehrere Authentifizierungsrichtlinien hinzu. Sie können auch die standardmäßig verfügbaren Authentifizierungsprofile für **ID-Token** und **OAuth-Token** konfigurieren.

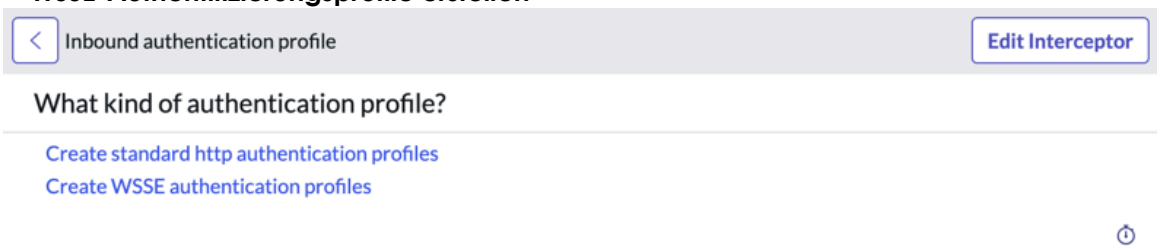
Vorbereitungen

Erforderliche Rolle: admin

Hinweis: Sie können Authentifizierungsrichtlinien, IP-Bereiche, rollenbasierte, anwenderbasierte usw. mit gegenseitiger Authentifizierung und anwenderdefinierter Authentifizierung anwenden.

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **Eingehende Authentifizierungsprofile**an.
2. Wählen Sie **Neu**.
   Das System zeigt die Nachricht an. `Welche Art von Authentifizierungsprofil?`
3. **Welche Art von Authentifizierungsprofilen auswählen?**.
   - **Standardmäßiges http-Authentifizierungsprofil erstellen**
   - **WSSE-Authentifizierungsprofile erstellen**



4. Füllen Sie die Felder des Formulars aus.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Standardauthentifizierungsprofil“.

Feld	Beschreibung
Name	Name zur Identifizierung der Authentifizierungsrichtlinie.
Beschreibung	Beschreibung der Authentifizierungsrichtlinie.
Aktiv	Option zum Aktivieren der Authentifizierungsrichtlinie.
Anwendung	Geltungsbereich der Authentifizierungsrichtlinie.
Typ	Typ der verfügbaren Authentifizierung. Sie können **Standardauthentifizierung**, **ID-Token**, **Zertifikatbasierte**Authentifizierung, **OAuth**oder **WSSE** (im Falle des WSSE-Authentifizierungsprofils) auswählen.
OAuth-Entität	OAuth-Entitätsprofil. Dieses Feld wird nur angezeigt, wenn **ID-Token** oder **OAuth** als **Typ**ausgewählt wird.

5. Doppelklicken Sie auf **Neue Zeile einfügen**.
6. Wählen Sie eine Authentifizierungsrichtlinie aus der Liste aus, und wählen Sie das Speichern-Symbol .

   Hinweis: Wählen Sie nicht die **Option „Zugriffsrichtlinie zulassen“** oder **„Zugriffsrichtlinie verweigern“**aus. Diese Richtlinien sind nur für Anwenderanmeldungen vorgesehen.

   Sie können eine oder mehrere Authentifizierungsrichtlinien für ein Authentifizierungsprofil hinzufügen.

   Wenn sich das Authentifizierungsprofil ändert, gibt der Autorisierungsheader einen Wert zurück, der für die zu diesem Zeitpunkt vorgenommenen Änderungen spezifisch ist. Um alle im Header „WWW-Authenticate“ zurückgegebenen Authentifizierungsschemata abzurufen, müssen Sie `glide.security.response.authenticate.header.auth_profile.first_scheme_only` auf **false**aktivieren. Die Antwort wird mit mehreren Headern zurückgegeben. Beispiel:

```
< WWW-Authenticate: BEARER realm="Service-now"
< WWW-Authenticate: BASIC realm="Service-now"
```

Erstellen Sie eine SOAP-API-Zugriffsrichtlinie

Erstellen Sie eine API-Zugriffsrichtlinie, und ordnen Sie ein Authentifizierungsprofil zu, um den Authentifizierungstyp für eine SOAP-API einzuschränken. Sie können beispielsweise eine API-Zugriffsrichtlinie erstellen, die nur die ID-Token-Authentifizierung für eine SOAP-API zulässt.

Vorbereitungen

- Stellen Sie sicher, dass ein Authentifizierungsprofil erstellt wird. Weitere Informationen finden Sie unter Authentifizierungsprofile erstellen.
- Erforderliche Rolle: admin

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

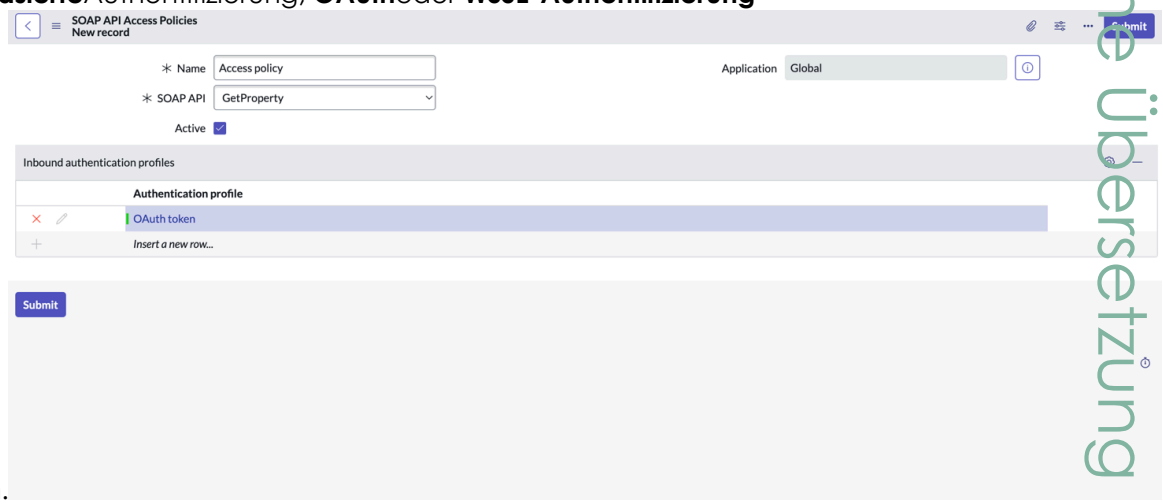
Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **Zugriffsrichtlinien für SOAP-API**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular „API-Zugriffsrichtlinien“.

Feld	Beschreibung
Name	Eindeutiger Name der API-Zugriffsrichtlinie.
SOAP-API	SOAP-API, auf die die Zugriffsrichtlinie angewendet wird. Beispiel: **GetProperty-API**.
Anwendung	Umfang der Anwendung.
Aktiv	Option zum Aktivieren der API-Zugriffsrichtlinie.

4. Doppelklicken Sie im Abschnitt Eingehende Authentifizierung auf **Neue Zeile einfügen**.
5. Wählen Sie ein eingehendes Authentifizierungsprofil aus der Liste aus, und klicken Sie auf das Speichern-Symbol .
   Sie können beispielsweise Basisauthentifizierung, **ID-Token**, **zertifikatsbasierte**Authentifizierung, **OAuth**oder **WSSE-Authentifizierung hinzufügen**.



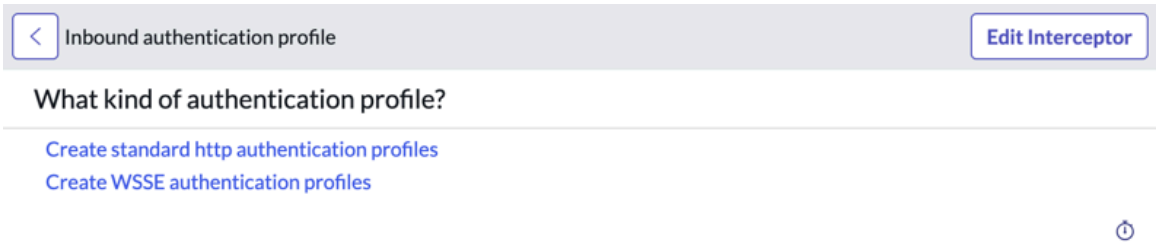
   a. Klicken Sie zum Hinzufügen eines oder mehrerer eingehender Authentifizierungsprofile auf **Neu**, um ein neues Profil zu erstellen.

   b. **Welche Art von Authentifizierungsprofilen auswählen?**.

   - **Standardmäßiges http-Authentifizierungsprofil erstellen**
   - **WSSE-Authentifizierungsprofile erstellen**

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

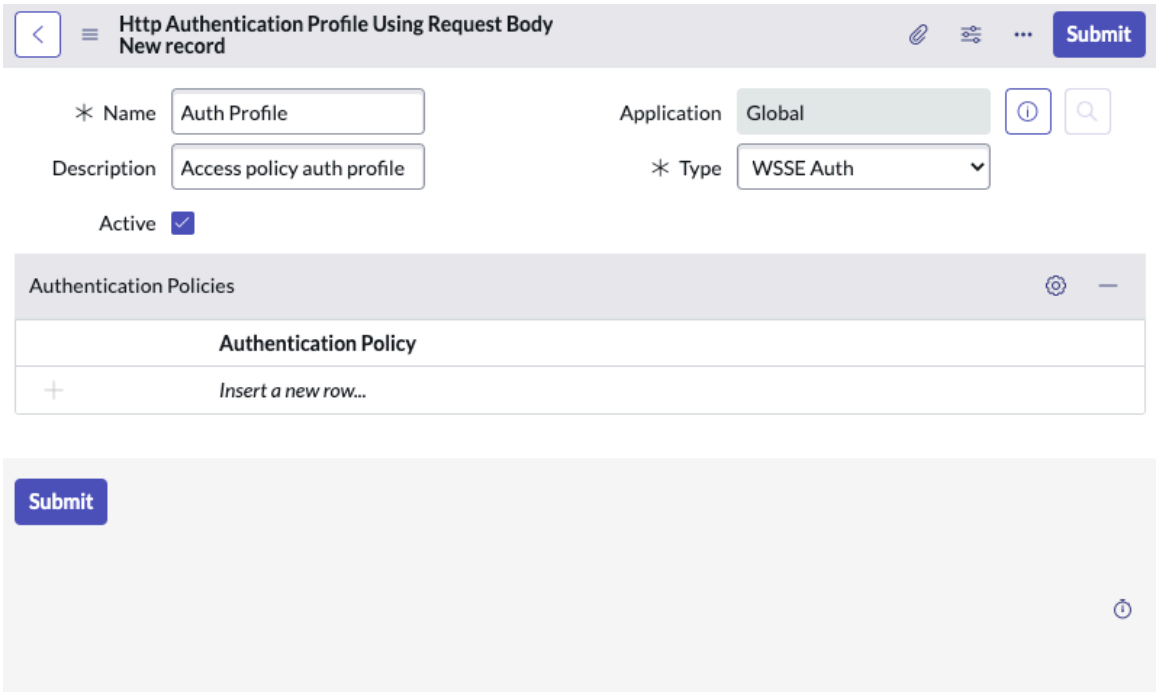


c. Füllen Sie die Felder im Formular aus, um ein WSSE-Authentifizierungsprofil zu erstellen.

WSSE-Authentifizierungsprofil

Feld	Beschreibung
Name	Eindeutiger Name der API-Zugriffsrichtlinie.
Beschreibung	Beschreibung des Authentifizierungsprofils.
Anwendung	Umfang der Anwendung.
Aktiv	Option zum Aktivieren der API-Zugriffsrichtlinie.
Typ	WSSE-Authentifizierung als Authentifizierungsprofil WSSE (Web Security).

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



d. Speichern Sie den Datensatz, nachdem Sie das Authentifizierungsprofil erstellt haben.

6. Klicken Sie auf **Absenden**, um die SOAP-API-Zugriffsrichtlinie zu übermitteln.

Erstellen Sie eine globale API-Zugriffsrichtlinie, um SOAP-APIs zu schützen

Erstellen Sie eine einzige globale API-Zugriffsrichtlinie, um alle SOAP-APIs zu schützen.

Vorbereitungen

- Erforderliche Rolle: admin
- Installieren Sie das Plugin „ **Prozessorzugriffsrichtlinie“** (`com.glide.processor.policy`).
- Stellen Sie sicher, dass ein Authentifizierungsprofil erstellt wird. Weitere Informationen finden Sie unter Authentifizierungsprofile erstellen.

In den folgenden Schritten wird beschrieben, wie Sie eine einzelne globale Zugriffsrichtlinie erstellen, um alle SOAP-APIs zu schützen.

Hinweis: Die auf den einzelnen SOAP-API-Ebenen definierten Richtlinien überschreiben die globale Zugriffsrichtlinie auf SOAP **-Prozessorebene**.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Zugriffsrichtlinien verarbeiten**an.

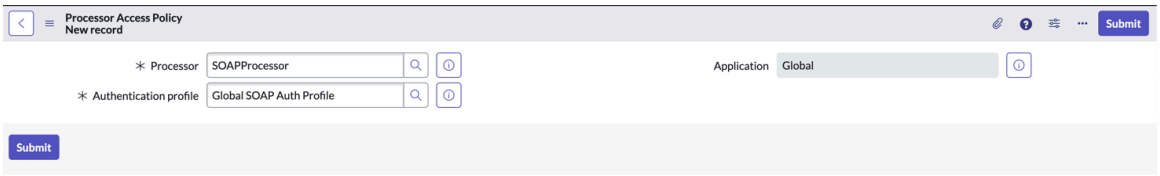
2. Füllen Sie die Felder des Formulars aus.

Formular „Prozesszugriffsrichtlinie“.

Feld	Beschreibung
Prozessor	Name zur Identifizierung der Authentifizierungsrichtlinie. Wählen Sie beispielsweise **SOAPProcessor** (Authentifizierungsprofil) aus.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Anwendung	Geltungsbereich der Authentifizierungsrichtlinie. Standard: Global
Authentifizierungsprofil	Typ des Authentifizierungsprofils. Wählen Sie **Globales SOAP-Authentifizierungsprofil**aus.



3. Wählen Sie **Absenden**.

Filterkriterien für APIs

Filterkriterien enthalten Filterbedingungen oder Abfragen, die als Richtlinieneingaben für eine Authentifizierungsrichtlinie verwendet werden. Richtlinieneingaben werden verwendet, um ein oder mehrere Filterkriterien zu gruppieren und die Richtlinienbedingungen einer Authentifizierungsrichtlinie zu definieren. Beispielsweise definieren IP-Filterkriterien eine IP-Adresse im CIDR-Format (Classless Inter-Domain Routing) oder einen Bereich von IP-Adressen.

Sie können Filterkriterien basierend auf der IP-Adresse des Benutzers, der Rolle und der Benutzergruppe, zu der er gehört, erstellen.

Hinweis: Sie können auch die Filterkriterien verwenden, die mit dem Modul **„Adaptive Authentifizierung** “ erstellt wurden. Weitere Informationen finden Sie unter Adaptive Authentifizierung.

Sie können Filterkriterien für APIs mit dem gleichen Prozess wie Filterkriterien für die adaptive Authentifizierung erstellen. Nähere Informationen hierzu finden Sie unter Filterkriterien.

Zugehörige Informationen

Erstellen Sie IP-Filterkriterien

Erstellen Sie Rollenfilterkriterien

Erstellen Sie Gruppenfilterkriterien

API-Authentifizierungsrichtlinien

Authentifizierungsrichtlinien werten Authentifizierungsanforderungen basierend auf den angegebenen Richtlinienbedingungen aus und gewähren oder verweigern den Zugriff je nach Übereinstimmungskriterien.

Sie können die integrierte globale Sperrrichtlinie verwenden oder eine Authentifizierungsrichtlinie gemäß Ihren Sicherheitsanforderungen erstellen. Die globale Blockierungsrichtlinie lehnt die Authentifizierungsanforderungen von Anwendern und APIs basierend auf den angegebenen Filterkriterien ab.

Hinweis: Verwenden oder ändern Sie die Richtlinien für zulassen Zugriff und die Richtlinie für verweigern Zugriff nicht. Diese Richtlinien sind nur für Anwenderanmeldungen vorgesehen.

Erstellen Sie eine API-Authentifizierungsrichtlinie

Mit Authentifizierungsrichtlinien können Sie Zugriffsbeschränkungen für die APIs basierend auf den angegebenen Filterkriterien erzwingen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur
1. Navigieren zu **Alle** > **System-Webservices** > **API-Authentifizierungsrichtlinie**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular aus.

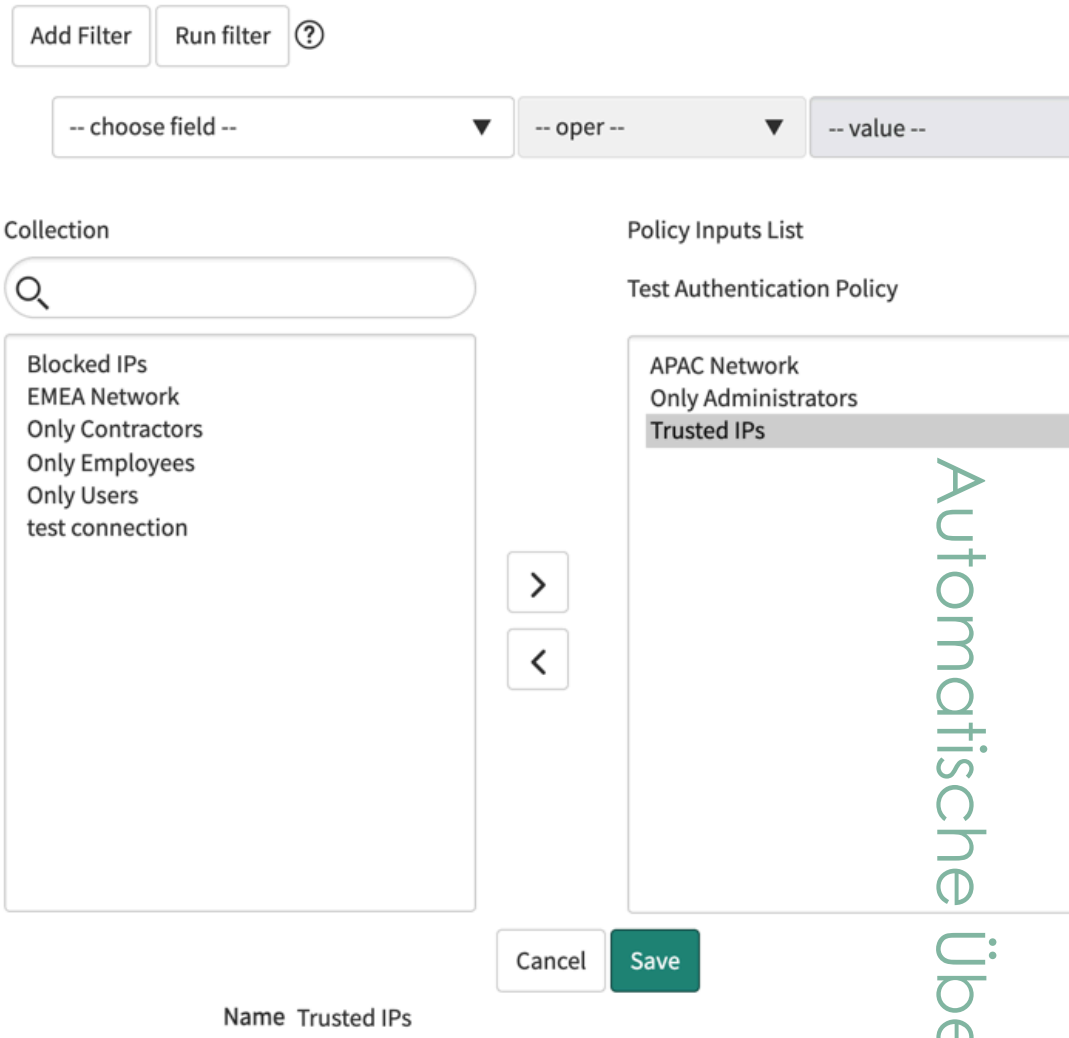
Formular „Richtlinie“.

Feld	Beschreibung
Name	Name zur Identifizierung der Richtlinie.
Beschreibung	Kurze Beschreibung der Richtlinie.
Anwendung	Umfang der Anwendung.

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
5. Wählen Sie auf der Registerkarte Richtlinieneingaben **Bearbeiten** aus, um die vorhandenen Filterkriterien hinzuzufügen.
   Sie können auch eine neue Richtlinieneingabe erstellen. Weitere Informationen finden Sie unter Richtlinieneingaben erstellen .

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Verschieben Sie ein oder mehrere Filterkriterien aus der Liste „Sammlungen“ in die Liste „Richtlinieneingaben“.



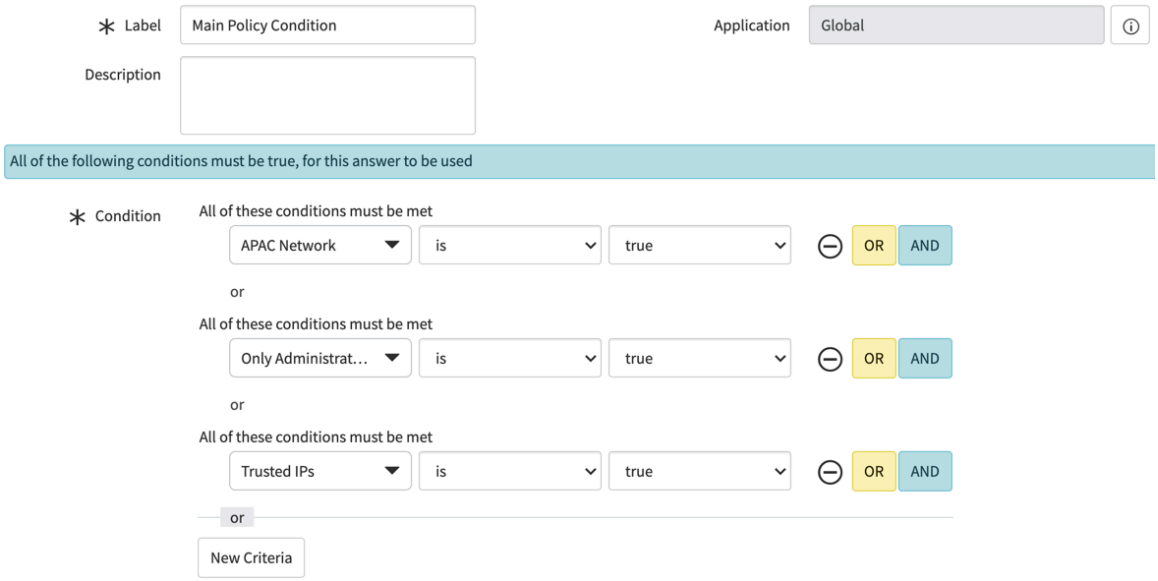
7. Wählen Sie **Speichern**.
8. Wählen Sie auf der Registerkarte Richtlinienbedingungen die Option **Neu**aus.
9. Füllen Sie die Felder im Formular aus.

Formular für Bedingungen

Feld	Beschreibung
Bezeichnung	Name der Richtlinienbedingung.
Beschreibung	Kurze Beschreibung der Richtlinienbedingung.
Anwendung	Umfang der Anwendung.
Bedingung	Eine oder mehrere Bedingungen, die mit dem **ODER** -Filter kombiniert werden.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



10. Wählen Sie **Absenden**.

Konfigurieren Sie die globale Blockierungsrichtlinie für APIs

Die globale Sperrrichtlinie lehnt die Authentifizierungsanforderungen von Anwendern und APIs basierend auf den angegebenen Richtlinienbedingungen ab. Diese Richtlinie kann als Alternative zur IP-Adresszugriffssteuerung verwendet werden.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **Globale Sperrrichtlinie**an.
2. Klicken Sie auf der Registerkarte **Richtlinieneingaben** auf **Bearbeiten**.
3. Wählen Sie ein oder mehrere Filterkriterien aus der Liste **Sammlung** aus, und verschieben Sie sie in die Liste **Globale Sperrrichtlinie**.
   Sie können auch zusätzliche Filter hinzufügen.
4. Klicken Sie auf der Registerkarte **Richtlinienbedingungen** auf **Neu**.
5. Füllen Sie diese Felder im Formular aus:

Formular „Bedingung“

Feld	Beschreibung
Bezeichnung	Name zur Identifizierung der Bedingung.
Beschreibung	Beschreibung der Bedingung
Bedingung	Logische Kombination aus mehreren Richtlinieneingaben (Filterkriterien), die zur Auswertung von Authentifizierungsanforderungen verwendet wird. Sie können beispielsweise Bedingungen erstellen, die nur Auftragnehmer aus einer Liste vertrauenswürdiger IP-Adressen zulassen.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugriffsrichtlinie für System-/Exportprozessoren

Fähigkeit für System-/Exportprozessoren, die Prozessorzugriffsrichtlinie zu nutzen, um alle Exportendpunkte zu sichern.

Fähigkeit, alle Exportendpunkte zu sichern und das eingehende Authentifizierungsprofil und die Prozessorzugriffsrichtlinien auf globaler Ebene oder Instanzebene anzuwenden.

Hinweis:

- Nicht-öffentliche Prozessoren, einschließlich Exportprozessoren wie CSV, PDF usw. werden für Zugriffsrichtlinien unterstützt.
- Skriptprozessoren werden auch für Zugriffsrichtlinien unterstützt.

Beispielanwendungsfälle

- Administratoren können den RSS-Prozessor mithilfe der API-Zugriffsrichtlinie blockieren, wenn sie nicht beabsichtigt sind, sie zu verwenden.
- Administratoren können ein Authentifizierungsprofil mit Standardauthentifizierung erstellen und eine Authentifizierungsrichtlinie zuordnen, die immer „falsch“ ergibt.

  Beispiel: Erstellen Sie IP-Kriterien mit einem Bereich von `0.0.0.0` bis `255.255.255.255` (fügen Sie auch IPv6-Adressraum hinzu), und fügen Sie dann eine Richtlinienbedingung mit dem Operator „false“ hinzu. Auf diese Weise werden Richtlinienbedingungen immer als „falsch“ ausgewertet, und die API-Zugriffsrichtlinie blockiert den Zugriff, unabhängig davon, woher die Anforderung stammt.

- Zugriff auf den Prozessor nur aus einem vertrauenswürdigen Netzwerk zulassen

Aktivieren Sie die Zugriffsrichtlinie für Prozessoren

Installieren Sie für den Prozessor das Plugin „Prozessorzugriffsrichtlinie“ (`com.glide.processor.policy`).

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Die folgenden Elemente werden mit der Prozessorzugriffsrichtlinie installiert:

- Systemeigenschaft: com.glide.auth.profile.supported.processor.list
- Modul in der Navigation: Zugriffsrichtlinien für Prozessor

Prozedur

1. Navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie das Plugin „Prozessorzugriffsrichtlinie“ (`com.glide.processor.policy`) mithilfe der Filterkriterien und der Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.

3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: `Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.`

Nach Abschluss der Installation wird eine Meldung angezeigt.

Nächste Maßnahme

an.
Konfigurieren Sie das Authentifizierungsprofil für die Prozessoren. Weitere Informationen finden Sie unter Konfigurieren Sie das Authentifizierungsprofil für den Prozessor.

Konfigurieren Sie das Authentifizierungsprofil für den Prozessor

Wenden Sie ein Authentifizierungsprofil für die Exportprozessoren an.

Vorbereitungen

Erforderliche Rolle: admin

Erforderliches Plugin: Processor Access Policy (`com.glide.processor.policy`)

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Zugriffsrichtlinien verarbeiten**an.
2. Um dem Prozessor ein Authentifizierungsprofil hinzuzufügen, klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

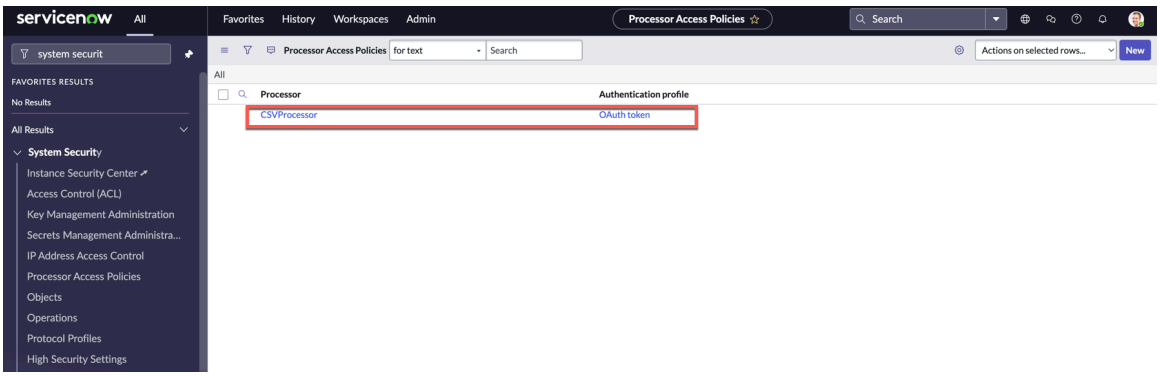
Formular „Prozesszugriffsrichtlinie“.

Feld	Beschreibung
Prozessor	Name zur Identifizierung der Authentifizierungsrichtlinie. **Hinweis:** Öffentliche Prozessoren werden nicht unterstützt. Wenn ein nicht unterstützter Prozessor ausgewählt ist, wird während der Übermittlung des Prozessors ein Fehler angezeigt.
Anwendung	Geltungsbereich der Authentifizierungsrichtlinie. Standard: Global
Authentifizierungsprofil	Typ des Authentifizierungsprofils. Sie können **ID-Token** oder **OAuth-Token**auswählen.

4. Klicken Sie auf **Absenden**.
   Das Authentifizierungsprofil wird auf den Prozessor angewendet.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispielsweise wird das OAuth-Authentifizierungsprofil für den CSV-Prozessor konfiguriert. In diesem Fall müssen Sie das OAuth-Zugriffstoken für den Export mit CSV als Exportoption verwenden.



Zertifikatbasierte Authentifizierung

Mit der zertifikatsbasierten Authentifizierung können Sie Anwenderanmeldungen oder eingehende API-Anforderungen mithilfe von Zertifikaten einer vertrauenswürdigen Zertifizierungsstelle gegenseitig authentifizieren.

Hinweis: Die zertifikatsbasierte Authentifizierung wird für lokale Instanzen und Instanzen mit aktivierter Edge Encryption nicht unterstützt.

Zertifikatbasierte Authentifizierung für Anmeldungen an der Anwenderoberfläche

Ermöglichen Sie Endanwendern, PIV-Karten (Personal Identity Verification) oder CAC-Karten zu verwenden, um sich bei Now Platform oder Serviceportal anzumelden, anstatt einen Anwendernamen und ein Passwort zu verwenden. Informationen zum Einrichten der gegenseitigen Authentifizierung für Anmeldungen an der Anwenderoberfläche finden Sie unter Richten Sie die zertifikatbasierte Authentifizierung ein.

Nachdem die zertifikatbasierte Authentifizierung eingerichtet wurde, können Endanwender die Einrichtung abschließen und sich anmelden. Weitere Informationen finden Sie unter Melden Sie sich mit der zertifikatbasierten Authentifizierung an.

Zertifikatbasierte Authentifizierung für eingehende Webservices

Authentifizieren Sie eingehende Anforderungen bei ServiceNow SOAP- und REST-APIs. Informationen zum Einrichten der gegenseitigen Authentifizierung für eingehende Webservices finden Sie unter Richten Sie die zertifikatbasierte Authentifizierung ein.

Richten Sie die zertifikatbasierte Authentifizierung ein

Richten Sie die gegenseitige Authentifizierung für anwenderoberflächenbasierte Anmeldungen oder für eingehende Webservices ein.

Vorbereitungen

Erforderliche Rolle: admin

Stellen Sie sicher, dass Ihre Instanz ein ADCv2-Lastenausgleichsmodul verwendet. Weitere Informationen finden Sie im Wissensartikel zurADCv2-Migration . Wenn Ihre Instanz nicht das Lastenausgleichsmodul ADCv2 verwendet, wenden Sie sich an Now Support.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

Richten Sie die zertifikatbasierte Authentifizierung ein, um:

- Ermöglichen Sie Endanwendern, sich mit PIV- oder CAC-Karten sicher bei Now Platform oder Serviceportal anzumelden. Nachdem die zertifikatbasierte Authentifizierung aktiviert wurde, können Sie das PEM-Zertifikat selbst registrieren, oder ein Administrator kann das Zertifikat für Sie zuordnen. Weitere Informationen finden Sie unter Melden Sie sich mit der zertifikatbasierten Authentifizierung an.
- Aktivieren Sie die gegenseitige Authentifizierung für eingehende Webservices. Sobald die zertifikatbasierte Authentifizierung eingerichtet ist, verwendet das System die bereitgestellten Zertifikate, um Anforderungen für den Zugriff auf ServiceNow REST- und SOAP-APIs gegenseitig zu authentifizieren.

Aktivieren Sie die Zertifikatbasierte Authentifizierung

Wenn Sie die Administratorrolle innehaben, können Sie das Plugin für die zertifikatsbasierte Authentifizierung (com.glide.auth.mutual) für Now Platform aktivieren.

Vorbereitungen
Erforderliche Rolle: admin.

Warum und wann dieser Vorgang ausgeführt wird
Die folgenden Tabellen werden mit der zertifikatsbasierten Authentifizierunginstalliert:

- sys_user_certificate
- sys_ca_certificate
- sys_ca_certificate_api_track

Prozedur

1. Navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie das Plugin „ Zertifikatbasierte Authentifizierung “ (com.glide.auth.mutual) mithilfe der Filterkriterien und der Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: `Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.`

   Nach Abschluss der Installation wird eine Meldung angezeigt.

Registrieren Sie das CA-Zertifikat

Registrieren Sie Stammzertifikate oder Zwischenzertifikate, um sie für die Authentifizierung verfügbar zu machen.

Vorbereitungen
Erforderliche Rolle: admin

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Zertifikatsbasierte Authentifizierung** > **CA-Zertifikatkette**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular „Zertifizierungszertifikat zur gegenseitigen Authentifizierung“.

Feld	Beschreibung
Name	Name zur Identifizierung des Zertifikats.
Ablaufbenachrichtigung	Option, um Benutzer zu warnen, wenn ein -Zertifikat abläuft.
Benachrichtigung bei Ablauf	Liste der Benutzer, die benachrichtigt werden sollen, wenn das Zertifikat abläuft.
Tage vor Ablauf benachrichtigen	Anzahl der Tage, in denen eine Benachrichtigung an Benutzer gesendet wird, bevor ein Zertifikat abläuft.
Aktiv	Option zum Aktivieren des Client-Zertifikats.
Format	PEM
Typ	Typ des Zertifikats. Verfügbare Optionen: ◦ **CA**-Zertifikat: Das CA-Stammzertifikat. Kann auch Zwischenzertifikate in die Kette aufnehmen. CA-Zertifikate werden automatisch mit dem Lastenausgleichsmodul synchronisiert. Verwenden Sie diese Option nach Möglichkeit, um zu vermeiden, dass ein erforderliches Zertifikat in der Kette fehlt. ◦ **Zwischenzertifikat**: Ein Zwischenzertifikat in der Zertifikatkette. Dieses Zertifikat verbleibt nur auf der Instanz und wird nicht mit dem Lastenausgleichsmodul synchronisiert. Verwenden Sie diese Option nur, wenn Sie einer vorhandenen Kette ein Zwischenzertifikat hinzufügen müssen.
Kurzbeschreibung	Kurze Beschreibung des Benutzer-Client-Zertifikats.

Hinweis: Während des Zertifikat-Uploads werden die schreibgeschützten Felder **Gültig ab**, **Läuft**ab, **Läuft ab in Tagen**ab, Aussteller und **Betreff**, **Zertifikatskette**und **PEM-Zertifikat**extrahiert und automatisch **ausgefüllt** werden.

4. Klicken Sie auf **Absenden**.
5. Wahlweise: Klicken Sie auf **Stores/Zertifikate** validieren, um das Zertifikat zu validieren.

Ordnen Sie das PEM-Zertifikat dem Anwender zu

Ordnen Sie Anwendern PEM-Zertifikate zu, damit sie sich mit PIV- oder CAC-Karten anmelden oder eingehende Anforderungen authentifizieren können. Sie können einem Benutzer mehrere PEM-Zertifikate zuordnen.

Vorbereitungen

- Erforderliche Rolle: admin
- Vergewissern Sie sich, dass Sie über das Privacy Enhanced Mail-Zertifikat (PEM) des Benutzers verfügen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Nach der Konfiguration zum Zuordnen des PEM-Zertifikats zum Anwender schlägt „Zertifikat verifizieren“ fehl. Dies liegt daran, dass das PEM-Zertifikat nicht gespeichert wird.

Prozedur

1. Navigieren zu **Alle** > **Zertifikatsbasierte Authentifizierung** > **Anwender-zu-Zertifikat-Zuordnung** und klicken Sie auf **Neu**.
2. Füllen Sie diese Felder des Formulars aus:

Formular „Anwender-Client-Zertifikat“.

Feld	Beschreibung
Name	Name des Anwender-Client-Zertifikats.
Ablaufbenachrichtigung	Option, um Benutzer zu warnen, wenn ein -Zertifikat abläuft.
Tage vor Ablauf benachrichtigen	Anzahl der Tage, in denen eine Benachrichtigung an Benutzer gesendet wird, bevor ein Zertifikat abläuft.
Benachrichtigung bei Ablauf	Liste der Benutzer, die benachrichtigt werden sollen, wenn das Zertifikat abläuft.
Aktiv	Option zum Aktivieren des Client-Zertifikats.
Anwender	Benutzer, der dem Client-Zertifikat zugeordnet ist. Das System empfängt das Client-Zertifikat entweder von der eingehenden Anforderung oder von der Zertifikatregistrierungund verwendet dann den in diesem Feld angegebenen Benutzer, um eine Sitzung zum Ausführen der Anforderung zu initiieren.
Kurzbeschreibung	Kurze Beschreibung des Benutzer-Client-Zertifikats.
Format	Das Privacy Enhanced Mail-Format (PEM) ist ein base64-codiertes DER-Zertifikat (Distinguished Encoding Rules).
Typ	Client-Zert. Dieses Feld ist schreibgeschützt.

Hinweis: Während des Zertifikat-Uploads werden die schreibgeschützten Felder **Gültig ab**, **Läuft**ab, **Läuftab in Tagen**ab, Aussteller und **Betreff** extrahiert und automatisch gefüllt werden.

3. Klicken Sie auf das Anhangsymbol, und laden Sie das Zertifikat hoch.
4. Klicken Sie auf **Absenden**.
   Das Zertifikat wird validiert und dem angegebenen Benutzer zugeordnet, wenn das Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle stammt.

Konfigurieren Sie Eigenschaften für die zertifikatbasierte Authentifizierung

Verwenden Sie die Systemeigenschaften, um die Funktionen der zertifikatsbasierten Authentifizierung zu aktivieren bzw. zu deaktivieren.

Vorbereitungen

Erforderliche Rolle: admin

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Zertifikatsbasierte Authentifizierung** > **Eigenschaften**an.
2. Füllen Sie die Felder des Formulars aus.

Formular „Eigenschaften der zertifikatsbasierten Authentifizierung“.

Eigenschaft	Beschreibung
Zertifikatbasierte Authentifizierung aktivieren	Option zum Aktivieren der zertifikatbasierten Authentifizierung für Anmeldungen über die Anwenderoberfläche und für eingehende Webservices. Standardwert: true
Option „Mit PIV/CAC anmelden“ im Anmeldebildschirm anzeigen	Zeigt die Option **Mit PIV/CAC-Karte** anmelden auf dem Anmeldebildschirm an. Ermöglicht Benutzern das Anmelden mit zertifikatbasierter Authentifizierung über die -Anwenderoberfläche. Standardwert: false
Automatische Weiterleitung für die zertifikatbasierte Anmeldung aktivieren	Bestimmt, ob der Anwender **auf Mit PIV/CAC-Karte** anmelden klicken muss, nachdem er ein registriertes Zertifikat ausgewählt und die PIN eingegeben hat. Aktivieren Sie diese Option, um den Benutzer automatisch anzumelden, nachdem er ein registriertes Client-Zertifikat ausgewählt und die PIN eingegeben hat. Deaktivieren Sie diese Option, damit der Anwender **auf Mit PIV/CAC-Karte** anmelden klicken muss, nachdem er ein registriertes Client-Zertifikat ausgewählt und die PIN eingegeben hat. Standardwert: false

Melden Sie sich mit der zertifikatbasierten Authentifizierung an

Nachdem Ihr Administrator die zertifikatbasierte Authentifizierung eingerichtet hat, können Sie das Client-Zertifikat registrieren und sich mit Ihrer PIV-Karte (Personal Identity Verification) oder CAC-Karte (Common Access Card) anmelden.

Registrieren Sie das Client-Zertifikat für Ihre PIV- oder CAC-Karte

Bevor Sie sich mit Ihrer PIV- oder CAC-Karte bei Now Platform anmelden, müssen Sie das Client-Zertifikat Ihrer PIV- oder CAC-Karte registrieren. Wenn Sie das Client-Zertifikat nicht registrieren können, wenden Sie sich an Ihren Administrator. Ihr Administrator kann auch das Client-Zertifikat Ihrer PIV- oder CAC-Karte registrieren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Stellen Sie sicher, dass die Zertifikatbasierte Authentifizierung aktiviert ist.
- Stellen Sie sicher, dass ein Kartenlesegerät an Ihren Computer verbunden und Ihre PIV- oder CAC-Karte eingesetzt ist.
- Erforderliche Rolle: keine

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie einen Administrator benötigen, um Ihr Client-Zertifikat zu registrieren, lesen Sie unter Ordnen Sie das PEM-Zertifikat dem Anwender zunach.

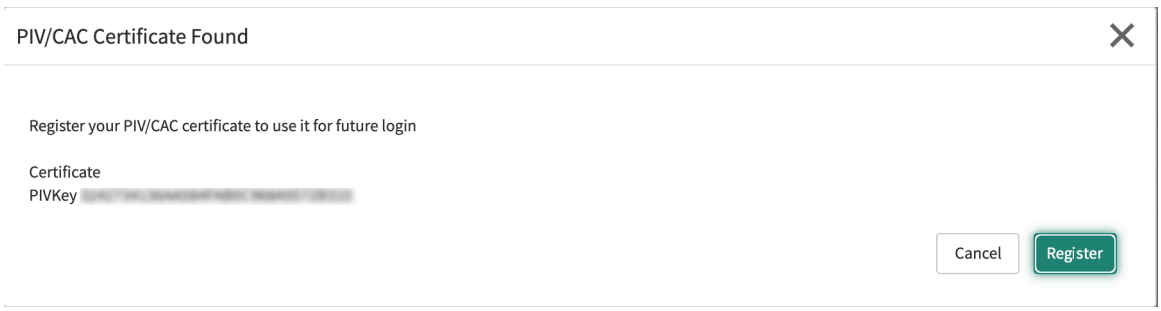
Prozedur

1. Melden Sie sich mit Ihrem Anwendernamen und Passwort bei Now Platform an.
2. Klicken Sie im **Benutzermenü** auf Ihren Namen, und wählen Sie **Profil**aus.



3. Klicken Sie unter **Zugehörige Links**auf **Client-Zertifikat registrieren**.

   Wenn ein gültiges Zertifikat verfügbar ist, wird die folgende Meldung angezeigt:

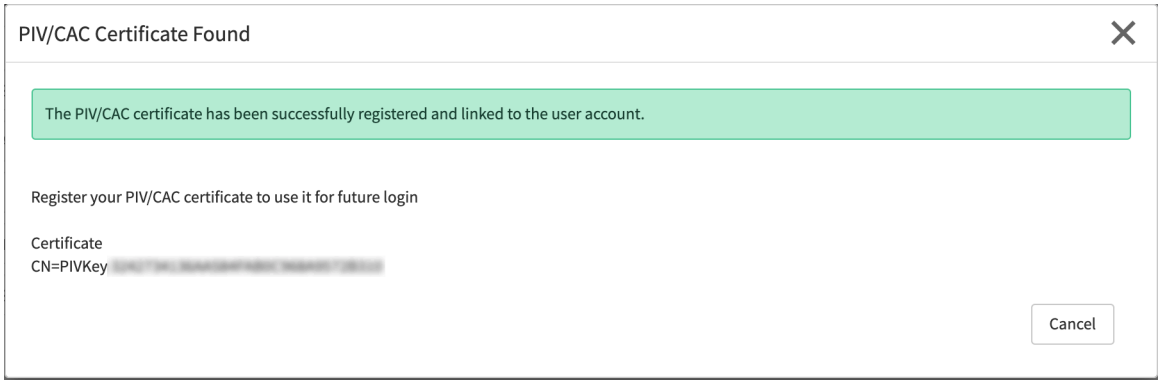


4. Klicken Sie auf **registrieren**.

   Nach einer erfolgreichen Registrierung wird die folgende Meldung angezeigt:

   ```
   Das PIV/CAC-Zertifikat wurde registriert und mit dem Anwenderaccount
   verknüpft.
   ```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Wenn Sie sich das nächste Mal bei Now Platform anmelden, können Sie sich mit Ihrer PIV- oder CAC-Karte anmelden. Weitere Informationen finden Sie unter Melden Sie sich mit der PIV- oder CAC-Karte bei Now Platform an.

Melden Sie sich mit der PIV- oder CAC-Karte bei Now Platform an

Sie können sich mit Ihrer PIV- oder CAC-Karte anstelle von Anwendername und Passwort anmelden, wenn die zertifikatsbasierte Authentifizierung unter Now Platformaktiviert ist.

Vorbereitungen

- Erforderliche Rolle: keine
- Stellen Sie sicher, dass die Zertifikatbasierte Authentifizierung aktiviert ist.
- Stellen Sie sicher, dass ein PIV- oder CAC-Kartenleser an Ihren Computer verbunden ist.
- Stellen Sie sicher, dass Ihnen ein Client-Zertifikat Ihrer PIV- oder CAC-Karte zugeordnet ist. Weitere Informationen finden Sie unter Registrieren Sie das CA-Zertifikat.

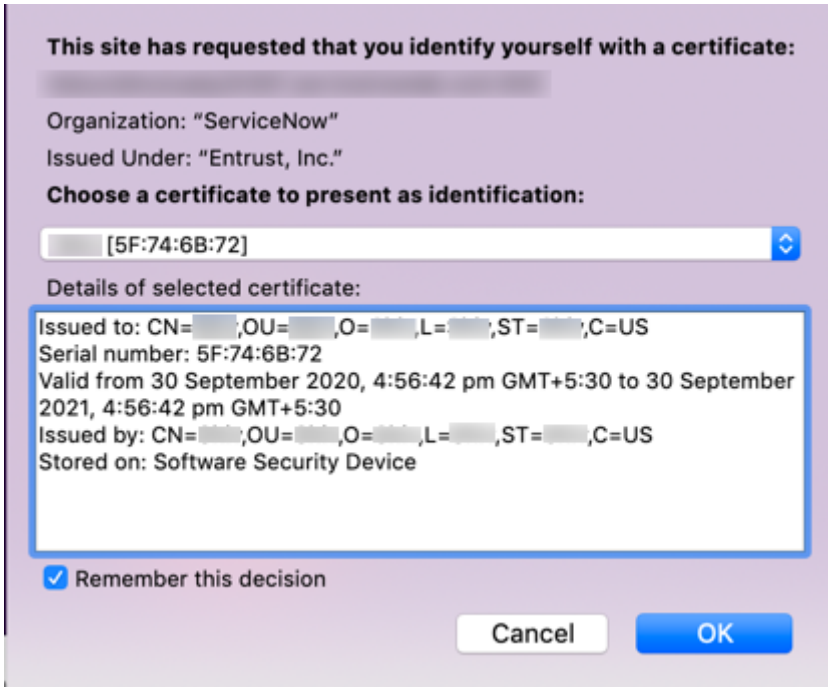
Prozedur

1. Führen Sie Ihre PIV- oder CAC-Karte in den Kartenleser ein.
2. Navigieren Sie in einem Browser zu Ihrer -Instanz.
   Der Browser fordert Sie zur Eingabe einer PIN für Ihre PIV- oder CAC-Karte auf.
3. Geben Sie die PIN Ihrer PIV- oder CAC-Karte in die Browseraufforderung ein.

   Hinweis: Wenn Sie Ihre PIN vergessen haben, wenden Sie sich an Ihren Administrator.

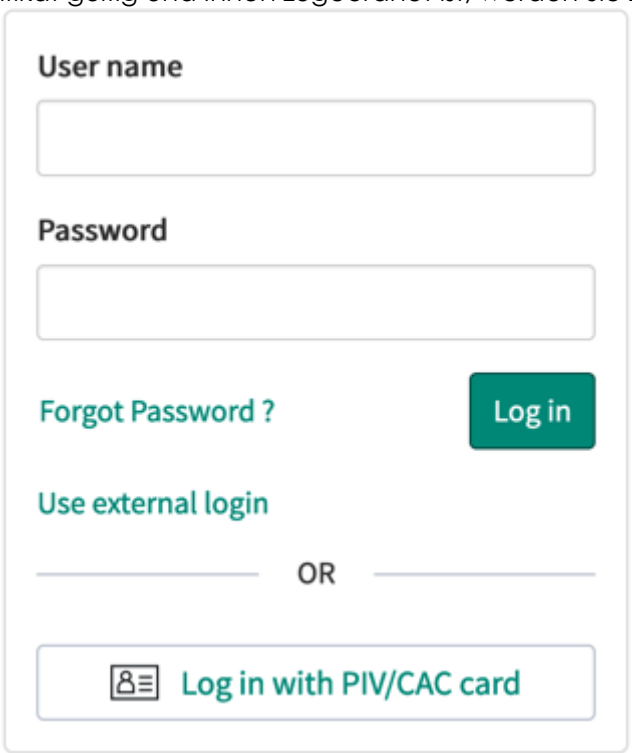
4. Wenn Sie eine korrekte PIN eingeben, zeigt der Browser eine Aufforderung zur Auswahl eines Zertifikats an.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Wählen Sie in der Browser-Eingabeaufforderung ein Zertifikat aus.

   Wenn das Zertifikat gültig und Ihnen zugeordnet ist, werden Sie zur Anmeldeseite



   weitergeleitet.

6. Klicken Sie **auf die Schaltfläche Mit PIV/CAC-Karte** anmelden.

   Um sich von der Now Platform abzumelden, müssen Sie den PIV oder CAC aus dem Kartenleser entfernen und dann den Browser schließen.

Ihre Client-Zertifikate verwalten

Zeigen Sie mit Ihrem Account verknüpfte Client-Zertifikate an, und löschen Sie sie.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Stellen Sie sicher, dass die Zertifikatbasierte Authentifizierung aktiviert ist.
- Erforderliche Rolle: keine

Prozedur

1. Melden Sie sich mit Ihrem Anwendernamen und Passwort bei Now Platform an.
2. Klicken Sie im **Benutzermenü** auf Ihren Namen, und wählen Sie **Profil**aus.



3. Klicken Sie unter **Zugehörige Links**auf **Ihre Client-Zertifikate verwalten**.
   Die Tabelle „Anwender-Client-Zertifikate“ [sys_user_certificate] wird geöffnet und zeigt Zertifikate an, die Ihrem Account zugeordnet sind.
4. Zeigen Sie mit Ihrem Account verknüpfte Zertifikate an, oder löschen Sie sie.

Zuordnung von anwenderdefinierten URLs zu Ihrer Instanz

Sie können Ihre Instanz ServiceNow von einer Unternehmens-Marken-URL oder einer anwenderdefinierten URL zugänglich machen.

Übersicht über anwenderdefinierte URLs

Sie können eine anwenderdefinierte URL verwenden, um den Zugriff auf die Instanz ServiceNow von einer oder mehreren unternehmensspezifischen oder anwenderdefinierten URLs zu ermöglichen.

Anwenderdefinierte URLs können einem bestimmten Portal zugeordnet werden. Beispielsweise kann der Administrator `http://support.acme.com` für das CSM-Portal und `http://hr.acme.com` für das HR-Portal definieren. In einer solchen Situation müssen Benutzer basierend auf der anwenderdefinierten URL, auf die sie zugreifen, zur Authentifizierung an andere IdPs umgeleitet werden.

Wichtig:

- Erstellen Sie keine anwenderdefinierte URL mit mehr als 100 Domänen pro Instanz.
- Sie müssen zuerst den anwenderdefinierten URL-Datensatz aus der Instanz ServiceNow löschen und dann alle DNS-Einträge (Domain Name Server) vom DNS-Server löschen.
- Jedes Löschen des DNS-Eintrags vom DNS-Server vor dem Löschen des anwenderdefinierten URL-Datensatzes aus der Instanz ServiceNow führt dazu, dass das Löschen anderer entsprechender anwenderdefinierter URL-Datensätze aus ServiceNowblockiert wird.

Von Tokyoaus können Sie Benutzern die automatische Weiterleitung zu angegebenen IdPs ermöglichen, die im anwenderdefinierten URL-Datensatz definiert sind.

Hinweis: Anwenderdefinierte URLs sind für lokale Kunden- oder Entwicklerinstanzen nicht verfügbar. Außerdem muss die URL öffentlich zugänglich sein.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nur der Besitzer der Domäne der obersten Ebene (TLD) oder einer beliebigen Subdomäne kann die anwenderdefinierte URL für eine DNS-Subdomäne konfigurieren. Beispielsweise kann Ihre -Instanz über die folgende festgelegte URL und zusätzliche anwenderdefinierte URLs verfügen:

Beispiel für eine anwenderdefinierte URL

Beispiel-URLs	Monatlich
`https://acme.service-now.com`	Der ursprüngliche Domänenname für Acme, der mit der Instanz ServiceNow geliefert wurde.
`https://support.acme.com`	Eine anwenderdefinierte URL, die Ihrer Instanz ServiceNow zugeordnet ist. Diese URL wird als Alias (CNAME) des ursprünglichen Domänennamens bezeichnet.
`https://US-support.acme.com`	Eine sekundäre anwenderdefinierte URL, die einem Serviceportal in Ihrer Instanz zugeordnet ist. Ihre Instanz von kann mehrere anwenderdefinierte URLs zum gleichen Serviceportal unterstützen.

Überlegungen zu anwenderdefinierten URLs außerhalb Ihrer Instanz

Bevor Sie eine anwenderdefinierte URL zuordnen können, müssen Sie eine URL von einem Domänenanbieter besitzen (oder erwerben). Es sind auch bestimmte Konfigurationen erforderlich, bevor Sie eine anwenderdefinierte URL in Ihrer -Instanz erstellen und zuordnen können.

Anwenderdefinierte URL-Konfigurationen

Konfigurationselemente	Beschreibung
Legen Sie den CNAME mit dem Anbieter fest	Der CNAME-Datensatz muss als ServiceNow -Instanz-URL festgelegt werden.
Bestimmen Sie Ihren dedizierten VIP-Status	Der Status „VIP“.

Hinweis: Wenn Sie CNAME-Datensätze löschen oder aktualisieren, die auf Ihre Instanz verweisen, müssen Sie diese Reihenfolge einhalten, um zu vermeiden, dass Datensätze in der Instanz hängen. Löschen Sie zuerst die CNAME-Datensätze aus Ihrer -Instanz, und entfernen oder aktualisieren Sie dann die CNAME-Einstellung bei Ihrem DNS-Anbieter.

Aktivieren Sie anwenderdefinierte URLs

Aktivieren Sie die Einrichtung von anwenderdefinierten URLs in Ihrer Instanz ServiceNow. Wenn Sie die Administratorrolle innehaben, können Sie das Plugin „Anwenderdefinierte URL“ (com.snc.customurl) aktivieren.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Plugins**an.
2. Suchen Sie das Plugin **Custom URL** (Anwenderdefinierte URL), und klicken Sie darauf.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wählen Sie nicht das Plugin **Custom URL - Intern** aus, bei dem es sich um eine interne Komponente für geskriptete anwenderdefinierte URL-APIs handelt.

3. Klicken Sie im Datensatz „Anwenderdefinierte URL“ auf den zugehörigen Link **Aktivieren/ Reparieren**.
4. Klicken Sie im Fenster „Plugin-Aktivierung“ auf **Aktivieren**.
   Wenn das Fenster „Plugin-Aktivierung“ mit einer Meldung erneut geöffnet wird, dass das Plugin aktiviert ist, klicken Sie auf **Formular schließen und neu laden, um auf diesem Formular** zu bleiben.
5. Suchen Sie in der zugehörigen Liste „Plugin-Dateien“ nach der folgenden Eigenschaft, und ändern Sie den Einstellungswert:

Option	Bezeichnung
glide.customurl.enabled	Um anwenderdefinierte URLs zu aktivieren, legen Sie den Wert auf **true**fest. Standardmäßig ist diese Eigenschaft auf **False**festgelegt, was bedeutet, dass Sie keine anwenderdefinierte URL zuordnen können. **Hinweis:** Um diese Funktion zu deaktivieren, legen Sie diese Eigenschaft wieder auf **False**fest.

6. Klicken Sie auf **Aktualisieren**.

Legen Sie eine anwenderdefinierte URL als Instanz-URL fest

Fügen Sie Ihrer Instanzkonfiguration eine anwenderdefinierte URL hinzu, die anstelle der URL ServiceNow verwendet wird.

Vorbereitungen

Erforderliche Rolle: admin
Sie müssen das Plugin „Anwenderdefinierte URL“ aktivieren und eine URL erworben oder registriert haben, bevor Sie die anwenderdefinierte URL zu Ihrer -Instanz hinzufügen können.

Prozedur

1. Navigieren zu **Alle** > **Anwenderdefinierte URL** > **Anwenderdefinierte URL**an.
2. Sie sollten entweder:
   - Klicken Sie auf **Neu**, um einen neuen Domänennamen zuzuordnen, der für Ihre Instanz neu ist.
   - Wählen Sie eine anwenderdefinierte URL aus, die bereits als Instanz-URL festgelegt wurde.
3. Füllen Sie die entsprechenden Felder aus:

Anwenderdefinierte URL-Felder

Feld	Beschreibung
Domänenname	Vollständig qualifizierter Domänenname (FQDN) der anwenderdefinierten URL. Der FQDN ist eine CNAME-Umleitung,

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	die im Namensserverdatensatz für die anwenderdefinierte Domäne erstellt wird. **Hinweis:** Im Namenserver für acme.com könnten Sie beispielsweise einen Eintrag erstellen: `support.acme.com 300 IN CNAME acme.servicenow.com`
Ist Instanz-URL	Aktivieren Sie die Checkbox, um diese anwenderdefinierte URL für alle ausgehenden URLs zu aktivieren. Nur eine aktive anwenderdefinierte URL kann die Instanz-URL sein. Um diese Einstellung für eine anwenderdefinierte URL zu aktivieren, klicken Sie im URL-Datensatz auf **Als Instanz-URL** festlegen. Alle vorherigen anwenderdefinierten URLs werden dann entfernt.
Status	Status des anwenderdefinierten URL-Datensatzes. Wenn der Status **Active**ist, ist die anwenderdefinierte URL bereitgestellt und kann verwendet werden.
Service Portal	Serviceportal, das Sie verwenden möchten, wenn Sie Benutzer über die anwenderdefinierte URL zu Ihrer Instanz umleiten.
Identitätsanbieter	Mit dem Identitätsanbieter für die anwenderdefinierte URL können Sie Benutzern die automatische Weiterleitung zu angegebenen IdPs ermöglichen, die im Datensatz der anwenderdefinierten URL definiert sind.

Eine anwenderdefinierte URL sollte innerhalb von sechs Stunden in Ihrer -Instanz aktiviert werden.

Hinweis:

- Sie müssen zuerst den anwenderdefinierten URL-Datensatz aus der Instanz ServiceNow löschen und dann alle DNS-Einträge (Domain Name Server) vom DNS-Server löschen.
- Jedes Löschen des DNS-Eintrags vom DNS-Server vor dem Löschen des anwenderdefinierten URL-Datensatzes aus der Instanz ServiceNow führt dazu, dass das Löschen anderer entsprechender anwenderdefinierter URL-Datensätze aus ServiceNowblockiert wird.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwenderdefinierte URL mit Identitätsanbieter

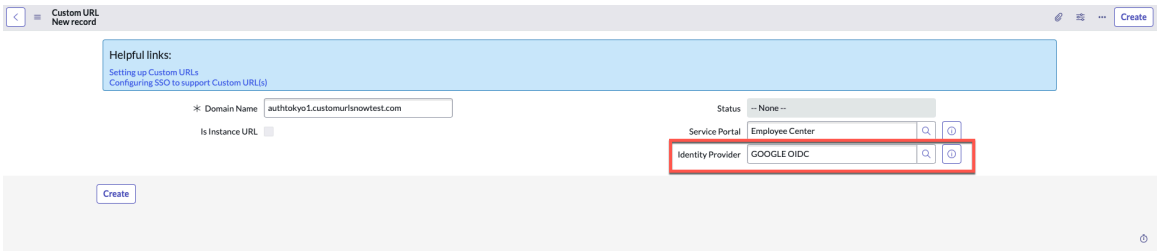
Legen Sie Ihre anwenderdefinierte URL mit dem Identitätsanbieter fest, damit sich der Anwender mit seinen IdPs anmelden kann.

Vorbereitungen

Erforderliche Rolle: admin

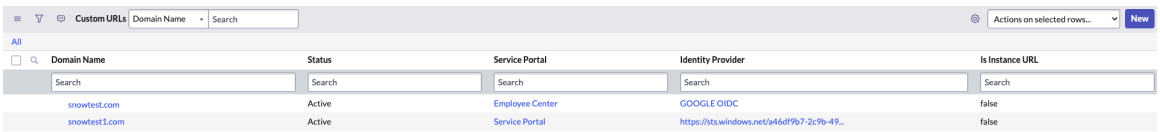
Prozedur

1. Navigieren zu **Alle** > **Anwenderdefinierte URL** > **Anwenderdefinierte URL**an.
2. Klicken Sie auf **Neu**.
3. Geben Sie die Details des IdP im Feld **Identitätsanbieter** an.
   Informationen zu anderen Feldern finden Sie unter Legen Sie eine anwenderdefinierte URL als Instanz-URL fest.



4. Klicken Sie auf **Erstellen**.

   Der Datensatz wird erstellt und auf der Seite „Anwenderdefinierte URL“ angezeigt.



   Wenn auf die anwenderdefinierte URL zugegriffen wird, wird der Benutzer zum konfigurierten Identitätsanbieter umgeleitet. In diesem Fall wird der Benutzer beim Zugriff auf `snowtest.com`zum **Mitarbeiter-Center**navigiert und dann zum Identitätsanbieter Google weitergeleitet.

   Hinweis:

   - Wenn das Feld Serviceportal leer ist und das Feld „Identitätsanbieter“ definiert ist und der Benutzer auf die anwenderdefinierte URL zugreift, wird er direkt zum konfigurierten Identitätsanbieter navigiert.
   - Wenn sowohl das Feld Serviceportal als auch das Feld Identitätsanbieter definiert sind und der Benutzer beim Zugriff auf die anwenderdefinierte URL mit dem definierten Feld [Serviceportal auf die anwenderdefinierte URL zugreift, wird er zum konfigurierten Identitätsanbieter navigiert.
   - Wenn sowohl das Feld Serviceportal als auch das Feld Identitätsanbieter definiert sind und der Benutzer beim Zugriff auf die anwenderdefinierte URL mit dem anderen, nicht definierten Portal auf den anwenderdefinierten URL zugreift, wird er zum automatisch umgeleiteten Identitätsanbieter navigiert, sofern er in der Instanz konfiguriert ist.

5. Melden Sie sich mit den Anmeldeinformationen bei der Anwendung an.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen zum anwenderdefinierten URL-Rechenzentrumsauftrag

Für jede anwenderdefinierte URL, die] Ihrer Instanz mit zugeordnet ist, gibt es einen entsprechenden ServiceNow-Rechenzentrumsauftrag, der ausgeführt wird und URL-Informationen anzeigt, die für Ihre Instanz relevant sind, wie in der Tabelle beschrieben.

Auftragsfeld	Beschreibung
Auftrags-ID	Eindeutige ID des Auftrags, der die Domäne der anwenderdefinierten URL überprüft.
Letzte Ausführung um	Datum und Uhrzeit der letzten Ausführung des Auftrags.
Nutzlast	Liste der Domänen oder anwenderdefinierten URLs, die zur CERT-Bereitstellung an das Rechenzentrum gesendet wurden.
Abrufanzahl	Anzahl der Abfragen der Ergebnisse für diesen Auftrag.
Ergebnis	Verifiziert und validiert jede Domäne und jede anwenderdefinierte URL, die in einer Nutzlast gesendet wird.
Status	Status des Rechenzentrumsauftrags.

Generieren Sie SP-Metadaten für anwenderdefinierte SAML/SSO-URL-Installationen

Bei einer SAML- oder SSO-Installation müssen die SP-Metadaten für den IdP generiert werden, bevor die anwenderdefinierte URL-Instanz generiert wird.

Vorbereitungen

Erforderliche Rolle: Administrator
Der IdP benötigt SP-Metadaten für die Instanz, um Anforderungen zu authentifizieren und weiterzuleiten.

Hinweis: Das Hinzufügen der Assertion Consumer Service-URL (SP-Anmelde-URL) kann für jeden IdP (Azure, ADFS oder Okta) unterschiedlich sein.

Prozedur

1. Wählen Sie Ihr installiertes SSO-Plugin:

Option	Bezeichnung
Mehrfachanbieter-SSO	Navigieren zu **Mehrfachanbieter-SSO** > **Identity Provider**an. Wählen Sie einen IdP aus, und klicken Sie auf die Schaltfläche **Metadaten generieren**. Die Integration generiert die SP-Metadaten der Instanz automatisch aus den Einstellungen für die Systemeigenschaft.
SAML 2 SSO	Navigieren zu **SAML 2 Single Sign-on** > **Metadaten**an. Die Integration generiert die SP-Metadaten der Instanz automatisch

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	aus den Einstellungen für die Systemeigenschaft.

2. Kopieren Sie die SP-Metadaten in das Textfeld.

Beispiel:

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
 entityID="https://yourinstance.service-now.com">
  <SPSSODescriptor AuthnRequestsSigned="false"
 WantAssertionsSigned="true"
 protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  <SingleLogoutService
 Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
 Location="https://yourinstance.service-now.com/navpage.do" />

 <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddres
s</NameIDFormat>
  <AssertionConsumerService isDefault="true" index="0"
 Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
 Location="https://yourinstance.service-now.com/navpage.do" />
  <AssertionConsumerService index="1"
 Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
 Location="https://yourinstance.service-now.com/consumer.do"/>
 </SPSSODescriptor>
</EntityDescriptor>
```

3. Stellen Sie dem IdP die SP-Metadaten der Instanz bereit.
Beispielsweise ermöglicht SSOCircle einem Benutzer, die SP-Metadaten online bereitzustellen.

4. Wahlweise: So richten Sie anwenderdefinierte URLs in Azure ein:

a. Wechseln Sie zu **App-Registrierungen**.

b. Wählen Sie im Menü **Alle Apps** aus.

c. Wählen Sie die **ServiceNow-App aus**.

d. Klicken Sie auf Einstellungen, um die URL zu konfigurieren.

5. Wahlweise: So richten Sie anwenderdefinierte URLs in Okta ein:

a. Erstellen Sie zwei ServiceNow UD Okta-Anwendungen.

b. One Okta-Anwendung für die Instanz-URL „service-now.com“.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. One Okta-Anwendung für die anwenderdefinierte URL

Hinweis:

- Deaktivieren **Sie „Authentifizierung** erzwingen“ in der Okta-Konfiguration, damit die **Testverbindung** erfolgreich ausgeführt wird.
- Wenn Sie den Identitätsanbieter-Datensatz testen, der der Basis-URL zugeordnet ist, müssen Sie sich bei der Instanz mit der Basis-URL anmelden.
- Wenn Sie den Identitätsanbieter testen, der der anwenderdefinierten URL zugeordnet ist, stellen Sie sicher, dass Sie sich mit der anwenderdefinierten URL bei der Instanz anmelden.

6. Wahlweise: Um die OAuth-Authentifizierung zu verwenden, richten Sie die Umleitungs-URL als alle registrierten anwenderdefinierten URLs in der OAuth-Anwendungsendpunktkonfiguration für die externen Client-Anwendungen ein. Die Umleitungs-URL ist gleichbedeutend mit der Rückruf-URL, an die der Autorisierungsserver umleitet.
7. Wahlweise: Zur Verwendung des Google reCAPTCHA-Service richten Sie ein API-Schlüsselpaar ein.

Fehler und Korrekturen für anwenderdefinierte URLs

Eine Liste häufiger Fehler und zugehöriger Korrekturen für die Einrichtung und Konfiguration einer anwenderdefinierten URL.

Fehler beim Setup

Fehlermeldung	Beheben
Anwenderdefinierte URL kann nicht erstellt werden. Versuchen Sie es später erneut.	Möglicherweise gibt es ein Problem außerhalb Ihrer Kontrolle, das die Erstellung der anwenderdefinierten URL beeinträchtigt. Führen Sie zu einem anderen Zeitpunkt aus, bevor Sie sich an den Support wenden. **Hinweis:** Das Erstellen einer anwenderdefinierten URL dauert normalerweise 30 Minuten. Wenn der Vorgang länger dauert, wenden Sie sich an https://support.servicenow.com/now?draw=case.
Die Anforderung für eine neue anwenderdefinierte URL kann nicht gesendet werden, da eine andere Anforderung für eine anwenderdefinierte URL für Ihre Instanz noch ausgeführt wird.	Überprüfen Sie den Status Ihrer Aufträge mit anwenderdefinierter URL, bevor Sie eine neue Anforderung senden.
Sie müssen die folgenden Eigenschaften löschen, bevor die Instanz-URL festgelegt werden kann: Glide Proxy, Glide Servlet.	

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fehlermeldung	Beheben
Die Bereitstellung von<custom_domain> ist noch in Bearbeitung. Dieser Vorgang kann bis zu x Stunden dauern. Ihr Instanzadministrator erhält eine Benachrichtigung, wenn dieser Prozess abgeschlossen ist.	Nachdem die Bereitstellung auf einer Instanz für eine anwenderdefinierte URL gestartet wurde, müssen Sie warten, bis der Prozess abgeschlossen ist, bevor sich der Status ändert.
<custom_domain>ist jetzt als neue Instanz-URL festgelegt.<base.service-now.com> ist noch in Betrieb, aber alle neuen URLs, z. B. in Benachrichtigungen, werden verwenden .	Nur eine URL kann als Instanz-URL festgelegt werden. Die anderen URLs, die Ihrer Instanz zugeordnet sind, können aktiv sein, aber nur die Instanz-URL kann Benachrichtigungen verwenden.
Die anwenderdefinierte URL<custom_domain> ist so festgelegt, dass sofort aus der Instanzkonfiguration entfernt und wiederhergestellt wird<base.service-now.com> . setzt eine Zuordnung zu dieser Instanz fort, solange der CNAME-Datensatz in Ihrem DNS festgelegt ist.	Diese Nachricht bestätigt, dass Sie Ihre anwenderdefinierte URL ändern möchten. Durch Akzeptieren dieser Bestätigung initiieren Sie die Änderung der URL zu Ihrer Instanz. Jede URL, die sich in Ihrer Domänennamenliste als anwenderdefinierte URL befindet, kann aktiv sein, es sei denn, Sie entfernen sie aus dem CNAME-Datensatz Ihres Providers.
glide.servlet.uri kann nicht geändert werden. Diese Eigenschaft wird von der anwenderdefinierten URL festgelegt.	
„glide.proxy.host“ kann nicht geändert werden. Diese Eigenschaft wird von der anwenderdefinierten URL festgelegt.	
Der CNAME-Datensatz für<custom_domain> zeigt nicht auf<base.service-now.com> .	Die Konfiguration auf der Seite des URL-Anbieters ist nicht korrekt. Überprüfen Sie Ihre Konfiguration für den CNAME-Datensatz.
Fehlender CNAME-Datensatz für<custom_domain> .	Der CNAME-Datensatz muss von Ihrem URL-Provider konfiguriert werden, bevor die anwenderdefinierte URL für Ihre Instanz festgelegt werden kann.

Installations-Exits

Installationsausgänge sind Anpassungen, die Java beenden, um ein Skript aufzurufen, bevor Sie zu Java zurückkehren.

Hinweis: Die hier beschriebene Funktionalität erfordert die **Admin**-Rolle.

Verfügbare Installations-Exits

Navigieren zu **Systemdefinition** > **Installationsausgänge**an. Einige Namen des Installationsausgangs (Anmeldung, Abmeldung, ValidatePassword, ExterneAuthentifizierung) sind reserviert und können nicht geändert werden. Andere Installationsausgänge können diese mit einem anwenderdefinierten Skript überschreiben, das das Skript im Standardinstallationsausstieg ersetzt.

Die folgenden Installations-Exits sind im Basissystem verfügbar:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installationsausgang	Beschreibung
Anmelden	Verwendet ein Anwendername-Passwort-Paar und authentifiziert sich mit dem Anwenderobjekt
Abmelden	Leitet den Anwender beim Abmelden zur Willkommensseite zurück; kann von LogoutRedirect überschrieben werden
LogoutRedirect	Leitet den Anwender beim Abmelden zu einer angegebenen URL weiter
ExterneAuthentifizierung	Authentifiziert mithilfe von Header, Parameter oder Cookie; kann von DigestSingleSignOn und PGPSingleSignOn überschrieben werden
DigestSingleSignOn	Authentifiziert sich mithilfe von Header, Parameter oder Cookie und entschlüsselt die Digest-Verschlüsselung
PGPSingleSignOn	Authentifiziert sich mithilfe von Header, Parameter oder Cookie und entschlüsselt die PGP-Verschlüsselung
Validieren SiePasswort	Standardmäßig ab Release Helsinki aktiv; Mit können Kunden ihre eigene Passwortvalidierung definieren. kann von ValidatePasswordStronger überschrieben werden
Validieren SiePasswordStronger	Erfordert, dass Passwörter mindestens 8 Zeichen lang sind und eine Ziffer, einen Großbuchstaben und einen Kleinbuchstaben enthalten
GetIntegrationSessionTimeout	Implementiert das Standardverhalten für die Zeitüberschreitung bei Integrationssitzungen.

Anmeldeänderungen

Die folgende Änderung am **Login** -Installations-Exit legt den Wert für die Sitzungszeitüberschreitung jedes Benutzers fest, während sich der Benutzer anmeldet. Wenn in diesem Beispiel der Benutzername *admin*lautet, wird für die Sitzung ein Timeout von 30 Sekunden festgelegt.

```
gs.include("PrototypeServer");

var Login = Class.create();
Login.prototype = {
 initialize : function() {
 },

        process : function() {
          // the request is passed in as a global
          var userName = request.getParameter("user_name");
          var userPassword = request.getParameter("user_password");

          var authed = GlideUser.authenticate(userName, userPassword);
          if (authed) {
             //
 ************************************************************
             // customization - if the userName == admin, set the session
             // timeout to be 30 seconds. You can implement your own
             // session timeout algorithm here by checking to see if a
 user
             // belongs to a certain group or has a certain role.
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
            // Values of setMaxInactiveInterval exceeding 1440 minutes
 are
            // treated as one day (1440 minutes).

           if (userName == "admin") {
              request.getSession().setMaxInactiveInterval(30);
            }
            //
 ************************************************************
            return GlideUser.getUser(userName);
          }

          this.loginFailed();

          return "login.failed";
        },

        loginFailed : function() {
          var message = GlideSysMessage.format("login_invalid");
          var gSession = GlideSession.get();
          gSession.addErrorMessage(message);

          var userName = request.getParameter("user_name");
          EventManager.queue("login.failed", "", userName, "");
       }

}
```

Die Zeitüberschreitung für Sitzungen kann auch entsprechend der IP-Adresse festgelegt werden.

```
gs.include("PrototypeServer");

var Login = Class.create();
Login.prototype = {
 initialize : function() {
 },

        process : function() {
          // the request is passed in as a global
          var userName = request.getParameter("user_name");
          var userPassword = request.getParameter("user_password");

          var authed = GlideUser.authenticate(userName, userPassword);
          if (authed) {

          //
 ************************************************************
          // customization - if the user is logging in from a particular
 IP
          // range starting with XXX.XXX you can implement your own
          // session timeout algorithm here by checking the login IP
          //
          // Values of setMaxInactiveInterval exceeding 1440 minutes are
          // treated as one day (1440 minutes).

          var clientIP = gs.getSession().getClientIP().toString();
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
            // if client IP starts with specified range
            if (clientIP.indexOf('XXX.XXX') == 0) {
               // set to 10 hours
               request.getSession().setMaxInactiveInterval(60 * 60 * 10);
            }
            //
 ************************************************************

               return GlideUser.getUser(userName);
            }

            this.loginFailed();

            return "login.failed";
          },

          loginFailed : function() {
            var message = GlideSysMessage.format("login_invalid");
            var gSession = GlideSession.get();
            gSession.addErrorMessage(message);

            var userName = request.getParameter("user_name");
            EventManager.queue("login.failed", "", userName, "");
          }

}
```

Zugehörige Informationen

Erzwingen Sie starke Passwörter

Authentifizierung mit IP-Adressbereich

Eine Möglichkeit, eine webbasierte Anwendung zu sichern, besteht darin, den Zugriff basierend auf der IP-Adresse einzuschränken.

Sie können den Zugriff auf eine bestimmte Adresse oder einen bestimmten Adressbereich blockieren, von denen Sie vermuten, dass sie böswilligen Personen gehören. Mit der -Instanz können Sie den Zugriff anhand der IP-Adresse steuern.

Hinweis: Verwenden Sie die Kontextrichtlinie der Vorauthentifizierung für die adaptive Authentifizierung (AA), um IP-basierte Authentifizierungen und Einschränkungen für zusätzliche Funktionen zu erzwingen. Weitere Informationen finden Sie unter Adaptive Authentifizierung.

Hinweise und Einschränkungen:

- Das System lässt Sie nicht zu, dass Sie sich aussperren. Wenn Sie also versuchen, eine Regel hinzuzufügen, die Ihre aktuelle Adresse aussperrt, warnt Sie das System und lehnt Ihre Eingabe ab.
- Wenn Sie sich in einem Unternehmensintranet befinden, gehen Sie beim Einrichten Ihrer IP-Regeln sehr vorsichtig vor. Die IP-Adresse, die Sie auf Ihrem Computer sehen (z. B. 10.10.10.25), hat keine Beziehung zu der IP-Adresse, als die Sie im Internet erscheinen. Ihr Unternehmen leitet Ihre Adresse wahrscheinlich per Proxy und/oder NAT an einen vorhersehbaren Satz ausgehender Adressen weiter, nach denen Sie wahrscheinlich Ihr Netzwerkteam fragen müssen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ein Benutzer, dessen Zugriff basierend auf einer Zugriffsregel eingeschränkt ist, ruft im Browser den Fehler 403 auf.
- Eingeschränkte Anwender verwenden keine Transaktionen, Semaphore und zählen auch nicht zum Zählen von Serverressourcen.
- Diese Funktion ersetzt oder überschreibt Ihre vorhandenen Zugriffssteuerungsregeln nicht, wenn Sie beispielsweise ein VPN für unser Rechenzentrum ausführen. Es handelt sich um eine zusätzliche Prüfung, die zusätzlich zu den Zugriffssteuerungen, die wir möglicherweise für Ihren PIX eingerichtet haben, erfüllt werden muss.
- Zulassungsregeln haben immer Vorrang vor Ablehnungsregeln. Wenn also eine Adresse sowohl zulässig (durch eine Regel) als auch abgelehnt (durch eine zweite Regel) ist, ist sie tatsächlich zulässig.
- Sternchen und CIDR-Blöcke werden derzeit nicht unterstützt.
- Bei weitergeleiteten Proxy-Adressen werden die Zulassungsregeln auf jede Adresse in der Kette und die Verweigerungsregeln auf jede Adresse in der Kette angewendet, wenn keine der Zulassungsregeln übereinstimmt.
- Die Authentifizierung auf Basis des IP-Bereichs kann die Übertragung von Update Sets bewirken. Wenn die IP-Adressen-Zugriffssteuerung für die Quellinstanz aktiviert ist, fügen Sie die IP-Adressen aller Anwendungsknoten, die Ihre Instanz unterstützen, als Ausnahmen hinzu.

  Hinweis: Melden Sie sich bei an, um die IP-Adresse Ihrer Instanz zu finden ServiceNow NOW Support , und suchen Sie nach dem Servicekatalogelement **Meine IP-Informationen**.

Hinweis: Weitere Informationen zu den Eigenschaften *com.snc.ipauthenticator* und *glide.ip.authenticate.strict*, die den Instanzzugriff auf bestimmte IP-Bereiche einschränken, finden Sie in den folgenden Themen unter Härtungseinstellungen für Instanzsicherheit:

- Beschränken Sie den Zugriff auf bestimmte IP-Bereiche
- Strikte IP-Beschränkung

IP-Adressen-Zugriffssteuerung

Wenden Sie eine IP-Zugriffssteuerung auf ausgehenden, eingehenden oder bidirektionalen Datenverkehr an. Das System blockiert eine IP-Adresse nur, wenn eine übereinstimmende Ablehnungsregel vorhanden ist und keine übereinstimmende Zulassungsregel vorhanden ist. Standardmäßig gibt es keine Einschränkungen für den Zugriff auf Ihre Instanz.

Vorbereitungen

Erforderliche Rolle: admin

Hinweis: Verwenden Sie die Kontextrichtlinie der Vorauthentifizierung für die adaptive Authentifizierung (AA), um IP-basierte Authentifizierungen und Einschränkungen für zusätzliche Funktionen zu erzwingen. Weitere Informationen finden Sie unter Adaptive Authentifizierung.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **IP-Adressen-Zugriffssteuerung** , um eine Liste Ihrer IP-Zugriffssteuerungen anzuzeigen.
   Möglicherweise müssen Sie das Plugin „Auf dem IP-Adressbereich basierende Authentifizierung“ [com.snc.ipauthenticator] aktivieren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Füllen Sie das Formular aus.

Hinweis: Melden Sie sich bei an, um die IP-Adresse Ihrer Instanz zu finden ServiceNow NOW Support , und suchen Sie nach dem Servicekatalogelement **Meine IP-Informationen**.

Feld	Beschreibung
Typ	Typ der einzuschließenden Zugriffssteuerungsregel. ◦ *Zulassen*: Jede IP-Adresse in diesem Bereich kann mit dieser Instanz interagieren. ◦ *Ablehnen*: Eine IP-Adresse in diesem Bereich kann nicht mit dieser Instanz interagieren, es sei denn, sie ist in einer Zulassungsregel aufgeführt. Wenn Sie Ablehnungsregeln hinzufügen, können Sie außerdem nicht Ihre eigene öffentliche IP-Adresse verweigern, oder Ihre Instanz aktualisiert keine Verweigerungsregel. **Hinweis:** Zur Unterstützung von Wartung, Upgrades und Kundenservice und Supportkönnen einige interne IPs von ServiceNow nicht durch Verweigerungsregeln blockiert werden.
Richtung	Richtung der IP-Zugriffssteuerungsregel. ◦ **Eingehend**: Lässt eingehende Transaktionen zu oder verweigert sie. Dies sind Transaktionen, die von außerhalb Ihrer Instanz initiiert werden. ◦ **Ausgehend**: Lässt ausgehende Transaktionen zu oder verweigert sie. Dies sind Transaktionen, die von Ihrer Instanz aus initiiert wurden. ◦ **Bidirektional**: Lässt eingehende und ausgehende Transaktionen zu oder verweigert sie.
Aktiv	Wenn diese Option ausgewählt ist, ist das Formular aktiv.
Beschreibung	Beschreibung der Zugriffssteuerung.
Bereichsstart	Startbereich von IP-Adressen, die zugelassen oder abgelehnt werden sollen. **Hinweis:** Diese Regeln wirken sich auch auf die Übertragung von Update Sets aus. Um sicherzustellen, dass die IP-Adressen-Zugriffssteuerung nicht zum Fehlschlagen von Update-Sätzen führt, fügen Sie die Zielinstanz als Ausnahme hinzu.
Bereichsende	Endbereich von IP-Adressen, die zugelassen oder abgelehnt werden sollen. **Hinweis:** Um den Zugriff auf bestimmte VPN-Adressen zu beschränken, geben Sie im Feld **Ablehnen** einen Ablehnungsbereich von **0,0.0.0** bis **255.255.255.255** ein, und geben Sie nur die spezifischen zulässigen VPN-Bereiche ein.

3. Klicken Sie auf **Absenden**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Suchen Sie nach abgelehnten IP-Adressen

Suchen Sie in den Knotenprotokolldateien der Instanz nach abgelehnten IP-Adressen.

Vorbereitungen
Erforderliche Rolle: admin.

Warum und wann dieser Vorgang ausgeführt wird
Protokolleinträge für blockierte IP-Adresse werden wie folgt angezeigt: `2015-10-21 18:37:43 (175) http-30 WARNUNG *** WARNUNG *** Sicherheitsbeschränkung: Zugriff eingeschränkt (xx.xx.xxx.xxx nicht autorisiert).`

Hinweis: Abgelehnte IP-Adressen sind die Knotenprotokolldateien der sichtbaren Instanz, die in den Systemprotokollen nicht sichtbar sind.

Prozedur

1. Navigieren zu **Alle** > **Systemprotokolle** > **Dienstprogramme** > **Knotenprotokolldateibrowser**an.
2. Durchsuchen Sie die Protokolle nach Kriterien wie Zeitraum und Nachricht.
3. Sie können Protokolldateien auch herunterladen, wenn Sie wissen, nach welchem Protokoll Sie suchen, indem Sie zu navigieren **Systemprotokolle** > **Dienstprogramme** > **Knotenprotokolldatei-Download**an.

LDAP-Integration

Mit einer LDAP-Integration kann Ihre -Instanz Ihren vorhandenen LDAP-Server als primäre Quelle für Benutzerdaten verwenden.

Administratoren integrieren mit einem LDAP-Verzeichnis (Leighted Directory Access Protocol), um den Benutzeranmeldungsprozess zu optimieren und administrative Aufgaben wie das Erstellen und Zuweisen von Rollen für Benutzer zu automatisieren. Eine LDAP-Integration ermöglicht es dem System, Ihren vorhandenen LDAP-Server als primäre Quelle für Benutzerdaten zu verwenden. Normalerweise ist eine LDAP-Integration auch Teil einer Single Sign-on-Implementierung.

Die Integration verwendet die Anmeldeinformationen des LDAP-Servicekontos, um den Benutzernamen (DN) vom LDAP-Server abzurufen. Angesichts des DN-Werts für den Benutzer führt die Integration dann eine erneute Bindung an LDAP mit dem DN und Passwort des Benutzers durch. Das vom Benutzer eingegebene Passwort ist vollständig in der HTTPS-Sitzung enthalten. Die Integration speichert niemals LDAP-Passwörter.

Die Integration verwendet eine schreibgeschützte Verbindung, die nie in das LDAP-Verzeichnis schreibt. Die Integration fragt nur Informationen ab und aktualisiert dann ihre interne Datenbank entsprechend.

Hinweis: Ausführliche Informationen zum Einrichten der Integration finden Sie unter Setup der LDAP-Integration.

Hinweis: Wenn Ihre Instanz eine LDAP-Integration verwendet und die Active Directory-Einstellungen erfordern, dass Anwender ihr Passwort bei der Anmeldung zurücksetzen, können sich Ihre Anwender nicht bei der Instanz anmelden. Die Instanz kann das Active Directory-Passwort eines Anwenders nicht ändern.

Funktionen der LDAP-Integration

Die Funktionen der LDAP-Integration umfassen Folgendes.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geplante LDAP-Aktualisierung

Ein geplanter Scan Ihres LDAP-Servers wird normalerweise einmal pro Nacht ausgeführt. Fragt die Attribute aller zutreffenden Anwenderdatensätze ab und vergleicht sie mit dem Account auf unseren Servern. Bei einem Unterschied ändern wir unseren Benutzerdatensatz mit dem geänderten Attribut. Die Belastung des LDAP-Servers während der Aktualisierung hängt davon ab, wie viele Datensätze abgefragt werden und wie viele Attribute verglichen werden. Wir empfehlen, die Aktualisierung außerhalb von Spitzenzeiten zu planen. Ein umfangreicher Aktualisierungsvorgang kann sich auf andere geplante Vorgänge auswirken, z. B. das Ausführen von Berichten, und sollte so geplant werden, dass Konflikte so gering wie möglich gehalten werden.

LDAP-Listener

Der LDAP-Listener ist unsere Version einer persistenten Abfrage (oder persistenten Suche). Wir stellen eine Dauerabfrage für Änderungen, die an Ihrem LDAP-Server vorgenommen wurden, und warten ständig nach einer Antwort. Vorausgesetzt, Ihr Server unterstützt eine persistente Suche, werden alle an einem Ihrer zutreffenden LDAP-Accounts vorgenommenen Änderungen an den LDAP-Listener zurückgegeben und innerhalb von etwa 10 Sekunden an Ihre Instanz gesendet. Dies ist ein äußerst nützliches Tool, mit dem wir eine Kopie der Accountdetails Ihrer Anwender nahezu in Echtzeit erstellen können, ohne auf die nächste geplante Aktualisierung warten zu müssen.

LDAP-Anmeldung bei Bedarf

Nachdem eine LDAP-Integration eingerichtet wurde, kann die Instanz neuen Benutzern erlauben, sich beim System anzumelden, auch wenn sie noch keinen Account bei der Instanz haben. Wenn ein neuer Benutzer versucht, sich bei der Instanz anzumelden, prüft die Integration, ob dieser Benutzer über einen Account in der Instanz verfügt. Wenn die Integration keinen vorhandenen Anwenderaccount findet, fragt sie automatisch den LDAP-Server nach dem eingegebenen Anwendernamen ab. Wenn ein passender LDAP-Account gefunden wird, versucht die Integration, sich mit dem vom Anwender eingegebenen Passwort zu authentifizieren. Wenn das Passwort gültig ist, erstellt die Instanz einen Account für den Anwender, füllt den Account mit allen zutreffenden LDAP-Informationen aus und meldet den Anwender bei der Instanz an.

Bei der bedarfsgesteuerten Anmeldung wird die Transformationszuordnung LDAP-Anwenderimport verwendet. Weitere Informationen zu Anforderungen für Transformationszuordnungen finden Sie unter LDAP-Transformationszuordnungen.

LDAP-Datenauffüllung

Hinweis: Die in dieser Integration beschriebene Funktionalität ist standardmäßig nicht verfügbar. Diese Integration umfasst Anpassungen nach der Bereitstellung, die von einem erfahrenen Administrator oder von ServiceNow Professional Services-Beratern durchgeführt werden.

Eine Integration mit den LDAP-Servern ermöglicht Ihnen, die Datenbank der Instanz schnell und einfach mit Benutzerdatensätzen aus der vorhandenen LDAP-Datenbank zu füllen. Um Inkonsistenzen bei Daten zu vermeiden, können Sie eingehende LDAP-Datensätze erstellen, ignorieren oder überspringen.

Sie können auch die von der Integration importierten Daten begrenzen, indem Sie LDAP-Attribute angeben, wodurch nur die Daten importiert werden, die Sie für eine Instanz verfügbar machen möchten. Normalerweise werden die von Ihnen angegebenen LDAP-Attribute Teil der

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integrationstransformationszuordnung. Wenn Sie keine LDAP-Attribute angeben, importiert die Integration alle verfügbaren Objektattribute vom LDAP-Server. Die Instanz speichert importierte LDAP-Daten in temporären Importsatztabellen. Je mehr Attribute Sie importieren, desto länger dauert der Import. Weitere Informationen finden Sie unter Geben Sie die LDAP-Attribute an.

LDAP-Authentifizierung

Verwenden Sie die LDAP-Authentifizierung für den Zugriff mit LDAP-Anmeldeinformationen.

Wenn ein Benutzer auf der Anmeldeseite Netzwerkanmeldeinformationen eingibt:

1. Die Instanz übergibt die Anmeldeinformationen an einen LDAP-Server, um die Instanz zu finden.
2. Bei RDNs validiert sie die DN-Zeichenfolge des Benutzers. Sie wird nur validiert, wenn für mindestens eine der LDAP-OU-Konfigurationen mit `„table=sys_user“` ein RDN konfiguriert ist.
3. Der LDAP-Server antwortet mit einer autorisierten oder nicht autorisierten Nachricht, die vom System verwendet wird, um zu bestimmen, ob der Zugriff gewährt werden soll.

Durch die Authentifizierung bei Ihrem LDAP-Server greifen Benutzer mit denselben Anmeldeinformationen auf die Plattform zu, die sie für andere interne Ressourcen in Ihrer Netzwerkdomäne verwenden. Außerdem können Sie vorhandene Passwort- und Sicherheitsrichtlinien wiederverwenden, die bereits vorhanden sind. Beispielsweise können für den LDAP-Server bereits Richtlinien für Kontosperrung und Passwortablauf gelten.

Wenn Sie LDAP aktivieren, aktualisiert das System die Anwenderdatensätze mit diesen Feldern.

Aktualisierungen des LDAP-Benutzerdatensatzes

Feld	Beschreibung
Quelle	Gibt an, ob LDAP zur Validierung eines Anwenders verwendet wird oder nicht. Wenn die Quelle mit LDAP beginnt, wird der Benutzer über LDAP validiert. Wenn die Quelle nicht mit LDAP beginnt, wird das Passwort im Benutzerdatensatz verwendet, um den Benutzer bei der Anmeldung zu validieren.
LDAP-Server	Gibt an, welcher LDAP-Server den Anwender authentifiziert, wenn mehrere LDAP-Server vorhanden sind.

Hinweis: Das System unterstützt keine LDAP-Passwortauthentifizierung über einen MID Server. Eine Instanz muss in der Lage sein, eine direkte Verbindung mit einem LDAP-Server herzustellen, um die Passwortauthentifizierung zu unterstützen.

Informationen zur LDAP-Integration

Mit einer LDAP-Integration kann Ihre -Instanz Ihren vorhandenen LDAP-Server als primäre Quelle für Benutzerdaten verwenden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Voraussetzungen für die LDAP-Integration

- Der Verzeichnisserviceserver muss LDAP v3-konform sein
- Eingehender Netzwerkzugriff durch die Firewall muss zugelassen werden (zum LDAP Server)
- Externe IP oder Name des LDAP-Servers
- Benutzeranmeldeinformationen mit schreibgeschütztem Zugriff
- Für LDAPS ein PKI-Zertifikat

Timing für die LDAP-Integration

LDAP-Integrationen werden normalerweise vor dem Go-Live der Instanz durchgeführt, können jedoch jederzeit integriert werden.

Datenintegrität des LDAP-Servers

Einige Benutzer machen sich Sorgen, dass eine Drittpartei (in diesem Fall die Instanz) Änderungen an Ihrem LDAP-Server vornimmt (schreibt). Bei einer LDAP-Integration schreibt Ihre Instanz nicht in das interne LDAP-Verzeichnis. Die Instanz fragt Informationen ab und aktualisiert ihre Datenbank entsprechend.

Es werden von der Instanz keine Änderungen am internen LDAP-Server vorgenommen. Der Serviceaccount ist schreibgeschützt.

Die meisten Änderungen (einschließlich Ergänzungen) an Ihrem LDAP-Server stehen der Instanz innerhalb von Sekunden zur Verfügung, je nachdem, wie viele Komponenten der vollständigen LDAP-Integration vorhanden sind.

Damit LDAP-Datensätze synchron bleiben, planen Sie einen regelmäßigen Scan des LDAP-Servers, um Änderungen zu erfassen.

Die Instanz synchronisiert keine Abteilungsdatensätze. Anwender und Gruppenmitgliedschaften werden vom LDAP-Listener-Mechanismus und einer täglichen vollständigen LDAP-Suche auf dem neuesten Stand gehalten. Die Instanz löscht jedoch keine dieser Einträge, nachdem sie aus LDAP entfernt wurden.

Wenn ein Eintrag gelöscht wird, wird auch der gesamte Verlauf gelöscht, und alle Verweise darauf werden gelöscht. Configuration Items (CIs), SLA-Vereinbarungen, Softwarelizenzen, Bestellungen und Servicekatalogeinträge haben alle einen Verweis auf die Abteilung. Wenn die Abteilung gelöscht wird, werden diese Verweise gelöscht. Es gibt viele Verweise auf Anwender, und wenn ein Anwender gelöscht wird, geht der gesamte Verlauf dessen verloren, was er getan hat. Derzeit wird die Entscheidung, ob gelöscht wird oder nicht, von unseren Kunden getroffen.

Sicherheit

Die Verbindung wird von einem einzelnen Computer mit einer festen IP-Adresse über einen bestimmten Port in Ihrer Firewall hergestellt. Die Authentifizierung erfolgt mit einem schreibgeschützten LDAP-Account Ihrer Wahl. Sie können Standard-LDAP verwenden oder die öffentliche Seite eines in Ihrem Verzeichnis installierten SSL-Zertifikatsladen. In diesem Fall können Sie LDAPS verwenden. Um eine weitere Sicherheitsebene hinzuzufügen, bieten wir auch einen Punkt-zu-Punkt-IPSEC-VPN-Tunnel an. Wenden Sie sich an Ihren Account Manager, um Details und Preise zu erfahren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sichere LDAP-Verbindungen

Verbindung	Beschreibung
MID-Server	Um Ihren LDAP-Server vor externem Netzwerkverkehr zu schützen, installieren Sie einen MID-Server im lokalen Netzwerk, und konfigurieren Sie das System so, dass die Kommunikation mit dem MID-Server über einen sicheren Kanal erfolgt.
LDAPS	Zum Herstellen einer verschlüsselten LDAPS-Verbindung laden Sie die öffentliche Seite des SSL-Zertifikats Ihres LDAP-Servers. Die Integration verwendet das -Zertifikat, um die gesamte Kommunikation zwischen dem LDAP-Server und der -Instanz zu verschlüsseln.
VPN	Wenn Sie den LDAP-Server mit einem verschlüsselten Punkt-zu-Punkt-IPSEC-VPN-Tunnel sichern möchten, wenden Sie sich an Ihren Account Manager, um Details und Preise zu erfahren.

Ein weiterer zu berücksichtigender Sicherheitsaspekt sind die in einer LDAP-Integration gemeinsam genutzten Daten. Um die für Ihre Instanz verfügbar gemachten Daten zu begrenzen, geben Sie Attribute in Ihrer Transformationszuordnung an. Weitere Informationen finden Sie unter LDAP-Transformationszuordnungen.

LDAP-Daten werden in die Instanz importiert

Es wird empfohlen, Attribute zu definieren, um nur die erforderlichen Daten zu importieren. Definierte Attribute werden der Instanzbenutzerdatenbank zugeordnet.

Die Frage, welche spezifischen Attribute benötigt werden, können wir nicht beantworten, da dies vom Umfang des Projekts und den Geschäftsanforderungen abhängt.

Unterstützte Typen von LDAP-Servern

Die Instanz wurde erfolgreich in Microsoft Active Directory, Novell, Domino (lotus Notes) und Open LDAP integriert. Wir verwenden JNDI als Schnittstelle zum LDAP Server. Solange Ihr LDAP-Server LDAP v3-konform ist, ist die Integration erfolgreich.

LDAP Single Sign-on

Neben der mit dem LDAP-Import bereitgestellten Funktion zum Auffüllen von Daten können Sie auch die von der Anwendung unterstützte externe Authentifizierungsfunktion verwenden, um zu verhindern, dass Ihre Benutzer sich jedes Mal neu anmelden müssen.

Mehrere LDAP-Domänen

Die empfohlene Methode für den Umgang mit mehreren Domänen besteht in der Erstellung eines separaten LDAP-Server-Datensatzes für jede Domäne. Jeder LDAP-Serverdatensatz muss auf einen Domänencontroller für diese Domäne verweisen. Dies bedeutet, dass das lokale Netzwerk Verbindungen mit jedem der Domänencontroller zulassen muss.

Nach der Erweiterung auf mehr als eine Netzwerkdomäne ist es wichtig, dass Sie eindeutige LDAP-Attribute für die Anwendungsanwendernamen und Importkoaleszenzwerte identifizieren. Ein allgemeines eindeutiges Zusammenfügungsattribut für Active Directory ist objectSid . Eindeutige Anwendernamen können je nach LDAP-Datendesign variieren. Allgemeine Attribute sind „ `email` “ oder „`userPrincipalName`“.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Grenzwerte für Verarbeitungsabfragen

Standardmäßig gilt für Active Directory 2000/2003 ein LDAP-Abfragelimit (maxPageSize) von 1000 Objekten, um übermäßige Last und Denial-of-Service-Angriffe zu verhindern. Es gibt zwei Methoden, um mit dieser Grenze umzugehen.

Standardmäßig wird die Abfrage so aufgeteilt, dass weniger als 1000 Objekte gleichzeitig zurückgegeben werden. Abfragen Sie beispielsweise nur nach Objekten, die mit dem Buchstaben „a“ beginnen, und fragen Sie dann nach „b“-Objekten ab. Die effizientere Methode für große Umgebungen besteht darin, Paging zu aktivieren. Paging wird standardmäßig auf allen Microsoft Active Directory-Servern unterstützt. Die Ergebnisse werden automatisch in mehrere Ergebnissätze aufgeteilt, sodass die Abfrage nicht in mehrere Anforderungen aufgeteilt werden muss.

LDAP-Abfragetyp

Bei Angabe eines LDAP-Passworts wird eine einfache Bindung durchgeführt. Wenn kein LDAP-Passwort angegeben wird, wird „none“ verwendet. In diesem Fall muss der LDAP-Server eine anonyme Anmeldung zulassen.

LDAP-Authentifizierung

Wir verwenden die bereitgestellten Servicekonto-Anmeldeinformationen für LDAP, um den Anwender-DN vom LDAP-Server abzurufen. Angesichts des DN-Werts für den Anwender erfolgt dann eine erneute Bindung mit LDAP anhand des DN des Anwenders und des bereitgestellten Passworts.

Passwortspeicher

Das vom Benutzer eingegebene Passwort ist vollständig in seiner HTTPS-Sitzung enthalten. Wir speichern dieses Passwort nirgendwo.

Richten Sie die LDAP-Authentifizierung ein

Diese Felder im Benutzerdatensatz beziehen sich auf LDAP:

- **Quelle**: Das Feld „Quelle“ gibt an, ob ein Anwender mit LDAP validiert wurde. Wenn das Quellfeld mit „ldap“ beginnt, wird der Anwender über LDAP validiert. Wenn das Feld „Quelle“ nicht mit „ldap“ beginnt, wird das Passwort im Benutzerdatensatz verwendet, um den Benutzer bei der Anmeldung zu validieren.
- **LDAP-Server**: Die Instanz unterstützt mehrere LDAP-Server, sodass das Feld LDAP-Server bestimmt, welcher Server zur Authentifizierung des Anwenders verwendet werden soll.

Anforderungen für die LDAP-Integration

Überprüfen Sie die Anforderungen für die LDAP-Integration, die ein PKI-Zertifikat und einen LDAP-konformen Verzeichnisdienstserver umfassen.

Für die LDAP-Integration benötigen Sie:

- Ein LDAP v3-konformer Verzeichnisdienstserver
  - Ermöglicht eingehenden Netzwerkzugriff über die Firewall (zum LDAP-Server)
  - (Optional) Akzeptiert die anonyme Anmeldung
  - (Optional) Unterstützt Paging für große LDAP-Abfragen

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die externe IP-Adresse oder der vollständig qualifizierte Domänenname des LDAP-Servers. Sie können auch einen MID-Server verwenden.
- Ein schreibgeschütztes LDAP-Konto Ihrer Wahl
- Bei mehreren Domänen Netzwerkzugriff für jeden Domänencontroller
- Für LDAPS ein PKI-Zertifikat
- Für den LDAP-Listener ein Microsoft Active Directory-Server, der persistente Abfragen unterstützt (ADNotify)

Unterstützte LDAP-Server

Die Instanz wurde erfolgreich in die folgenden Server integriert, da JNDI als Schnittstelle mit dem LDAP-Server verwendet wird:

- Microsoft Active Directory
- Novell
- Domino (Flower Notes)
- Öffnen Sie LDAP

LDAP-Abfragegrenzwerte

Standardmäßig gilt für Active Directory 2000/2003 ein LDAP-Abfragelimit (maxPageSize) von 1000 Objekten, um übermäßige Last und Denial-of-Service-Angriffe zu verhindern. Das System hat zwei Methoden, um mit diesem Grenzwert umzugehen.

- Standardmäßig wird die Abfrage so aufgeteilt, dass weniger als 1000 Objekte gleichzeitig zurückgegeben werden. Abfragen Sie beispielsweise nur nach Objekten, die mit dem Buchstaben „a“ beginnen, und fragen Sie dann nach „b“-Objekten ab.
- Die effizientere Methode für große Umgebungen besteht darin, Paging zu aktivieren, das standardmäßig auf allen Microsoft Active Directory-Servern unterstützt wird. Durch Paging werden die Ergebnisse automatisch in mehrere Ergebnissätze aufgeteilt, sodass die Integration die Abfrage nicht in mehrere Anforderungen aufteilen muss.

Setup der LDAP-Integration

Administratoren können die LDAP-Integration aktivieren, um die Anmeldung von Benutzern aus dem LDAP-Verzeichnis ihres Unternehmens zu ermöglichen.

LDAP verwendet normalerweise eine dieser Arten von Kommunikationskanälen.

LDAP-Kommunikationskanäle

Verbindung	Beschreibung	LDAP-Importunterstützung?	Unterstützung für LDAP-Authentifizierung?
MID-Serververbindung	Kommuniziert standardmäßig über HTTP auf Port 80. Für diesen Kommunikationskanal ist kein Zertifikat erforderlich. Die Verbindung zwischen dem MID-Server und der Instanz erfolgt über HTTPS (Port 443). Sie können den MID-Server zum Importieren von	Ja	Nein

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

LDAP-Kommunikationskanäle (Fortsetzung)

Verbindung	Beschreibung	LDAP-Importunterstützung?	Unterstützung für LDAP-Authentifizierung?
	Daten über LDAP verwenden, aber Sie können den MID-Server nicht für die LDAP-Authentifizierung verwenden. Fahren Sie mit dem Definieren des LDAP-Servers fort.		
Standard-LDAP-Integration	Kommuniziert standardmäßig über TCP auf Port 389. Für diesen Kommunikationskanal ist kein Zertifikat erforderlich. Fahren Sie mit dem Definieren des LDAP-Servers fort.	Ja	Ja
SSL-verschlüsselte LDAP-Integration (LDAPS)	Kommuniziert standardmäßig über TCP auf Port 636. Dieser Kommunikationskanal erfordert ein Zertifikat. Fahren Sie mit Installieren Sie das LDAP X.509-SSL-Zertifikat fort, um das Zertifikat abzurufen und hochzuladen.	Ja	Ja
VPN-Verbindung	Kommuniziert über einen IPSEC-Tunnel. Erwerben oder erstellen Sie einen IPSEC-Tunnel in Ihrem lokalen Netzwerk. Fahren Sie mit dem Definieren des LDAP-Servers fort.	Ja	Ja

Bei Verwendung eines MID-Servers stellt der MID-Server eine Verbindung zur -Instanz her und der MID-Server stellt außerdem eine Verbindung zum LDAP-Server her. In beiden Fällen initiiert der MID Server die Verbindung:

1. Zuerst stellt der MID-Server über LDAP an Port 389 eine Verbindung zum LDAP-Server her.
2. Dann initiiert der MID Server eine HTTPS-verschlüsselte Verbindung zur Instanz an Port 443, um die Daten zur Instanz zu übertragen.

Weitere Informationen zu VPNs, MID-Servern und LDAP finden Sie unter Sie benötigen kein VPN Teil II in der Community.

Installieren Sie das LDAP X.509-SSL-Zertifikat

Sie können ein X.509-Zertifikat für Ihre LDAP-Integration installieren.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Erwerben oder generieren Sie ein SSL-Zertifikat auf Ihrem LDAP-Server.
2. Navigieren zu **LDAP** > **Zertifikat** und klicken Sie auf **Neu**.
3. Füllen Sie die Formularfelder aus:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Der Zertifikatname.
Ablaufbenachrichtigung	Wählen Sie diese Option aus, um eine Benachrichtigung an die Anwender zu senden, die im Feld Bei **Ablauf benachrichtigen** ausgewählt sind. Dies ist standardmäßig aktiviert.
Benachrichtigung bei Ablauf	Wählen Sie die Anwender aus, um die Benachrichtigung über den Ablauf des Zertifikats wiederzugeben. Wenn keine Benutzer ausgewählt sind, wird der angemeldete Benutzer standardmäßig zusammen mit den letzten beiden angemeldeten Benutzern mit der Administratorrolle hinzugefügt.
Tage vor Ablauf benachrichtigen	Die Anzahl der Tage vor Ablauf, in der die Instanz die Benachrichtigung sendet. Geben Sie einen Wert von mindestens 20 ein. Bei Instanzen, die auf Istanbul und höher aktualisiert wurden, ist dieser Wert auf 20 festgelegt, sofern kein größerer Wert angegeben ist.
Aktiv	Ein Kontrollkästchen, das angibt, dass dieses Zertifikat aktiv ist.
Format	Das Format des Zertifikats.
Typ	Der Zertifikatcontainer. Die Instanz von erkennt Zertifikate aus Truststores, Java-Schlüsselspeichern und PKCS#12-Schlüsselspeichern.
Gültig ab	Die Instanz fügt diesem Feld automatisch das Gültigkeitsdatum des Zertifikats hinzu. Hängen Sie das Zertifikat an den X.509-Zertifikatdatensatz an, um dieses Feld auszufüllen.
Läuft ab	Die Instanz fügt automatisch das Ablaufdatum des Zertifikats zu diesem Feld hinzu. Hängen Sie das Zertifikat an den X.509-Zertifikatdatensatz an, um dieses Feld auszufüllen.
Läuft in Tagen ab	Die berechnete Anzahl von Tagen bis zum Ablauf.
Kurzbeschreibung	Eine Beschreibung für das Zertifikat.
Bearbeiter	Die Instanz fügt den Zertifikataussteller diesem Feld automatisch hinzu. Hängen Sie das Zertifikat an den X.509-Zertifikatdatensatz an, um dieses Feld auszufüllen.
Betreff	Die Instanz fügt den Zertifikatantragsteller automatisch zu diesem Feld hinzu. Hängen Sie das Zertifikat an den X.509-Zertifikatdatensatz an, um dieses Feld auszufüllen.
PEM-Zertifikat	Geben Sie den Wert des X509-Zertifikats ein.

Hinweis: Die Integration signiert das Zertifikat derzeit nicht in der Kommunikation zwischen der Instanz und dem IdP.

4. Klicken Sie auf **Speichern**.

Nächste Maßnahme

Klicken Sie auf **Stores/Zertifikate validieren**, um den Truststore und das Zertifikat zu testen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Definieren Sie einen LDAP-Server

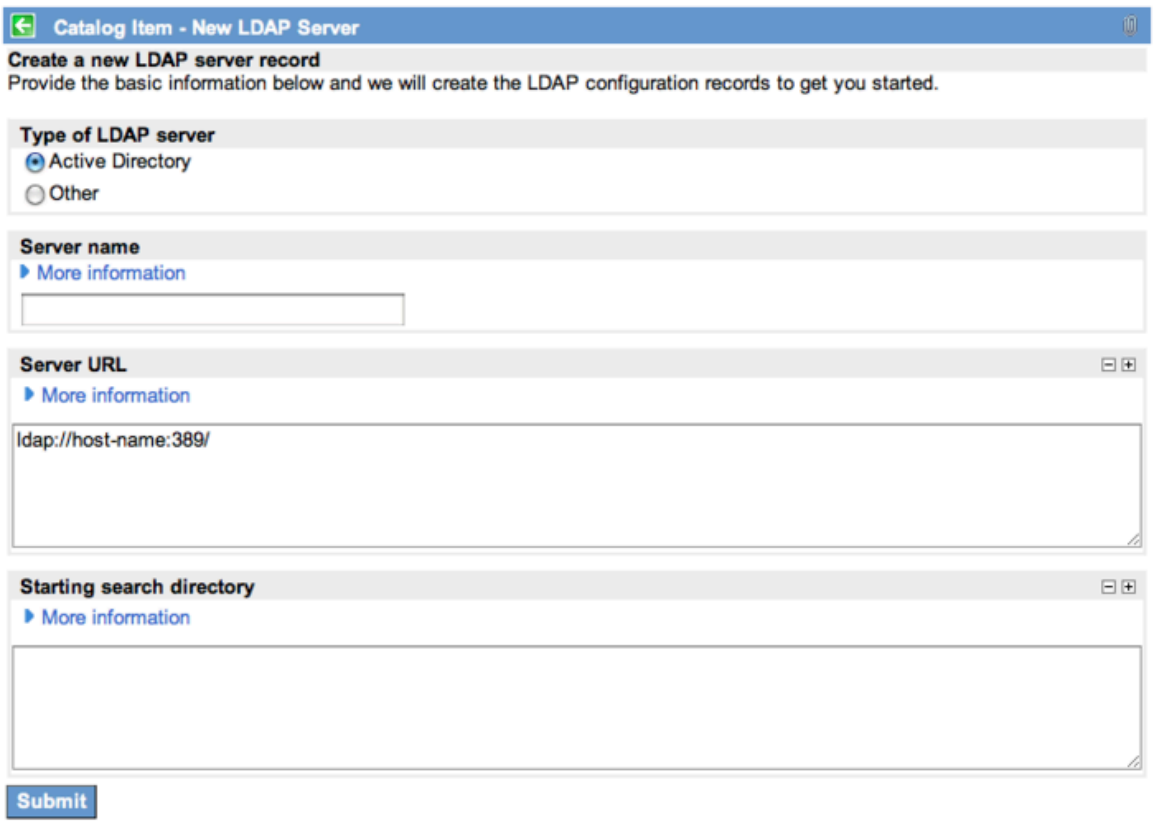
Erstellen Sie einen neuen LDAP-Server-Datensatz in der -Instanz.

Vorbereitungen

Erforderliche Rolle: admin.

Prozedur

1. Navigieren zu **Alle** > **System-LDAP** > **Neuen Server erstellen**an.
2. Füllen Sie die Formularfelder aus.



Im Feld **Server-URL** werden die gültigen URLs aller Server durch ein Leerzeichen getrennt. Server werden zuerst nach dem Betriebsstatus sortiert, wobei die Server, die sich in der Liste befinden, zuerst und dann nach dem von **Ihnen angegebenen Reihenfolgewertsortiert** werden. Der erste aufgeführte Server ist der primäre LDAP-Server. Bei den anderen handelt es sich um redundante Server.

Hinweis: Es gibt eine geringfügige Verzögerung zwischen der Änderung des tatsächlichen Betriebsstatus und der Anzeige.

Alternativ können Sie einen redundanten LDAP-Server hinzufügen, indem Sie zu einem vorhandenen LDAP-Server-Datensatz navigieren und eine Zeile in die eingebettete Liste der LDAP-Server-URLs einfügen.

3. Klicken Sie auf **Absenden**.

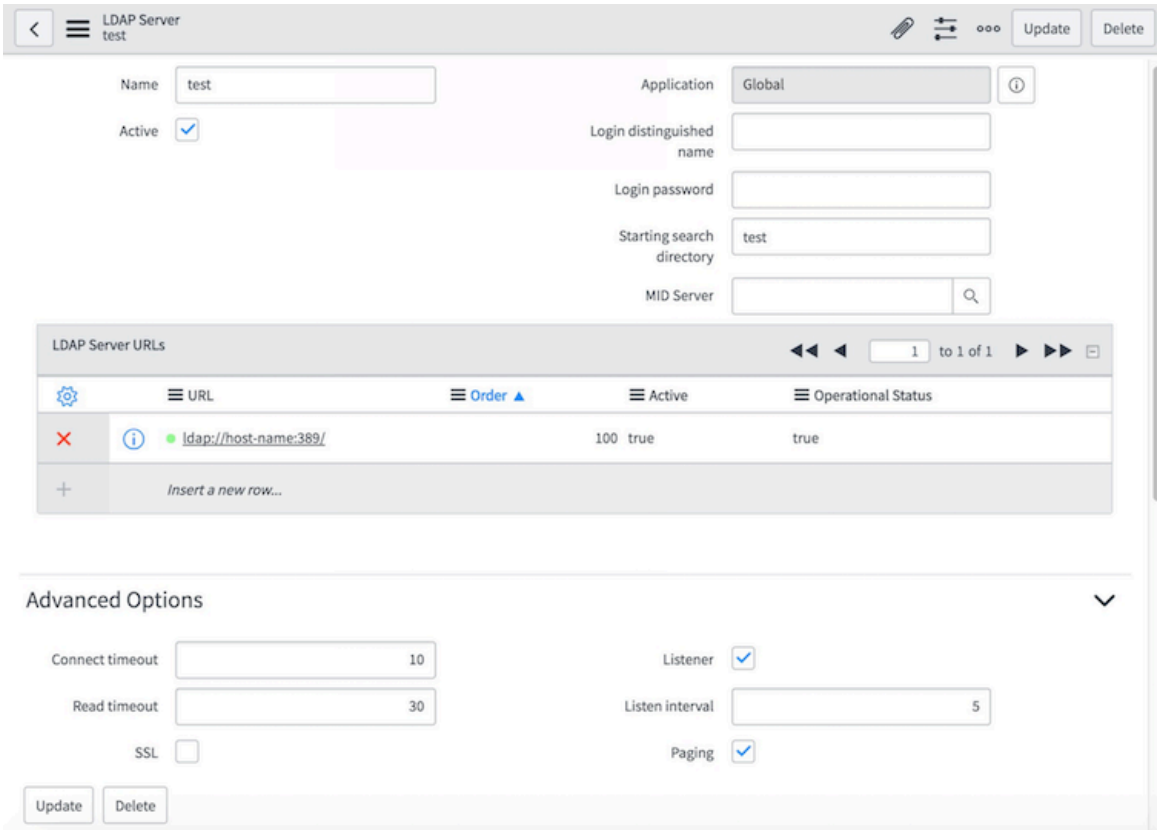
Hinweis: Sie können auch einen vorhandenen LDAP-Server-Datensatz ändern, indem Sie zu navigieren **System-LDAP** > **LDAP-Server** und nimmt die erforderlichen Änderungen vor.

4. Nehmen Sie bei Bedarf Änderungen an den Feldern vor.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular des LDAP-Servers



Feld	Beschreibung
Name	Geben Sie den Namen des Servers ein.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, wenn der Server aktiv ist.
LDAP-Server-URLs	Geben Sie die URLs des primären und des Sicherungs-LDAP-Servers ein. Server werden zuerst nach dem Betriebsstatus sortiert, wobei die Server, die sich in der Liste befinden, zuerst und dann nach dem von Ihnen angegebenen Reihenfolgewert sortiert werden. Der erste aufgeführte Server ist der primäre LDAP-Server. Bei den anderen handelt es sich um redundante Server.
Server-URL	Geben Sie die URL des Servers ein. Konfigurieren Sie das Formular so, dass dieses Feld bei Bedarf hinzugefügt wird. Es handelt sich um ein berechnetes schreibgeschütztes Feld, das die Liste der LDAP-Server anzeigt, die Sie auch im Feld **LDAP-Server-URLs** sehen, durch ein Leerzeichen getrennt und nach Betriebsstatus und Reihenfolgewert der URLs geordnet.
Eindeutiger Anmeldename	Geben Sie den Distinguished Name (DN) des Anwenders ein, der die LDAP-Verbindung authentifiziert. Für den Zugriff auf einen LDAP-Verzeichnisserver muss der Anwendername im Format eines vollständigen eindeutigen Namens angegeben werden: `servicenow@service-now.com`
Anmeldepasswort	Geben Sie das Passwort des Servers ein.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Suche im Verzeichnis wird gestartet	Geben Sie den relativen eindeutigen Namen (Relative Distinguished Name, RDN) des Standardsuchverzeichnisses ein. Alle Abfragen an diesen LDAP-Server werden von diesem RDN gestartet.
MID-Server	Wählen Sie den MID-Server aus, den Sie für die Verbindung mit dem LDAP-Server verwenden möchten. Die Verwendung eines MID-Servers zum Herstellen einer LDAP-Verbindung verhindert, dass der LDAP-Server dem externen Netzwerkdatenverkehr ausgesetzt wird. Außerdem muss kein VPN-Tunnel zwischen dem LDAP-Server und den ServiceNow -Rechenzentren eingerichtet werden. **Hinweis:** ◦ Der MID-Serveranwender muss über die Rolle „user_admin“ verfügen, um LDAP-Server-Konfigurationsdatensätze lesen zu können. ◦ Die folgenden sind mit dem MID Server nicht verfügbar: ▪ LDAP-Authentifizierung ▪ SSL-Verbindung
Connect-Zeitüberschreitung	Wenn ein MID-Server konfiguriert ist, kommt es unabhängig von dieser Einstellung nach 10 Sekunden zu einer Zeitüberschreitung. Diese Einstellung ist hartcodiert und kann nicht geändert werden.
Zeitüberschreitung beim Lesen	Geben Sie die Anzahl der Sekunden an, die der Integration zum Lesen von LDAP-Daten zur Verfügung stehen. Die Integration beendet das Lesen von LDAP-Daten, nachdem die Verbindung die Lesezeitüberschreitung überschritten hat. Wenn Sie eine SSL-Verbindung aktivieren, können Sie mit der Systemeigenschaft *com.glide.ssl.read.timeout* auch einen Wert für die Lesezeitüberschreitung festlegen. Wenn Sie Timeout-Werte sowohl für dieses Feld als auch für die Systemeigenschaft eingeben, hat der niedrigste Timeout-Wert Vorrang.
SSL	Aktivieren Sie dieses Kontrollkästchen, wenn der LDAP-Server eine SSL-verschlüsselte Verbindung herstellen soll. Wenn Sie einen MID-Server ausgewählt haben, ist dieses Feld nicht verfügbar. Wenn Sie eine LDAPS-Integration verwenden und der standardmäßige SSL-Port 636 ist, ist keine weitere Konfiguration erforderlich. SSL wird automatisch aktiviert. Definieren Sie die alternativen SSL-Verbindungseigenschaften, wenn die LDAPS-Integration einen anderen SSL-Port verwendet. **Hinweis:** Stellen Sie sicher, dass ein Netzwerkadministrator die lokale Firewall so konfiguriert, dass der Anwendungsserver auf den LDAP-Server zugreifen kann. Wenn sich der LDAP-Server in einem internen Netzwerk befindet, leitet (oder NAT) die IP-Adresse des Anwendungsservers durch die Firewall an den richtigen Port weiter.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Listener	Aktivieren Sie dieses Kontrollkästchen, um die Integration für die regelmäßige Abfrage von Microsoft Active Directory-Servern oder LDAP-Servern zu aktivieren, die die persistente Steuerung von Suchanforderungen unterstützen. Wenn Sie einen MID-Server ausgewählt haben, ist die Listener-Funktionalität für diesen MID-Server verfügbar. Weitere Informationen finden Sie unter Aktivieren Sie einen LDAP-Listener, und legen Sie Systemeigenschaften fest.
Abhörintervall (Timeout-Wert)	Geben Sie den Wert für die Listener-Zeitüberschreitung in der Anzahl der Minuten an, die die Integration bei jeder Verbindung nach LDAP-Daten lauscht. Die Integration beendet die Überwachung von LDAP-Daten, wenn die Verbindung das Überwachungsintervall überschreitet.
Paging	Aktivieren Sie dieses Kontrollkästchen, damit der LDAP-Server LDAP-Attributdaten in mehrere Ergebnissätze aufteilt, anstatt mehrere Abfragen zu senden.

Hinweis: Wenn Sie ein LDAP-Passwort angeben, führt die Integration einen einfachen Bindungsvorgang aus. Wenn Sie kein LDAP-Passwort angeben, muss der LDAP-Server eine anonyme Anmeldung zulassen, oder die Integration kann nicht an den LDAP-Server gebunden werden.

Ergebnisse
Wenn ein LDAP-Serverdatensatz auf „Aktiv“ festgelegt ist, testet das System automatisch jede Verbindung, um sie zu validieren.
Validierungen umfassen:

- Der LDAP-Server ist unter der angegebenen URL und dem angegebenen Port zugänglich
- Die URL des LDAP-Servers ist ordnungsgemäß formatiert
- Die Anmeldeinformationen sind gültig

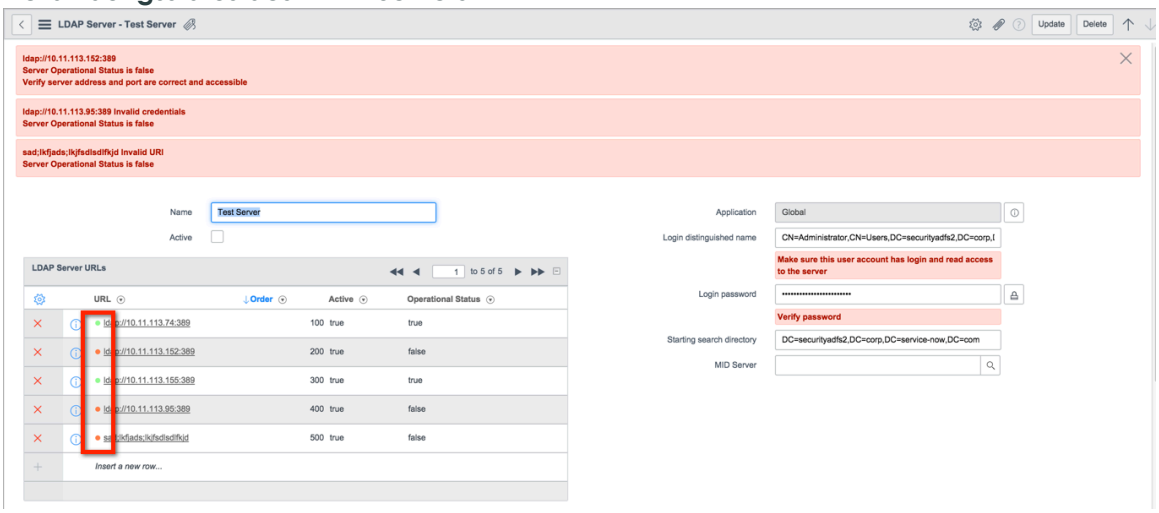
Ab dem Fuji-Release zeigt das System neben jeder Server-URL farbige Punkte an:

Symbole für die Verbindung mit dem LDAP-Server

Farbe	Beschreibung
Grün	Der Server, der aktiv und betriebsbereit ist.
Grau	Der Server ist weder aktiv noch betriebsbereit.
Rot	Der Server ist aktiv, aber nicht betriebsbereit.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verbindungsstatus des LDAP-Servers



Aktivieren Sie einen LDAP-Listener, und legen Sie Systemeigenschaften fest

Das Aktivieren eines Listeners ist optional. Wenn diese Option aktiviert ist, benachrichtigt ein Listener das System, LDAP-Datensätze bald nach einem Update auf dem LDAP-Server zu verarbeiten.

Vorbereitungen

Erforderliche Rolle: admin.

Warum und wann dieser Vorgang ausgeführt wird

Ein Listener ist ein dedizierter Prozess, der regelmäßig nach Änderungen auf dem LDAP-Server sucht.

Der Listener kann auf einem Microsoft Active Directory-Server bereitgestellt werden, der persistente Abfragen (ADNotify) unterstützt, oder auf einem LDAP-Server, der die persistente Steuerung von Suchanforderungen unterstützt (mit OID 2.16.840.1.113730.3.4.3).

Wenn der LDAP-Server eine persistente Suche unterstützt, erkennt der LDAP-Listener alle Benutzer- und Gruppenänderungen, die an einem der entsprechenden LDAP-Accounts vorgenommen wurden, und leitet sie innerhalb von etwa 10 Sekunden an Ihre Instanz weiter. Dadurch kann die Instanz fast in Echtzeit über eine Kopie der Kontodetails Ihrer Benutzer verfügen, ohne auf die nächste geplante Aktualisierung warten zu müssen. Der LDAP-Listener kann nur Objekte synchronisieren, die den Tabellen „Anwender“ [sys_users] und „Gruppe“ [sys_user_group] zugeordnet sind.

Hinweis: Wenn ein Benutzer über den Listener hinzugefügt wird, der Benutzer jedoch die durch den OU-Filter definierten Anforderungen nicht erfüllt, ignoriert die Instanz den Datensatz auf dem LDAP-Server. Wenn die Kriterien erfüllt sind, wird der Benutzer der Instanz hinzugefügt.

So aktivieren Sie einen Listener:

Prozedur

1. Navigieren zu **Alle** > **System-LDAP** > **LDAP-Server**an.
2. Wählen Sie den zu konfigurierenden LDAP-Server aus.
3. Aktivieren Sie das Kontrollkästchen **Listener**.
4. Klicken Sie auf **Aktualisieren**.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Das System importiert nur Benutzerdatensätze, die dem LDAP-OU-Filter entsprechen. Eingehende Anwenderdatensätze, die die Filteranforderungen nicht erfüllen, werden als ungültig gekennzeichnet und vom Import ignoriert. Administratoren können ausführliche LDAP-Protokollierung aktivieren, um zu bestimmen, ob eingehende Datensätze nicht mit dem LDAP-OU-Filter übereinstimmen.

5. Wahlweise: Navigieren Sie zur Tabelle „Systemeigenschaften“ [sys_properties], und legen Sie die Systemeigenschaften für den LDAP-Listener fest.

Eigenschaften des LDAP-Listeners

Eigenschaft	Beschreibung
glide.ldap.listener.use_background_transaction	Bei „wahr“ wird der LDAP-Listener als Hintergrundtran gestartet. Durch Ausführen des LDAP-Listeners als Hintergrundtransaktion kann die Quotenregel LDAP- Stopp-Transaktion die Transaktion nach Erreichen de Dauer (standardmäßig 5 Minuten) abbrechen. Diese verhindert, dass ein LDAP-Listener unbegrenzt wartet **Hinweis:** Diese Eigenschaft gilt nur für LDAP-Ve die keinen MID-Server verwenden. Verwenden S *glide.ldap.listener.mid.use_background_* um das Verhalten von LDAP-Verbindungen zu st über einen MID-Server gehen. ◦ Typ: Wahr | Falsch ◦ Standardwert: false ◦ Speicherort: zu Tabelle „Systemeigenschaften“ [sys hinzufügen
glide.ldap.listener.mid.use_background_transaction	Bei „wahr“ wird der LDAP-Listener als Hintergrundtran gestartet. Durch Ausführen des LDAP-Listeners als Hintergrundtransaktion kann die Mengenregel LDAP- Stopp-MID-Transaktion die Transaktion abbrechen, n maximale Dauer erreicht ist (standardmäßig 5 Minut Verhalten verhindert, dass ein LDAP-Listener unbegre **Hinweis:** Diese Eigenschaft gilt nur für LDAP-Ve die einen MID-Server verwenden. Verwenden Sie *glide.ldap.listener.use_background_tran* das Verhalten von LDAP-Verbindungen zu steue über einen MID-Server hergestellt werden. ◦ Typ: Wahr | Falsch ◦ Standardwert: false ◦ Speicherort: zu Tabelle „Systemeigenschaften“ [sys hinzufügen
glide.ldap.listener.mid.one_listener	Bei „wahr“ wird nur eine einzelne ECC-Warteschlang erstellt, um den LDAP-Listener über einen MID-Server starten oder anzuhalten. Bei „false“ können mehrere Warteschlangennachrichten erstellt werden, was zur

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	mehrerer Threads zum Starten oder Stoppen des LDA führt. ◦ Typ: Wahr | Falsch ◦ Standardwert: true ◦ Speicherort: zu Tabelle „Systemeigenschaften“ [sy hinzufügen

Geben Sie die LDAP-Attribute an

Geben Sie die Attribute an, die in LDAP-Serverabfragen enthalten sind, indem Sie das Feld LDAP- **Serverattribute** verwenden. Dies kann sowohl die Leistung als auch die Sicherheit verbessern.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Standardmäßig lädt das System alle Attribute für jedes Objekt, für das es die Berechtigung zum Lesen von Ihrem LDAP-Server hat. Im Feld **Attribute** können Sie die von der LDAP-Abfrage zurückgegebenen Attribute angeben und dadurch einschränken. Die Verwendung dieses Ansatzes für große LDAP-Importe kann die Geschwindigkeit dieser Importe erheblich verbessern.

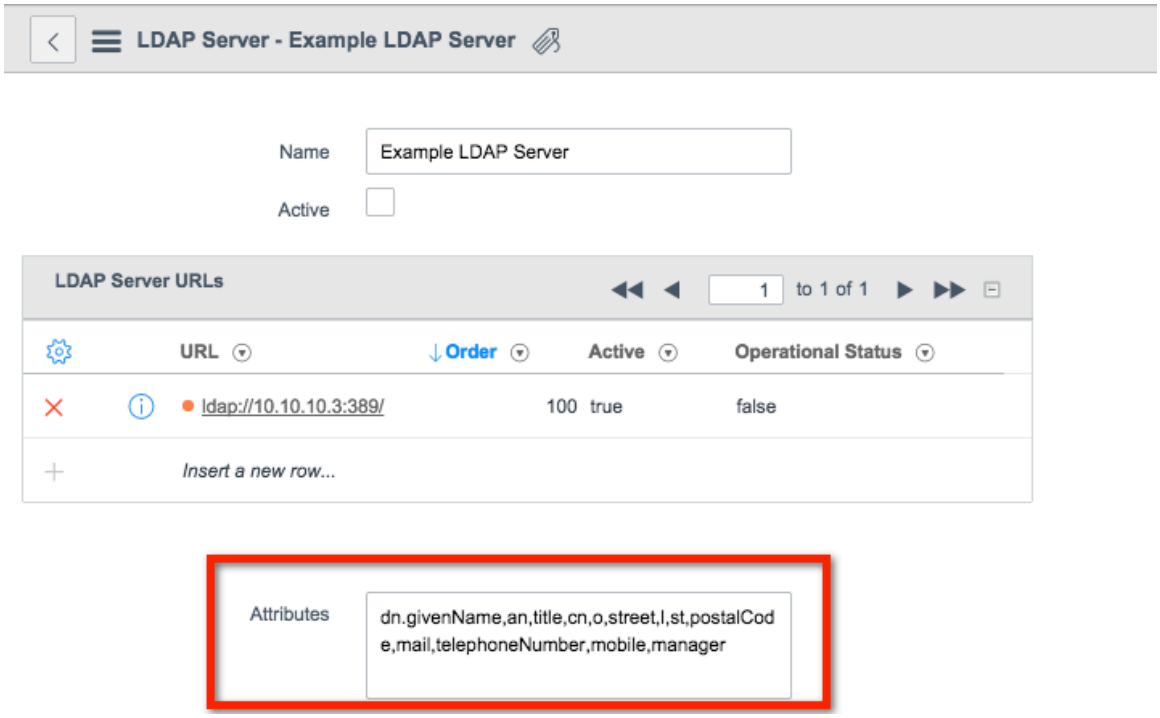
Prozedur

Definieren Sie Attribute nach Möglichkeit explizit.

Wenn Informationen vorhanden sind, die der Instanz nicht angezeigt werden sollen, schließen Sie das Attribut aus. Wenn Sie keine LDAP-Serverattribute angeben, können Anwendertransaktionen für längere Zeit einfrieren, wenn neue Attribute zu einem LDAP-Serverobjekt hinzugefügt werden, da das System mit dem Laden von Daten aus den neuen Attributen ausgelastet sein wird.

Hinweis: Um die unter Transformationszuordnung für LDAP-Daten auswählen oder erstellen beschriebenen Manager-Suchskripts zu verwenden, geben Sie **manager** und **dn** (distinguished name) im Feld **Attribute** an. Keines der Attribute muss Teil einer Transformationszuordnung sein.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Testen Sie eine LDAP-Verbindung

Die Instanz testet die Verbindung jedes Mal automatisch, wenn ein Benutzer das Formular „LDAP-Server“ öffnet. Alternativ können Sie die Verbindung zum LDAP-Server manuell im Formular „LDAP-Server“ testen.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig werden im Formular des LDAP-Servers Fehlermeldungen angezeigt, wenn beim Herstellen der Verbindung mit dem LDAP-Server Probleme auftreten.

Hinweis: Mitarbeiter können auch die Konnektivität zwischen der -Instanz und dem LDAP-Server überprüfen. Wenden Sie sich an den technischen Support, um Unterstützung bei der Überprüfung der LDAP-Konnektivität zu erhalten.

So testen Sie manuell eine Verbindung:

Prozedur

1. Navigieren zu **Alle** > **System-LDAP** > **LDAP-Server**an.
2. Wählen Sie den zu testenden LDAP-Server aus.
3. Klicken Sie unter **„Zugehörige Links**“ auf **Testverbindung**.
4. Klicken Sie unter **Zugehörige Links**auf **Durchsuchen**, um sicherzustellen, dass die entsprechende LDAP-Verzeichnisstruktur für das System sichtbar ist.
5. Wahlweise: Wenn die Verbindung erfolgreich war, klicken Sie auf **Durchsuchen**, um die LDAP-Quellverzeichnisstruktur anzuzeigen, die für die Instanz sichtbar ist.

Hinweis: Die Felder „ **Filter** “ und **„RDN“** auf der linken Seite des Fensters „Durchsuchen“ werden ignoriert, wenn Sie das Suchfeld auf der rechten Seite verwenden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Die Instanz ändert den Betriebsstatus von LDAP-Servern abhängig vom Ergebnis des Verbindungstests.

- Wenn Ihre Instanz eine Verbindung zu einem Server herstellt, dessen **Betriebsstatus** den Wert **„down“**aufweist, wird der Wert des **Betriebsstatus** automatisch in „ **up**“ geändert. Diese Funktionalität wird sowohl für automatische als auch für manuelle Verbindungstests unterstützt.
- Wenn zu einem Server, dessen **Betriebsstatus** der Wert **up**ist, keine Verbindung hergestellt werden kann, wird der Wert des **Betriebsstatus** automatisch in **down**geändert. Diese Funktionalität wird nur für automatische Verbindungstests unterstützt, nicht für manuelle Tests.

Definieren von LDAP-Organisationseinheiten

Eine Definition einer Organisationseinheit (OE) gibt die LDAP-Quellverzeichnisse an, die für die Integration verfügbar sind.

Vorbereitungen

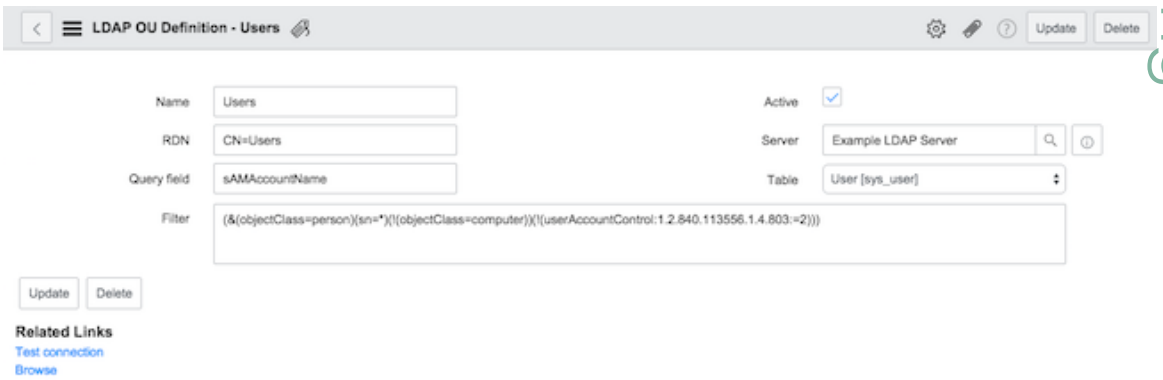
Erforderliche Rolle: admin.

Warum und wann dieser Vorgang ausgeführt wird

OU-Definitionen können Standorte, Personen oder Benutzergruppen enthalten. Jede LDAP-Serverdefinition enthält zwei OU-Beispieldefinitionen: eine zum Importieren von Gruppen in das System und eine für Benutzer.

Prozedur

1. Navigieren zu **Alle** > **System-LDAP** > **LDAP-Server**an.
2. Wählen Sie den zu konfigurierenden LDAP-Server aus.
3. Wählen Sie in der zugehörigen Liste **„LDAP-OU-Definitionen** “ entweder die OE-Definition für **Gruppen** oder **Benutzer** aus.
4. Füllen Sie das Formular „LDAP-OU-Definition“ aus (siehe Tabelle).
5. Klicken Sie auf **Aktualisieren**.
   Das System testet die Verbindung zum LDAP-Server automatisch.
6. Klicken Sie unter **Zugehörige Links**auf **Durchsuchen**, um die LDAP-Verzeichnisdatensätze anzuzeigen, die von der OU-Definition zurückgegeben werden.



© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „OE-Definition“.

Feld	Beschreibung
Name	Geben Sie den Namen an, den die Integration beim Verweisen auf diese OE verwendet. Der Name, den Sie hier eingeben, wird zu einem LDAP-Ziel im Datenquellen-Datensatz.
RDN	Geben Sie den relativen eindeutigen Namen des zu durchsuchenden Unterverzeichnisses an. Dieser RDN wird mit dem Start-Suchverzeichnis des Verzeichnisses aus der LDAP-Serverdefinition kombiniert, um das Unterverzeichnis zu identifizieren, das Informationen für diese Organisationseinheit enthält. Die Beispiel-OU-Definition verwendet beispielsweise den RDN-Wert `CN=Users`, um das LDAP-Verzeichnis `CN=Users,DC=service-now,DC=com` und alle Verzeichnisse unterhalb dieses Punkts zu durchsuchen. Dieses Feld muss mit einem Unterverzeichnis in Ihrem LDAP-System übereinstimmen.
Abfragefeld	Geben Sie den Namen des Attributs auf dem LDAP-Server an, um Datensätze abzufragen. Das Abfragefeld muss sowohl in einzelnen als auch in mehreren Domäneninstanzen eindeutig sein. Um beste Ergebnisse zu erzielen, verwenden Sie E-Mail-Adressen oder andere Anmeldeinformationen, die den Benutzer in einer Instanz mit mehreren Domänen eindeutig identifizieren. Active Directory verwendet das Attribut **sAMAccountName**. Andere LDAP-Server verwenden in der Regel das Attribut **cn**. **Hinweis:** Das Feld „ **Abfrage** “ muss dem Feld „ **Anwender-ID** “ in der Tabelle „Benutzer“ [sys_user] zugeordnet sein. Wenn sich beispielsweise ein Active Directory-Anwender als `boe.example anmeldet`, müssen ein Anwenderdatensatz mit dem Anwender- **ID** -Wert **„joe.example“** und ein LDAP-Datensatz mit dem **sAMAccountName** -Wert **„joe.example“ vorhanden sein**.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um die OE-Definition zu aktivieren und Administratoren das Testen des Imports von Daten zu ermöglichen. Die Integration kann jedoch nur Daten aus aktiven OU-Definitionen in das System importieren.
Tabelle	Geben Sie die Tabelle an, die die zugeordneten Daten von Ihrem LDAP-Server empfängt. Wählen Sie für Benutzer **Benutzer (sys_user)**und für Gruppen **Gruppe (sys_group) aus**.
Filter	Geben Sie eine LDAP-Filterzeichenfolge ein, um bestimmte Datensätze für den Import aus der OE auszuwählen. Je spezifischer die LDAP-Filterabfrage ist, desto effizienter ist die Abfrage. Beispielsweise verwendet die LDAP-OU-Definition für Benutzer den folgenden Filter, um Datensätze auszuwählen, die als Personen klassifiziert sind, einen **sn** -Attributwert aufweisen, keine Computer sind und nicht als inaktiv gekennzeichnet sind: `(&(objectClass=person)(sn=*)(!(objectClass=computer)) (!(userAccountControl:1.2.840.113556.1.4.803:=2)))` Eine Beschreibung der LDAP-Filtersyntax finden Sie, indem Sie im Internet nach `LDAP-Filter RFC`suchen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Example: Beispiele für Definitionen von Organisationseinheiten

Angenommen, Sie verwenden einen LDAP-Server mit folgender Verzeichnisstruktur:

dc=meine-domäne,dc=com

- OU=Gruppen
  - cn=Development
  - cn=HR
  - cn = Vertrieb
- OU=Benutzer
  - OU=Development
  - OU = HR
  - OU = Vertrieb

Angenommen, Sie möchten die HR-Gruppe und HR-Benutzer aus der Anwendung ausschließen. Führen Sie die folgenden Schritte aus:

1. Erstellen Sie einen LDAP-Server-Datensatz mit dem Start-Suchverzeichnis dc=my-domain,dc=com.
2. Erstellen Sie einen OE-Definitionsdatensatz für OU = Gruppen mit einem Filter zum Ausschluss von cn = HR.
3. Erstellen Sie einen OE-Definitionsdatensatz für OU=Users mit einem Filter zum Ausschließen von OU=HR.

Wenn Sie keine zusätzlichen Attribute oder Filter mit einer OU-Definition angeben, gibt die LDAP-Abfrage die gesamte Unterstruktur aus dem Startverzeichnis und dem RDN zurück.

In diesen Beispielen hätte eine OU-Definition mit dem RDN-Wert OU=Groups und keinem Filter alle Gruppen zurückgegeben. Ebenso hätte eine OU-Definition mit dem RDN-Wert OU=Users und keinem Filter alle Anwender und untergeordneten Organisationseinheiten zurückgegeben.

Erstellen Sie eine Datenquelle für LDAP

Jede LDAP-Definition von Organisationseinheiten (OE) hat eine eigene zugehörige Liste von Datenquellen.

Vorbereitungen
Erforderliche Rolle: admin

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Hinweis: Sowohl der **LDAP-Server** als auch die **LDAP-OU-Definition** müssen aktiv sein, damit die Testlastaktion ordnungsgemäß funktioniert. Wenn die Testlast zum ersten Mal aktiviert wird, führt das System Stichproben aus bis zu 20 Datensätzen durch, um die Länge der Felder des Importsatzes zu bestimmen. Wenn die als Stichproben erfassten Datensätze keine Werte für das Feld **Anwender-ID** enthalten, setzt das System die Feldlänge für alle nachfolgenden Importe auf die Standardlänge von 40. Der Import schneidet alle importierten Daten ab, die die Länge des Importsatz-Tabellenfelds überschreiten. Darüber hinaus wird das Feld „ **Anwender-ID** “ auf maximal 40 Zeichen gekürzt. Beachten Sie, dass die 20 geladenen Datensätze nicht umgewandelt werden können und nur zu Testzwecken dienen. Wenn die Testdatensätze Werte für das Feld **Anwender-ID** enthalten, wird die Feldlänge basierend auf der Feldlänge der längsten Anwender-ID in den Testdatensätzen festgelegt.

So erstellen Sie eine neue Datenquelle:

Prozedur

1. Navigieren zu **Alle** > **System-LDAP** > **LDAP-Server**an.
2. Wählen Sie den zu konfigurierenden LDAP-Server aus.
3. Wählen Sie in der zugehörigen Liste „ **LDAP-OU-Definitionen** “ ein Element aus, z. B. **Gruppen** oder **Benutzer**.
4. Klicken Sie in der zugehörigen Liste „ **Datenquellen“** auf **Neu**.
5. Füllen Sie das Formular „Datenquelle“ aus (siehe Tabelle).
6. Klicken Sie auf **Absenden**.
7. Klicken Sie unter **Zugehörige Links**auf **Testladen von 20 Datensätzen**, um zu testen, ob die Datenquelle LDAP-Daten in die Importtabelle importieren kann.

Formular „Datenquellen“.

Feld	Beschreibung
Name	Geben Sie den Namen an, den die Integration beim Verweisen auf diese Datenquelle verwendet.
Tabellenname für Importsatz	Geben Sie den Namen der Bereitstellungstabelle ein, in der das System die importierten LDAP-Datensätze und -Attribute vorübergehend platziert. Überprüfen Sie diese Tabelle, um importierte LDAP-Datensätze anzuzeigen. Sie können denselben Importsatz-Tabellennamen für alle LDAP-Datenquellen verwenden.
Typ	Wählen Sie **LDAP** aus, um anzugeben, dass die importierten Daten LDAP-Daten sind. Nachdem Sie den Typ **LDAP**ausgewählt haben, zeigt das Formular das Feld **LDAP-Ziel** an.
LDAP-Ziel	Wählen Sie die LDAP-OU-Definition aus, die dieser Datenquelle zugeordnet ist.

LDAP-Anwender automatisch bereitstellen

Sie stellen automatisch Benutzer bereit, die sich im LDAP-Server, aber noch nicht in Ihrer Instanz befinden.

Vorbereitungen

Erforderliche Rolle: admin

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

Erstellen Sie in der Tabelle „Systemeigenschaften“ [sys_properties] die folgenden Eigenschaften:

LDAP-Eigenschaften

LDAP-Eigenschaft	Beschreibung
glide.ldap.authentication	Aktiviert die LDAP-Authentifizierung, indem Anwender LDAP zur Authentifizierung verwenden. Legen Sie diese Eigenschaft auf „ **true** “ (den Standardwert) fest.
glide.ldap.user.autoprovision	Aktiviert das LDAP-System, um automatisch Anwender in der Tabelle „Anwender“ [sys_user] zu erstellen, wenn der Anwender in LDAP vorhanden ist, sich aber noch nicht in der Instanz befindet. Legen Sie diese Eigenschaft auf „ **true** “ (den Standardwert) fest.

Beide Eigenschaften müssen auf „ **true** “ festgelegt werden, damit die automatische Bereitstellung funktioniert.

LDAP-Integration über MID Server

Administratoren können die Integration mithilfe einer LDAP-Datenquelle über einen MID-Server (Management, Instrumentation, and Discovery) durchführen.

Der MID-Server ermöglicht die Kommunikation und das Verschieben von Daten zwischen Now Platform und externen Anwendungen, Datenquellen und Services. Weitere Informationen zur Installation eines MID-Servers finden Sie unter MID-Server-Installation .

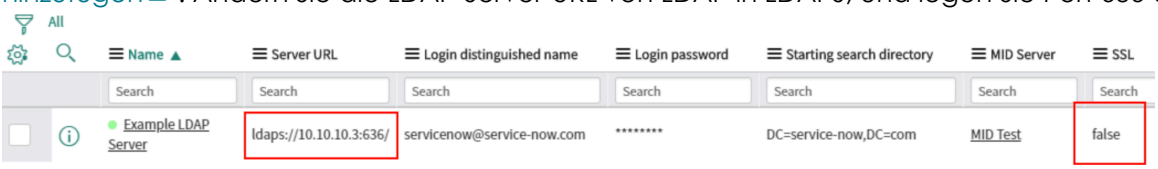
Die Verwendung eines MID-Servers zum Herstellen einer LDAP-Verbindung verhindert, dass der LDAP-Server dem externen Netzwerkdatenverkehr ausgesetzt wird. Sie müssen keinen VPN-Tunnel zwischen Ihrem LDAP-Server und Rechenzentren einrichten. Der MID-Server-Benutzer muss über die Rolle „user_admin“ verfügen, um LDAP-Server-Konfigurationsdatensätze lesen zu können.

Hinweis: Der MID-Server lässt die Verwendung der UI-Aktion nicht zu<instance> `/sys_ui_action.do?sys_id=1b4f7ef30a0001060058e223c9a5744c`, um Anwender- und Gruppendatensätze aus LDAP zu aktualisieren.

Eine MID-Serververbindung kommuniziert standardmäßig über HTTP auf Port 80. Für diesen Kommunikationskanal ist kein Zertifikat erforderlich. Die Verbindung zwischen dem MID-Server und der Instanz erfolgt über HTTPS (Port 443). Die Instanz stellt über LDAP oder LDAPS eine direkte Verbindung zum LDAP-Server her. Diese Verbindung kann entweder über das Internet oder über einen VPN-Tunnel hergestellt werden.

Hinweis: LDAP kann nicht über den MID Server mit Passwortauthentifizierung kommunizieren.

Für eine sichere Kommunikation über SSL müssen Sie ein SSL-Zertifikat für den MID-Server hinzufügen . Ändern Sie die LDAP-Server-URL von LDAP in LDAPS, und legen Sie Port 636 an.



© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn Sie einen neuen LDAP-Server erstellen, wird die SSL-Kennzeichnung des MID-Servers standardmäßig auf „false“ festgelegt. Sie können dieses Verhalten ignorieren.

Informationen zum Festlegen von Verbindungseigenschaften für einen bestimmten LDAP-Server finden Sie unter Definieren Sie einen LDAP-Server.

Konfigurieren Sie die LDAP-Verbindungsüberwachung

Sie können die Überwachung und Benachrichtigungen von LDAP-Verbindungen ändern oder deaktivieren.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Die Instanz sendet automatisch eine E-Mail an Benutzer, die in der LDAP-Administratorgruppe konfiguriert sind, wenn eine LDAP-Serververbindung fehlschlägt. Hierfür wird die E-Mail-Benachrichtigung “ verwendet, die von der geplanten Aufgabe **„LDAP-Verbindungstest“** gestartet wird. Diese E-Mail-Benachrichtigung ist standardmäßig aktiviert.

Hinweis: Die Instanz sendet die E-Mail-Benachrichtigung nur, wenn mindestens ein Mitglied in der LDAP-Administratorgruppe vorhanden ist. Achten Sie darauf, diese Gruppe mit den Anwendern zu füllen, die die E-Mail erhalten sollen.

Standardmäßig testet die regelmäßige Aufgabe die Verbindung alle 15 Minuten. So ändern Sie dieses Intervall oder deaktivieren die Überwachung:

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Geplante Aufgaben**an.
2. Öffnen **Sie den LDAP-Verbindungstest**.
3. Führen Sie einen der folgenden Schritte aus:
   - Ändern Sie das Intervall im Feld **Wiederholungsintervall**.
   - Deaktivieren Sie die Überwachung, indem Sie das Kontrollkästchen **Aktiv** deaktivieren.

Sie importieren Binärdaten über einen MID Server

Als Administrator können Sie BLOB-Daten (Binary Large Object) mit einer LDAP-Integration über den MID Server importieren.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Fügen Sie der Systemeigenschaft `glide.ldap.binary_attributes`den Namen der LDAP-Spalte hinzu, aus der Sie Binärdaten importieren möchten.
2. Fügen Sie eine MID-Server-Eigenschaft mit dem Namen `glide.ldap.binary_attributes` und dem gleichen Wert hinzu, den Sie für die Systemeigenschaft festgelegt haben.

Problembehandlung bei der LDAP-Integration über MID-Server

Bei der Integration von LDAP über den MID-Server können in den folgenden Bereichen Probleme auftreten.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können diese Probleme beheben, indem Sie sich die Ausgaben in der ECC-Warteschlange (External Communication Channel) (Externer Kommunikationskanal) ansehen.**Discovery** > **Ausgabe und Artefakte** > **ECC-Warteschlange**) an.

Testverbindungsprobleme

Bei der Definition von OUs auf dem Server gibt es die zugehörige Liste **Testverbindung**, mit der die LDAP-Verbindung verifiziert wird. Wenn Sie auf diesen Link klicken, sollte die ECC-Warteschlange eine einzelne Ausgabenachricht mit dem **Themennamen LDAPConnectionTesterProbe anzeigen**. Nach Abschluss des Tests auf dem MID Server sollte in der ECC-Warteschlange eine Eingabenachricht mit demselben Themennamen angezeigt werden. Wenn in der Spalte „ **Name** “ für die Eingabenachricht „ **true**“ angezeigt wird, war der Test erfolgreich. Führen Sie einen Drilldown in den Datensatz durch, um die Nutzlast anzuzeigen und sicherzustellen, dass sie keine Fehlermeldungen enthält.

Testverbindung

Created	Agent	Topic	Name	Source	Queue	State	Processed
2013-07-29 13:24:17	mid.server.local_mid	LDAPConnectionTesterProbe	true	04a952038f21010036bf21ca47e79a30	input	processed	2013-07-29 13:24:19
2013-07-29 13:24:04	mid.server.local_mid	LDAPConnectionTesterProbe		04a952038f21010036bf21ca47e79a30	output	processed	2013-07-29 13:24:17

Durchsuchen Sie Probleme

Bei der Definition von OUs auf dem Server gibt es eine zugehörige Liste **Durchsuchen**, mit der die LDAP-Verzeichnisdatensätze angezeigt werden, die von der OU-Definition zurückgegeben werden. Wenn Sie auf diesen Link klicken, sollte in der ECC-Warteschlange eine einzelne Ausgabenachricht mit dem **Themennamen LDAPBrowseProbe angezeigt werden**. Nachdem Daten vom MID-Server zurückgegeben wurden, sollte die ECC-Warteschlange eine Eingabenachricht mit demselben Themennamen anzeigen. Wenn in der Spalte „ **Name** “ für die Eingabenachricht „ **true**“ angezeigt wird, war der Test erfolgreich. Führen Sie einen Drilldown in den Datensatz durch, um die Nutzlast anzuzeigen und sicherzustellen, dass sie keine Fehlermeldungen enthält.

Importprobleme laden

Beim Hochladen von Daten (z. B. mit der Funktion „Testladen von 20 Datensätzen“) sollte in der ECC-Warteschlange eine einzelne Ausgabenachricht mit dem **Themennamen LDAPProbe angezeigt werden**.

Nachdem Daten vom MID-Server zurückgegeben wurden, sollte die ECC-Warteschlange eine weitere Eingabenachricht mit der Bezeichnung **LDAPProbeCompleted anzeigen**. Die Spalte „ **Name** “ für diese Eingabenachricht zeigt die Gesamtzahl der zurückgegebenen Datensätze an.

Zusätzliche Eingabenachrichten, auch **LDAPProbe**genannt, werden angezeigt. In der Spalte „ **Name** “ für diese Eingabenachricht wird die höchste Datensatznummer im Batch angezeigt. Wenn die Gesamtzahl der zurückgegebenen Datensätze 258 beträgt und die Batchgröße 200 beträgt (Standardeinstellung), werden zwei eingehende LDAPProbe-Nachrichten (200, 258) und eine eingehende LDAPProbeCompleted-Nachricht (258) empfangen.

Führen Sie einen Drilldown in den Datensatz durch, um die Nutzlast anzuzeigen und sicherzustellen, dass sie keine Fehlermeldungen enthält.

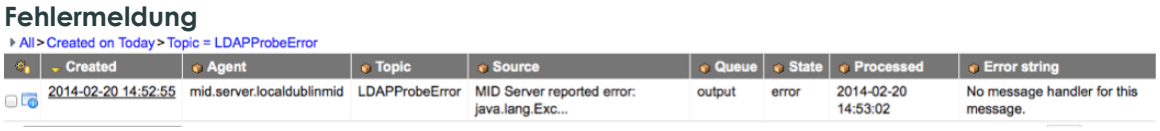
Importlast

Created	Agent	Topic	Name	Source	Queue	State	Processed
2013-07-29 13:09:48	mid.server.local_mid	LDAPProbeCompleted	11	ed0a0d7a8f32010036bf21ca47e79a56	input	processed	2013-07-29 13:09:51
2013-07-29 13:09:48	LDAPProbeResult	LDAPProbe	11	ed0a0d7a8f32010036bf21ca47e79a56	input	processed	2013-07-29 13:09:51
2013-07-29 13:09:36	mid.server.local_mid	LDAPProbe		ed0a0d7a8f32010036bf21ca47e79a56	output	processed	2013-07-29 13:09:46

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Achten Sie auch auf die Ausgabenachricht **LDAPProbeError**.



Klicken Sie auf den Link in der Spalte **Name**, um die Details des Fehlers anzuzeigen.

LDAP-Paging

LDAP-Paging funktioniert nicht, wenn die Paging-Größe auf dem LDAP-Server kleiner als 1000 ist. Legen Sie die MID-Servereigenschaft *glide.ldap.max_results* auf einen Wert fest, der kleiner oder gleich der Paginggröße des LDAP-Servers ist.

LDAP kann keine Binärdaten importieren

Um Binärdaten über LDAP zu importieren, z. B. ein Anwenderfoto, müssen Sie das Binärattribut in die MID-Servereigenschaft *glide.ldap.binary_attributes*aufnehmen. Im Beispiel für ein Anwenderfoto kann das Attribut `jpegphoto`sein.

Daten importieren und zuordnen

Der LDAP-Import ordnet Felder in Ihrer LDAP-Datenbank Feldern in Ihrer -Instanz zu.

Hinweis: Die LDAP-Zuordnung wirkt sich auf die Leistung aus. Daher wird empfohlen, sie außerhalb der Spitzenzeiten zu planen oder einige Datensätze gleichzeitig zu verarbeiten, um die Systemverfügbarkeit aufrechtzuerhalten.

Definieren Sie eine Transformationszuordnung, die nur die erforderlichen oder erforderlichen Attribute importiert. Je nach Version der verwendeten Instanz variiert die Methode zur Angabe von LDAP-Zuordnungsbeziehungen.

Am einfachsten können Sie herausfinden, ob Sie eine Version ausführen, die die System-LDAP-Anwendung für die LDAP-Integration verwendet, indem Sie die Anwendung im Anwendungsnavigator suchen.

Die Option **Business-Regeln** ausführen wird nur für die Zieltabelle angewendet. Nur Transformationszuordnungen, die der Zieltabelle zugeordnet sind, führen die Business-Regeln aus, die verschiedenen Tabellen zugeordnet sind. Wenn Sie eine Benutzergruppe aktualisieren und für eine Benutzergruppentabelle Geschäftsregeln ausgeführt werden, müssen für die Gruppe Rollen definiert sein.

Zuordnungsoptionen für LDAP-Import

System-LDAP-Anwendung?	Karte
Ja	Verwenden Sie eine Transformationszuordnung, um Ihre Zuordnung anzugeben.
Nein	Verwenden Sie eine veraltete LDAP -Importzuordnung, um Ihre Zuordnung anzugeben, oder die standardmäßige LDAP-Transformation, die in Baselineinstanzen enthalten ist. Denken Sie daran, das Feld „Zusammenfügen“ so anzupassen, dass es mit den **richtigen** Feldern übereinstimmt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geplante Importe

Ein geplanter Import ermöglicht Administratoren das Importieren von LDAP-Daten nach einem regelmäßigen Zeitplan. Standardmäßig enthält die LDAP-Integration zwei Beispiele für geplante Importe:

- Example LDAP User Import (LDAP-Anwenderimportbeispiel)
- Example LDAP Group Import (LDAP-Gruppenimportbeispiel)

Keines der Beispiele ist standardmäßig aktiv. Ändern Sie diese geplanten Importe, um sie an die Geschäftsanforderungen Ihres Unternehmens anzupassen.

LDAP-Transformationszuordnungen

Die Transformationszuordnung verschiebt Daten aus der Importsatztabelle in die Zieltabelle (Anwender oder Gruppe).

Die LDAP-Integration verwendet Standard-Importsätze und Transformationszuordnungen. Sie können auch anwenderdefinierte LDAP-Transformationszuordnungen erstellen.

Wichtig: Unabhängig davon, ob Sie anwenderdefinierte LDAP-Transformationszuordnungen auswählen oder erstellen, muss eine aktive Transformationszuordnung für eine Reihe von Quell- und Zieltabellen vorhanden sein. Das Aktivieren mehrerer Transformationszuordnungen für dieselben Quell- und Zieltabellen kann zu doppelten Einträgen in der Zieltabelle führen, es sei denn, Sie fügen sie anhand der übereinstimmenden Felder zusammen.

Standardmäßige LDAP-Transformationszuordnungen

Standardmäßig stellt das System zwei Transformationszuordnungen für LDAP-Daten bereit.

Standardmäßige LDAP-Transformationszuordnungen

Transform Map	Quelltabelle	Zieltabelle	Beschreibung
LDAP-Anwenderimport	[ldap_import]	[sys_user]	Standard-Transformationszuordnung zum Erstellen von Anwenderdatensätzen aus LDAP-Anmeldeinformationen als Teil der bedarfsgesteuerten LDAP-Anmeldung. Enthält Zuordnungen für einen Active Directory LDAP-Server.
LDAP-Gruppenimport	[ldap_group_import]	[sys_user_group]	Standard-Transformationszuordnung zum Erstellen von Gruppendatensätzen aus LDAP-OUs. Enthält Zuordnungen für einen Active Directory LDAP-Server.

Hinweis: Standardmäßig verfügt das System nicht über eine Transformationszuordnung für LDAP-Abteilungsdatensätze.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anforderungen für anwenderdefinierte LDAP-Transformationszuordnungen

Wenn Sie eine anwenderdefinierte Transformationszuordnung erstellen möchten, muss die Transformationszuordnung die folgenden Zuordnungsanforderungen erfüllen.

Anforderungen für anwenderdefinierte LDAP-Transformationszuordnungen

Quelltabelle	Quellfeld	Zieltabelle	Zielfeld	Zusammenfügen	Beschreibung
`ldap_import`	`u_source`	`sys_user`	Quelle	falsch	Das Feld **u_source gibt** den LDAP DN des importierten Benutzers oder der importierten Gruppe an. Das System verwendet dieses Feld, um zu bestimmen, dass ein Benutzer eine LDAP Authentifizierung benötigt, um den Manager eines Benutzers zu finden und um Benutzer in Gruppen einzuteilen.
`ldap_import`	Wählen Sie eines der folgenden Felder aus: • `u_samaccountname` • `u_dn` • `u_cn`	`sys_user`	`user_name`	wahr	Wenn LDAP in Active Directory integriert wird, wählen **Sie u_samaccountname** als Quellfeld aus. Wenn andere LDAP-Verzeichnisse verwendet werden, wählen **Sie u_dn** oder **u_cn** als Quellfeld aus.

Unterschiede zwischen LDAP-Transformationszuordnungen und Legacy-Importzuordnungen

Bei der Angabe von LDAP-Zuordnungsbeziehungen mithilfe von Transformationszuordnungen gibt es einen großen Unterschied in der Art und Weise, wie Referenzfelder für Manager und Abteilung festgelegt werden.

Wenn Sie eine Transformationszuordnungverwenden, müssen Sie ein Transformationsskript verwenden, um Referenzen zu erstellen. Dies liegt daran, dass der Wert, der einem LDAP-Attribut wie „Manager“ zugeordnet ist, der Distinguished Name (DN) des Managers ist.

Ohne zusätzliche Logik wird ein Benutzerdatensatz mit einem Managernamen erstellt, der dem eindeutigen Namen dieses Benutzers in LDAP entspricht. Die Integration enthält ein Transformationsskript, um die Erstellung dieser Referenzen zu erleichtern. Die Standardtransformationszuordnung „LDAP User Import“ enthält Transformationsskripts für diese Referenzen.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorhandene Zuordnungsbeziehungen

Wenn Sie Importzuordnungen aus der Vorgängerversion in Transformationszuordnungen aktualisieren, können Sie die LDAP-Zuordnungsbeziehungen beibehalten, die vor dem Hinzufügen der System-LDAP-Anwendung vorhanden waren. Der LDAP-Server verfügt über ein Zuordnungsfeld, das auf die Legacy- **Importzuordnung** verweist.

Hinweis: Standardmäßig ist dieses Feld ausgeblendet. Sie müssen daher das Formular konfigurieren, um es anzuzeigen.

Wenn Sie zur Verwendung einer Transformationszuordnung übergehen möchten, löschen Sie den Verweis auf die Legacy-Importzuordnung.

Zuordnungseinstellungen für LDAP-Import

Verifizieren und verwenden Sie Attribute, um die Felder zu beschränken, die die Integration aus der LDAP-Quelle importiert. Darüber hinaus ist es wichtig, das Feld „user_name“ dem LDAP-Attribut zuzuordnen, das die Anmelde-ID des Benutzers enthält. Für Active Directory ist dies normalerweise das Attribut sAMAccountName. Wenn Sie ein binäres Attribut (z. B. „objectSID“ oder „objectGUID“) importieren und zusammenfügen möchten, müssen Sie ein anwenderdefiniertes Transformationsskript erstellen.

Hinweis: Jeder Wert, der dem Feld „user_name“ zugeordnet ist, muss eindeutig sein.

Wenn Sie keine Transformationszuordnung (z. B. LDAP User Import) angeben, verwendet die Integration die folgenden Standardzuordnungen:

Standardzuordnung für LDAP-Import

Anwenderfeld oder Variable	LDAP-Attribut
user_name	sAMAccountName
E-Mail	E-Mail
Telefon	Telefonnummer
home_phone	homePhone
mobile_phone	Mobile
first_name	gegebenerName
last_name	sn
Titel	Titel
department	department
Manager	Manager
Middle_name	Initialen
u_memberof	groups
u_member	Mitglieder
u_manager	Manager

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

LDAP-Datentransformation

Wenn ein LDAP-Attribut einfache Daten enthält, verknüpft die Transformationszuordnung ein importiertes LDAP-Attribut mit einem entsprechenden Feld in der Zieltabelle (Anwender oder Gruppe). Beispiel: Beispieldaten im Attribut sAMAccountName werden dem Feld **Benutzer-ID** in der Benutzertabelle zugeordnet.

Wenn die importierten LDAP-Daten einem Referenzfeld zugeordnet sind, sucht die Instanz nach einem vorhandenen übereinstimmenden Datensatz. Wenn kein passender Datensatz vorhanden ist, erstellt die Instanz einen neuen Datensatz für das Referenzfeld, sofern die Feldzuordnung nichts anderes vorgibt.

Angenommen, das LDAP-Attribut l ist dem Referenzfeld **Standort** in der Benutzertabelle zugeordnet. Immer wenn der Import einen Attributwert importiert, der nicht mit einem vorhandenen Standortdatensatzwert übereinstimmt, erstellt die Transformationszuordnung einen neuen Standortdatensatz. Der neue Standortdatensatz hat den gleichen Wert wie das importierte Attribut, und der importierte Benutzerdatensatz enthält jetzt einen Link zum neuen Standortdatensatz.

Es kann jedoch vorkommen, dass das LDAP-Attribut einen Distinguished Name (DN) zurückgibt, der im Wesentlichen ein Verweis auf einen anderen Datensatz im LDAP-Verzeichnis ist. Beispielsweise enthält das Attribut „manager" normalerweise den eindeutigen Namen für den Manager des aktuellen LDAP-Verzeichniseintrags. Ein importierter DN verwendet normalerweise eine lange Textzeichenfolge wie: cn=Beth Anglin,OU=Users,Dc=my-domain,dc=com.

> ⚠ **Warnung:** Stellen Sie sicher, dass Ihre Zielfelder lang genug sind, um einen DN zu enthalten. Viele Textfelder verwenden die Standardlänge von 40, was für einige DN-Werte möglicherweise nicht lang genug ist. Das System ServiceNow schneidet jeden Wert ab, der die Feldlänge überschreitet.

Administratoren möchten normalerweise nicht, dass das System neue Benutzer aus dem DN-Wert erstellt, da der neue Benutzer keine Zuordnung zu einem vorhandenen Benutzer hat. Stattdessen möchten Administratoren, dass der Import den vorhandenen Benutzerdatensatz des Managers findet und dem neu importierten Benutzer zuordnet. Die `Skripteinbindung LDAPUtils` enthält die Funktionen `setManager` und `processManagers`, die einen DN analysieren und nach einem vorhandenen Benutzer suchen können. Um die besten Ergebnisse zu erzielen, verwenden Sie diese Funktionen, um eine anwenderdefinierte Transformationszuordnung zu erstellen.

Beispiel: Das Skript für die `LDAP-Anwenderimport` -Transformationszuordnung ruft die Funktion `setManager auf` :

```
//
// The manager coming in from LDAP is the DN value for the manager.
// The line of code below will locate the manager that matches the
// DN value and set it into the target record.  If you are not
// interested in getting the manager from LDAP then remove or
// comment out the line below
ldapUtils. setManager (source , target ) ;
```

In einigen Fällen importiert die Integration den Datensatz eines Benutzers, bevor sie den Benutzerdatensatz des zugehörigen Managers importiert. Um solche Fälle zu behandeln, können Sie die Funktion `„processManagers" aufrufen`, nachdem die Transformation abgeschlossen ist. Beispielsweise ruft die Transformationszuordnung **LDAP User Import** ein `onComplete` -Transformationsskript auf, um die Funktion `processManagers aufzurufen`.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
// It is possible that the manager for a user did not exist in the
 database when // the user was processed and therefore we could not
 locate and set the manager field. // The processManagers call below will
 find all those records for which a manager could  // not be found and
 attempt to locate the manager again. This happens at the end of the  //
 import and therefore all users should have been created and we should be
 able to  // locate the manager at this point
ldapUtils. processManagers ( ) ;
```

Entfernen oder kommentieren Sie die Funktionsaufrufe „ `setManager`“ und „`processManagers`“, wenn Ihre LDAP-Integration das Attribut „manager“ nicht verwendet.

LDAP-Skripting

Erstellen Sie anwenderdefinierte Transformationszuordnungen, Skripts und Geschäftsregeln, um die Anforderungen beim Importieren von Daten anzugeben.

Anwenderdefinierte Transformationszuordnungen müssen `onStart-` und `onAfter-` Transformationsskripts enthalten.

Das `onStart-` Skript muss die `LDAPUtils` -Skripteinbindung aufrufen und mit der Protokollierung beginnen. Die Transformationszuordnung „ **LDAP User Import** “ besitzt beispielsweise ein `onStart` -Skript, das diesen Code verwendet:

```
gs.include ( "LDAPUtils" ) ; var ldapUtils  = new LDAPUtils ( ) ;
ldapUtils. setLog (log ) ;
```

Das Skript `onAfter` sollte die Funktion `addMembers aufrufen`. Beispiel:

```
ldapUtils.addMembers (source , target ) ;
```

Legen Sie deaktivierte Active Directory-Anwender auf inaktiv fest

Verwenden Sie das folgende Skript, um Anwender automatisch zu deaktivieren, wenn der zugehörige AD-Anwender deaktiviert wird.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können deaktivierte Active Directory-Anwender identifizieren, indem Sie den Wert des Attributs `userAccountControl überprüfen`. Diese Regel wird immer dann ausgeführt, wenn sich der Wert von `userAccountControl` ändert, und deaktiviert Anwender-Accounts, wenn die **Anwenderaccount-Steuerung** einen deaktivierten AD-Account anzeigt.

Verwenden Sie das folgende Skript, um Anwender automatisch zu deaktivieren, wenn der zugehörige AD-Anwender deaktiviert wird.

Prozedur

1. Konfigurieren Sie das Benutzerformular, und erstellen Sie ein neues Ganzzahlfeld namens **Benutzeraccount-Steuerung**.
2. Fügen Sie dem neuen Feld eine Zuordnung für userAccountControl (extern) hinzu.
3. Erstellen Sie eine neue Geschäftsregel mit den folgenden Eigenschaften:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geschäftsregel „AD-Anwender“ deaktivieren

Business-Regelfeld	Wert
Name	Deaktivieren Sie AD-Anwender
Tabelle	Benutzer [sys_user]
Wann	Vorher
Bedingung	current.u_user_account_control.changes()

Das Feld „Skript“ muss Folgendes enthalten:

```
var disabledFlag = 2;
//perform a bitwise comparison on userAccountControl to see if the 2
 bit flag is enabled
if (current.u_user_account_control & disabledFlag) {
  gs.log('Disabling user: ' + current.user_name + 'userAccountControl='
 + current.u_user_account_control);
  current.active='false';
  current.locked_out='true';
}
```

Weisen Sie LDAP-Feldwerte zu

Sie können ein Skript verwenden, um jedem Feld, für das eine Feldzuordnung vorhanden ist, einen Wert zuzuweisen.

Um beispielsweise dem Feld „sys_user.company“ einen Wert zuzuweisen, erstellen Sie eine Feldzuordnung für das Unternehmensfeld, und fügen Sie folgendes Transformationsskript hinzu:

```
company = "Don's Sporting Goods";
```

Bestimmte LDAP-Anwender ausschließen

Wenn Sie die LDAP-Anwenderliste mithilfe von LDAP-Filtereigenschaften nicht vollständig filtern können, können Sie Benutzer mit einem Zuordnungsskript ausschließen.

Nachdem Sie die Logik zur Identifizierung eines Anwenders ausgeführt haben, der nicht importiert werden darf, setzen Sie das Feld „user_name“ auf eine leere Zeichenfolge. Dadurch wird dieser Anwender nicht importiert.

```
user_name='';
```

Eine Möglichkeit, die herauszufilternden Benutzer zu identifizieren, besteht darin, im Attribut `DistinguishedName` nach einer Zeichenfolge zu suchen. Dieses Skript schließt beispielsweise Accounts aus, die sich nicht in einer Benutzer-OE befinden. Sie können dieses Skript verwenden, wenn Sie zu viele Anwender-OEs haben, um sie in die LDAP-Option der Ziel-OU aufzunehmen.

```
//vdn is a variable mapped to distinguishedName
gs.include("LDAPUtils");
var vdn = source.getElement(this.distinguishedName);
if (vdn.indexOf('OU=Users')<0) {
  user_name='';
  gs.log('LDAP Import Skipping User: ' + vdn);
}
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine komplexere Filtermethode ist die Verwendung regulärer Ausdrücke.

```
//vcn is a variable mapped to cn
//vdn is a variable mapped to distinguishedName
//c is the regular expression string
gs.include("LDAPUtils");
var vdn = source.getElement(this.distinguishedName);
var vcn = source.getElement(this.cn);
var c = /^[a-z][a-z][a-z][0-9][0-9][0-9]$/;
var nvcn = vcn.toLowerCase();
//test to see if the cn is in the form of 3 letters followed by 3
 numbers, only import these
if (c.test(nvcn)) {
 user_name = nvcn;
} else {
 gs.log("LDAP import rejected username: " + vcn + " for DN: " + vdn);
 user_name = "";
}
```

Legen Sie die Auswahlaktion für Referenzfeldimporte fest

Die LDAP-Transformationszuordnung bestimmt, wie Felder in der Importsatztabelle Feldern in vorhandenen Tabellen wie Incident oder Benutzer zugeordnet werden.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn die LDAP-Transformationszuordnung ein Feld in der Importsatztabelle aktualisiert, erstellt die Integration automatisch einen neuen Datensatz, sobald ein neuer Datensatz in den LDAP-Daten vorhanden ist. Wenn die LDAP-Transformationszuordnung ein Referenzfeld aktualisiert, das Daten aus einer anderen Tabelle speichert, kann der Administrator neue LDAP-Datensätze erstellen, ignorieren oder ablehnen.
Wenn die Integration beispielsweise einen neuen Abteilungsdatensatz erhält, der mit keiner vorhandenen Abteilung übereinstimmt, können Sie alle anderen LDAP-Datensatzfelder aktualisieren, ohne einen neuen Abteilungsdatensatz in der Instanz zu erstellen. Mit der Transformationszuordnung können Sie die Datensatzerstellungsoptionen für jedes Referenzfeld festlegen.

Prozedur

1. Navigieren zu **Alle** > **System-LDAP** > **Transformationszuordnungen**an.
2. Wählen Sie in der zugehörigen Liste „ **Feldzuordnungen** “ im Feld Auswahlaktion eine der folgenden Aktionen aus:
   - **erstellen** – erstellt einen neuen Referenzfelddatensatz, wenn kein übereinstimmender Datensatz vorhanden ist.
   - **ignorieren** – ignoriert neue Datensätze im Referenzfeld und schließt die Verarbeitung aller anderen Felder in der Transformationszuordnung ab.
   - **Ablehnen** – Stoppt die Transformation für den gesamten Datensatz.

   Hinweis: Die **Feldzuordnung** zeigt nur das Feld Auswahlaktion für Referenzfelder an.

Verifizieren Sie die LDAP-Zuordnung

Aktualisieren Sie nach dem Erstellen einer LDAP-Transformationszuordnung die LDAP-Daten, um sicherzustellen, dass die Transformationszuordnung wie erwartet funktioniert.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **System-LDAP** > **Geplante Lasten**an.
2. Klicken Sie auf Ihren LDAP-Importauftrag.
3. Klicken Sie auf **Jetzt ausführen**.

Problembehandlung für LDAP-Integration

Wenn Sie Ihren LDAP-Server integrieren und Fragen haben, können die folgenden Punkte Ihnen bei der Behebung des Problems helfen.

Vorabschecks

- Wenn LDAP nicht verfügbar ist, können sich Benutzer nicht bei der Instanz anmelden. Es empfiehlt sich, lokale Administratorkonten zu verwenden, damit Administratoren bei einem Ausfall von LDAP weiterhin auf die Instanz zugreifen können.
- Überprüfen Sie den Serviceaccount, um sicherzustellen, dass er nicht abgelaufen oder gesperrt ist.
- Überprüfen Sie das Format des Anwendernamens. Anstatt nur den Anwendernamen zu verwenden, versuchen Sie es mit der Domäne mit dem Anwendernamen oder mit der Domäne username@domain.
- Stellen Sie `sicher`, dass Sie den Eintrag `system_id` im Datensatz ldap_server_config geändert haben. Wenn Sie `system_id` unbeabsichtigt mit einem Update Set ändern, verweist `system_id` auf den falschen Knoten für die Zielinstanz und funktioniert nicht.

Fehlercodes

Die LDAP-Protokolldatei listet branchenübliche Fehlercodes für LDAP und Active Directory (AD) auf. Die LDAP-Protokolldatei ist in der Wrapper-Datei enthalten. Die LDAP-Fehlercodes sind zweistellige Nummern, während die Active Directory-Fehlercodes dreistellige Nummern sind. Eine Liste der häufigsten Fehlercodes finden Sie unter LDAP-Fehlercodes.

Integration mehrerer Domänen

Sie können mehrere Domänen innerhalb derselben Gesamtstruktur oder in vollständig nicht vertrauenswürdigen Domänen integrieren. Es wird empfohlen, für jede Domäne einen separaten LDAP-Server-Datensatz zu erstellen. Jeder LDAP-Serverdatensatz muss auf einen Domänencontroller für die angegebene Domäne verweisen. Das bedeutet, dass Sie Verbindungen mit jedem der Domänencontroller zulassen müssen. Mehrere AD-Gesamtstrukturen über LDAP mit einem LDAP-Account werden nicht unterstützt.

Wenn Sie auf mehr als eine Domäne erweitern, ist es wichtig, dass Sie eindeutige LDAP-Attribute für die Anwendungsanwendernamen und Importkoaleszenzwerte identifizieren. Ein allgemeines eindeutiges Zusammenfügungsattribut für Active Directory ist `objectSid`. Eindeutige Anwendernamen variieren je nach LDAP-Datendesign. Häufige eindeutige Attribute sind „ `email` “ oder „`userPrincipalName`“.

Eingehende Datensätze

Unter LDAP-Transformationszuordnungen erfahren Sie, wie Sie festlegen, wie die Integration eingehende LDAP-Datensätze verarbeitet, für die keine übereinstimmenden Werte in Referenzfeldern vorhanden sind.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Häufige Authentifizierungsfehler

- Anwender kann sich nicht anmelden (ungültiger DN)
- Ungültige CN
- Ungültige Verbindung

Automatische LDAP-Verbindungstests

Sie können Verbindungen zu LDAP-Servern manuell testen oder zulassen, dass ServiceNow die Verbindungen automatisch testet.

Das System testet die Verbindung automatisch:

- Jedes Mal, wenn ein Benutzer das LDAP Server-Formular öffnet.
- Über die geplante Aufgabe „LDAP-Verbindungstest“, die standardmäßig alle 15 Minuten ausgeführt wird

  Sie können ändern, wie häufig diese geplante Aufgabe ausgeführt wird. Wenn diese geplante Aufgabe keine Verbindung herstellen kann, wiederholt eine neue einmalige geplante Aufgabe den Verbindungstest entweder nach fünf Minuten oder nach der Hälfte des Werts für das **Wiederholungsintervall** in der geplanten Aufgabe, je nachdem, was zuerst eintritt.

Fehlermeldungen werden im Formular angezeigt, wenn beim Herstellen der Verbindung mit dem LDAP-Server Probleme auftreten. Außerdem werden Testverbindungen für Server hinter einem MID-Server unterstützt.

Zeigen Sie den LDAP-Monitor an

Aktuelle Informationen zu LDAP-Servern und -Listenern können Sie mit dem LDAP-Monitor anzeigen.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Die verfügbaren Status sind:

- Aktiv
- Inaktiv
- Fehler
- Aktiv (wird heruntergefahren...)
- Fehler (Wird heruntergefahren...)

Zusätzlich zum aktuellen Status zeigt der Monitor auch Folgendes an:

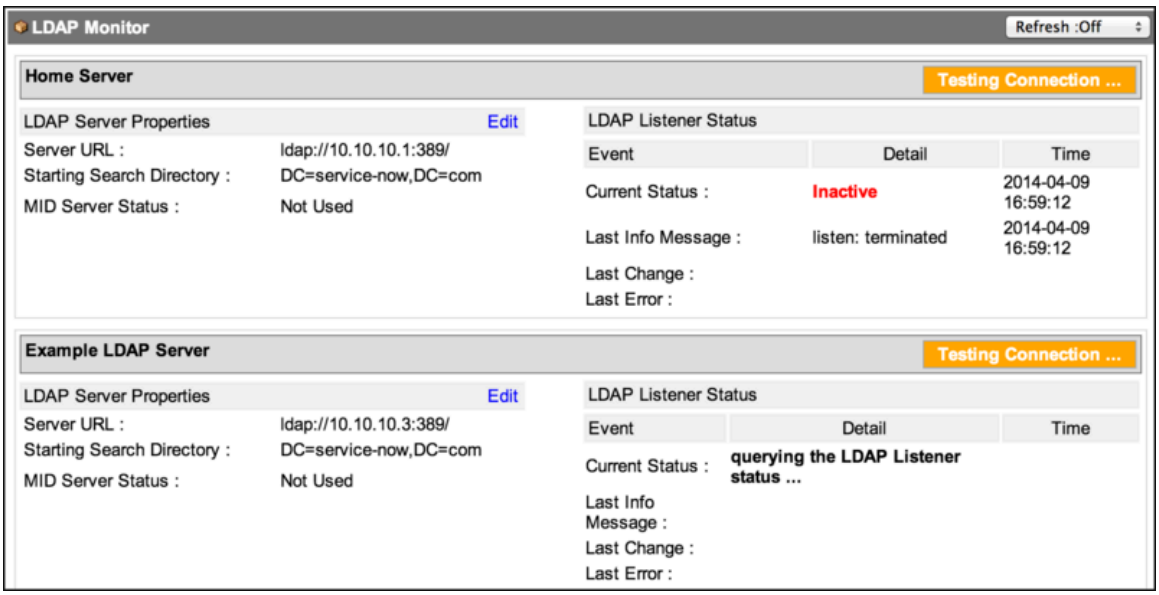
- Die letzte vom Listener erkannte Nachricht, z. B. Warten auf LDAP-Änderungen, Verbindungsfehler usw.
- Die letzte LDAP-Anwenderänderung, z. B. neuer Anwender, aktualisierter Anwender usw.
- Der letzte aufgetretene Fehler.

So zeigen Sie den LDAP-Monitor an:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

Navigieren zu **Alle** > **LDAP** > **System-LDAP** > **LDAP-Überwachung**an.



Beschreibungen der Eigenschaften und Felder im Bildschirm finden Sie in der Tabelle.

LDAP-Monitor

Feld	Beschreibung
Neu laden	Sie können die Aktualisierungsrate konfigurieren, indem Sie in der Kopfzeile der LDAP- **Serverüberwachung** auf das Feld Aktualisieren klicken und die Anzahl der Sekunden zwischen den einzelnen Datenaktualisierungen auswählen. Sie können auch **Keine** auswählen, um die Aktualisierung zu unterdrücken.
Verbindungsstatus	Die Serververbindungsanzeige befindet sich auf der rechten Seite über den Feldern für den LDAP-Listener-Status. Wenn der Server verbunden ist, ist das Feld grün und zeigt *Verbunden*an. Wenn der Server nicht verbunden ist, ist das Feld rot und zeigt *Not Connected*(Nicht verbunden) an. Wenn die Serververbindung getestet wird, ist das Feld gelb und zeigt *Verbindung*wird getestet .
Eigenschaften des LDAP-Servers	
Bearbeiten	Während Sie LDAP-Server überwachen, können Sie Änderungen an den Eigenschaften vornehmen, indem Sie im Bildschirm „LDAP-Serverüberwachung“ auf **Bearbeiten** klicken.
Server-URL	Die Kombination aus Servername und Serverport, an dem der LDAP-Server lauscht. Häufig ist für den Port einer der folgenden Werte festgelegt: • 389: Der Standardport für die Verbindung mit LDAP im Klartext • 636: Der Standardport für die Verbindung mit LDAP über eine SSL-Verbindung Beispielwert: ldap://10.10.10.3:389/

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Ihr LDAP-Server kann über mehr als eine URL-Adresse verfügen. Dadurch werden NICHT mehrere Verzeichnisstrukturen eingerichtet, aus denen Sie Daten importieren können, was durch Erstellen eines weiteren LDAP-Servereintrags erreicht wird. Wenn Sie mehrere LDAP-Server haben, wird jedoch Redundanz bereitgestellt, um einen Single Point of Failure zu vermeiden. Die LDAP-URL-Adressen werden durch ein Leerzeichen getrennt, und das System testet automatisch nacheinander jede Serveradresse, bis eine gültige Verbindung hergestellt werden kann.
Suche im Verzeichnis wird gestartet	Startverzeichnis oder RDN (Relative Distinguished Name, relativer differenzierter Name), von dem das System die Suche nach Benutzern oder Gruppen beginnt. Beispielwert: DC=service-now,DC=com ÜBER diesem Punkt sind keine Daten für den Import verfügbar. Die Instanz hat Einblick in das angegebene Verzeichnis und die Verzeichnisse darunter in der LDAP-Hierarchie.
MID-Serverstatus	Der aktuelle Verbindungsstatus des MID-Servers.
Status des LDAP-Listeners	
Aktueller Status	Dies gibt an, ob der Listener aktiv ist.
Letzte Infonachricht	Hier werden die letzte Nachricht angezeigt, die der LDAP-Server in Bezug auf Anwender- und Gruppenänderungen empfangen hat, sowie die Uhrzeit, zu der die Nachricht empfangen wurde.
Letzter Change	Zeigt die letzte am LDAP-Server vorgenommene Änderung und die Uhrzeit an.
Letzter Fehler	Hier werden der letzte Fehler, der auf dem LDAP-Server aufgetreten ist, und die Uhrzeit des Auftretens angezeigt.

LDAP-Fehlercodes

Die LDAP-Protokolldatei listet branchenübliche Fehlercodes für LDAP und Active Directory (AD) auf.

Standardfehlercodes

Standard-LDAP-Fehler

Fehler-/ Datencode	Text	Beschreibung
0	LDAP_SUCCESS	Gibt an, dass der angeforderte Clientvorgang erfolgreich abgeschlossen wurde.
2	LDAP_PROTOKOLL_FEHLER	Gibt an, dass der Server eine ungültige oder falsch formatierte Anforderung vom Client erhalten hat.
3	LDAP_ZEITGRENZWERT_ÜBERSCHREITET	Gibt an, dass die vom Client oder Server angegebene Zeitbegrenzung des Vorgangs überschritten wurde. Bei

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standard-LDAP-Fehler (Fortsetzung)

Fehler-/ Datencode	Text	Beschreibung
		Suchvorgängen werden unvollständige Ergebnisse zurückgegeben.
4	LDAP_GRÖSSENGRENZWERT_ÜBERSCHREITET	Gibt an, dass bei einem Suchvorgang die vom Client oder Server angegebene Größenbeschränkung überschritten wurde. Es werden unvollständige Ergebnisse zurückgegeben.
5	LDAP_COMPARE_FALSE	Zeigt keine Fehlerbedingung an. Gibt an, dass die Ergebnisse eines Vergleichsvorgangs „falsch“ sind.
6	LDAP_COMPARE_WAHR	Zeigt keine Fehlerbedingung an. Gibt an, dass die Ergebnisse eines Vergleichsvorgangs „wahr“ sind.
7	LDAP_Auth_method_not_supported	Gibt an, dass der Client während eines Bindungsvorgangs eine Authentifizierungsmethode angefordert hat, die vom LDAP-Server nicht unterstützt wird.
8	LDAP_Strong_Auth_Required	Zeigt eine der folgenden Optionen an: Bei Bindungsanforderungen akzeptiert der LDAP-Server nur eine starke Authentifizierung. In einer Client-Anforderung hat der Client einen Vorgang wie Löschen angefordert, der eine starke Authentifizierung erfordert. In einer nicht angeforderten Benachrichtigung über die Trennung der Verbindung erkennt der LDAP-Server, dass die Sicherheit, die die Kommunikation zwischen Client und Server schützt, unerwartet ausgefallen ist oder gefährdet wurde.
9		Reserviert
10	LDAP_REFERRAL	Zeigt keine Fehlerbedingung an. In LDAPv3 gibt an, dass der Server den Zieleintrag der Anforderung nicht enthält, die Server im Verweisfeld jedoch möglicherweise.
11	LDAP_ADMINGRENZWERT_ÜBERSCHREITET	Gibt an, dass ein von einer Verwaltungsbehörde festgelegter LDAP-Servergrenzwert überschritten wurde.
12	LDAP_NICHT VERFÜGBAR_KRITISCH_EXTENSION	Gibt an, dass der LDAP-Server eine Anforderung nicht erfüllen konnte, da mindestens eine kritische Erweiterung nicht verfügbar war. Entweder unterstützt der Server das Steuerelement nicht,

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standard-LDAP-Fehler (Fortsetzung)

Fehler-/ Datencode	Text	Beschreibung
		oder das Steuerelement ist für den Vorgangstyp nicht geeignet.
13	LDAP_VERTRAULICHKEIT_ERFORDERLICH	Gibt an, dass die Sitzung nicht durch ein Protokoll wie Transport Layer Security (TLS) geschützt wird, das Sitzungsvertraulichkeit bietet.
14	LDAP_SASL_BIND_IN_PROGRESS	Zeigt keine Fehlerbedingung an, zeigt jedoch an, dass der Server für den nächsten Schritt im Prozess bereit ist. Der Client muss dem Server denselben SASL-Mechanismus senden, um den Prozess fortzusetzen.
15		Nicht verwendet.
16	LDAP_NO_SUCH_ATTRIBUTE	Gibt an, dass das im Änderungs- oder Vergleichsvorgang angegebene Attribut im Eintrag nicht vorhanden ist.
17	LDAP_UNDEFINED_TYPE	Gibt an, dass das im Änderungs- oder Hinzufügevorgang angegebene Attribut im Schema des LDAP-Servers nicht vorhanden ist.
18	LDAP_INAPRIATE_MATCHING	Gibt an, dass die im Suchfilter angegebene Übereinstimmungsregel nicht mit einer Regel übereinstimmt, die für die Syntax des Attributs definiert ist.
19	LDAP_CONSTRAINT_VIOLATION	Gibt an, dass der Attributwert, der in einem Vorgang zum Ändern, Hinzufügen oder Ändern eines DN angegeben wird, gegen Einschränkungen für das Attribut verstößt. Die Einschränkung kann entweder Größe oder Inhalt sein (nur Zeichenfolge, keine Binärdatei).
20	LDAP_TYPE_ODER_WERT_VORHANDEN	Gibt an, dass der in einem Änderungs- oder Hinzufügevorgang angegebene Attributwert bereits als Wert für dieses Attribut vorhanden ist.
21	LDAP_INVALID_SYNTAX	Gibt an, dass der in einem Vorgang zum Hinzufügen, Vergleichen oder Ändern angegebene Attributwert eine nicht erkannte oder ungültige Syntax für das Attribut ist.
22-31		Nicht verwendet.
32	LDAP_NO_SUCH_OBJECT	Gibt an, dass das Zielobjekt nicht gefunden werden konnte. Dieser Code wird für die folgenden Vorgänge nicht zurückgegeben: Suchvorgänge, die die Suchbasis finden, aber keine Einträge

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standard-LDAP-Fehler (Fortsetzung)

Fehler-/ Datencode	Text	Beschreibung
		finden können, die dem Suchfilter entsprechen. Binden Sie Vorgänge.
33	LDAP_ALIAS_PROBLEM	Gibt an, dass beim Dereferenzieren eines Alias ein Fehler aufgetreten ist.
34	LDAP_INVALID_DN_SYNTAX	Gibt an, dass die Syntax des DN falsch ist. (Wenn die DN-Syntax korrekt ist, die Strukturregeln des LDAP-Servers den Vorgang jedoch nicht zulassen, gibt der Server den Code 53 zurück: LDAP_UNWILLING_TO_PERFORM.)
35	LDAP_IS_LEAF	Gibt an, dass der angegebene Vorgang nicht für einen untergeordneten Eintrag ausgeführt werden kann. (Dieser Code befindet sich derzeit nicht in den LDAP-Spezifikationen, ist jedoch für diese Konstante reserviert.)
36	LDAP_ALIAS_DEREF_PROBLEM	Gibt an, dass während eines Suchvorgangs entweder der Client keine Zugriffsrechte zum Lesen des Namens des Alias-Objekts hat oder eine Dereferenzierung nicht zulässig ist.
37-47		Nicht verwendet.
48	LDAP_INAPPROPRIATE_Auth	Gibt an, dass der Client während eines Bindungsvorgangs versucht, eine Authentifizierungsmethode zu verwenden, die er nicht ordnungsgemäß verwenden kann. Beispielsweise kann eine der folgenden Bedingungen diesen Fehler verursachen: Der Client gibt einfache Anmeldeinformationen zurück, wenn sichere Anmeldeinformationen erforderlich sind...ODER... Der Client gibt einen DN und ein Passwort für eine einfache Bindung zurück, wenn für den Eintrag kein Passwort definiert ist.
49	LDAP_Ungültige_Anmeldeinformationen	Gibt an, dass während eines Bindungsvorgangs eines der folgenden Ereignisse aufgetreten ist: Der Client hat entweder einen falschen DN oder ein falsches Passwort übergeben, oder das Passwort ist falsch, da es abgelaufen ist, die Angriffserkennung das Konto gesperrt hat oder ein anderer ähnlicher Grund. Weitere Informationen finden Sie im Datencode.
49 / 52e	AD_Ungültige Anmeldeinformationen	Gibt einen Fehler „AcceptSecurityContext“ in Active

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standard-LDAP-Fehler (Fortsetzung)

Fehler-/ Datencode	Text	Beschreibung
		Directory (AD) an, der zurückgegeben wird, wenn der Anwendername gültig ist, die Kombination aus Passwort und Anwenderanmeldeinformationen jedoch ungültig ist. Dies ist das AD-Äquivalent des LDAP-Fehlercodes 49.
49 / 525	ANWENDER NICHT GEFUNDEN	Gibt einen „AcceptSecurityContext"-Datenfehler in Active Directory (AD) an, der zurückgegeben wird, wenn der Anwendername ungültig ist.
49 / 530	NOT_PERMITTED_TO_LOGON_AT_THIS_TIME	Gibt einen „AcceptSecurityContext"-Datenfehler in Active Directory (AD) an, bei dem es sich um einen Anmeldefehler handelt, da sich der Anwender zu diesem Zeitpunkt nicht anmelden darf. Gibt nur zurück, wenn ein gültiger Anwendername und gültige Passwort-Anmeldeinformationen vorhanden sind.
49 / 531	BESCHRÄNKT_AUF_SPEZIELLE_MASCHINE	Gibt einen „AcceptSecurityContext"-Datenfehler in Active Directory (AD) an, bei dem es sich um einen Anmeldefehler handelt, da sich der Anwender nicht von diesem Computer aus anmelden darf. Gibt nur zurück, wenn ein gültiger Anwendername und gültige Passwort-Anmeldeinformationen vorhanden sind.
49 / 532	PASSWORD_expired	Gibt einen Active Directory (AD)-AcceptSecurityContext-Datenfehler an, bei dem es sich um einen Anmeldefehler handelt. Das angegebene Account-Passwort ist abgelaufen. Gibt nur zurück, wenn gültige Anmeldeinformationen mit Anwendername und Passwort vorhanden sind.
49 / 533	ACCOUNT_DISABLED	Gibt einen Active Directory (AD)-AcceptSecurityContext-Datenfehler an, bei dem es sich um einen Anmeldefehler handelt. Der Account ist derzeit deaktiviert. Gibt nur zurück, wenn gültige Anmeldeinformationen mit Anwendername und Passwort vorhanden sind.
49 / 568	ERROR_TOO_MANY_CONTEXT_IDS	Gibt an, dass während eines Anmeldeversuchs der Sicherheitskontext des Anwenders zu viele Sicherheits-IDs angesammelt hat. Dies ist ein Problem mit dem spezifischen LDAP-Anwenderobjekt/

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standard-LDAP-Fehler (Fortsetzung)

Fehler-/ Datencode	Text	Beschreibung
		-Account, das vom LDAP-Administrator untersucht werden sollte.
49 / 701	ACCOUNT_EXPIRED	Gibt einen Active Directory (AD)-AcceptSecurityContext-Datenfehler an, bei dem es sich um einen Anmeldefehler handelt. Der Account des Anwenders ist abgelaufen. Gibt nur zurück, wenn gültige Anmeldeinformationen mit Anwendername und Passwort vorhanden sind.
49 / 773	DER ANWENDER MUSS PASSWORT ZURÜCKSETZEN	Gibt einen Active Directory (AD)-AcceptSecurityContext-Datenfehler an. Das Passwort des Benutzers muss vor der ersten Anmeldung geändert werden. Gibt nur zurück, wenn gültige Anmeldeinformationen mit Anwendername und Passwort vorhanden sind.
50	LDAP_INSUFFICIENT_ACCESS	Gibt an, dass der Anrufer nicht über ausreichende Rechte zum Ausführen des angeforderten Vorgangs verfügt.
51	LDAP_BUSY	Gibt an, dass der LDAP-Server zu ausgelastet ist, um die Client-Anforderung zu verarbeiten. Wenn der Client jedoch wartet und die Anforderung erneut übermittelt, kann der Server sie dann möglicherweise verarbeiten.
52	LDAP_NICHT VERFÜGBAR	Gibt an, dass der LDAP-Server die Bindungsanforderung des Clients nicht verarbeiten kann, normalerweise weil er heruntergefahren wird.
52e	AD_Ungültige Anmeldeinformationen	Gibt einen Fehler „AcceptSecurityContext“ in Active Directory (AD) an, der zurückgegeben wird, wenn der Anwendername gültig ist, die Kombination aus Passwort und Anwenderanmeldeinformationen jedoch ungültig ist. Dies ist das AD-Äquivalent des LDAP-Fehlercodes 49: LDAP_INVALID_CREDENTALS.
53	LDAP_UNWILLING_TO_PERFORM	Gibt an, dass der LDAP-Server die Anforderung aufgrund serverdefinierter Einschränkungen nicht verarbeiten kann. Dieser Fehler wird aus den folgenden Gründen zurückgegeben: Die Anforderung zum Hinzufügen eines Eintrags verstößt gegen die Strukturregeln des Servers...ODER...Die Anforderung zum

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standard-LDAP-Fehler (Fortsetzung)

Fehler-/ Datencode	Text	Beschreibung
		Ändern des Attributs gibt Attribute an, die von Anwendern nicht geändert werden können...ODER...Passwortbeschränkungen verhindern die Aktion... ODER...Verbindungsbeschränkungen verhindern die Aktion.
54	LDAP_LOOP_DETECT	Gibt an, dass der Client einen Alias oder eine Verweisschleife erkannt hat und diese Anforderung daher nicht abschließen kann.
55-63		Nicht verwendet.
64	LDAP_NAMEN_VIOLATION	Gibt an, dass der Vorgang zum Hinzufügen oder Ändern von DNs gegen die Strukturregeln des Schemas verstößt. Beispiel: Die Anforderung platziert den Eintrag unter einem Alias. Die Anforderung platziert den Eintrag in einem untergeordneten Container, der gemäß den Containment-Regeln verboten ist. Der RDN für den Eintrag verwendet einen verbotenen Attributtyp.
65	LDAP_OBJECT_CLASS_VIOLATION	Gibt an, dass der Vorgang zum Hinzufügen, Ändern oder Ändern von DNs gegen die Objektklassenregeln für den Eintrag verstößt. Beispielsweise geben die folgenden Arten von Anforderungen diesen Fehler zurück: Der Vorgang zum Hinzufügen oder Ändern versucht, einen Eintrag ohne Wert für ein erforderliches Attribut hinzuzufügen. Beim Vorgang zum Hinzufügen oder Ändern wird versucht, einen Eintrag mit einem Wert für ein Attribut hinzuzufügen, das in der Klassendefinition nicht enthalten ist. Beim Änderungsvorgang wird versucht, ein erforderliches Attribut zu entfernen, ohne die Hilfsklasse zu entfernen, die das Attribut als erforderlich definiert.
66	LDAP_NOT_ALLOWED_ON_NONLEAF	Gibt an, dass der angeforderte Vorgang nur für Blatteinträge zulässig ist. Beispielsweise geben die folgenden Arten von Anforderungen diesen Fehler zurück: Der Client fordert einen Löschvorgang für einen übergeordneten Eintrag an. Der Client fordert einen Vorgang zum Ändern des DN für einen übergeordneten Eintrag an.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standard-LDAP-Fehler (Fortsetzung)

Fehler-/ Datencode	Text	Beschreibung
67	LDAP_NOT_ALLOWED_ON_RDN	Gibt an, dass beim Ändern versucht wurde, einen Attributwert zu entfernen, der den relativen eindeutigen Namen des Eintrags bildet.
68	LDAP_ALREADY_EXISTS	Gibt an, dass beim Hinzufügen versucht wurde, einen bereits vorhandenen Eintrag hinzuzufügen, oder dass beim Ändern versucht wurde, einen Eintrag in den Namen eines bereits vorhandenen Eintrags umzubenennen.
69	LDAP_NO_OBJECT_CLASS_MODS	Gibt an, dass im Änderungsvorgang versucht wurde, die Strukturregeln einer Objektklasse zu ändern.
70	LDAP_Ergebnisse_zu_groß	Reserviert für CLDAP.
71	LDAP_AFFECTS_MULTIPLE_DSAS	Gibt an, dass der Vorgang zum Ändern des DN den Eintrag von einem LDAP-Server zu einem anderen verschiebt und mehr als einen LDAP-Server erfordert.
72-79		Nicht verwendet.
80	LDAP_other	Gibt eine unbekannte Fehlerbedingung an. Dies ist der Standardwert für NDS-Fehlercodes, die keinen anderen LDAP-Fehlercodes zugeordnet sind.
775	ANWENDER_KONTO_SPERRE	Gibt an, dass sich Anwender nicht anmelden können, da der Anwenderaccount gesperrt ist.

Anwenderdefinierte Fehlercodes

Anwenderdefinierte LDAP-Fehlercodes

Fehler-/Datencode	Text
10000	LDAP_FEHLER_GENERELL
10001	LDAP_FEHLER_Mal_FORMED_URL
10002	LDAP_FEHLER_UNAUTHENTISCH_BINDUNG
10300	LDAP_FEHLER_KOMMUNICATION_EXCEPTION
10301	LDAP_FEHLER_Socket_Zeitüberschreitung
10302	LDAP_FEHLER_VERBINDUNG_VERWEIGERT
10303	LDAP_FEHLER_VERBINDUNG_ZURÜCKSETZEN
10304	LDAP_FEHLER_KEINE_ROUTE
10305	LDAP_FEHLER_UNKNOW_HOST

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwenderdefinierte LDAP-Fehlercodes (Fortsetzung)

Fehler-/Datencode	Text
10400	LDAP_FEHLER_SSL_EXCEPTION
10401	LDAP_FEHLER_SSL_LEER_CERT_STORE
10402	LDAP_FEHLER_SSL_CERT_NOT_FOUND
10403	LDAP_FEHLER_SSL_CERT_ABGELAUFEN
10500	LDAP_FEHLER_INVALID_SEARCH_FILTER_EXCEPTION

Einmalpasswort senden, wenn der LDAP-Server ausfällt

Es ist eine LDAP-Eigenschaft verfügbar, um einem Benutzer ein einmaliges Passwort zu senden, wenn er sich nicht anmelden kann, weil der LDAP-Server ausgefallen ist. Sie können auch eine andere Eigenschaft konfigurieren, um zu steuern, wie lange das Passwort gültig ist.

Vorbereitungen

Erforderliche Rolle: admin
Um ein Einmalpasswort zu erhalten, muss der Benutzer in seinem Benutzerprofil Benachrichtigungen aktiviert haben. Die Benachrichtigung ist nur eine E-Mail-Nachricht. SMS-Nachrichten werden nicht unterstützt.

Warum und wann dieser Vorgang ausgeführt wird

Beide Eigenschaften sind standardmäßig aktiviert. Der Standardwert für die Eigenschaft, die die Passwortgültigkeit steuert, beträgt 10 Minuten.

Prozedur

1. Öffnen Sie die Liste der Systemeigenschaften, indem Sie im Filter des Anwendungsnavigators `sys_properties.list eingeben`.
2. Suchen Sie die Eigenschaft *`glide.ldap.onetime.password.enabled`*.
3. Legen Sie die Eigenschaft auf `true fest`.
4. Um die Gültigkeitsdauer des Passworts für einen Benutzer zu ändern, legen Sie die folgende Eigenschaft auf eine Ganzzahl von Minuten fest: *`glide.authenticate.onetime.password.validity`*.

Synchronisierung von LDAP-Datensätzen

Administratoren können inaktive, deaktivierte oder gelöschte LDAP-Datensätze mit ihren eigenen LDAP-Datensätzen synchronisieren.

Bei der Synchronisierung von LDAP-Datensätzen werden inaktive Datensätze auf dem LDAP-Server erkannt und die entsprechenden LDAP-Datensätze aktualisiert. Das Erkennen inaktiver LDAP-Datensätze umfasst das Definieren konsistenter Datenindikatoren für jedes Benutzerobjekt, das Importieren von LDAP-Daten und das Auswerten der Datenindikatoren.

Ein Datenindikator kann:

- Ein Datumsfeld
- Mitgliedschaft in einer bestimmten OE (identifizieren durch Analysieren des *`dn`*-Attributs) unter Verwendung des *`useraccountcontrol`*-Attributs
- Eine Kombination dieser Indikatoren

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Importierte Daten gelangen über Importsatztabellen in die Instanz, wo die Daten ausgewertet und verarbeitet werden können.

Der Importprozess kann LDAP-Aktualisierungsfilterfür mehrere Importaufträge verwenden, um verschiedene Arten von Benutzerdatensätzen aufzuteilen und Datensätze für eine separate Verarbeitung zu trennen.

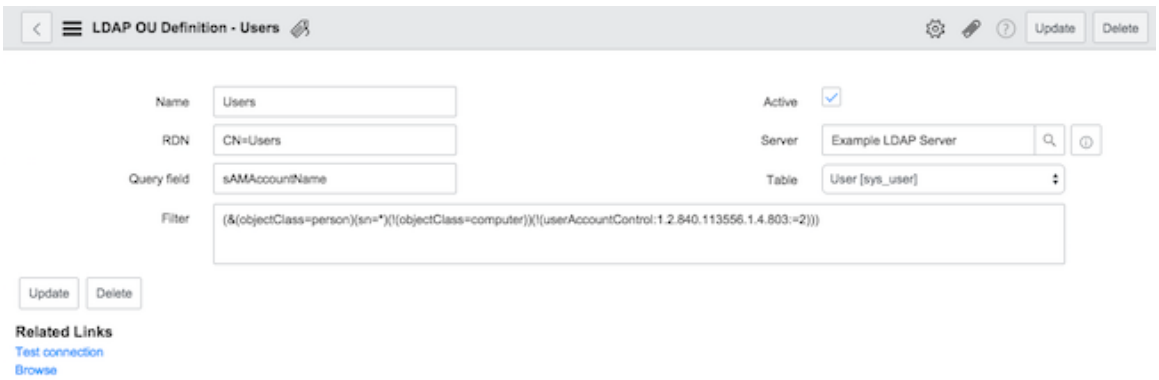
LDAP-Aktualisierungsfilter

Filter für den LDAP-Aktualisierungsprozess können verwendet werden, um eine Verarbeitung anzugeben, die Einfügungen von deaktivierten Anwendern ignoriert.

Sie können den LDAP-OU-Filter lösen, um alle Daten in in Ihre Importsatztabelle zu übernehmen (einschließlich inaktiver Benutzer), und dann eine Verarbeitung angeben, die Einfügungen deaktivierter Benutzer ignoriert. Die OE-Beispieldefinition „Anwender“, die die Instanz in ihrem vordefinierten LDAP-Beispiel bereitstellt, enthält einen Filter.

Dieser Filter ist wichtig, da er definiert, welche Benutzerdatensätze zur Auswertung in die Importsatztabelle aufgenommen werden. Dadurch wird eine geringere Datenlast erzielt, die Einschränkung dieses Filters besteht jedoch darin, dass er inaktive Anwender herausfiltert, sodass die Datensätze inaktiver Anwender nicht in die temporären Tabellen des Importsatzes importiert werden. Da die inaktiven Benutzerdatensätze nicht sichtbar sind, können die Datensatzindikatoren nicht ausgewertet werden.

LDAP-OU-Filter



Um innerhalb des LDAP-Hauptaktualisierungsprozesses zu filtern, ändern Sie den Filter so, dass alle Benutzerdatensätze einbezogen werden. Als Ergebnis werden alle Datensätze in die temporäre Tabelle des Importsatzes geladen und können dort ausgewertet und transformiert werden.

Hinweis: Hier gibt es eine Vorsichtsmaßnahme: Da bei der Filterung alle Datensätze einbezogen werden, erhalten Sie möglicherweise eine große Anzahl älterer inaktiver LDAP-Konten, die nicht in die Instanz eingefügt werden sollten. Ein Benutzerdatensatz sollte niemals für einen deaktivierten Benutzer erstellt werden.

LDAP-Extraktion

Ein LDAP-Extraktionsprozess kann implementiert werden, um deaktivierte Benutzer zu erkennen.

Ein Auszug aus Ihrer LDAP-Quelle kann nach deaktivierten Anwendern gefiltert werden, indem eine aktive Kennzeichnung verwendet wird, die für jeden Datensatz im Import auf „falsch“ festgelegt werden kann. Geben Sie an („target.active=false“), und kopieren Sie sie in das Feld **Skript** direkt im Datensatz der Tabellentransformationszuordnung.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorteile

Diese Methode bietet folgende Vorteile:

- Einfaches Skripting
- Vorhandene Benutzerdatensätze sind an der Verarbeitung nicht beteiligt
- Inaktive Anwender werden nicht in eine temporäre Importtabelle geladen
- Keine Auswirkung auf die Leistung

Nachteile

Nachteile dieser Methode:

- Ein zusätzlicher Prozess wird erstellt
- Der Extraktsatz muss an einem Ort platziert werden, auf den Ihre Datenquelle zugreifen kann

Alternative Methode

LDAP-Aktualisierungsfilter Verwenden Sie mehrere Importaufträge, um verschiedene Arten von Benutzerdatensätzen aufzuteilen und Datensätze für die separate Verarbeitung zu trennen.

Inaktive LDAP-Anwenderaccounts

Erkennen Sie, dass ein vorhandenes, aktuelles Anwenderkonto inaktiv ist oder in einem Active Directory (AD) LDAP deaktiviert oder gelöscht wurde.

Ein häufiges Problem bei der LDAP-Integration besteht darin, deaktivierte oder gelöschte Benutzer in Active Directory (AD) zu erkennen und dann in der Instanz zu deaktivieren. In einem Active Directory LDAP wird normalerweise ein Filter festgelegt, um inaktive Anwender bei der Aktualisierung auszuschließen, damit die Instanz keine Anwender berücksichtigt, die in AD deaktiviert oder gelöscht werden. Das Problem besteht darin, wie erkannt werden kann, dass ein vorhandener, aktueller Benutzer inaktiv ist oder aus AD gelöscht wurde.

Weitere Informationen zum Auffinden inaktiver Accounts finden Sie unter Inaktive LDAP-Accounts mithilfe des Felds userAccountControl suchen .

Hinweis: Es wird empfohlen, Benutzerdatensätze und alle anderen Arten von Datensätzen zu deaktivieren und nicht zu löschen. Jeder Datensatz ist mit anderen Datensätzen verknüpft, und durch das Löschen eines Datensatzes werden alle Beziehungen zu diesen anderen Datensätzen gelöscht. Durch das Deaktivieren von Datensätzen bleiben diese Beziehungen bestehen.

Suchen Sie mithilfe des Felds „userAccountControl“ nach inaktiven LDAP-Accounts

Identifiziert, wenn ein Active Directory-Anwender (AD) gelöscht (oder deaktiviert) wird

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Eine Methode besteht darin, den aktiven Status von AD-Anwendern nachzuverfolgen und eine Geschäftsregel zu erstellen, um entsprechende Accounts zu aktualisieren, wenn ein AD-Account inaktiv ist.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Erstellen Sie ein neues Zeichenfolgenfeld in der Benutzertabelle [sys_user], um den Wert des AD **-Felds userAccountControl nachzuverfolgen**.
   Beispiel: `u_ad_user_account`.
2. Erstellen Sie ein LDAP-Transformationsskript, um den Feldwert festzulegen.

   Example

   ```
   target.u_ad_user_account = source.userAccountControl
   ```

3. Aktualisieren Sie den LDAP-Filter so, dass deaktivierte AD-Accounts angezeigt werden.

   Example
   Hier ist ein Beispiel für einen Filter.

   ```
   (&(objectClass=person)(sn=*)(!(objectClass=computer))(!
   (userAccountControl:1.2.840.113556.1.4.803:=2)))
   ```

   Hier ist ein Beispiel für einen Ersatzfilter, den Sie verwenden können.

   ```
   (&(objectClass=person)(sn=*)(!(objectClass=computer)))
   ```

4. Erstellen Sie eine onChange-Geschäftsregel, um das Feld „Aktiv“ auf „false“ zu setzen, wenn das Feld u_ad_user_account den Wert 514 aufweist.
   „514“ gibt einen inaktiven Account an.

LDAP-Skriptbeispiele

In den folgenden Skriptbeispielen wird davon ausgegangen, dass Sie Active Directory (AD) für Ihren LDAP-Server verwenden.

Attributwertskript für userAccountControl

In diesem Beispiel wird die Quelle für die Attributwerte „userAccountControl“ getestet, die einem deaktivierten Anwender (514 oder 546) zugeordnet sind.

```
//Deactivate LDAP-disabled users during transform based on
 'userAccountControl' attribute
if(source.u_useraccountcontrol == '514' || source.u_useraccountcontrol ==
 '546'){
   target.active=false;
   target.locked_out=true;
}
```

Hier ist ein Beispiel für eine Bitweise Prüfung:

```
if(source.u_useraccountcontrol & 2){
   active = false;
}
```

Attributskript userAccountControl

In diesem Beispiel wird das Attribut userAccountControl untersucht, es wird jedoch nicht auf bestimmte Werte getestet. Sie enthält auch die Option zur erneuten Aktivierung von LDAP-Benutzeraccounts.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
/*
* Deactivate LDAP-disabled users during transform based on
 'userAccountControl' attribute
* Convert the userAccountControl attribute back to a hex value
*/
var ctrl = parseInt(source.u_useraccountcontrol, 10);
ctrl = ctrl.toString(16);

/*
* The only digit we care about is the final one
* A final hex digit value of '2' in 'ctrl' means disabled
*/
if(ctrl.substr(-1) == "2"){

   //Deactivate and lock the user account
   target.active = false;
   target.locked_out = true;

   //Ignore any insert of a disabled record
   if(action == 'insert'){
      ignore = true;
   }
}
/* Optional: Uncomment else block to reactivate and unlock the user
 account
else {
   target.active = true;
   target.locked_out = ctrl.substr(-2, 1) == "1";
}
*/
```

onBefore-Transformationszuordnungsskript

Hier sehen Sie ein Beispiel für ein onBefore-Transformationszuordnungsskript. Das Skript identifiziert deaktivierte und eingefügte Datensätze. Wenn eine Einfügung eines deaktivierten Anwenders erfolgt, ignoriert die Vorgangstransformation den Datensatz.

```
//Ignore any insert of a disabled record as defined by the
 'userAccountControl' attribute
var uc = source.u_useraccountcontrol;
if((uc == '514' || uc == '546') && action == 'insert'){
   ignore = true;
}
```

DN-Mitgliedsskript

Dieses Skriptbeispiel bietet Flexibilität, indem nicht auf die userAccountControl-Werte 546 und 514 zurückgegriffen wird, sondern überprüft wird, ob der Anwender Mitglied eines bestimmten Distinguished Name (DN) ist. Sie können dieses Skript entweder im Feld „ **Skript** “ des Datensatzes „Tabellentransformationszuordnung“ oder in einem onBefore-Transformationszuordnungsskript verwenden.

```
//Deactivate LDAP-disabled users during transform based on OU membership
 in 'dn'
if(source.u_dn.indexOf('OU=Disabled Accounts') > -1){
   target.active = false;
   target.locked_out = true;
}
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Active Directory-Anwendungsmodus (ADAM)

Active Directory Application Mode (ADAM) ist ein LDAP-konformer Verzeichnisdienst (Leichtgewichtler Verzeichniszugriff).

Hinweis: Um dieses Thema zu verstehen, sind Grundkenntnisse im Umgang mit dem Server Microsoft Windows und Active Directory erforderlich. Sie müssen auch über Administratorrechte für den Server verfügen, den Sie für ADAM konfigurieren.

Dies sind Beispielverfahren. Aufgrund von Installations- und Umgebungsvariationen können wir keinen direkten Support anbieten. Wir empfehlen, mit einem -Berater Microsoft zusammenzuarbeiten.

ADAM lässt sich einfach installieren und wird als Service unter den Betriebssystemen Windows ausgeführt. Es kann vollständig angepasst und als Anwendungskomponente verteilt oder als eigenständiges LDAP-Verzeichnis verwendet werden. ADAM verwendet die gleichen Technologien wie Active Directory-Domänencontroller (einschließlich Replikations- und Delegierungsfunktionen) und verfügt über eigene Verwaltungs- und Anpassungsfunktionen. Er kann als Service Windows ausgeführt werden. ADAM kann unter den Betriebssystemen Windows XP, 2000, 2003 und 2008 installiert werden. ADAM ist Bestandteil von Windows Server 2003 R2 und Windows Server 2008. Für frühere Betriebssysteme ist ein Download unter http://www.microsoft.com/downloads http://www.microsoft.com/downloads verfügbar.

Sicherheit

Einige Sicherheitsrichtlinien des Unternehmens verbieten externen Lieferanten und Partnern, eine direkte Verbindung zu einem Active Directory-Domänencontroller (AD) herzustellen. Wenn das Verfügbarmachen bestimmter AD-Objekte oder -Attribute für einen externen Lieferanten oder Partner verboten ist, kann der Zugriff auf Objekte und Attribute mithilfe von AD Security Access Control Entries (ACE oder ACL) blockiert werden. Abhängig von den Sicherheitsanforderungen kann diese Methode die Integration komplexer machen. Es wird empfohlen, mehrere Domänen und Gesamtstrukturen zu konsolidieren. Wenn alle LDAP-Importe und -Authentifizierungen über eine einzige Quelle geleitet werden müssen, kann ADAM als konsolidierte Quelle verwendet werden. Mit Release Windows 2008 wurde diese Funktionalität in Light-Weight-Directory Service, LDS umbenannt. Die Installation und Konfiguration ähnelt Windows Server 2003 R2.

Empfohlene Kenntnisse

Für diese Aufgabe müssen Sie AD, Objektklassen und Attribute verstehen. Für eine erfolgreiche Integration müssen Sie sich mit der aktuellen AD-Objektstruktur auskennen, mit Active Directory-Delegierungen vertraut sein und über eine Strategie verfügen, wie und zu welchen Zwecken ADAM verwendet werden kann. Wenn Sie mit AD oder ADAM nicht vertraut sind, wenden Sie sich an Ihren AD-Administrator, um eine neue ADAM-Umgebung zu konfigurieren.

Treuhänder

Wenn *userProxy*– Objekte verwendet werden, muss der Computer, der ADAM hostet, ein Mitglied der Domäne sein, die die AD-Konten enthält, oder Mitglied einer vertrauenswürdigen Domäne.

Interne Konnektivität

Wenn *userProxy*– Objekte verwendet werden, muss der ADAM-Computer in der Lage sein, eine Verbindung zu den zugehörigen Domänencontrollern herzustellen, um die Proxy-Authentifizierung durchzuführen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Konfigurieren einer -Instanz mit ADAM

Bei der ersten Installation werden die ADAM-Dateien auf Ihren Computer kopiert, die erforderlichen Komponenten registriert und die Anwendungsverknüpfungen erstellt.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig werden alle Anwendungsdateien im `Verzeichnis %systemroot%\ADAM`installiert.

- Windows Server 2003 R2 - ADAM kann mit installiert werden **Systemsteuerung > Programme hinzufügen und entfernen > Manager für optionale Komponenten**an.
- Windows Server 2000 und Windows XP – Heruntergeladen http://www.microsoft.com/downloads von Microsoft.

Erstellen Sie den ersten Instanzservice, der als erster von ADAM gehosteter Verzeichnisdienst fungiert. Führen Sie einen der folgenden Schritte aus:

Prozedur

- Führen *`Sie „adaminstall.exe`*"im ADAM-Ordner aus.
- Verwenden Sie die Tastenkombination **ADAM-Instanz erstellen** aus dem **Startmenü > Programme > ADAM** Ordner.

1. Wählen Sie die Installationsoption **Eine eindeutige Instanz** aus.

   Hinweis: Sie können diese Option verwenden, um ein Instanzreplikat auf einem zweiten Server zu installieren und so ein fehlersicheres System bereitzustellen.

2. Füllen Sie die Felder aus.

ADAM-Instanz

Feld	Beschreibung
Instanzname	Wird hauptsächlich zur Identifizierung des Windows -Servicenamens und -Anzeigenamens verwendet
Ports	legt die für LDAP- und LDAPS-Listener zu verwendenden Portnummern fest. Der standardmäßige LDAP-Port ist 389, LDAPS 636. Wenn diese Ports auf dem Server verwendet werden, wählt der Setup-Assistent neue Ports aus. Arbeiten Sie mit Ihrem Netzwerkadministrator zusammen, um die am besten geeigneten Ports zu ermitteln
Anwendungsverzeichnispartition	erstellt eine Anwendungsverzeichnispartition. In diesem Schritt nicht erforderlich. Wir empfehlen, die neue Partition jetzt zu erstellen. Es empfiehlt sich, den gleichen eindeutigen Namen wie für Ihre Gesamtstruktur oder Domäne zu verwenden, aber die Domäne der höchsten Ebene durch

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	„adam“ anstelle von „com“ oder „local“ zu ersetzen. Wenn Ihre Gesamtstrukturpartition beispielsweise *dc=myCompany,dc=com* ist, können Sie die ADAM-Partition als *dc=myCompany,dc=adam* erstellen.
Dateispeicherorte	wählt den Speicherort für die ADAM-Partitionsdaten aus.
Service-Account-Auswahl	wählt einen Serviceaccount aus, unter dem die Instanz ausgeführt wird. Für eigenständige Services können Sie das Standard-Netzwerk-Servicekonto verwenden. Wenn Sie Replikate verwenden möchten, müssen Sie ein Konto verwenden, das Zugriff auf alle ADAM-Instanzen hat.
ADAM-Administratoren	Delegierung im ADAM-Verzeichnis, die die integrierte Windows-Authentifizierung nutzt. Auf diese Weise wird der anfängliche Zugriff für die -Administration gewährt. Sobald dem ursprünglichen Account Rechte gewährt wurden, delegiert dieser Benutzer oder diese Gruppe Rechte an andere Windows- oder ADAM-Benutzer. Sie können die Standardeinstellung auswählen, um nur dem aktuellen Anwender Administratorzugriff zu gewähren, oder den Zugriff je nach Bedarf einem anderen Anwender oder einer anderen Gruppe gewähren.
Importieren Sie LDIF-Dateien	die zu importierenden Dateien. „MS-UserProxy“ ist die wichtigste zu importierende Datei. Es empfiehlt sich jedoch, alle verfügbaren Dateien hinzuzufügen, da das Schema nur wenig Overhead hat und Sie sich nicht Gedanken über eine spätere Erweiterung machen müssen, wenn Ihre Anforderungen größer werden. Bestätigen Sie die Details, und der Assistent schließt die Konfiguration ab.

Zugehörige Informationen

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Richten Sie die ADAM-Konsole ein

Richten Sie die ADAM-Konsole ein. Obwohl es viele Ähnlichkeiten zwischen ADAM und Active Directory gibt, kann die Verwaltung sehr unterschiedlich sein, da es keine Verwaltungskonsole für **Benutzer und Computer** gibt.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Der Großteil der allgemeinen Administration wird mit der ADAM ADSI MMC-Konsole durchgeführt, die über das **ADAM** -Startmenü verfügbar ist. Wenn Sie die ADAM-ADSI-Konsole zum ersten Mal ausführen, müssen Sie eine Verbindung zu der von Ihnen erstellten Partition herstellen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Klicken Sie mit der rechten Maustaste auf das Element **ADAM ADSI Bearbeiten** im linken Frame.
2. Geben Sie der neuen Verbindung einen Namen, und aktualisieren Sie die Felder für Servername und Port mit den Informationen, die beim Erstellen der Instanz verwendet wurden.
3. Wählen Sie den **eindeutigen Namen** oder **Benennungskontext** aus, und geben Sie den eindeutigen Namen der zuvor erstellten Anwendungspartition an.
   Sie können eine Verbindung zu den *Konfigurations- und Schemapartitionen* herstellen, um erweiterte Konfigurationsoptionen zu erhalten.
   Sie sollten jetzt Einblick in die Partition und die Standardcontainer für LostAndFound, NTDS-Kontingente und Rollen haben. Der Rollencontainer wurde noch nicht konfiguriert.

Zugehörige Informationen

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Erstellen Sie Container und Organisationseinheiten für ADAM

Gruppieren Sie in ADAM gespeicherte Objekte logisch in Containern und Organisationseinheiten (OE), wie in Active Directory.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Klicken Sie mit der rechten Maustaste auf die Stammpartition, und navigieren Sie zu **Neu** > **Objekt** > **organisationseinheit**an.

   Hinweis: Sie können auch die Liste anderer verfügbarer Objekte anzeigen. Diese Liste variiert je nach den Schemaerweiterungen, die beim Importieren der LDF-Dateien installiert wurden.

2. Wenn Sie zur Eingabe eines Werts aufgefordert werden, geben Sie den Namen der OE ein, z. B. `Benutzer`.
   Auf dem Bildschirm wird die Schaltfläche **Weitere Attribute** angezeigt.
3. Verwenden Sie die Schaltfläche, um zusätzlichen Attributen Werte zuzuweisen.
   Für die OEs und Container sind keine zusätzlichen Werte erforderlich.
   Nach dem Erstellen der OEs werden die neuen OEs als untergeordnetes Element des Stammobjekts aufgeführt.

Zugehörige Informationen

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Delegierung mit ADAM

Sobald die OE-Struktur erstellt wurde, definieren Sie die Berechtigungsdelegierungen, um die Objekte ordnungsgemäß für eingeschränkte Benutzer zu sichern.

Wie bei Active Directory gibt es zwei allgemeine Möglichkeiten, Berechtigungen zu erteilen:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Fügen Sie einer Gruppe Anwender hinzu, die bereits über die entsprechenden Berechtigungen verfügen.
- Definieren Sie neue Berechtigungen für die ADAM-Objekte.

Für diese Aufgabe besprechen wir Berechtigungen auf Objektebene. Informationen zu Gruppenmitgliedschaften finden Sie im Abschnitt Gruppenadministration.

Da es keine Benutzer- und Computerkonsole für ADAM gibt, werden alle Berechtigungen auf Objektebene mit dem Active Directory-Dienstprogramm *DSACLS.exe* definiert. Diese Datei befindet sich im ADAM-Programmverzeichnis. Beim Ausführen von ADAM-Dienstprogrammen starten Sie am besten die Eingabeaufforderung für ADAM-Tools. Dadurch wird sichergestellt, dass die richtigen Versionen der Tools verwendet werden. DSALCS wird zum Anzeigen und Festlegen von Objektzugriffsrechten verwendet.

Beispiel: „`dsacls \\localhost:50010\dc=myCompany,dc=adam`“ zeigt die Berechtigungen an, die dem Stamm der Partition *dc=myCompany,dc=adam* zugewiesen sind, die auf dem lokalen Host, Port 50010, ausgeführt wird. DSACLS ist ein komplexes Tool, das zum Erstellen komplexer Delegierungen verwendet wird. *„DSACLS /?" ausführen.* für Nutzungshinweise.

Zugehörige Informationen

Erstellen Sie Container und Organisationseinheiten für ADAM

Verwenden Sie ADAMSync, um ADAM auszufüllen

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Ausfüllen von ADAM-Objekten

Zu den ADAM-Objekten gehören Anwenderobjekte, UserProxy-Objekte und Gruppenobjekte.

Anwenderobjekte

Anwender können mit der ADAM ADSI-Bearbeitungskonsole genau wie bei der OU-Erstellung erstellt werden. Benutzer können auch mit AD-Befehlszeilentools administriert werden, was den Umfang dieses Dokuments sprengt. Das einzige obligatorische Attribut für neue Anwenderobjekte ist *cn*, bei dem es sich um einen Kurznamen oder den vollständigen Namen des Anwenders handelt. Es gibt auch eine Vielzahl optionaler Attribute, die den Active Directory-Benutzerattributen ähneln. Sie können auf die vollständige Liste der Attribute zugreifen, indem Sie Eigenschaften aus dem Benutzerobjekt auswählen.

UserProxy-Objekte

Für die LDAP-Integration ServiceNow empfehlen wir die Verwendung *von UserProxy-* Objekten in ADAM, die ein Proxy-Konto erstellen, das eine Verknüpfung mit dem zugehörigen AD-Anwenderaccount herstellt. Auf diese Weise können Sie festlegen, dass ADAM die Anmeldeinformationen mit AD-Anwendernamen und Passwörtern aus der Domäne authentifiziert, ohne dass ServiceNow eine direkte Verbindung zum Domänencontroller herstellen muss. *UserProxy-* Objekte sind AD- und ADAM-Anwenderobjekten sehr ähnlich. Sie speichern keine Passwörter und verfügen über ein *objectSID*-Attribut, das die SID aus dem verknüpften AD-Anwenderobjekt enthält. So funktioniert der Proxy. *UserProxy-* Objekte werden mit der *ADSIEdit*-Konsole oder Befehlszeilentools erstellt, dies kann jedoch mühsam sein. Es wird empfohlen, einen automatisierten Prozess wie unten definiert zu verwenden.

Gruppenobjekte

Gruppen werden mit der ADSIEdit-Konsole und den AD-Befehlszeilentools erstellt. Gruppenkonzepte sind ähnlich wie AD und werden zur Integration von Gruppen und

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mitgliedern in ServiceNowverwendet. Der größte Unterschied besteht darin, dass ADAM-Gruppen Mitglieder aus ADAM oder aus vertrauenswürdigen AD-Domänen enthalten können.

Automatisiert die ADAM-Objekterstellung

Wenn Sie Active Directory-Konten mit ADAM synchronisieren möchten, empfehlen wir die Verwendung von Microsoft *ADAMSync* Tool. Dies ist die häufigste Verwendung von ADAM für die ServiceNow LDAP-Integration.

Über Berechtigungsdelegierung

ADAM enthält einige integrierte Gruppen mit Standardberechtigungen. Diese Gruppen befinden sich im Container *cn=roles,dc=myCompany,dc=adam*. Diese ähneln Gruppen auf Domänenebene und haben Rechte für Objekte in der aktuellen Partition. Ähnlich wie bei AD-Gesamtstrukturen können Sie auch eine höhere Berechtigungsebene festlegen, indem Sie die Standardgruppen in *cn=roles,cn=configuration,dc=myCompany,dc=adam verwenden*. Sie müssen eine Verbindung zur Konfigurationspartition in *ADSIEdit herstellen*. Die Administratorgruppe enthält standardmäßig den Account, der während des Setups angegeben wurde. Dieses Mitglied ist nicht immer sichtbar, da es über die Konfigurationsgruppen geerbt wird. Administratoren haben vollständige Kontrolle über alle Partitionsobjekte. Die Gruppe „Leser“ enthält standardmäßig keine Mitglieder und hat Lesezugriff auf alle Objekte in der Partition. Die Gruppe „Anwender“ ist genau wie in Active Directory eine dynamische Gruppe. Sie enthält vorübergehend alle in der Partition erstellten ADAM-Anwender.

Zugehörige Informationen

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Testen und Behandeln von ADAM-Setups

Zum Testen wird primär das Tool LDP verwendet. Auf diese Weise können Sie die Anwenderauthentifizierung vollständig testen.

Der Großteil der Objektverwaltung kann mit der ADAM ADSI-Bearbeitungskonsole durchgeführt werden, die Zugriff auf die gesamte Sammlung von Objekten und Attributen bietet. Die höchste Kontroll- und Problembehandlungsebene für ADAM-Services ist die Verwendung des Service Windows, der während des Setups der Instanz erstellt wurde. Der Servicename variiert und hängt vom Namen der erstellten Instanz ab. Dieser Service muss ausgeführt werden, damit der ADAM-Service ausgeführt werden kann. Wenn Verbindungsprobleme auftreten, überprüfen Sie die Netzwerkkonfigurationen, um sicherzustellen, dass Sie über den entsprechenden Netzwerkzugriff verfügen, um eine Verbindung zum Server und ADAM-Port herzustellen. Für jede installierte ADAM-Instanz wird ein Windows-Ereignisprotokoll erstellt. Dies ist auch ein hervorragendes Tool für die Problembehandlung bei ADAM-Services.

Das Sicherheitsereignisprotokoll Windows ist auch hilfreich bei der Problembehandlung *von userProxy-* Authentifizierungen. Alle *userProxy-Anmeldeversuche* werden im Sicherheitsprotokoll protokolliert und verweisen auf die Remote-Client-Geräteadresse, den eindeutigen Namen des Anwenders, der sich anmelden möchte, und das Ergebnis oder den Statuscode.

Zugehörige Informationen

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherung und Wiederherstellung mit ADAM

Alle ADAM-Daten können mit standardmäßigen Dateisystem-Sicherungsmethoden gesichert werden.

Redundanz

ADAM verfügt über integrierte Replikationsdienstprogramme, die auf der gleichen Technologie wie AD basieren. Ein vollständiges Replikat mit Lese- und Schreibzugriff einer ADAM-Partition kann auf demselben oder einem anderen Computer vorhanden sein. Sie können dieses Replikat auf verschiedene Arten verwenden, um eine fehlersichere LDAP-Integration mit der -Instanz bereitzustellen. Eine Option besteht darin, beide Partitionen für die Instanz über die Firewall verfügbar zu machen und beide Server im Feld „Server“ der LDAP-Eigenschaften zu definieren.

Zugehörige Informationen

Active Directory-Anwendungsmodus (ADAM)

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Verwenden Sie LDAPS mit ADAM

Die Standardkonfiguration für *die userProxy-* Objektauthentifizierung dient der Erzwingung der LDAPS-Kommunikation (sicheres LDAP). LDAPS erfordert SSL-Zertifikate, um den Netzwerkdatenverkehr zu sichern.

Um diese Anforderung zu entfernen, führen Sie die folgende Änderung mithilfe der mit der Konfigurationspartition verbundenen *ADSIEdit* -Konsole durch.

```
Object: CN=Directory Service, CN=Windows NT, CN=Services,
 CN=Configuration
Attribute: msDS-Other-Setings
Value: change RequiresSecureProxyBind from 1 (enforced) to 0 (disabled)
```

Starten Sie den ADAM-Service neu, um die neue Einstellung zu verwenden.

Um sichere Bindungen zu unterstützen und die übertragenen Anwender- und Passwortinformationen zu verschlüsseln, muss ein SSL-Zertifikat auf dem Server und einem beliebigen LDAP-Client installiert sein. Da der ADAM-Service nur begrenzte und kontrollierte Verwendungszwecke bietet, ist es möglich, ein selbstsigniertes Zertifikat zu verwenden, das die Anforderungen erfüllt, ohne dass Zertifikatkosten anfallen oder eine CA-Infrastruktur (Certificate Authority) aufgebaut wird. Wenn Sie bereits eine Zertifizierungsstelle haben, können Sie ein Zertifikat ausstellen. Andernfalls erstellen Sie ein selbstsigniertes Zertifikat.

Erstellen eines selbstsignierten Zertifikats

Zur Verwendung des *Selfssl-* Dienstprogramms müssen Internetinformationsdienste (IIS) installiert sein. Dieser Service kann entfernt werden, nachdem Sie das Zertifikat generiert haben. Sie können das Dienstprogramm „selfssl.exe“ aus dem IIS Resource Kit abrufen. Wenn IIS bereits installiert ist, erstellen Sie eine neue Website, damit die aktuellen Websites nicht von der Zertifikatgenerierung betroffen sind. SelfSSL muss das neue selbst ausgestellte Zertifikat vorübergehend an eine gültige Website anhängen.

Selfssl ist ein Befehlszeilentool und verfügt über die folgenden allgemeinen Parameter.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Selfssl-Parameterbeschreibungen

Parameter	Beschreibung
/T	Fügt das Zertifikat zu „Vertrauenswürdige Zertifikate“ auf dem lokalen Computer hinzu
/N:cn	Legen Sie den allgemeinen Namen des Zertifikats fest. Dieser muss mit dem vollqualifizierten Domänennamen des Servers übereinstimmen, der den Webservice unter Verwendung des Zertifikats ausführt
/K	Legt die Stärke der Schlüsselgröße in Bit fest
/V	Anzahl der Tage, die das Zertifikat gültig ist
/S	ID der Website, an die das Zertifikat angehängt werden soll
/S	IP-Port des Webservice

Das allgemeine Namensattribut muss mit dem externen Namen oder der Adresse übereinstimmen, die die Instanz für die Verbindung mit Ihrem ADAM-Computer verwendet. Sie müssen die Website-ID der IIS-Website abrufen, es sei denn, Sie verwenden die Standardwebsite 1, die nicht im Selfssl-Befehl definiert werden muss. Ein Beispielbefehl zum Generieren eines Zertifikats für myCompany wäre:

```
selfssl /N:CN=myCompany.externaldomain.com /K:1024 /V:3650 /S:12345 /
P:50001 /T
```

Mit dieser Anweisung wird ein Zertifikat erstellt, das 10 Jahre lang gültig ist. Legen Sie den Wert auf eine beliebige Dauer fest. Beachten Sie jedoch, dass das neue Zertifikat generiert und an die Instanz übermittelt werden muss, bevor das alte abläuft. Wir empfehlen, das Ablaufdatum auf dem Zertifikat zu notieren.

Sobald das Zertifikat generiert wurde, können Sie es von der Website entfernen oder die gesamte Website löschen, wenn Sie eine temporäre Website erstellt haben.

Zugehörige Informationen

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Weisen Sie das Zertifikat ADAM zu

Installieren Sie ein SSL-Zertifikat auf dem Server und einem beliebigen LDAP-Client, um sichere Bindungen zu unterstützen und die übertragenen Anwender- und Passwortinformationen zu verschlüsseln.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Da der ADAM-Service nur begrenzte und kontrollierte Verwendungszwecke bietet, ist es möglich, ein selbstsigniertes Zertifikat zu verwenden, um Ihre Anforderungen zu erfüllen, ohne Zertifikatkosten zu verursachen oder eine Zertifizierungsstellen-Infrastruktur (CA) aufzubauen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Öffnen Sie die MMC-Konsole für Zertifikate, und erstellen Sie zwei Konsolenverbindungen, eine für lokale Computerzertifikate und eine andere für lokale Computerservices-Zertifikate im neuen ADAM-Service.
   Das neue Zertifikat finden Sie unter `Zertifikate (Lokaler Computer)\Personal\Zertifikate`.
2. Kopieren Sie das Zertifikat in den Container für den ADAM-Service `Certificates – Service (ADAM Service Name)\ADAM_ADAM Service Name\Trusted Root Certificates\Certificates`, und kopieren Sie das Zertifikat nach `Certificates – Service (ADAM Service Name)\ADAM_ADAM Service Name\Personal\Certificates`.
3. Öffnen Sie die Registerkarte „Details“ des von Ihnen kopierten Zertifikats, notieren Sie sich den Datumsstempel Gültig ab, und weisen Sie der Zertifikatschlüsseldatei Lesezugriff zu. Wechseln Sie zu `C:\Dokumente und Einstellungen\Alle Benutzer\Anwendungsdaten\Microsoft\Crypto\RSA\MachineKeys`, und identifizieren Sie das Zertifikat mit dem entsprechenden Zeitstempel. Weisen Sie dem Servicekonto, in dem ADAM ausgeführt wird, Lese- und Ausführungsrechte zu. Standardmäßig ist dies **Netzwerkservice**.
4. Starten Sie den ADAM-Service neu, um das neue Zertifikat zu aktivieren.

Zugehörige Informationen

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Exportieren Sie das Zertifikat des öffentlichen Schlüssels

LDAPS-Clients, einschließlich der -Instanz, benötigen das Zertifikat des öffentlichen Schlüssels, um eine sichere Verbindung zu ADAM herzustellen.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Exportieren Sie aus den oben verwendeten Serverzertifikatskonsolen einen öffentlichen Schlüssel, der von den Clients verwendet werden soll.

Prozedur

1. Wählen Sie das Zertifikat aus, klicken Sie mit der rechten Maustaste, und wählen Sie **Alle Aufgaben/Export**aus.
   Exportieren Sie den privaten Schlüssel nicht. Wählen Sie das Standardformat „X.509 mit DER-codierter Binärdatei“ aus, und geben Sie den Namen der Exportdatei an.
2. Installieren Sie das öffentliche Zertifikat auf den LDAP-Clients, die über LDAPS eine Verbindung zum Server herstellen.
   Wenn Sie dazu aufgefordert werden, fügen Sie das Zertifikat dem Speicher der *`vertrauenswürdigen Stammzertifizierungsstellen`* hinzu.

Zugehörige Informationen

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Account für den Active Directory Application Mode-Zugriff (ADAM).

Das System benötigt einen Benutzeraccount, um die in die Anwendungsinstanz importierten ADAM-Objektinformationen (Active Directory Application Mode) zu lesen.

Erstellen Sie den Account mit einer der folgenden Methoden:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erstellen Sie ein lokales ADAM-Anwenderaccount, weisen Sie ihm ein Passwort zu, und weisen Sie ihm Berechtigungen zu.
- Weisen Sie einem Domänenkonto Windows in der ADAM-Partition die Berechtigung zu.
- Verwenden Sie ein *userProxy*-Konto.

Wenn Sie ADAM als LDAP-Quelle verwenden, müssen Sie den vollqualifizierten Distinguished Name (FQDN) des ADAM-Kontos im Feld „ **Distinguished Name** für Anmeldung“ des LDAP-Servers angeben.

Zugehörige Informationen

Active Directory-Anwendungsmodus (ADAM)

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Testen Sie die LDAPS-Verbindungen

Testen Sie die LDAPS-Verbindungen. Es gibt zwei Konsolenverbindungen, eine für lokale Computerzertifikate und eine für Zertifikate für lokale Computerservices im neuen ADAM-Service.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Führen *Sie „LDP.exe"* im ADAM-Installationsordner `c:\windows\adam` aus.
   Stellen Sie sicher, dass die ADAM-Version ausgewählt ist, da dies nicht der standardmäßige Windows LDP-Client ist.
2. Öffnen Sie eine neue Verbindung über das Menü **Verbindung/Verbinden**.
   Der Servername muss mit dem CN übereinstimmen, das dem Zertifikat zugewiesen ist.
3. Geben Sie den **LDAPS-Port** ein, und aktivieren Sie das Kontrollkästchen **SSL**.
   Eine erfolgreiche Verbindung führt zu allgemeinen Serverinformationen und keinen Fehlern.
4. Binden Sie den Service an (melden Sie sich an).
   Um typische LDAP-Client-Verbindungen zu replizieren, wählen Sie die Option Einfache Bindung aus. Geben Sie einen gültigen eindeutigen Namen für den ADAM-Anwender oder *UserProxy* in das Anwenderfeld und das zugehörige Passwort ein.
   Wenn eine Antwortmeldung mit dem Hinweis „Authentifiziert als:…“ angezeigt wird. dann wurde erfolgreich eine LDAPS-Verbindung hergestellt.

Zugehörige Informationen

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Verwenden Sie ADAMSync, um ADAM auszufüllen

Administratoren verwenden MS ADAMSync, um LDAP-Verzeichnisse zu füllen, die MS ADAM verwenden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

In diesem Dokument wird davon ausgegangen, dass Sie mindestens über ein grundlegendes Verständnis von Microsoft Windows Server, Active Directory und ADAM verfügen und bereits eine funktionsfähige Instanz Active Directory-Anwendungsmodus (ADAM) mit einer Partition haben.

Dies sind Beispielverfahren. Aufgrund der Komplexität und der Tatsache, dass es in Ihrer Umgebung ausgeführt wird, können wir keinen direkten Support anbieten. Wir empfehlen Ihnen, sich bei Problemen an Microsoft oder einen Microsoft -Berater zu wenden.

Sobald ADAM installiert und die erste Partition erstellt wurde, können Sie sie mit Objekten füllen.

Die folgenden Optionen sind verfügbar:

- Manuelle Objekterstellung mit GUI oder Skripts. Diese Option ist ineffizient und langsam.
- Integrieren Sie mit Active Directory mithilfe des Microsoft Integration Information Server. Diese Option bietet letztendlich die meiste Flexibilität und Funktionalität, erfordert jedoch einige erweiterte Konfigurationen. Es ist eine kostenlose Version von MIIS verfügbar, die mit Active Directory, ADAM undMicrosoft Global Address Lists von Exchange kompatibel ist. Sofern Sie bereits Erfahrung mit MIIS haben, empfehlen wir Ihnen nicht, eine neue Umgebung nur für die LDAP-Integration zu implementieren.
- Verwenden Sie ADAMSync, ein Synchronisierungstool, das Microsoft mit ADAM bereitstellt. Dies ist die Option, die hier erläutert wird.

Definieren Sie ADAM-Anwenderaccounts

Definieren Sie Benutzeraccounts in ADAM. Ein Benutzerkonto wird für die Instanz verwendet, mit der eine Verbindung hergestellt werden soll, und das andere Benutzerkonto wird für ADAMSync verwendet.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Diese Konten können lokale ADAM-Anwenderobjekte, UserProxy-Objekte oder ein Windows-Konto aus einer vertrauenswürdigen Domäne sein.

Das Konto *ADAM User* erfordert schreibgeschützten Zugriff auf die Verzeichnisstruktur, die Sie in Ihre -Instanz importieren. Am besten erreichen Sie dies, indem Sie den Account dem Mitgliedsattribut in der Lesergruppe in cn=roles,dc=myCompany,dc=adam hinzufügen.

Neue ADAM-Anwenderaccounts sind standardmäßig deaktiviert. Sie müssen die neuen Konten aktivieren und ein Passwort festlegen.

Prozedur

1. Aktivieren Sie Anwender, indem Sie das Attribut „msDS-UserAccountDisabled“ in FALSCH ändern.
2. Klicken Sie mit der rechten Maustaste auf das Benutzerobjekt, und setzen Sie das Passwort zurück.
3. Testen Sie die neuen Accounts mithilfe von LDP wie in Active Directory-Anwendungsmodus (ADAM) definiert, um sicherzustellen, dass eine Verbindung hergestellt werden kann. Verwenden Sie den **LDAP** > **Ansicht/Struktur** Lassen Sie dabei den Basis-DN leer, um sicherzustellen, dass Sie die Objekte im Verzeichnis mit den neuen Accounts anzeigen

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

können. Im linken Bereich sollten die Konfiguration, das Schema und die Domänenpartition sichtbar sein. Durchlaufen Sie die Domänenpartition. Wenn Sie ein neues lokales ADAM-Konto verwenden, wird „Keine untergeordneten Elemente“ angezeigt, was bedeutet, dass Sie keinen Lesezugriff auf die Objekte haben. Überprüfen Sie die Setup-Gruppenmitgliedschaften, und wiederholen Sie den Test.

ADAMSync verwendet den Account *ADAMSync User* zum Verwalten von Objekten in der ADAM-Partition. Dieser Account erfordert Rechte auf Administratorebene, da er ADAM-Objekte erstellt, aktualisiert und löscht.

ADAMSync verwendet den Account *ADAMSync AD*, um die AD-Objekte zu lesen, die mit ADAM synchronisiert werden.

Richten Sie ADAMSync ein

ADAMSync ist in Windows Server 2003 R2 enthalten. Laden Sie ADAMSync herunter, und installieren Sie es, wenn Sie ein anderes Betriebssystem verwenden.

Das Schema wird erweitert

Das ADAM-Schema muss erweitert werden, um ADAMSync zu unterstützen.

1. Führen Sie den folgenden Befehl aus c:\windows\adam aus, um die ADAMSync-Schemaerweiterungen zu importieren. Möglicherweise müssen Sie „server:port“ ändern und Anmeldeinformationen hinzufügen, wenn der aktuelle Anwender keinen Zugriff hat. Weitere Informationen finden Sie in der Datei „AdemSyncMetadata.ldf“.

```
ldifde -i -f MS-AdamSyncMetadata.LDF -s localhost:50000 -j . -c
 "cn=Configuration,dc=X" #configurationNamingContext
```

2. Machen Sie dasselbe mit MS-AdamSchemaW2k3.ldf, um Windows 2003-Attribute zu unterstützen.

```
ldifde -i -u -f MS-AdamSchemaW2K3.LDF -s localhost:50000 -j . -c
 "cn=Configuration,dc=X" #configurationNamingContext
```

Empfohlene Schemaänderungen

Hier sind einige zusätzliche Schemaänderungen, die wir empfehlen.

1. Öffnen Sie eine neue MMC-Konsole, und fügen Sie das ADAM-Schema-Snap-in hinzu.
2. Stellen Sie eine Verbindung zur ADAM-Instanz her.
3. Erweitern Sie den Ordner Klassen, suchen Sie die Klasse userProxy, öffnen Sie **Eigenschaften**.
4. Überprüfen Sie die folgenden optionalen Attribute auf der Registerkarte Attribute, und fügen Sie alle hinzu, die noch nicht vorhanden sind.
   - Unternehmen
   - department
   - bestimmteNane
   - E-Mail
   - PhysicalDeliveryOfficeName
   - sAMAccountName
   - sn
   - Telefonnummer
   - Titel

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- userAccountControl
- userPrincipalName

5. Starten Sie den ADAM-Service neu, um die neuen Einstellungen zu aktivieren.

Installieren Sie die ADAM-Konfigurationsdatei

Installieren Sie die ADAM-Konfigurationsdatei über die Windows-Befehlszeile.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Installieren Sie die Konfigurationsdatei.

```
C:\WINDOWS\adam>adamsync /install localhost:50000
MS-AdamSyncConf-SNC.XML
```

2. Führen Sie die Synchronisierungsdatei aus, um sich bei der -Konsole anzumelden.

```
C:\WINDOWS\adam>adamsync /sync localhost:50000
"ou=users,dc=service-now,dc=adam" /log -
```

3. Überprüfen Sie die Ergebnisse mit der ADSIEdit-Konsole.
   Sie sollten die neuen Objekte und Attribute sehen, die von ADAMSync erstellt wurden.
4. Führen Sie LDAP aus, um die UserProxy-Authentifizierung zu testen.
   Automatisierung des Synchronisierungsprozesses

   Richten Sie den Synchronisierungsprozess als geplante Windows Aufgabe ein. Sie müssen die Anmeldeinformationen entweder in der Konfigurationsdatei oder in der Befehlszeile angeben oder die geplante Aufgabe mit einem Account ausführen, der über Zugriff verfügt.

   Besondere Hinweise

   - Sie können mehrere Konfigurationsdateien und geplante Aufgaben erstellen, um ADAM aus mehreren Quellen zu synchronisieren.

     In diesem Beispiel wird das Attribut „sAMAccountName“ importiert, das als Anwendungsanmeldung verwendet werden kann. Wenn Sie die Synchronisierungsquelle aufrufen möchten, müssen Sie sicherstellen, dass Sie über einen eindeutigen Attributwert verfügen, der für die Anmeldeinformationen verwendet werden kann. sAMAccountName ist innerhalb einer Domäne garantiert eindeutig, jedoch nicht domänenübergreifend.

   - Wenn Sie Microsoft Exchange verwenden, empfehlen wir, cn=SystemMailbox*-Objekte als Teil der Objektfilterkonfiguration auszuschließen.

ADAM-Beispielkonfigurationsdateien

Alle Konfigurationen für ADAMSync werden in XML-Dateien gespeichert.

Standardkonfigurationsdatei mit Kommentaren

In der ADAMSync-Installation ist eine Standardkonfigurationsdatei namens „MS-AdamSyncConf.xml“ enthalten. Erstellen Sie eine Kopie dieser Datei, damit Sie ein

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Basisbeispiel haben, auf das Sie in Zukunft zugreifen können. Dieses Beispiel ist die Standardkonfigurationsdatei mit hinzugefügten Kommentaren.

```
<?xml version="1.0"?>
<doc>
 <configuration>
<!-- Sync File Description -->
<description>MyCompany ADAMSync Configuration</description>
  <security-mode>object</security-mode>;
<!-- source-ad-name = fqdn of the domain controller -->;

 <source-ad-
name>;fully.qualified.domain.name.of.domain.controller</source-ad-name>;
<!-- source-ad-partition = root AD domain partition -->;
  <source-ad-partition>;dc=myCompany,dc=com</source-ad-partition>;
<!-- source-ad-account = use this to specify an account to connect to AD
 -->;
<!-- if not used, the current user will be used  -->;
  <source-ad-account>;</source-ad-account>;
  <account-domain>;</account-domain>;
<!-- target-dn = target ADAM OU -->;
  <target-dn>;ou=servicenow users,dc=myCompany,dc=adam</target-dn>;
  <query>;
<!-- base-dn = should be the root AD partition if you want all users -->;
   <base-dn>;dc=myCompany,dc=com</base-dn>;
<!-- object-filter = standard ldap query format, this will grab all users
 -->;
<!-- need to review results to see if you should modify this filter -->;
   <object-filter>;(objectCategory=person)</object-filter>;
   <attributes>;
<!-- include=userproxy requires objectSID to link back to the AD account
 -->;
    <include>;objectSID</include>;
    <include>;givenName</include>;
    <include>;sn</include>;
    <include>;description</include>;
    <include>;title</include>;
    <include>;company</include>;
    <include>;department</include>;
    <include>;mail</include>;
    <include>;physicalDeliveryOfficeName</include>;
    <include>;telephoneNumber</include>;
    <include>;sAMAccountName</include>;
   </attributes>;
  </query>;
<!-- map for user-to-userproxy object types -->;
  <user-proxy>;
    <source-object-class>;user</source-object-class>;
    <target-object-class>;userProxy</target-object-class>;
  </user-proxy>;
  <schedule>;
   <aging>;
    <frequency>;0</frequency>;
    <num-objects>;0</num-objects>;
   </aging>;
   <schtasks-cmd>;</schtasks-cmd>;
  </schedule>;
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
 </configuration>;
 <synchronizer-state>;
  <dirsync-cookie>;</dirsync-cookie>;
  <status>;</status>;
  <authoritative-adam-instance>;</authoritative-adam-instance>;
  <configuration-file-guid>;</configuration-file-guid>;
  <last-sync-attempt-time>;</last-sync-attempt-time>;
  <last-sync-success-time>;</last-sync-success-time>;
  <last-sync-error-time>;</last-sync-error-time>;
  <last-sync-error-string>;</last-sync-error-string>;
  <consecutive-sync-failures>;</consecutive-sync-failures>;
  <user-credentials>;</user-credentials>;
  <runs-since-last-object-update>;</runs-since-last-object-update>;
  <runs-since-last-full-sync>;</runs-since-last-full-sync>;
 </synchronizer-state>;
</doc>;
```

Konfigurationsdatei für LDAP-Filter

Sie können eine beliebige Filterstufe im Wert object-filter in der Konfigurationsdatei angeben. Verwenden Sie die Standard-LDAP-Abfragesyntax mit den folgenden XML-Escape-Zeichen anstelle der Standardoperatoren.

- AND = "&" durch & ersetzen
- ODER = "|" (vertikale Linie) durch | ersetzen
- NOT = "!“ ersetzen durch !

Referenzkonfigurationsdatei

Hier ist eine tatsächliche Konfigurationsdatei, auf die als Beispiel verwiesen werden kann.

```
<?xml version="1.0"?>;
<doc>;
 <configuration>;
<description>;SNCTest ADAMSync Configuration</description>;
  <security-mode>;object</security-mode>;
  <source-ad-name>;domaincontroller.service-now.com</source-ad-name>;
  <source-ad-partition>;dc=service-now,dc=com</source-ad-partition>;
  <source-ad-account>;</source-ad-account>;
  <account-domain>;</account-domain>;
  <target-dn>;ou=servicenow users,dc=service-now,dc=adam</target-dn>;
  <query>;
   <base-dn>;dc=service-now,dc=com</base-dn>;
   <object-filter>;(objectCategory=person)</object-filter>;
   <attributes>;
    <include>;objectSID</include>;
    <include>;givenName</include>;
    <include>;sn</include>;
    <include>;description</include>;
    <include>;title</include>;
    <include>;company</include>;
    <include>;department</include>;
    <include>;mail</include>;
    <include>;physicalDeliveryOfficeName</include>;
    <include>;telephoneNumber</include>;
    <include>;userAccountControl</include>;
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
   </attributes>;
  </query>;
  <user-proxy>;
    <source-object-class>;user</source-object-class>;
    <target-object-class>;userProxy</target-object-class>;
  </user-proxy>;
  <schedule>;
   <aging>;
    <frequency>;0</frequency>;
    <num-objects>;0</num-objects>;
   </aging>;
   <schtasks-cmd>;</schtasks-cmd>;
  </schedule>;
 </configuration>;
 <synchronizer-state>;
  <dirsync-cookie>;</dirsync-cookie>;
  <status>;</status>;
  <authoritative-adam-instance>;</authoritative-adam-instance>;
  <configuration-file-guid>;</configuration-file-guid>;
  <last-sync-attempt-time>;</last-sync-attempt-time>;
  <last-sync-success-time>;</last-sync-success-time>;
  <last-sync-error-time>;</last-sync-error-time>;
  <last-sync-error-string>;</last-sync-error-string>;
  <consecutive-sync-failures>;</consecutive-sync-failures>;
  <user-credentials>;</user-credentials>;
  <runs-since-last-object-update>;</runs-since-last-object-update>;
  <runs-since-last-full-sync>;</runs-since-last-full-sync>;
 </synchronizer-state>;
</doc>;
```

Konfigurieren Sie Microsoft Active Directory für die sichere LDAPS-Kommunikation

Verwenden Sie Zertifikatpaare, um die LDAPS-Kommunikation mit Microsoft Active Directory (AD) zu aktivieren.

Hinweis: Diese Verfahren wurden mit der Windows 2003 R2 Standard Edition entwickelt und getestet und funktionieren mit allen Versionen von Windows 2003.

Die sichere LDAP-Kommunikation (LDAPS) ähnelt der SSL-Kommunikation (HTTPS), da die Daten zwischen Servern und Clients verschlüsselt werden. Um dies zu erreichen, verwenden Server und Clients gemeinsame Informationen mithilfe von Zertifikatpaaren. Der Server enthält das Zertifikat des privaten Schlüssels und die Clients das Zertifikat des öffentlichen Schlüssels. Diese Zertifikate sind erforderlich, um die LDAPS-Kommunikation mit Microsoft Active Directory (AD) zu aktivieren.

Zur Konfiguration von LDAPS für Active Directory müssen Sie:

- Stellen Sie sicher, dass die Active Directory-Domäne eingerichtet ist und dass die Instanz über die Firewall eine Verbindung zum Active Directory-Server herstellen kann.
- Stellen Sie sicher, dass eine Zertifizierungsstelle (Certificate Authority, CA) vorhanden ist, die ein Zertifikat für den Domänencontroller (DC) ausstellen kann. Wenn Sie noch nicht über eine CA-Infrastruktur verfügen, gibt es zwei Optionen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Richten Sie eine eigenständige CA ein, um das Zertifikat auszustellen
- Fordern Sie ein Drittparteizertifikat an

- Wenn Sie bereits über eine Zertifizierungsstelle verfügen, können Sie ein Zertifikat von einer internen Zertifizierungsstelle generieren.

Alle Zertifikate haben ein definiertes Ablaufdatum, das in den Zertifikateigenschaften angezeigt werden kann. Wenn das Zertifikat abläuft, schlägt der gesamte LDAPS-Datenverkehr fehl, und Ihre Benutzer können sich nicht mehr bei der Instanz anmelden. Um dieses Problem zu beheben, muss ein neues Zertifikat ausgestellt und in Ihrer Instanz installiert werden.

Die Standardablaufdauer für Microsoft CA-Zertifikate beträgt ein Jahr. Zertifikate von externen Zertifizierungsstellen werden normalerweise in Raten von einem Jahr erworben. Notieren Sie sich, wenn Ihr Zertifikat abläuft, oder verwenden Sie die Ablaufbenachrichtigungsfunktion der Anwendung (befindet sich in). **System-LDAP** > **Zertifikate**) an. Stellen Sie sicher, dass Sie ein neues Zertifikat bereit haben, bevor das alte abläuft. So haben Sie Zeit, das neue Zertifikat zu installieren und zu testen, bevor das alte abläuft.

Richten Sie eine eigenständige Zertifizierungsstelle für Active Directory ein

Der erste Schritt zur Konfiguration von Microsoft Active Directory für den SSL-Zugriff besteht im Einrichten einer eigenständigen Zertifizierungsstelle (Certificate Authority, CA).

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Machen Sie sich keine Gedanken über die Auslastung zusätzlicher Ressourcen, da beide erforderlichen Services (IIS und CA) nach dem Ausstellen der Zertifikate deaktiviert werden können.

Prozedur

1. Installieren Sie den Internetinformationsserver (IIS).
2. Installieren Sie Zertifizierungsstellenservices im eigenständigen Modus.
3. Vergewissern Sie sich, dass die Webanwendung für die Zertifikatservices installiert und aktiv ist.

Nächste Maßnahme
Erweitern Sie mithilfe der IIS-Manager-Konsole den lokalen Computer, und wählen Sie *Websites*aus. Der Status der **Standardwebsite** muss „ *Wird*ausgeführt“ sein. Unter der **Standardwebsite** sollte auch eine *ZertSrv*-Anwendung angezeigt werden. Wenn die Website nicht ausgeführt wird oder die Anwendung fehlt, müssen Sie das Problem beheben, bevor Sie fortfahren.

Generiert ein Zertifikat von einer internen Zertifizierungsstelle

Wenn Sie Microsoft Active Directory für den SSL-Zugriff konfigurieren, müssen Sie ein internes Zertifikat generieren und das externe Zertifikat anfordern.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Diese Schritte gelten für Microsoft CA-Services. Wenn Sie eine andere interne CA-Plattform verwenden, wenden Sie sich an den lokalen CA-Administrator.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie auf dem Domänencontroller (DC), für den Sie ein Zertifikat erstellen möchten, zu `http://localhost/certsrv`, oder geben Sie den Namen des CA-Servers an, wenn es sich um einen Remote-Server handelt.
2. Klicken Sie auf der Willkommensseite auf **Zertifikat***anfordern, und wählen Sie erweiterte Zertifikatanforderung aus*.
3. Wählen Sie auf der Seite „Erweiterte Zertifikatanforderung“ **Erstellen** und Anforderung an diese Zertifizierungsstelle senden aus.
4. Schließen Sie die erweiterte Zertifikatanforderung wie folgt ab:

Felder für die Anforderung eines erweiterten Zertifikats

Feld	Eintrag
Name	Der vollqualifizierte Domänenname (FQDN) des DC, der das Zertifikat anfordert.
E-Mail	Die E-Mail-Adresse der Person, die für das Zertifikat verantwortlich ist.
Unternehmen	Ihr Unternehmensname.
Einstellungen für wichtige Optionen	
Erstellen Sie einen neuen Schlüsselsatz	Wählen Sie es aus.
CSR	Kryptografischer Microsoft RSA-Kanal.
Schlüsselnutzung	Exchange
Schlüsselgröße	1024 wird empfohlen. Die Instanz unterstützt bis zu 2048.
Name des automatischen Schlüsselcontainers	Wählen Sie es aus.
Speichern Sie das Zertifikat im Zertifikatspeicher des lokalen Computers	Wählen Sie es aus.

5. Klicken Sie auf **Absenden**.
   Sie werden zu einer Seite weitergeleitet, die Ihre **Anforderungs-ID**bereitstellt. Notieren Sie sich diese ID.
6. Um die ausstehende Anforderung zu verarbeiten, gehen Sie wie folgt vor:
   a. Öffnen Sie die Zertifizierungsstellen-Verwaltungskonsole.
   b. Erweitern Sie den Serverknoten, und wählen Sie **Ausstehende Anforderungen**aus.
   c. Suchen Sie die Anforderungs-ID für die gerade übermittelte Anforderung, klicken Sie mit der rechten Maustaste, und wählen Sie *Alle Aufgaben/Problem aus, um die Anforderung zu genehmigen und das Zertifikat auszustellen*.
7. Um das ausgestellte Zertifikat abzurufen, gehen Sie wie folgt vor:
   a. Navigieren Sie von dem DC aus, von dem Sie die Anforderung gestellt haben zu `http://localhost/certsrv`, oder geben Sie den Namen des CA-Servers an, wenn es sich um einen Remote-Server handelt.
   b. Wählen Sie `Den Status einer ausstehenden Zertifikatanforderung anzeigen aus`.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Wählen Sie den Link zum neuen Zertifikat.

d. Wählen Sie den Link **Dieses Zertifikat installieren aus**.

Nächste Maßnahme
Sie müssen ein Drittparteizertifikat anfordern. Zertifikate von externen Zertifizierungsstellen können bereits ab 30 USD pro Jahr erworben werden. Ausführliche Informationen zum Anfordern eines Zertifikats von einer externen Zertifizierungsstelle finden Sie im Microsoft-Artikel 321051 . Nachdem Sie empfangen, installiert und getestet wurde, befolgen Sie das Exportverfahren.

Testen Sie die LDAPS-Konnektivität lokal

Testen Sie die LDAPS-Konnektivität nach der Installation der internen und Drittparteizertifikate, wenn Sie Microsoft Active Directory für den SSL-Zugriff konfigurieren.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Stellen Sie sicher, dass die Windows-Supporttools auf dem Domänencontroller (DC) installiert sind.
   Das Supporttools-Setup (suptools.msi) finden Sie im Verzeichnis `\Support\Tools` auf Ihrer Windows Server-CD.
2. Navigieren zu **Start** > **Alle Programme** > **Windows-Supporttools** > **Befehlszeile**an.
   Geben Sie in der Befehlszeile „`ldp`“ ein, um das Tool zu starten.
3. *Wählen* Sie im LDP-Fenster die Option aus **Verbindung** > **Verbinden** und stellen Sie den lokalen FQDN und die Portnummer (636) bereit.
   Wählen Sie auch *SSL*aus.
   Bei Erfolg wird ein Fenster mit Informationen zur Active Directory-SSL-Verbindung angezeigt.
   Wenn die Verbindung nicht erfolgreich ist, versuchen Sie, Ihr System neu zu starten, und wiederholen Sie diesen Vorgang.

Exportieren Sie das Public Key-Zertifikat, um das LDAP-Zertifikat zu vertrauen

Exportieren Sie das Zertifikat des öffentlichen Schlüssels, und importieren Sie es in die Anwendung, wenn Sie Microsoft Active Directory für den SSL-Zugriff konfigurieren.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn Ihre Zertifizierungsstelle kein vertrauenswürdiger Drittanbieter ist, müssen Sie das Zertifikat für die ausstellende CA exportieren, damit wir ihr und durch Zuordnung auch dem LDAP-Serverzertifikat vertrauen können. Benutzer von MS Certificate Services können den Zertifikatpfad anzeigen, indem sie das Zertifikat in der für den Export verwendeten Konsole anzeigen. wählen Sie die Registerkarte **Zertifikatpfad**. Sie müssen alle Zertifikate in der Kette exportieren. Sie können das CA-Zertifikat im selben Ordner wie das LDAP-Zertifikat finden, indem Sie im Zertifikatpfad nach dem Namen suchen. Senden Sie alle Zertifikate für den Import in Ihre Instanz.

Prozedur

1. Fügen Sie über eine aktuelle oder neue MMC-Konsole das Snap-in „Zertifikat (Lokaler Computer)“ hinzu.
2. Öffnen Sie den Ordner „ `Persönlich/Zertifikate` “.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Suchen Sie das neue Zertifikat.
   In der Spalte Ausgestellt an wird der FQDN des Domänencontrollers angezeigt.
4. Klicken Sie mit der rechten Maustaste auf das Zertifikat, und wählen Sie *Alle Aufgaben/ Export*aus.
5. In DER- oder Base-64-Format exportieren.
   Benennen Sie die Datei im Format `MyCompany.cer`. Dies ist das öffentliche Schlüsselzertifikat, das in der Instanz für die sichere Kommunikation mit Ihrem Domänencontroller verwendet werden muss.
6. Testen Sie LDAPS lokal, bevor Sie das Zertifikat an die Instanz senden.

Nächste Maßnahme
Importieren Sie nach Abschluss dieses Verfahrens das Zertifikat des öffentlichen Schlüssels in die Anwendung.
Informationen zum Hochladen des Zertifikats in die Anwendung finden Sie unter Installieren Sie das LDAP X.509-SSL-Zertifikat.

Globale LDAP-Katalognutzung

Einem DC kann die Rolle „Globaler Katalog“ (GC) gewährt werden. Die Rolle „Globaler Katalog“ (GC) ist ein LDAP-konformes Verzeichnis, das aus einer Teildarstellung jedes Objekts aus jeder Domäne in einer Gesamtstruktur besteht.

Administratoren konfigurieren Active Directory für das Hosten von LDAP-Verzeichnisinformationen (Lightedge Directory Access Protocol) mit einer der folgenden Hosting-Methoden.

- Die gängige Methode zum Hosten von LDAP-Verzeichnisinformationen ist die Verwendung des Standard-LDAP oder LDAPS (sicheres LDAP) an den Ports 389 oder 636. Diese Standard-LDAP-Ports sind immer auf einem Domänencontroller (DC) vorhanden und werden selten geändert. Der Zugriff auf diese Verzeichnispartition ermöglicht den Zugriff auf alle Objekte innerhalb der Domäne, die auf dem DC gehostet wird. Es gibt keine Möglichkeit, mit dieser Methode auf Objekte aus anderen Domänen zuzugreifen.
- Einem DC kann auch die Rolle Global Catalog (GC) gewährt werden. Die Rolle „Globaler Katalog“ (GC) ist ein LDAP-konformes Verzeichnis, das aus einer Teildarstellung jedes Objekts aus jeder Domäne in der Gesamtstruktur besteht. Auf dieses LDAP-Verzeichnis kann über Port 3268 zugegriffen werden, LDAPS über Port 3269. Die Zertifikatanforderungen für LDAPS- und LDAP-Standardports sind identisch.

LDAP-Abhängigkeiten des globalen Katalogs

- Für den Domänencontroller, mit dem Ihre -Instanz eine Verbindung herstellt, muss die Rolle „Globaler Katalog“ aktiviert sein.
- Firewall-Regeln müssen eingehenden Datenverkehr zum Domänen-Controller auf Port 3268 (LDAP) oder 3269 (LDAPS) zulassen.

Besondere Hinweise

- Nicht alle Attribute werden in der GC-Partition repliziert. Allgemeine Attribute wie Vorname, Nachname, E-Mail-Adresse, Telefonnummer, Beschreibung und Adresse sind enthalten. Zusätzliche Attribute können dem GC hinzugefügt werden, sollten jedoch eingeschränkt werden, um die Auswirkungen auf den Datenverkehr der Gesamtstrukturreplikation zu minimieren.
- Standard-LDAP-Integrationen verwenden in der Regel „sAMAccountName“ als Anwender-ID der Instanz und als Zusammenfügungsschlüssel in der LDAP-Importzuordnung, da diese innerhalb einer Domäne garantiert eindeutig ist. Dieses Attribut ist beim Anzeigen einer

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

gesamten Gesamtstruktur von Domänen nicht mehr eindeutig. Ein neues eindeutiges Attribut muss identifiziert werden und muss als UserID und Verbindungsschlüssel angegeben werden. Diese müssen nicht das gleiche Attribut sein und können je nach Ihrem Gesamtstrukturdesign variieren. Wenden Sie sich an Ihren Active Directory-Administrator. Normalerweise ist userPrinicpalName ein domänenübergreifendes eindeutiges Attribut. Dies ist jedoch möglicherweise kein anwenderfreundlicher Name für die Anmeldung, er kann jedoch für den eindeutigen Bezeichner bei Importen verwendet werden. Ein häufiges Attribut, das für die UserID verwendet wird, ist die E-Mail-Adresse. Diese Entscheidungen wirken sich auf die LDAP-Eigenschaften und die LDAP-Zuordnung aus.

- Der für den Zusammenfügungsschlüssel in der LDAP-Importzuordnung verwendete Wert muss eindeutig sein und für jedes importierte Objekt vorhanden sein. Wenn sie nicht eindeutig ist oder nicht vorhanden ist, werden falsche Datensätze mit Änderungen aktualisiert.
- Wenn Sie bereits eine LDAP-Integration haben und diese in eine GC ändern möchten, ändern Sie den Importkoaleszierungsschlüssel. Die neuen Schlüsselwerte müssen importiert werden, bevor Sie den Zusammenfügungsschlüssel ändern können.
- Wenn Sie Änderungen an Ihrer LDAP-Integration vornehmen, die Ihre Integration unterbrechen, sollte der erste Schritt darin bestehen, diese Änderungen rückgängig zu machen. Wenden Sie sich anschließend an Kundenservice und Support, um vollständige Informationen zu Ihrem Versuch zu erhalten.

Kleinere OpenLDAP-Schemaänderung

In OpenLDAP 2.3-Systemen, die die Back-BDB (Berkley-Back-End) verwenden, nehmen Administratoren eine geringfügige Änderung an ihrem Schema vor, um die Integration zu erleichtern.

> ⚠ **Warnung:** Die hier beschriebene Anpassung wurde für die Verwendung in bestimmten Fällen entwickelt und wird von Now Support nicht unterstützt. Diese Methode wird wie sie ist zur Verfügung gestellt und sollte vor der Implementierung gründlich getestet werden. Veröffentlichen Sie alle Fragen und Kommentare zu dieser Anpassung in unserem Community-Forum .

In OpenLDAP 2.3 bietet „back-bdb“ eingeschränkte Unterstützung für Ungleichheitsindexierung (Reihenfolge). Sie ist nur für die Syntax „generalizedTime“ und „ChangeSequenceNumber“ implementiert. Sie kann nicht für eine Syntax unterstützt werden, die Teilzeichenfolgen unterstützt. Suchfilter, die Ungleichheiten enthalten, werden anhand des Anwesenheitsindex verarbeitet.

Wir empfehlen, zu diesem Zweck ein anwenderdefiniertes Attribut zu erstellen, anstatt das zu ändern, was bereits indiziert oder im Schema vorhanden ist (z. B. *servnowid*).

Ändern Sie das OpenLDAP-Schema

Ändern Sie das OpenLDAP-Schema. Diese Schritte beschreiben eine von einem unserer Kunden bereitgestellte Schemaänderung an OpenLDAP 2.3, die ihm bei der Integration in seine Instanz geholfen hat.

Vorbereitungen
Erforderliche Rolle: admin

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Warnung: Die hier beschriebene Anpassung wurde für die Verwendung in bestimmten Fällen entwickelt und wird von Now Support nicht unterstützt. Diese Methode wird wie sie ist zur Verfügung gestellt und sollte vor der Implementierung gründlich getestet werden. Veröffentlichen Sie alle Fragen und Kommentare zu dieser Anpassung in unserem Community-Forum .

So ändern Sie das OpenLDAP-Schema für die Integration mit der -Instanz:

Prozedur

1. Erstellen Sie ein anwenderdefiniertes Attribut.

   Example

   ```
   attribute ( 1.3.6.1.4.1.3403000.2.1.8

       NAME 'servnowid'
     ORDERING caseIgnoreOrderingMatch
     EQUALITY caseIgnoreMatch
     SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
   ```

2. Fügt das Attribut in die ausgewählte Objektklassen-OID ein.

   Example

   ```
   objectclass ( 1.3.6.1.4.1.3403000.2.2.1
       NAME 'BcfUserIdentifiers' SUP top AUXILIARY
     MAY ( uniqid $ unixid $ servnowid ) )
   ```

   In OpenLDAP 2.3 können Sie die Serverkonfigurationen dynamisch ändern, aber Sie können nur das Schema erweitern. Sie können das vorhandene Schema nicht ändern oder löschen. Anstatt eine weitere Objektklasse für dieses Attribut in der dynamischen Konfiguration zu erstellen, verwenden Sie die statische Konfigurationsdatei (slapd.conf).

3. Fügen Sie in slapd.conf die Indexierung für das neue Attribut im Abschnitt „bdb“ Ihres Hauptdatenbank-Back-Ends ein.

   Example

   ```
   database bdb (configs here) ....

   index servnowid pres

   (other indexes here) .....
   ```

4. Führen Sie als Stamm slapindex aus, um dieses Attribut zu indizieren und in Suchfiltern verfügbar zu machen.
   Stellen Sie sicher, dass der OpenLDAP-Daemon nicht ausgeführt wird oder sich im schreibgeschützten Modus befindet, bevor Sie slapindex starten.

Datensatz-LDAP-Löschungen

Standardmäßig löscht die Instanz keine Einträge, nachdem sie aus LDAP gelöscht wurden.

Durch das Löschen eines Eintrags, der auch als Datensatzbezeichnet wird, werden auch der gesamte Verlauf und Verweise auf den gelöschten Eintrag gelöscht.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel: Configuration Items (CIs), SLA-Vereinbarungen, Softwarelizenzen, Bestellungen und Servicekatalogeinträge haben alle einen Verweis auf die Abteilung, und wenn eine Abteilung gelöscht wird, löscht die Integration alle Verweise auf die Abteilung. Außerdem gehen durch das Löschen eines Anwenders der gesamte Verlauf der Aktionen dieses Anwenders verloren.

Entscheiden Sie, ob beibehalten oder Löschen Sie alle Datensätze aus einer Tabelle entsprechend den Anforderungen Ihrer Organisation beibehalten werden soll.

Begrenzen Sie gleichzeitige Sitzungen

Sie können die Anzahl der gleichzeitigen interaktiven Sitzungen für einen Benutzer oder eine Rolle in einer Instanz auf allen Knoten begrenzen.

Untersuchen



Lernen Sie die Funktionen und den Geschäftsnutzen der Begrenzung gleichzeitiger Sitzungen kennen.

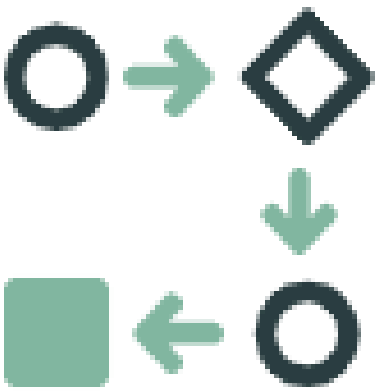
Aktivieren



Erfahren Sie, wie Sie die Begrenzung gleichzeitiger Sitzungen aktivieren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Festlegen



Legen Sie für einen Anwender oder eine Rolle einen Grenzwert für gleichzeitige Sitzungen fest.

Deaktivieren



Erfahren Sie, wie Sie die Begrenzung gleichzeitiger Sitzungen deaktivieren.

Begrenzung gleichzeitiger Sitzungen erkunden

Sie können die Anzahl der gleichzeitigen interaktiven Sitzungen für einen Benutzer oder eine Rolle in einer Instanz auf allen Knoten begrenzen.

Gleichzeitige interaktive Sitzungen beziehen sich auf die Anzahl der Sitzungen, die ein Benutzer pro Instanz ServiceNow aktiv haben kann. Eine aktive Instanzsitzung tritt bei jeder neuen Anmeldung bei einer bestimmten Instanz ServiceNow auf. Standardmäßig gibt es keine Beschränkungen für die Anzahl der aktiven Instanzsitzungen, über die ein Benutzer verfügen kann.

Mit dem Jakarta-Release können Sie die Anzahl der aktiven, gleichzeitigen Sitzungen pro Benutzer begrenzen. Wenn sich der Anwender nach Erreichen der maximalen Anzahl aktiver Sitzungen anmeldet, wird die älteste aktive Sitzung beendet und eine neue interaktive Sitzung aktiviert. Wenn ein Benutzer versucht, über einen Browser auf eine geschlossene Sitzung zuzugreifen, wird er zur Anmeldeseite weitergeleitet.

Hinweis: Das Plugin „ **Gleichzeitige Sitzungen** begrenzen“ muss aktiv sein, um eine maximale Anzahl von Sitzungen zu aktivieren. Grenzwerte werden durch die Eigenschaft „glide.authenticate.max.concurrent.interactive.sessions“ festgelegt. Ein maximaler Grenzwert gilt für alle Benutzer oder Rollen, für die die Eigenschaft „limit“ aktiv ist. Für einen Benutzer oder eine mit dem Benutzer verbundene Rolle muss der Wert limit_concurrent_sessions auf „wahr“ festgelegt sein, damit der Grenzwert für zu initiierende Sitzungen festgelegt wird. Beim Jakarta-Release unterstützt diese Funktion keine Sitzungen, die über die native mobile App oder nicht interaktive Mechanismen erstellt wurden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein typischer Anwendungsfall, wenn maximal 1 gleichzeitige Sitzung festgelegt ist:

1. Der Anwender greift über Chrome auf die ursprüngliche Instanz ServiceNow zu.
2. Nachdem sich der Benutzer erfolgreich angemeldet hat, erstellt ServiceNow Sitzung 1 (S1) für den Benutzer.
3. Der Benutzer beschließt, einen weiteren Zugriff auf die Instanz ServiceNow über Firefox zu initiieren.
4. Nachdem sich der Benutzer erfolgreich angemeldet hat, erstellt ServiceNow Sitzung 2 (S2) für den Benutzer.
5. Da für den Benutzer ein maximales Limit für gleichzeitige Sitzungen von 1 gilt, wird die S1-Sitzung ungültig, wenn S2 erstellt wird.
6. Wenn der Benutzer über Chrome zurückkehrt, um auf die S1-Instanz ServiceNow zuzugreifen, wird er zur Anmeldeseite weitergeleitet, da S1 ungültig ist.

Die Begrenzungen gleichzeitiger Sitzungen funktionieren mit allen ServiceNow -Authentifizierungsmechanismen: SAML, LDAP und lokale Datenbankauthentifizierung. Es funktioniert auch mit der Multifaktor-Authentifizierung und allen interaktiven ServiceNow Authentifizierungsmechanismen. Die Quelle der Sitzung kann über die Tabelle **„sys_user_session“** unter der Spalte „ **Typ**“ angezeigt werden. Mögliche Werte:

- Webbrowser
- Mobiler Browser
- ServiceNow Mobile App
- Nicht interaktiv (SOAP, WSDL, OAuth)

Plugin „Gleichzeitige Sitzungen begrenzen“ aktivieren und konfigurieren

Wenn Sie die Administratorrolle innehaben, können Sie das Plugin „Gleichzeitige Sitzungen begrenzen“ (com.glide.limit.gleichzeitige.sitzungen) aktivieren.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Plugins**an.
2. Suchen Sie das Plugin „Gleichzeitige Sitzungen begrenzen“, und klicken Sie darauf.
3. Überprüfen Sie im System-Plugin-Formular die Plugin-Details, und klicken Sie dann auf den zugehörigen Link **Aktivieren/Aktualisieren**.
4. Klicken Sie auf **Aktivieren**.
5. Um diese Funktion zu aktivieren und eine Obergrenze für gleichzeitige Sitzungen festzulegen, wechseln Sie zur Registerkarte **Plugin-Dateien**, suchen Sie die folgenden Eigenschaften, und ändern Sie die Einstellungswerte.

Option	Bezeichnung
glide.authenticate.limit.gleichzeitige.interaktive.sitzungen	Sie können die Beschränkung gleichzeitiger Sitzungen aktivieren, indem Sie den Wert auf **true festlegen**. Standardmäßig ist diese Eigenschaft auf **False**festgelegt. Dies bedeutet, dass die Anzahl der interaktiven

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	Sitzungen, die ein Anwender aktiv haben kann, unbegrenzt ist. **Hinweis:** Um diese Funktion zu deaktivieren, legen Sie diese Eigenschaft wieder auf **False**fest.
glide.authenticate.max.gleichzeitige.interaktive.sitzungen	Sie können die maximale Anzahl gleichzeitiger aktiver interaktiver Sitzungen festlegen, die ein Benutzer in der Instanz über alle Knoten hinweg haben kann.

6. Wahlweise: Bei Bedarf können Sie auch die folgenden Eigenschaften ändern.

Option	Bezeichnung
glide.authenticate.session.types.to.limit-.gleichzeitigkeit	Diese Eigenschaft schränkt die Sitzungstypen ein. Standardmäßig haben nur die Webbrowsersitzungen ein Limit. Zu den Sitzungstypen gehören: ◦ Webbrowser (1) ◦ Mobiler Browser (2) ◦ ServiceNow Mobile-App (3) ◦ Nicht interaktiv (10) Sie können konfigurieren und den Wert auf „1“ für einen Webbrowser, „2“ für einen mobilen Browser oder „1,2“ für beide festlegen. **Hinweis:** Nur Webbrowser- und Mobile-Browsersitzungen können ein Limit haben. Es gibt keine Grenzwerte für Sitzungen, die aus der mobilen App ServiceNow stammen, oder für nicht interaktive Sitzungen.
glide.authenticate.limit.gleichzeitige.sitzungen.über.alle.knoten	Diese Eigenschaft schränkt die Anzahl gleichzeitiger Sitzungen pro Knoten ein, anstatt sie für alle Knoten einer Instanz ServiceNow zu beschränken. Standardmäßig ist der Wert auf „true“ festgelegt, wodurch Benutzersitzungen auf allen Knoten eingeschränkt werden. Wenn die Eigenschaft auf „false“ festgelegt ist, gelten nur die Sitzungen auf diesem Knoten und nicht die auf den anderen Knoten dem Grenzwert.

7. Klicken Sie auf **Aktualisieren**, damit die Einstellungen wirksam werden.

Nächste Maßnahme

Festlegen eines Grenzwerts für gleichzeitige Sitzungen nach Anwender oder Rolle.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Liste der Plugins (Xanadu)

Festlegen eines Grenzwerts für gleichzeitige Sitzungen nach Anwender oder Rolle

Sie können ein Limit für gleichzeitige Sitzungen für einen bestimmten Anwender oder eine bestimmte Rolle festlegen.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Anwenderadministration** > **Anwender** oder **Anwenderadministration** > **Rollen**an.
2. Wählen Sie den Benutzer oder die Rolle aus, für den bzw. die ein **Limit für gleichzeitige Sitzungen festgelegt werden soll, aktivieren Sie das Kontrollkästchen Gleichzeitige Sitzungen** begrenzen, und klicken Sie auf **Aktualisieren**.
   Der Benutzer oder die Rolle hat ein Limit dafür, wie viele gleichzeitige Sitzungen gleichzeitig geöffnet sein können.

Gleichzeitige Sitzungsbegrenzung nach Anwender oder Rolle deaktivieren

Sie können die Beschränkung gleichzeitiger Sitzungen für einen bestimmten Benutzer oder eine bestimmte Rolle deaktivieren.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Anwenderadministration** > **Anwender** oder **Anwenderadministration** > **Rollen**an.
2. Wählen Sie einen Benutzer oder eine Rolle aus, für die Sie die Begrenzung gleichzeitiger Sitzungen deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Gleichzeitige Sitzungen** begrenzen, und klicken Sie auf **Aktualisieren**.
   Für Benutzer bzw. Rollen gilt keine Begrenzung der Anzahl gleichzeitig geöffneter Sitzungen.

Lokale Authentifizierung

Verwenden Sie die lokale Authentifizierung ServiceNow®, um die Benutzeranmeldung auf einem lokalen Gerät zu sichern.

Die lokale Authentifizierung ist eine Methode zum Überprüfen der Identität eines Benutzers auf einem lokalen Gerät. Es verwendet eindeutige Merkmale oder Anmeldeinformationen, die der Benutzer besitzt, um die Anmeldung des Benutzers zu validieren.

Verwenden Sie die lokalen Authentifizierungsfunktionen von ServiceNow®], um auf Ihren lokalen Geräten sicher auf die Instanz ServiceNow® zuzugreifen.

Anmelde- und Authentifizierungssicherheit

Konfigurieren Sie Optionen für die Anmeldesicherheit, um den Zugriff auf Ihre Instanz zu steuern.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie Ihre Anmeldesicherheit



Erfahren Sie, wie die Anmeldesicherheit konfiguriert wird.

Definieren Sie Anmeldeszenarien



Definieren Sie Anmeldeszenarien.

Passwortzurücksetzung



Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erfahren Sie mehr über das Zurücksetzen des Anmeldepassworts.

Anmelden und Authentifizierungssicherheit erkunden

Konfigurieren Sie Optionen für die Anmeldesicherheit, um den Zugriff auf Ihre Instanz zu steuern.

Sicherheitsoptionen

Sie können verschiedene Aspekte der Sicherheit bei der Anwenderanmeldung und -authentifizierung steuern:

Funktion	Beschreibung	Verwandte Themen
Steuerelemente zum An- und Abmelden	Steuern Sie verschiedene Dimensionen des An- und Abmeldevorgangs für Anwender, z. B. Festlegen einer Zielseite, die dem Anwender bei der Anmeldung angezeigt wird, und steuern Sie, wie sich Anwender abmelden.	• Anmeldeszenarien definieren • Konfigurieren der Bestätigungsaufforderung für die Abmeldung • Installations-Exits • Sperrung für fehlgeschlagene Anmeldeversuche angeben
Authentifizierungssicherheit	Steuern Sie den Prozess zum Zurücksetzen des Passworts und Funktionen wie die Option „Anwendernamen speichern“. Sie können auch IP-adressbasierte Steuerungen für den Zugriff auf die Instanz verwenden und eine Nonce implementieren, die mit der Single Sign-on-Digest-Authentifizierung verwendet werden soll.	• Konfigurieren Sie Ihre Passwortrichtlinie • Passwortzurücksetzung • Anwendernamen speichern • Authentifizierung mit IP-Adressbereich • Implementieren einer Nonce

Anmeldeszenarien definieren

Sie können alle Benutzer nach der Anmeldung auf dieselbe Seite verweisen.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn sich Benutzer direkt bei einer Instanz anmelden, z. B. über http://{instance_name}.service-now.com/, geht das System wie folgt vor:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Greift auf den Wert in der Eigenschaft *glide.entry.page.script*zu. Der Standardwert der Eigenschaft wird von einer Skripteinbindung mit dem Namen *CMSEntryPage abgeleitet*.
2. Leitet den Anwender zur Anmeldeseite der Instanz um, wenn die Einstiegsseite eine Anmeldung erfordert.
3. Wendet ggf. Anmelderegeln auf den Anwender an.

So erzwingen Sie, dass das System alle Benutzer nach der Anmeldung auf dieselbe Seite leitet:

Prozedur

1. Navigieren zu **Alle** > **Inhaltsmanagement** > **Konfiguration** > **Konfigurationsseite**an.
2. Wählen Sie einen Wert für das Feld *Anmeldeseite* aus, oder erstellen Sie nach Bedarf eine neue Seite.

   Wenn diese Seite nicht die Standardseite der Website ist, wird immer hierher umgeleitet. Wenn es sich um eine Website-Standardseite handelt, werden Anmelderegeln angewendet. Wenn dieser Wert NULL ist, verwendet das System „navpage.do“ als Einstiegsseite. Geben Sie hier keine Anmeldeseite ein. andernfalls müssen sich Benutzer zweimal anmelden.

   Melden Sie sich bei einer Instanz an, um auf einen Datensatz zuzugreifen:

   Wenn sich Benutzer bei einer Instanz anmelden, um auf einen Datensatz mit seinem global eindeutigen Bezeichner (sys_id) zuzugreifen, z. B. http://{instance}.service-now.com/incident.do?sys_id={sys_id}, dann führt das System Folgendes aus: folgende:

   a. Leitet den Anwender zu einer Anmeldeseite, wenn er noch nicht angemeldet ist.
   b. Leitet den Anwender zum entsprechenden Datensatz weiter, wenn er darauf zugreifen darf. Wenn der Benutzer keine Zugriffsrechte für den Datensatz hat, wird eine Meldung über die Verweigerung des Zugriffs angezeigt.

   Anmeldung beim Serviceportal oder bei einer CMS-Website:

   Wenn sich Benutzer beim Serviceportal oder einer CMS-Website anmelden, z. B. http://<instance> .service-now.com/site-name/page.do, führt das System Folgendes aus:

   - Wenn im Feld Anmeldeseite im Serviceportal- oder CMS- *Websiteformular* ein Wert angegeben ist, wird der Benutzer zu dieser Anmeldeseite weitergeleitet, und es werden ggf. Anmelderegeln auf den Benutzer angewendet.
   - Wenn keine Anmeldeseite angegeben ist, wird der Benutzer zum Wert im Feld *Homepage* im Serviceportal- oder CMS-Websiteformular weitergeleitet.

   Melden Sie sich beim Serviceportal oder bei einer CMS-Website an, um auf einen Datensatz zuzugreifen:

   Wenn sich Benutzer beim Serviceportal oder einer CMS-Website anmelden, um auf einen Datensatz zuzugreifen, z. B. http://{instance}.service-now.com/ess/incident_detail.do?sysparm_document_key=incident,{sys_id}, folgt das System das gleiche Verfahren und führt den Benutzer schließlich zum Datensatz. Wenn der Benutzer keine Zugriffsrechte für den Datensatz hat, wird eine Meldung über die Verweigerung des Zugriffs angezeigt.

Anmeldungen und das Mitarbeiter-Selfserviceportal

Das System verfolgt die erste Startseite, auf die ein Benutzer zuzugreifen versucht, auch wenn er sich beim Mitarbeiter-Selfserviceportal anmelden möchte.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Betrachten Sie die folgenden Szenarien.

Beispiel 1:

1. Ein Benutzer ist nicht angemeldet und versucht dann, mit einer bestimmten SYS-ID in der URL auf einen Datensatz zuzugreifen.
2. Das System leitet den Benutzer zur Anmeldeseite um.
3. Anstatt sich anzumelden, versucht der Benutzer, auf eine andere Website zuzugreifen, z. B. das Mitarbeiter-Selfserviceportal (/ess).
4. Das System leitet den Benutzer erneut zur Anmeldeseite zurück.
5. Der Benutzer meldet sich an und wird zu dem Datensatz weitergeleitet, auf den der Benutzer zuerst zuzugreifen hat, und nicht zum Mitarbeiter-Selfserviceportal.

Beispiel 2:

1. Ein Benutzer ist nicht angemeldet und versucht dann, mit einer bestimmten SYS-ID in der URL über das Mitarbeiter-Selfserviceportal (/ess) auf einen Datensatz zuzugreifen.
2. Das System leitet den Benutzer zur Anmeldeseite um.
3. Anstatt sich anzumelden, versucht der Benutzer, über das Mitarbeiter-Selfserviceportal auf einen anderen Datensatz zuzugreifen.
4. Das System leitet den Benutzer erneut zur Anmeldeseite zurück.
5. Der Benutzer meldet sich an und wird zum ersten Datensatz und nicht zum zweiten weitergeleitet.

Geben Sie eine Anmeldezielseite an

Standardmäßig wird Benutzern bei der Anmeldung ihre Homepage angezeigt. Sie können eine andere Anmeldezielseite angeben, indem Sie eine Systemeigenschaft oder das Content-Management-System verwenden.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Um eine Anmeldezielseite für alle Benutzer anzugeben, ändern Sie den Eigenschaftswert in der Tabelle „sys_properties“.

Prozedur

1. Geben Sie im Navigationsfilter `sys_properties.list` ein.
2. Suchen Sie die Systemeigenschaft **glide.login.home**.
3. Geben Sie im Feld **Wert** den Namen der Seite ein, die allen Anwendern bei der Anmeldung angezeigt wird.

   Verwenden<page name> `.do`; Sie können den Teil `http://''instance''.service-now.com/` in der URL weglassen. Um den Seitennamen oder die URL einer Seite im System zu ermitteln, können Sie auf einen Link zeigen. Mögliche Seiten sind „`welcome.do`“ und „`incident.do`“.

   Um eine Dashboard-Zielseite anzugeben, legen Sie die Eigenschaft auf `$dashboards.do?dashboard`=fest<SYS_ID> . Ersetzen<SYS_ID> mit der sys_id des Dashboards.

   Um Benutzer zum Serviceportal zu leiten, legen Sie die Eigenschaft auf „`/sp`“fest

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Diese Eigenschaft ist systemweit gültig, d. h., wenn sie festgelegt wird, wirkt sie sich auf alle Anwender aus. Um eine Anmeldung speziell für Benutzer ohne Rollen festzulegen, können Sie dieselben Schritte anwenden und die Eigenschaft **„glide.entry.loggedin.page_ess“** verwenden.

Sie können auch eine Anmeldezielseite mit dem Content-Management-System angeben.

Sperrung für fehlgeschlagene Anmeldeversuche angeben

Das System bietet inaktive Skriptaktionen, mit denen Sie die Anzahl der fehlgeschlagenen Anmeldeversuche angeben können, bevor ein Benutzeraccount gesperrt wird, und mit denen die Anzahl nach einer erfolgreichen Anmeldung zurückgesetzt wird.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

Navigieren zu **Alle** > **Systemrichtlinie** > **Skriptaktionen** um die Skripts anzuzeigen oder zu aktivieren.

Hinweis: Ab der Kingston-Release werden die Skriptaktionen **SNC-Benutzersperrprüfung mit automatischer Entsperrung** und **SNC-Benutzerlöschung** nach einem zBoot aktiviert.

Weitere Informationen zu Eigenschaften, die sich auf fehlgeschlagene Anmeldeversuche auswirken, finden Sie unter Fehlgeschlagene Anmeldeversuche verwalten (Härtung der Instanzsicherheit) in den Härtungseinstellungen für die Instanzsicherheit.

Skriptaktion	Beschreibung
SNC-Benutzersperrprüfung mit automatischer Entsperrung	• Verwendet den Wert der Eigenschaft *glide.user.max_unlock_attempts*, um den Grenzwert für fehlgeschlagene Anmeldeversuche festzulegen. • Entsperrt den Benutzeraccount nach dem für die Eigenschaft *glide.user.unlock_timeout_in_mins* angegebenen Zeitraum. Wenn kein Wert angegeben ist, entsperrt das System den Benutzeraccount nach dem Standardzeitraum von 15 Minuten.
SNC-Benutzersperrprüfung	Verfolgt die Anzahl der fehlgeschlagenen Anmeldeversuche und sperrt den Benutzeraccount nach einer angegebenen Anzahl von fehlgeschlagenen Anmeldeversuchen (Standard: 5).
SNC-Benutzerlöschung	Aktualisiert den Benutzerdatensatz nach einer erfolgreichen Anmeldung: Setzt die Anzahl der fehlgeschlagenen Anmeldeversuche zurück und aktualisiert das Datum der letzten Anmeldung.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme
Jedes Mal, wenn ein Benutzer versucht, sich anzumelden, wird die Aktion in einem Ereignisprotokoll aufgezeichnet. Sie können ein Protokoll der fehlgeschlagenen Anmeldeversuche anzeigen.

1. Navigieren zu **Systemrichtlinie** > **Ereignisprotokolle**an.
2. Filtern Sie im Feld **Name** nach **login.failed**. Sie können den versuchten Anmeldenamen, das Datum und die IP-Adresse anzeigen, die für den Versuch protokolliert wurden.

Machen Sie UI-Seiten öffentlich oder privat

Sie können Seiten öffentlich machen, wenn Sie möchten, dass Ihre Anwender die Seiten sehen, ohne sich anzumelden.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Die meisten Seiten können nur von angemeldeten Anwendern angezeigt werden. Eine begrenzte Anzahl von Seiten ist öffentlich, sodass Anwender sich nicht anmelden müssen, um sie anzuzeigen, z. B. die Willkommensseite, die Startseite sowie die Anmelde- und Abmeldeseiten.

⚠ **Warnung:** Für die Funktionalität vieler Funktionen sind mehrere öffentliche Seiten des Basissystems erforderlich. Öffentliche Seiten des Basissystems nicht deaktivieren.

Prozedur
1. Geben Sie im Anwendungsnavigator-Filter `sys_public.list ein`.
2. Klicken Sie auf **Neu**.
3. Erstellen Sie in der Tabelle „sys_public“ einen Datensatz mit den folgenden Werten.

Feld	Beschreibung
Seite	Der Name der Seite. Beispiel: $sp
Aktiv	Wenn diese Option ausgewählt ist, ist die Seite öffentlich zugänglich. Deaktivieren Sie die Option „Aktiv“, wenn die Seite privat sein soll.

4. Klicken Sie auf **Speichern**.
   Wenn Sie „aktiv“ auf „wahr“ setzen, ist die Seite öffentlich, also jeder, der sie besucht<instance_name> `/sp` oder `/$sp.do` kann auf die Seite zugreifen.

Anforderungen an die Passwortkomplexität

Passwörter in Ihrer Instanz ServiceNow® müssen die Komplexitätsanforderungen erfüllen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

Untersuchen



Lernen Sie die Funktionen und den Geschäftsnutzen der Komplexitätsanforderungen für Passwörter kennen.

Aktivieren



Erfahren Sie, wie Sie die Anforderungen an die Passwortkomplexität aktivieren.

Konfigurieren



Konfigurieren Sie die Komplexitätsanforderungen für das Passwort.

Referenz: Nicht unterstützte Passwortzeichen



© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informieren Sie sich über die nicht unterstützten Passwortzeichen.

Machen Sie sich mit den Komplexitätsanforderungen für Passwörter vertraut

Passwörter in Ihrer Instanz ServiceNow® müssen die Komplexitätsanforderungen erfüllen.

Mit der Richtlinieneinstellung „Passwortkomplexitätsanforderungen“ wird festgelegt, ob Passwörter eine Reihe von Richtlinien für sichere Passwörter erfüllen müssen.

Anforderungen an die Passwortkomplexität werden erzwungen, wenn ein Passwort geändert oder erstellt wird.

Die Anforderungen an die Passwortkomplexität erfüllen und funktionieren auf folgender Grundlage:

- Wenn die Eigenschaft *glide.apply.password_policy.on_login* aktiviert ist, wird die Passwortrichtlinienprüfung während der Anmeldung für den Benutzer erzwungen. Bei der Anmeldung muss der Benutzer die Passwortrichtlinie einhalten und das Passwort für die Instanz ändern.
- Die Anforderungen der Passwortrichtlinie basieren auf der Basic Multilanguage Plane (BMP), die Zeichen für alle modernen Sprachen enthält. ServiceNow Instanzen werden mit BMPs von etwa 10.000 Zeichen geliefert.
- Für Ihre Instanz können Passwörter innerhalb der zulässigen BMPs festgelegt werden. Passwörter, die diesen BMPs nicht entsprechen, sind nicht zulässig.

Bei Bedarf können Sie festlegen, dass Passwörter regelmäßig, mindestens alle 90 Tage, geändert werden.

Anforderungen und gesperrte Zeichen

Um eine sichere Netzwerkumgebung zu ermöglichen, müssen Benutzer sichere Passwörter verwenden, die eine Kombination aus Buchstaben, Ziffern und Symbolen enthalten. Diese Kombinationen tragen dazu bei, nicht autorisierte Benutzer zu verhindern, die normalerweise manuelle oder automatisierte Methoden verwenden, um schwache Passwörter zu erraten.

Das Passwort für Ihre Instanz muss die folgenden Anforderungen erfüllen:

- Mindestens 8 Zeichen.
- Maximal 100 Zeichen.
- Enthält Kleinbuchstaben und Großbuchstaben
- Enthält Sonderzeichen.
- Enthält Ziffern.

Sie können eine Liste häufig ungültiger Passwörter sperren, z. B. die folgenden:

- Vorhersehbare und sich wiederholende Sequenzen wie „123456“, „qwerty“, „!@#$%^“, „aaaaa“ usw.
- Mitarbeitername oder Anwendernamen.
- Relevante Marken- oder Produktnamen.
- Standorte wie Unternehmenszentrale, Stadt, Land usw.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Unternehmensspezifische interne Begriffe oder Abkürzungen.
- Emojis

Hinweis: Anwender-, marken- oder unternehmensspezifische Zeichen, die nicht im Passwort verwendet werden können, können auf der Seite „Passwortrichtlinie“ oder „Passwort ausschließen“ konfiguriert werden.

Passwortrichtlinien für Ihre Instanz aktivieren

Implementieren Sie Passwortrichtlinien-Steuerungen bei der Anmeldung. Erzwingen Sie die Passwortänderung durch Anwender, wenn das Passwort die Kriterien der Passwortrichtlinie nicht erfüllt.

Vorbereitungen

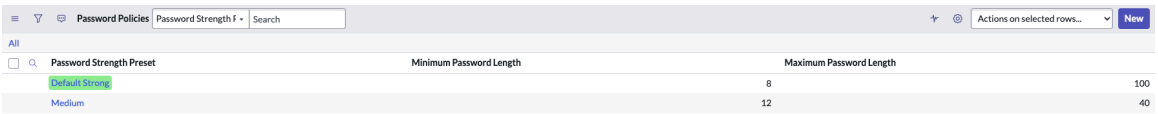
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Das Plugin „Password Policy“ (com.glide.password_policy) ist standardmäßig aktiviert. Die Richtlinie tritt in Kraft, wenn ein Benutzer das Passwort ändert oder zurücksetzt.
Das Feld **Vorgegebene Passwortstärke** wird automatisch auf **Standardmäßig stark**gesetzt. Wenn Sie neue Kriterien hinzufügen möchten, können Sie wie folgt vorgehen.

Wenn Sie Ihre Instanz über den Installations-Exit *ValidatePasswordStronger* oder die Eigenschaft „Anmeldeinformationsspeicher für Passwortzurücksetzung“ *pwd_cred_store*] angepasst haben, erfahren Sie unter den Eigenschaften der Passwortrichtlinie, wie Sie eine Passwortrichtlinie für Ihre Instanz implementieren.

Hinweis: Die aktive Passwortrichtlinie wird für die Instanz wie dargestellt hervorgehoben.



Um die Passwortrichtlinie zu ändern, navigieren Sie zu **Alle** > **Passwortzurücksetzung** > **Anmeldeinformationsspeicher**, wählen Sie die Anmeldeinformationen aus, und ändern Sie das Feld **Passwortrichtlinie** in die erforderliche Richtlinieneingabe.

Prozedur

1. Navigieren zu **Alle** > **Passwortrichtlinie** > **Passwortrichtlinien**an.
2. Klicken Sie auf **Neu**.
   Das Formular „Passwortrichtlinie“ wird angezeigt.
3. Geben Sie den **Namen** für Ihre Passwortrichtlinie an.
4. Wählen Sie im Abschnitt „Passwortrichtlinienkriterien“ im Feld **Passwortstärke** -Voreinstellung eine der folgenden Voreinstellungen aus.

Vorgegebene Passwortstärke	Beschreibung
Standard	Füllt die Felder für die erforderlichen Passwortzeichen automatisch wie folgt aus:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorgegebene Passwortstärke	Beschreibung
	◦ Legt **die Mindestanzahl der Großbuchstaben** auf 1 fest. ◦ Legt die **Mindestanzahl der Kleinbuchstaben** auf 1 fest. ◦ Legt mindestens ein **numerisches Zeichen** auf 1 fest. ◦ Legt die **Mindestanzahl für Sonderzeichen** auf 0 fest. Die minimale Passwortlänge beträgt 8 Zeichen, die maximale 100 Zeichen.
Mittel	Füllt die Felder für die erforderlichen Passwortzeichen automatisch wie folgt aus: ◦ Legt **die Mindestanzahl der Großbuchstaben** auf 1 fest. ◦ Legt die **Mindestanzahl der Kleinbuchstaben** auf 1 fest. ◦ Legt mindestens ein **numerisches Zeichen** auf 1 fest. ◦ Legt die **Mindestanzahl von Sonderzeichen** auf 1 fest. Die minimale Passwortlänge beträgt 12 Zeichen, die maximale 40 Zeichen.
Hoch	Füllt die Felder für die erforderlichen Passwortzeichen automatisch wie folgt aus: ◦ Legt **die Mindestanzahl der Großbuchstaben** auf 1 fest. ◦ Legt **mindestens ein Kleinbuchstabe** auf 2 fest. ◦ Legt mindestens ein **numerisches Zeichen** auf 1 fest. ◦ Legt die **Mindestanzahl für Sonderzeichen** auf 3 fest. Die minimale Passwortlänge beträgt 8 Zeichen, die maximale 100 Zeichen.
Standardmäßig stark	Füllt die Felder für die erforderlichen Passwortzeichen automatisch wie folgt aus: ◦ Legt **die Mindestanzahl der Großbuchstaben** auf 1 fest. ◦ Legt die **Mindestanzahl der Kleinbuchstaben** auf 1 fest.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorgegebene Passwortstärke	Beschreibung
	◦ Legt mindestens ein **numerisches Zeichen** auf 1 fest. ◦ Legt die **Mindestanzahl von Sonderzeichen** auf 1 fest. Die minimale Passwortlänge beträgt 8 Zeichen, die maximale 100 Zeichen.
Anwenderdefiniert	Füllt die Felder für die erforderlichen Passwortzeichen automatisch wie folgt aus: ◦ Legt **die Mindestanzahl der Großbuchstaben** auf 1 fest. ◦ Legt die **Mindestanzahl der Kleinbuchstaben** auf 1 fest. ◦ Legt mindestens ein **numerisches Zeichen** auf 1 fest. ◦ Legt die **Mindestanzahl von Sonderzeichen** auf 1 fest. Die minimale Passwortlänge beträgt 8 Zeichen, die maximale 100 Zeichen. Sie können auch das angezeigte **Skript für die Passwortrichtlinie** anpassen.
Erweitert	Wenn Sie **Erweitert** wählen, werden **Passwortregelskript** und **Passwortstärkeskript**angezeigt. Basierend auf Ihren Anforderungen können Sie diese Skripts anpassen.

Hinweis: Die Passwortrichtlinie wird basierend auf der ausgewählten Voreinstellung angewendet.

5. Füllen Sie die verbleibenden Felder des Formulars aus.

Formular „Passwortrichtlinie“.

Feld	Beschreibung
Mindestlänge von Passwörtern	Mindestlänge des Passworts. Diese Option wird für alle Voreinstellungen außer **Erweitert**angezeigt. Legen Sie dieses Feld auf mindestens 8–10 Zeichen fest.
Maximale Passwortlänge	Maximale Länge des Passworts. Diese Option wird für alle Voreinstellungen außer **Erweitert**angezeigt. Legen Sie dieses Feld auf maximal 100 Zeichen fest.
Mindestanzahl der Großbuchstaben	Mindestanzahl von Großbuchstaben im Passwort, von 0 bis 10.
Mindestanzahl der Kleinbuchstaben	Mindestanzahl von Kleinbuchstaben im Passwort, von 0 bis 10.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Mindestanzahl der numerischen Zeichen	Mindestanzahl von Zeichen im Passwort, von 0 bis 10.
Mindestanzahl der Sonderzeichen	Mindestanzahl von Sonderzeichen im Passwort, von 0 bis 10.
Eingeschlossene Sonderzeichen	Lassen Sie einen eingeschränkten Satz von Sonderzeichen ohne Trennzeichen zu. Wenn Sie beispielsweise `$,!`, können Anwender nur „$“ und „!“ verwenden. als Sonderzeichen im Passwort. Es können keine anderen Sonderzeichen verwendet werden. Ein Passwort mit anderen Sonderzeichen ist nicht zulässig.
Ausgeschlossene Sonderzeichen	Lassen Sie einen eingeschränkten Satz von Sonderzeichen ohne Trennzeichen zu. Beispiel: Wenn Sie `@$!`, können Anwender „@“, „$“ und „!“ nicht verwenden. als Sonderzeichen in ihren Passwörtern. **Hinweis:** Diese Option ist verfügbar, wenn die Eigenschaft *glide.password_policy.use_excluded_special_ch* aktiviert ist.
Anwenderdaten nicht zulassen	Option zum Nichtzulassen von Benutzerdaten, die sich auf die Authentifizierung beziehen.
Schwellenwert für Sequenzlänge	Die Sequenzlänge Ihres Passworts.
Schwellenwert für Wiederholungslänge	Die Wiederholungslänge Ihres Passworts. **Hinweis:** ◦ Sowohl der Schwellenwert für die Sequenzlänge als auch der Schwellenwert für die Wiederholungslänge dürfen maximal acht Zeichen haben. Mit diesen Feldern können Sie schwache Kombinationen von Passwörtern einschränken, die vorhersehbare und sich wiederholende Sequenzen aufweisen, wie z. B. „123456“, „qwerty“, „!@#$%^“, „aaaaa“ usw. ◦ Wenn **die voreingestellte Passwortstärke** auf **Standardmäßig stark**festgelegt ist, wird die Länge sowohl für den Schwellenwert für die Sequenzlänge als auch für die Wiederholungslänge auf vier Zeichen festgelegt.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Passwort testen	Geben Sie in diesem Feld Ihr tatsächliches Passwort ein.

6. Klicken **Sie auf Passwort testen**.
7. Nachdem das Passwort als gültig getestet wurde, klicken Sie auf **Absenden**, um das Passwort zu übermitteln.

Hinweis: Testen Sie Ihr Passwort immer, bevor Sie es absenden.

Eigenschaften der Passwortrichtlinie

Mit den Eigenschaften der Passwortrichtlinie können Sie Passwortrichtlinien verwalten, Listenpasswörter ausschließen und während der Anmeldung eine Passwortrichtlinie anwenden.

Navigieren zu **Passwortrichtlinie** > **Eigenschaften** um die Eigenschaften der Passwortrichtlinie anzuzeigen und zu bearbeiten.

Eigenschaft	Beschreibung
glide.enable.password_policy	Aktiviert eine Passwortrichtlinie für Ihre Instanz. Die Richtlinie tritt in Kraft, wenn ein Benutzer ein Passwort ändert oder zurücksetzt. Diese Eigenschaft wird automatisch auf **true**festgelegt. **Hinweis:** • Wenn Ihre Instanz über den Installations-Exit von *ValidatePasswordStronger* oder Ihren Anmeldeinformationsspeicher für die Passwortzurücksetzung [pwd_cred_store] angepasst wird, müssen Sie diese Eigenschaft erstellen und Ihren Systemeigenschaften hinzufügen. • Vor Release Orlando : Wenn Ihre Instanz mit dem Installations-Exit *ValidatePasswordStronger* angepasst wurde, müssen Sie die Eigenschaft „Passwortrichtlinie“ erstellen, damit die Passwortrichtlinie funktioniert. • Ab Release Orlando gibt es keine Anpassung des Installations-Exits mehr. Die Eigenschaften der Passwortrichtlinie funktionieren standardmäßig. Diese Eigenschaften können manuell deaktiviert werden.
glide.enable.blacklist_password	Verbietet die Verwendung bestimmter Passwörter. Der Administrator

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	kann Passwörter in die Tabelle der ausgeschlossenen Passwörter einfügen. Diese Eigenschaft wird automatisch auf **true**festgelegt.
glide.apply.password_policy.on_login	Zwingt Anwender dazu, die Passwörter bei der nächsten Anmeldung zu ändern, wenn die vorhandenen Passwörter nicht der aktuellen Passwortrichtlinie entsprechen. Diese Eigenschaft wird automatisch auf **false**festgelegt. Wenn Sie den Wert auf „ **wahr** “ setzen, wird während der Anmeldung eine Passwortrichtlinie erzwungen. **Hinweis:** Durch das Aktivieren dieser Eigenschaft wird möglicherweise eine erhebliche Anzahl von Anwendern, die die neue Passwortrichtlinie nicht einhalten, gezwungen, ihre Passwörter zu ändern.
glide.password_policy.user_excluded_spezial_zeichen	Ermöglicht Benutzern die Verwendung der Option für ausgeschlossene Sonderzeichen im Formular „Passwortrichtlinie“.
glide.validate.sys_user.password.field	Aktiviert die Validierung des Anwenderpassworts anhand der Passwortrichtlinie, wenn ein Administrator das Formular „sys_user“ oder die Listenansicht bearbeitet.
glide.password.policy.generate.password.field.disabled	Deaktiviert das Feld **Passwort** im Popup-Fenster „Passwort festlegen“ im Formular „sys_user“.
glide.user.show.password.field	Aktiviert das Feld **Passwort** im Formular „sys_user“.
glide.password_policy.debug	Aktiviert die Debug-Protokollierung für die Passwortrichtlinie.

Konfigurieren Sie Ihre Passwortrichtlinie

Mit den Kriterien der Passwortrichtlinie können Sie Ihr Passwort schützen und die Mindestanforderungen an die Passwortkomplexität erfüllen.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Das Plugin „Passwortrichtlinie“ [com.glide.password_policy] ist standardmäßig aktiviert. Sie tritt in Kraft, wenn ein Benutzer das Passwort ändert oder zurücksetzt. Wenn Sie Ihre Instanz über den ValidatePasswordStronger-Installations-Exit oder den Anmeldeinformationsspeicher für die Passwortzurücksetzung [pwd_cred_store] angepasst haben, finden Sie weitere Informationen unter Eigenschaften der Passwortrichtlinie.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

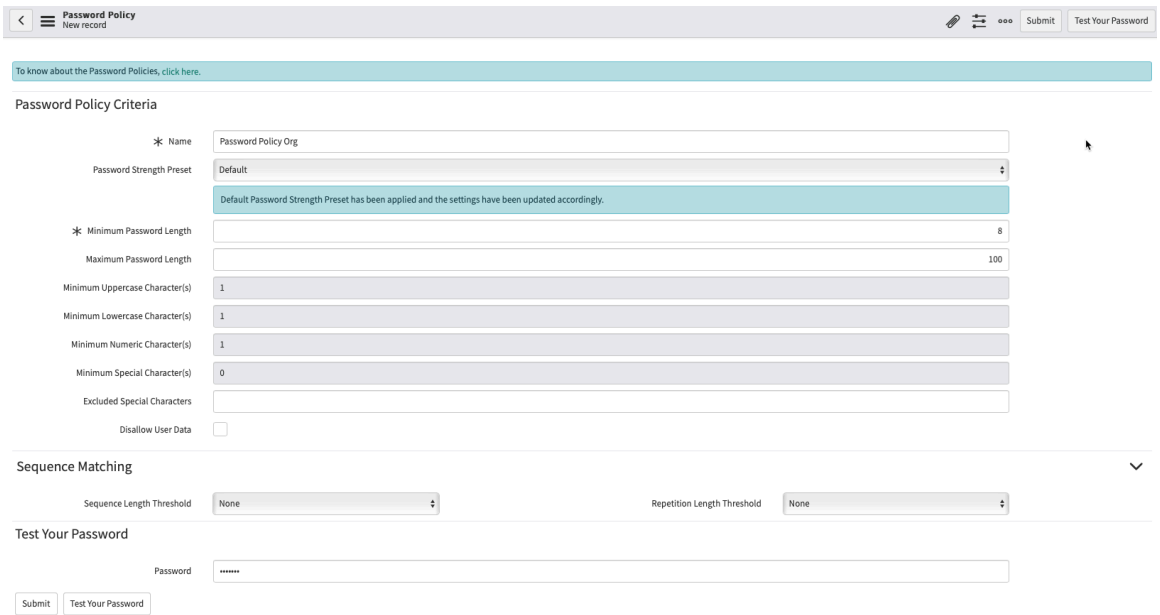
1. Navigieren zu **Alle** > **Passwortrichtlinie** > **Passwortrichtlinien**an.

   Hinweis: Die Voreinstellung „**Standardmäßig stark** “ ist als Standardkriterium für die Passwortakzeptanz aktiviert. Wenn Sie ein neues Kriterium hinzufügen möchten, können Sie die folgenden Schritte ausführen.

2. Klicken Sie auf **Neu**.

   Die Datensatzseite „Passwortrichtlinie neu“ enthält die folgenden Abschnitte, die Sie zum Festlegen Ihres Passworts angeben müssen:

   - **Passwortrichtlinienkriterien**
   - **Sequenzabgleich**
   - **Passwort testen**



3. Geben Sie den **Namen** für Ihre Passwortrichtlinie an.
4. Wählen Sie im Abschnitt **„Passwortrichtlinienkriterien“** die Voreinstellung aus **Passwortstärke-**Voreinstellung aus. Folgende Voreinstellungen sind verfügbar:

Vorgegebene Passwortstärke und ihre Beschreibung

Vorgegebene Passwortstärke	Beschreibung
Standard	Wenn Sie **Standard** auswählen, werden die erforderlichen Passwortzeichen automatisch wie folgt ausgefüllt: ◦ Mindestens ein Großbuchstabe ◦ Mindestens ein Kleinbuchstabe ◦ Mindestens ein numerisches Zeichen
Mittel	Wenn Sie „ **Mittel** “ auswählen, werden die erforderlichen Passwortzeichen basierend auf den folgenden Zeichen automatisch ausgefüllt:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorgegebene Passwortstärke	Beschreibung
	◦ Mindestens ein Großbuchstabe ◦ Mindestens ein Kleinbuchstabe ◦ Mindestens ein numerisches Zeichen ◦ Mindestens ein Sonderzeichen
Hoch	Wenn Sie „ **Hoch** “ auswählen, werden die Passwortzeichen automatisch wie folgt ausgefüllt: ◦ Mindestens ein Großbuchstabe ◦ Mindestens zwei Großbuchstaben ◦ Mindestens ein numerisches Zeichen ◦ Mindestens drei Sonderzeichen
Standardmäßig stark	Wenn Sie „ **Standardmäßig stark** “ auswählen, werden die erforderlichen Passwortzeichen basierend auf den folgenden Zeichen automatisch ausgefüllt: ◦ Mindestens ein Großbuchstabe ◦ Mindestens ein Kleinbuchstabe ◦ Mindestens ein numerisches Zeichen ◦ Mindestens ein Sonderzeichen
Anwenderdefiniert	Wenn **Sie „Anwenderdefiniert** “ auswählen, werden die erforderlichen Passwortzeichen basierend auf den folgenden Zeichen automatisch ausgefüllt: ◦ Mindestens ein Großbuchstabe ◦ Mindestens ein Kleinbuchstabe ◦ Mindestens ein numerisches Zeichen ◦ Mindestens ein Sonderzeichen Sie können auch das angezeigte **Skript für die Passwortrichtlinie** anpassen.
Erweitert	Wenn Sie **Erweitert** wählen, werden **Passwortregelskript** und **Passwortstärkeskript**angezeigt. Basierend auf Ihren Anforderungen können Sie diese Skripts anpassen.

Hinweis: Die Passwortrichtlinie wird basierend auf der ausgewählten Voreinstellung angewendet.

5. Geben Sie die in der Tabelle beschriebenen Felder an:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Passwortrichtlinie“.

Feld	Beschreibung
Mindestlänge von Passwörtern	Mindestlänge des Passworts. Diese Option wird für alle Voreinstellungen außer **Erweitert**angezeigt. **Hinweis: Die Mindestlänge von Passwörtern** ist ein Pflichtfeld. Es wird empfohlen, es auf mindestens 8–10 Zeichen festzulegen.
Maximale Passwortlänge	Maximale Länge des Passworts. Diese Option wird für alle Voreinstellungen außer **Erweitert**angezeigt. **Hinweis: „Maximale Passwortlänge** “ ist ein optionales Feld. Es wird empfohlen, es auf maximal 100 Zeichen festzulegen.
Mindestanzahl der Großbuchstaben	Mindestanzahl von Großbuchstaben im Passwort, von 0 bis 10.
Mindestanzahl der Kleinbuchstaben	Mindestanzahl von Kleinbuchstaben im Passwort, von 0 bis 10.
Mindestanzahl der numerischen Zeichen	Mindestanzahl von Zeichen im Passwort, von 0 bis 10.
Mindestanzahl der Sonderzeichen	Mindestanzahl von Sonderzeichen im Passwort, von 0 bis 10.
Eingeschlossene Sonderzeichen	Lassen Sie einen eingeschränkten Satz von Sonderzeichen ohne Trennzeichen zu. Wenn Sie beispielsweise "$,!“ eingeben, Benutzer können nur „$“ und „!“ verwenden. als Sonderzeichen im Passwort. Es können keine anderen Sonderzeichen verwendet werden, und ein Passwort mit anderen Sonderzeichen ist nicht zulässig.
Ausgeschlossene Sonderzeichen	Lassen Sie einen eingeschränkten Satz von Sonderzeichen ohne Trennzeichen zu. Wenn beispielsweise '@$!' eingegeben wurde, dürfen Anwender nicht „@“, „$“ und „!“ verwenden. als Sonderzeichen in ihren Passwörtern. **Hinweis:** Diese Option ist verfügbar, wenn die Eigenschaft „glide.password_policy.use_excluded_special_char“ aktiviert ist.
Anwenderdaten nicht zulassen	Sie ist aktiviert, um die Anwenderdaten nicht zuzulassen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Geben Sie im Abschnitt „ **Sequenzabgleich“ Schwellenwert für Sequenzlänge und Schwellenwert** für **Wiederholungslänge**an.

   Hinweis:

   - Sowohl der Schwellenwert für die Sequenzlänge als auch der Schwellenwert für die Wiederholungslänge dürfen maximal acht Zeichen haben. Mit diesen Feldern können Sie schwache Kombinationen von Passwörtern einschränken, die vorhersehbare und sich wiederholende Sequenzen aufweisen, wie z. B. „123456“, „qwerty“, „!@#$%^“, „aaaaa“ usw.
   - Für **Standardmäßig stark**werden sowohl für den Schwellenwert für die Sequenzlänge als auch für den Schwellenwert für die Wiederholungslänge vier Zeichen ausgewählt.

7. Geben Sie im Abschnitt „Passwort **testen“ Ihr** Passwort an.
8. Klicken **Sie auf Passwort testen**.
9. Sobald das Passwort gültig ist, klicken Sie auf **Absenden**, um das Passwort zu übermitteln.

Hinweis: Testen Sie Ihr Passwort immer, bevor Sie es absenden.

Passwort für einen Benutzer konfigurieren

Legen Sie das Passwort Ihres Anwenders für die Instanz basierend auf der konfigurierten Passwortrichtlinie fest.

Vorbereitungen

Benutzer, die für das Festlegen des Passworts für die erste Anmeldung erstellt wurden. Weitere Informationen finden Sie unter Benutzer erstellen .

Um das Feld „ **Passwort** “ direkt im Anwenderformular auszufüllen, aktivieren Sie das **Feld „Anzeige des Passworts aktivieren“ im Formular** „sys_user“ (glide.user.show.password.field). Weitere Informationen zu den Eigenschaften finden Sie unter Eigenschaften der Passwortrichtlinie.

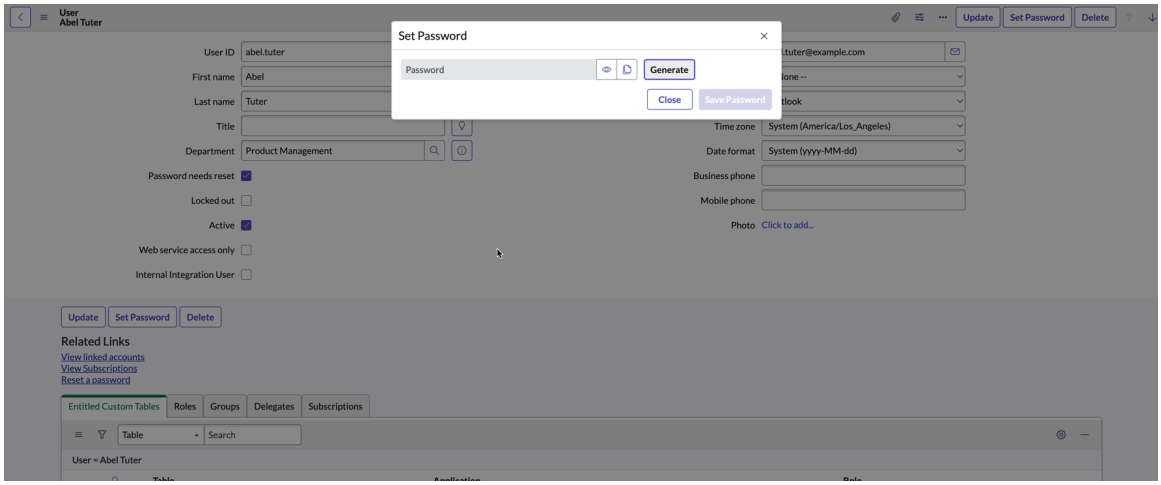
Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Anwenderadministration** > **Anwender**an.
2. Wählen Sie den Benutzer aus der Liste auf der Seite Benutzer aus.
3. Um das Passwort gemäß der Passwortrichtlinie festzulegen, klicken Sie auf **Passwort**festlegen .

   Das Popup-Fenster „Passwort festlegen“ wird angezeigt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Führen Sie unter „Passwort festlegen“ die folgenden Schritte aus.

a. Klicken Sie auf **Generieren**, um das Passwort zu generieren.



b. Klicken Sie auf das Symbol Anzeigen, um das Passwort anzuzeigen.



Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Klicken Sie auf das Symbol **Kopieren**, um das Passwort zu kopieren und für den Anwender freizugeben.



5. Klicken **Sie auf Passwort speichern**.

   Das Passwort ist für den Anwender festgelegt. Außerdem wird das Kontrollkästchen Passwort benötigt REST automatisch aktiviert.

   Der Anwender muss bei der ersten Anmeldung dasselbe Passwort für die Anmeldung verwenden und das Passwort bei der Anmeldung gemäß der von den Administratoren konfigurierten Passwortrichtlinie ändern.

Ausschließen von Passwörtern über Passwortrichtlinien in Ihrer Instanz

Fügen Sie der Tabelle „Ausgeschlossene Passwörter“ Passwörter hinzu, um zu verhindern, dass bestimmte Passwörter von Benutzern in Ihrer Instanz verwendet werden.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können beliebig viele Passwörter sperren. Einige der Beispiele lauten wie folgt:

- Vorhersehbare und sich wiederholende Sequenzen, z. B. „123456“, „qwerty“, „!@#$%^“, „aaaaa“ usw.
- Mitarbeitername oder Anwendernamen.
- Relevante Marken- oder Produktnamen.
- Standorte, z. B. Unternehmenssitz, Stadt, Land usw.
- Unternehmensspezifische interne Begriffe oder Abkürzungen.
- Emojis

Prozedur

1. Navigieren zu **Alle** > **Passwortrichtlinie** > **Ausgeschlossene Passwörter**an.
2. Um Ihrer Ausschlussliste ein Passwort hinzuzufügen, klicken Sie auf **Neu**, und geben Sie das Passwort ein.
3. Navigieren zu **Passwortrichtlinie** > **Ausschlusslistenverwaltung** um das Passwort Ihrer Benutzer zu steuern und zu verhindern, dass Benutzer ein falsches Passwort für die Instanz verwenden.

   Die **Ausschlusslistenverwaltung** verfügt über etwa 5000 häufig verwendete Passwörter.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nicht unterstützte Passwortzeichen

Es gibt Passwortzeichen, die nicht unterstützt werden. Benutzer können diese Zeichen aufgrund der Anforderungen an die Passwortkomplexität ServiceNow nicht verwenden.

Um eine sichere Netzwerkumgebung zu ermöglichen, müssen Benutzer sichere Passwörter verwenden, die eine Kombination aus Buchstaben, Ziffern und Symbolen enthalten. Diese Kombinationen tragen dazu bei, nicht autorisierte Benutzer zu verhindern, die normalerweise manuelle oder automatisierte Methoden verwenden, um schwache Passwörter zu erraten.

- Die Anforderungen der Passwortrichtlinie basieren auf der Basic Multilanguage Plane (BMP), die Zeichen für alle modernen Sprachen enthält. Die Instanz ServiceNow wird mit BMPs von etwa 10.000 Zeichen geliefert.
- Passwortzeichen innerhalb dieser zulässigen BMPs können für Ihre Instanz festgelegt werden. Passwortzeichen, die nicht innerhalb dieser zulässigen BMPs liegen, sind nicht zulässig.

Hinweis: Anwender- oder unternehmensspezifische Zeichen, die nicht im Passwort verwendet werden können, können in der Liste „Passwort ausschließen“ konfiguriert werden.

Weitere Informationen zu den Eigenschaften der Passwortrichtlinie finden Sie unter Eigenschaften der Passwortrichtlinie.

Passwortzurücksetzung

Der standardmäßige Self-Service-Passwortzurücksetzung-Prozess ermöglicht es einem Benutzer, das Passwort ohne Hilfe von Service-Desk-Mitarbeitern zurückzusetzen.

Example: Der standardmäßige Self-Service-Ablauf für das Zurücksetzen des Passworts

1. Wenn sich ein Benutzer nicht an das Passwort erinnert, kann er auf den Link **Passwort vergessen?** auf dem Anmeldebildschirm klicken.
2. Die Anwendung Passwortzurücksetzung wird gestartet. Auf der Seite **Identität** identifiziert sich der Benutzer durch Eingabe eines **Benutzernamens**.
3. Auf der Seite **Überprüfen** weist der Benutzer nach, dass er die Person ist, die mit dem Benutzernamen verknüpft ist. In diesem Beispiel gibt der Benutzer die E-Mail-Adresse ein, die dem Benutzerprofil zugeordnet ist. Der Administrator kann eine andere Überprüfungsmethode konfigurieren oder zusätzliche Überprüfungen erfordern, z. B. eine persönliche Frage, die nur der Benutzer beantworten kann.
4. Auf der Seite **Zurücksetzen** wird der Benutzer angewiesen, die E-Mail auf Anweisungen zu überprüfen.
5. Der Benutzer öffnet die E-Mail und klickt auf den Link **Hier**, um das Passwort zurückzusetzen. Der Link ist für einen von Ihnen angegebenen Zeitraum gültig (verwenden Sie die Eigenschaft „ **password_reset.request.expiry**“).
6. Die Seite **Passwort zurücksetzen** führt den Benutzer durch den Prozess zum Zurücksetzen des Passworts.

Der standardmäßige Self-Service-Passwortzurücksetzung-Prozess (`com.glideapp.password_reset`) definiert:

- Den URI, der angibt, wohin Benutzer beim Klicken auf **Passwort vergessen?** umgeleitet werden. Standardmäßig lautet dieser Wert **/$pwd_reset.do?sysparm_url=ss_default**. Dies ist derselbe Wert, der in der Eigenschaft *`glide.security.password_reset.uri`* verwendet wird. In früheren Releases wurde dieser Wert auf **/reset_password.do** festgelegt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die Option **URL zum Zurücksetzen des Passworts aktivieren**, die angibt, dass der Benutzer nach dem Klicken auf **Passwort vergessen?** eine E-Mail mit einem Link zum Zurücksetzen des Passworts erhalten sollte.
- Der Verifizierungsablauf „Persönliche Daten – E-Mail-Adresse eingeben“, der den dreischrittigen Prozess für die Passwortzurücksetzung angibt.

Anweisungen zum Zugriff auf dieses Formular und zum Konfigurieren der Felder finden Sie unter Prozess zum Zurücksetzen des Passworts konfigurieren.

Hinweis:

- Diese Funktion steht für lokal authentifizierte Benutzer zur Verfügung, die den in ihrem Benutzerdatensatz angegebenen Benutzernamen und das entsprechende Passwort eingeben. Benutzer, die sich über eine SSO-Lösung oder eine LDAP-Integration bei der Instanz anmelden, können Passwörter nicht mit dem Selfservice-Beispielprozess Passwortzurücksetzung zurücksetzen.
- Der Endbenutzer muss die Benachrichtigungseinstellungen aktivieren und konfigurieren. Weitere Informationen finden Sie unter Abonnementbasierte Benachrichtigungen . Administratoren könnendie E-Mail ändern, die an den Endanwender gesendet wird.

Ändern Sie den Text der Benachrichtigungs-E-Mail Passwortzurücksetzung .

Benutzer des Selfservice-Prozesses Passwortzurücksetzung erhalten eine E-Mail-Benachrichtigung, wenn sie die Zurücksetzung des Passworts anfordern. Sie können den Text der E-Mail und andere Aspekte der Benachrichtigung ändern.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Dieser Prozess ist nur relevant, wenn es sich bei den Anwendern um auf Abonnement basierende Benachrichtigungen handelt.

Prozedur

1. Navigieren zu **Alle** > **Systembenachrichtigung** > **Benachrichtigungen**an.
2. Wählen Sie die Benachrichtigung **„URL zur Passwortzurücksetzung“ aus**.
3. Ändern Sie den Text der E-Mail im Abschnitt **Was sie enthalten** wird.
   Informationen zum Konfigurieren anderer Aspekte der Benachrichtigung finden Sie unter E-Mail-Benachrichtigung erstellen .

Passwortzurücksetzung -Eigenschaften werden konfiguriert

Sie können Eigenschaften angeben, die die Passwortzurücksetzung-Erfahrung für Endbenutzer konfigurieren.

Vorbereitungen
Erforderliche Rolle: password_reset_admin

Warum und wann dieser Vorgang ausgeführt wird
Es gibt zwar keine Bereichsgrenzen für die Werte, die Sie für Eigenschaften eingeben können, es sollten jedoch nur positive Ganzzahlwerte ab 1 verwendet werden. Wenn Sie den Grenzwert für den oberen Bereich einer Eigenschaft festlegen, müssen Sie die vom Benutzer ausgeführte Aufgabe berücksichtigen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie werden beispielsweise nicht zulassen wollen, dass Benutzer 100 Versuche haben, um ihre Identität zu bestätigen. Ein üblicherer Wert sind 3 Versuche. Ebenso wenig werden Sie wollen, dass Benutzer während des Registrierungsprozesses 30 Sicherheitsfragen auswählen und beantworten müssen. Eine häufiger verwendete Anzahl von Sicherheitsfragen liegt zwischen 5 und 7.

Prozedur

1. Navigieren zu **Alle** > **Passwortzurücksetzung** > **Eigenschaften**an.
   Informationen zu den Eigenschaften Passwortzurücksetzung finden Sie unter Passwortzurücksetzung globale Eigenschaften an.
2. Aktualisieren Sie die Einstellungen nach Bedarf, und klicken Sie dann auf **Speichern**.

Anwendernamen speichern

Wenn bei der **Anmeldung** das Kontrollkästchen Anwendernamen speichern aktiviert ist, wird ein Cookie auf dem Computer des Benutzers gespeichert. Dieses Cookie authentifiziert den Anwender bei nachfolgenden Aufrufen automatisch.

Wenn sich der Benutzer abmeldet, wird das Cookie gelöscht. Der Standardwert des Kontrollkästchens „Anwendernamen speichern“ wird von einer Eigenschaft gesteuert, und ob das Kontrollkästchen auf der **Anmeldeseite** angezeigt wird, wird von einer anderen Eigenschaft gesteuert.

Die beiden Eigenschaften *glide.ui.user_cookie.life_span_in_days* und *glide.ui.user_cookie.max_life_span_in_days* steuern den vom System generierten Cookie-Ablaufwert für glide_user. Wenn ein Benutzer auf eine Instanz mit aktiviertem „Benutzernamen speichern“ zugreift, wird der Ablaufzeitraum für Cookies durch den Zugriff zurückgesetzt, bis der maximale (glide.ui.user_cookie.max_life_span_in_days) Grenzwert für die Lebensdauer erreicht ist.

Hinweis: Weitere Informationen zu diesen Eigenschaften finden Sie in den folgenden Themen unter Härtungseinstellungen für Instanzsicherheit:

- Absolute Zeitüberschreitung für Sitzung
- Zeitüberschreitung des Sitzungsfensters

Standardwert des Kontrollkästchens „Anwendernamen speichern“ ändern

Sie können den Standardwert des Kontrollkästchens Anwendernamen **speichern** ändern.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **UI-Eigenschaften**an.
2. Suchen Sie die Eigenschaft [*Default value of "Remember me" checkbox on login page* (*glide.ui.remember.me.default*).
3. Um den Standardwert des Kontrollkästchens Anwendernamen speichern auf **Nein festzulegen**,deaktivieren Sie das Kontrollkästchen.
4. Um den Standardwert des Kontrollkästchens Anwendernamen speichern auf **Ja** wiederherzustellen, aktivieren **Sie**das Kontrollkästchen für die Eigenschaften.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kontrollkästchen „Anwendernamen speichern“ entfernen

Sie können das Kontrollkästchen „Anwendernamen **speichern** “ entfernen, damit Anwender keinen Zugriff auf diese Funktion haben.

Vorbereitungen
Erforderliche Rolle: security_admin

Hinweis: Weitere Informationen zu dieser Eigenschaft finden Sie unter „Anwendernamen speichern“ entfernen in Härtungseinstellungen für Instanzsicherheit.

Prozedur

1. Erhöhen Sie Ihre Rolle auf security_admin.
2. Navigieren zu **Systemeigenschaften** > **UI-Eigenschaften**an.
3. Suchen Sie die Eigenschaft [*Remove "Remember me" checkbox from login page* (*glide.ui.forgetme*).
4. Aktivieren Sie das Kontrollkästchen für die Eigenschaften.
   Diese Einstellung entfernt das Kontrollkästchen „ **Anwendernamen** speichern“, macht vorhandene Cookies ungültig und deaktiviert die Funktion „Anwendernamen speichern“ vollständig.
5. Um das Kontrollkästchen Anwendernamen speichern auf der Anmeldeseite wiederherzustellen, **deaktivieren Sie** das Kontrollkästchen für die Eigenschaften.

Konfigurieren der Bestätigungsaufforderung für die Abmeldung

Sie können eine Aufforderung zur Bestätigung der Abmeldung aktivieren, um zu verhindern, dass Benutzer sich versehentlich abmelden.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Hinweis: Das folgende Verfahren funktioniert nur in UI-Versionen vor Core-UI, der neuesten und am häufigsten verwendeten Version.

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **System**an.
2. Suchen Sie die Eigenschaft **Anwender auffordern, eine Abmeldeanforderung zu bestätigen**, und aktivieren Sie das Kontrollkästchen.
3. Wenn der Benutzer auf die Schaltfläche **Abmelden** klickt, wird ein Bestätigungsdialogfeld angezeigt.

Implementieren einer Nonce

Sie können eine Nonce implementieren, die mit der Single Sign-on-Digest-Authentifizierung verwendet werden soll.

Um eine Nonce mit den unverschlüsselten oder verschlüsselten Token-Methoden des Single Sign-on zu verwenden, gelten die folgenden Schritte mit nur wenigen geringfügigen Änderungen.

Hinweis: Die Nonce wird nur für Anmeldeanforderungen verwendet, nicht für andere Arten von Anforderungen. Wenn das System nach der Anmeldung einen Nonce-Wert erhält, wird die Nonce nicht verbraucht.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorteile

Die Verwendung einer Nonce verhindert, dass ein böswilliger Benutzer einen Wiederholungsangriff ausführt, um sich bei Ihrem System anzumelden.

Nonce-Prozessablauf

Wenn ein Kunde das Single Sign-on mit Digest-Token implementiert hat und die Sicherheit einer Nonce hinzufügen möchte, folgt er einem bestimmten Prozess-Flow.

1. Ein Benutzer meldet sich beim Portal des Kunden an.
2. Der Kunde generiert die erforderlichen SSO-Parameter und hängt eine zufällige Nonce an. Wenn der Kunde beispielsweise die Authentifizierungsantwort über die Abfragezeichenfolge weitergeleitet hat, kann dies etwa so aussehen:

```
SM_USER=itil&DE_USER=V1QuWMmxSfBgfRS099X0cAjKo5Q=&NONCE=1407743018
```

Die -Instanz empfängt diese Anforderung und ruft die Authentifizierungsvariablen ab. Bevor versucht wird, die Integrität der Authentifizierungsantwort zu überprüfen, gleicht die Instanz die Nonce mit einer internen Tabelle (u_authentication_nonce) ab, um sicherzustellen, dass sie noch nicht vorhanden ist. Wenn die Nonce in dieser Tabelle nicht vorhanden ist, wird sie der Tabelle hinzugefügt, und der Authentifizierungsprozess kann fortgesetzt werden. Wenn dieser Nonce-Wert jedoch bereits in der Tabelle vorhanden ist, wird der Authentifizierungsversuch abgebrochen und der Fehlercode `„failed_missing_requirement“` zurückgegeben, der den Benutzer normalerweise zur Anmeldeseite zurückführt.

Implementieren Sie eine Nonce

Fügen Sie dem Authentifizierungsheader eine kryptografische Nonce hinzu, um sicherzustellen, dass sie nur einmal verwendet werden kann.

- Erstellen Sie eine Systemeigenschaft mit dem Namen *`glide.authenticate.header.nonce_key`*, und legen Sie ihren Wert auf den Variablennamen fest, den Sie für die Nonce verwenden, z. B. NONCE oder NCE.
- Erstellen Sie eine neue Tabelle mit der Bezeichnung `u_authentication_nonce`. Fügen Sie der Tabelle ein Feld mit der Bezeichnung `u_nonce hinzu`.
- Gehe zu **Systemeigenschaften** > **Installationsausgänge** und erstellen Sie ein Element namens „`DigestSingleSignOnNonce“`, das „ExternalAuthentication“ (*`glide.authenticate.external_property`*) überschreibt.
- Fügen Sie dem Skriptteil des neu erstellten DigestSingleSignOnNonce den folgenden Code hinzu.

```
gs.include("PrototypeServer");

var DigestSingleSignOnNonce = Class.create();
DigestSingleSignOnNonce.prototype = {

 process : function() {

  var headerKey = GlideProperties.get("glide.authenticate.header.key",
 "SM_USER");
  var headerDigestKey =
 GlideProperties.get("glide.authenticate.header.encrypted_key",
 "DIGEST");
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
 var headerNonceKey =
GlideProperties.get("glide.authenticate.header.nonce_key", "NCE");
 var fieldName =
GlideProperties.get("glide.authenticate.header.value", "user_name");
 var fkey = GlideProperties.get("glide.authenticate.secret_key");

 // Look in the Headers
 var data = request.getHeader(headerKey);
 var encdata = request.getHeader(headerDigestKey);
 var nonce = request.getHeader(headerNonceKey);

 // If not, then check the URL Parameters
 if (data == null || encdata == null || nonce == null) {
  data = request.getParameter(headerKey);
  encdata = request.getParameter(headerDigestKey);
  nonce = request.getParameter(headerNonceKey);
 }

 // then maybe its a cookie
 if (data == null || encdata == null || nonce == null) {
  var cookies = request.getCookies();
  data = GlideCookieMan.getCookieValue(cookies, headerKey);
  encdata = GlideCookieMan.getCookieValue(cookies, headerDigestKey);
  nonce = GlideCookieMan.getCookieValue(cookies, headerNonceKey);
 }

 // if found run encryption
 if (data != null && encdata != null && nonce != null) {
  try {

   // Replace all spaces with plus(+)'s, converted in url
   encdata = encdata.replaceAll(' ', '+');

   // ----- Encrypt the username|nonce
   var key = this.getDigest( data + "|" + nonce, fkey);

   // Check for match of received encoded data
   // and your encoding of user name
   if (encdata == key) {
    var ugr = new GlideRecord("sys_user");
    ugr.initialize();
    if (!ugr.isValidField(fieldName)) {
     GlideLog.warn("External authorization is set to use field: '"+
fieldName + "' which doesn't exist");
     return "failed_missing_requirement";
    }
    ugr.addQuery(fieldName, data);
    ugr.query();
    if (!ugr.next()) {
     var userLoad = GlideUser.getUser(data);
     if (userLoad == null)
      return "failed_authentication";

     ugr.initialize();
     ugr.addQuery(fieldName, data);
     ugr.query();
     if (!ugr.next())
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
      return "failed_authentication";

    }

    if (this.processNonce(nonce)){
     var userName = ugr.getValue("user_name");
     return userName;
    }
    else return "failed_missing_requirement";
    }
   else {

    return "failed_authentication";
   }
  } catch(e) {
   gs.log(e);
   return "failed_authentication";
  }
  // Encoded data didn't match recieved Encoded data
 } else {

  return "failed_missing_requirement";
 }
},

getDigest : function( data, fkey ) {
 try {
  // default to something JDK 1.4 has
  var MAC_ALG = "HmacSHA1";
  return SncAuthentication.encode(data, fkey, MAC_ALG);

 } catch (e) {
  gs.log(e.toString());
  throw 'failed_missing_requirement';
 }
} ,

processNonce : function( sentNonce ) {
 var ngr = new GlideRecord("u_authentication_nonce");

 ngr.addQuery("u_nonce", sentNonce);
 ngr.query();
 if (ngr.next()) {
  gs.log("This SSO entry has already been processed! (Nonce: " +
sentNonce + ")");
  return false;
 }
 var ngrNew = new GlideRecord("u_authentication_nonce");
 ngrNew.initialize();
 ngrNew.u_nonce = sentNonce;
 ngrNew.insert();
 gs.log("Inserted new nonce: " + sentNonce);
 return true;
}
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
};
```

- Sobald Sie Ihren neuen Installations-Exit gespeichert haben, wechseln Sie zum DigestSingleSignOn-Installations-Exit, und vergewissern Sie sich, dass Aktiv=falsch festgelegt ist.

Ihre Instanz sollte jetzt für die Implementierung einer Nonce konfiguriert sein.

Multifaktor-Authentifizierung (MFA)

Erfahren Sie, wie Sie die Multifaktor-Authentifizierung aktivieren und konfigurieren.

Untersuchen



Lernen Sie die Funktionen und den Geschäftsnutzen von MFA kennen.

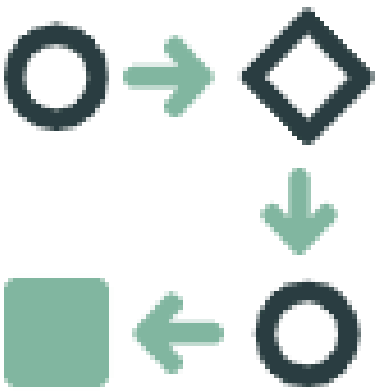
Aktivieren



Erfahren Sie, wie MFA aktiviert wird.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden



Konfigurieren und verwenden Sie die MFA.

MFA mit Single Sign-on (SSO)



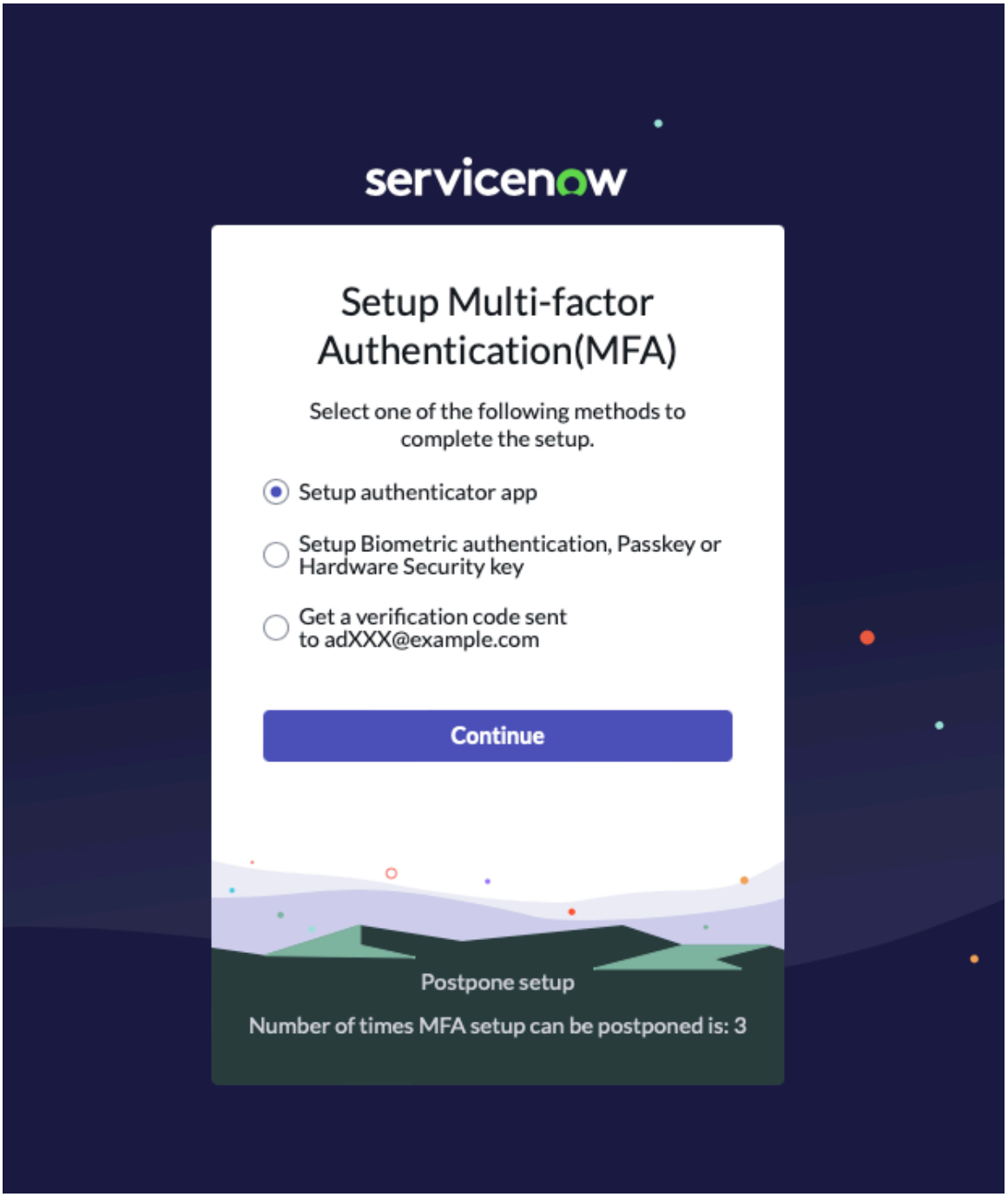
Erfahren Sie, wie MFA mit Single Sign-on (SSO) konfiguriert wird.

Mehrstufige Authentifizierung erkunden

Die Multifaktor-Authentifizierung (MFA) ist eine Authentifizierungsmethode, bei der Anwender neben ihren Standardanmeldeinformationen auch andere Informationen angeben müssen.

ServiceNow bietet MFA-Optionen wie das Einrichten einer Authentifikator-App, Biometrie, Passkey oder Hardware-Sicherheitsschlüssel, SMS und E-Mail für die Authentifizierung. Sie können den FIDO2-Authentifikator, Passkeys, biometrische Authentifikatoren und Hardware-Sicherheitsschlüssel als Multifaktor-Authentifizierungsfaktor (MFA) verwenden, ohne dass ein Setup einer Authentifikator-App erforderlich ist.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Wenn der Anwender das Setup mit einem Faktor abgeschlossen hat, kann er dennoch zu seiner Profilseite wechseln und das Setup für die verbleibenden Faktoren abschließen.

MFA aktivieren

Aktivieren Sie das Plugin „ **Integration – Multifaktor-Authentifizierung** “ (com.snc.integration.multifactor.authentication), um mit der Verwendung von MFA für eine -Instanz zu beginnen. MFA ist standardmäßig am ServiceNowaktiviert.

Multifaktor-Kriterien

Verwenden Sie Multifaktor-Kriterien, um zu bestimmen, welche Anwender und Rollen die zweistufige Multifaktor-Überprüfung verwenden müssen. Sie können eines dieser Kriterien oder eine Kombination davon verwenden, um Ihren Geschäftsanforderungen gerecht zu werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwenderbasierte Multifaktor-Kriterien

Verwenden Sie anwenderbasierte Multifaktor-Kriterien, um einzelne Anwender auszuwählen, die sich mit MFA anmelden müssen. Administratoren aktualisieren das Feld **„Multifaktor-Authentifizierung** aktivieren“ in einem Benutzerdatensatz, um die MFA-Anforderungen für einen Benutzer zu aktivieren oder zu deaktivieren. Details zu diesem Vorgang finden Sie unter Konfigurieren Sie anwenderbasierte Multifaktor-Kriterien.

Rollenbasierte Multifaktor-Kriterien

Verwenden Sie rollenbasierte Multifaktor-Kriterien, um die MFA-Anmeldung für alle Anwender zu erfordern, die einer bestimmten Rolle zugewiesen sind. Der Datensatz Rollenbasierte Multifaktor **-Authentifizierung** in der Tabelle Multifaktor **-Kriterien** [multi_factor_criteria] enthält die Liste der Rollen, die eine MFA-Anmeldung erfordern. Einzelheiten zum Verwalten dieser Liste finden Sie unter Konfigurieren Sie rollenbasierte Multifaktor-Kriterien.

Richtlinienbasierte Multifaktor-Kriterien für adaptive Authentifizierung

Verwenden Sie die adaptive Authentifizierung, um zu bestimmen, wann Ihre Instanz MFA erfordert. Die adaptive Authentifizierung verwendet Authentifizierungsrichtlinien, um Kriterien wie die IP-Adresse eines Anwenders oder Anwendergruppen auszuwerten. Weitere Informationen zur Funktion „Adaptive Authentifizierung“ finden Sie unter Adaptive Authentifizierung.

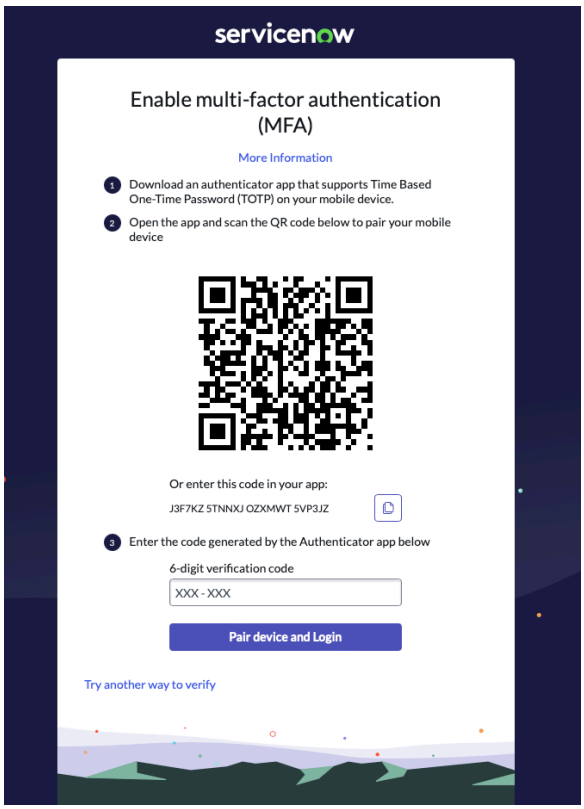
Methoden der Multifaktor-Authentifizierung

Anwender können zusätzlich zu ihrem Anwendernamen und ihrem Passwort die folgenden Optionen verwenden, um die Anforderungen der Multifaktor-Authentifizierung zu erfüllen. Die Anwender können MFA-Faktoren wie Authentifikatoranwendungen, biometrische Scanner, Hardwareschlüssel und SMS unabhängig einrichten.

Authentifikatoranwendungen

Eine Authentifikatoranwendung ist eine Drittanbietersoftware, die temporäre Passcodes generiert. Anwender können diese Passcodes zusammen mit ihrem Passwort verwenden, um sich bei einer Instanz anzumelden, die eine Multifaktor-Authentifizierung (MFA) erfordert. Weitere Informationen zu diesen Anwendungen finden Sie unter Authentifikatoranwendungen.

Befolgen Sie die Anweisungen auf dem Bildschirm, um die Authentifikatoranwendung einzurichten.



© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Biometrische Scanner

Biometrische Authentifikatoren verwenden Fingerabdruck- oder Gesichtserkennung, um Benutzer zu identifizieren. Ihre Anwender können diese Authentifikatoren auf ihren Geräten als Teil des Multifaktor-Anmeldevorgangs verwenden. Weitere Informationen zur Registrierung biometrischer Authentifikatoren finden Sie unter Registrieren Sie einen biometrischen Authentifikator.



Hardwareschlüssel

Hardwareschlüssel sind physische Hardware, die Sie zur Authentifizierung verwenden können. Hardwareschlüssel werden zur Authentifizierung in einen Port Ihres Geräts eingefügt. Weitere Informationen zur Registrierung von Hardwareschlüsseln finden Sie unter Registrieren Sie einen Hardware-Sicherheitsschlüssel.



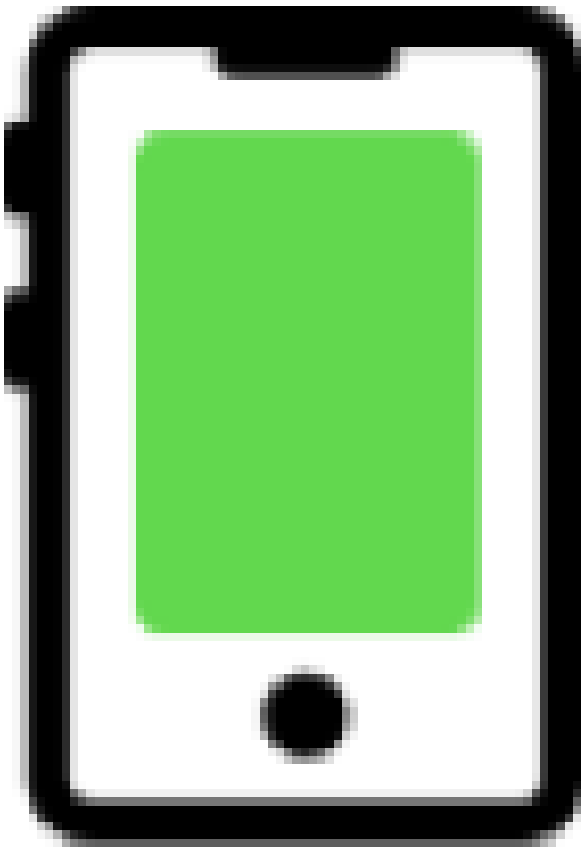
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SMS

Administratoren können die Instanz ServiceNow so konfigurieren, dass Benutzer, die versuchen, sich mit SMS-basiertem OTP bei der Instanz anzumelden.

Wenn Benutzer versuchen, sich bei ServiceNowanzumelden, wird die SMS-OTP an die Mobiltelefonnummer gesendet, die dem Datensatz „sys_user“ zugeordnet ist. Benutzer können den sechsstelligen Verifizierungscode eingeben, der an das Mobilgerät gesendet wurde, und ihre Identität überprüfen.

Weitere Informationen finden Sie unter Mehrstufige Authentifizierung mit SMS.



E-Mail

Administratoren können die Instanz ServiceNow so konfigurieren, dass Benutzer, die versuchen, sich mit E-Mail-basiertem OTP bei der Instanz anzumelden.

Wenn Anwender versuchen, sich bei ServiceNowanzumelden, wird die E-Mail-OTP an die E-Mail-Adresse des Anwenders gesendet. Benutzer können den sechsstelligen Verifizierungscode eingeben, der an die E-Mail-Adresse gesendet wurde, und ihre Identität überprüfen.

Weitere Informationen finden Sie unter Mehrstufige Authentifizierung mit E-Mail.



Eigenschaften Multifaktor-Authentifizierung

Verwenden Sie die Eigenschaften der Multifaktor-Authentifizierung, um MFA in Ihrer Instanz zu aktivieren, zu deaktivieren und zu konfigurieren. Einzelheiten zu diesen Eigenschaften finden Sie unter Systemeigenschaften der Multifaktor-Authentifizierung.

MFA, unterstützte Methoden und Workflows konfigurieren

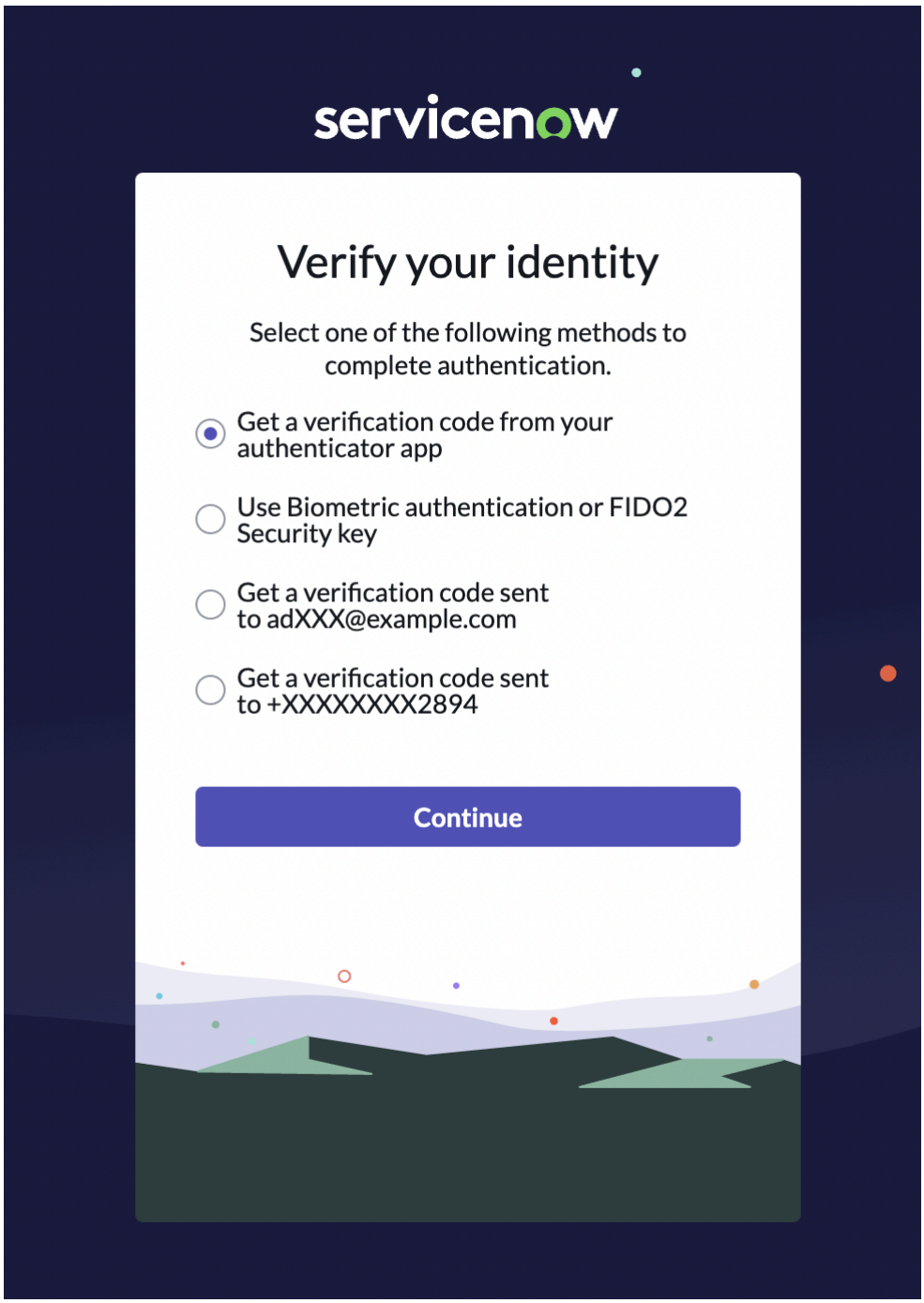
MFA, auch bekannt als zweistufige Verifizierung, ist eine Sicherheitsanforderung, die angibt, dass Benutzer mehr als einen Satz von Anmeldeinformationen eingeben müssen, um auf eine Instanz zuzugreifen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Basisebene der Authentifizierung bei einer Instanz ist die lokale Datenbankauthentifizierung, bei der Benutzer ihren Anwendernamen und ihr Passwort eingeben. Mit MFA können Administratoren und Benutzer eine zweite Authentifizierungsebene verlangen.

Die zweite Authentifizierungsebene kann auf Folgendem basieren:

- Ein Passcode aus einer Authentifizierungs-App
- Ein Hardwareschlüssel
- Ein biometrischer Authentifikator, z. B. ein Fingerabdrucklesegerät oder eine Gesichtserkennung.
- SMS oder E-Mail



© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Als Administrator können Sie MFA für einzelne Anwender oder alle Anwender in einer bestimmten Rolle einrichten. Sie können Ihren Anwendern auch ermöglichen, sich für MFA zu entscheiden und zu verwenden.

Aktivierung

Das Plugin *Integration – Multifactor Authentication* (com.snc.integration.multifactor.authentication) wird standardmäßig auf Ihrer Instanz installiert, muss jedoch von einem Administrator mithilfe einer Systemeigenschaft aktiviert werden. Details finden Sie unter Systemeigenschaften der Multifaktor-Authentifizierung.

Hinweis: Nach dem Klonen einer Instanz müssen Sie MFA in der geklonten Instanz erneut aktivieren. Weitere Informationen finden Sie in den KB-Artikeln KB0657100 , KB0860689 ,KB0825390 , KB0779908 , KB0717367 , KB0727991 .

Unterstützte Authentifizierungsmethoden

Sie können MFA mit den folgenden Authentifizierungsmethoden verwenden:

- Lokale Datenbankauthentifizierung (native ServiceNow Authentifizierung)
- LDAP-Integration
- SSO SAML
- SSO-OIDC

Workflow zur Einrichtung der Multifaktor-Authentifizierung

Der Administrator aktiviert die Multifaktor-Authentifizierung

Das Plugin „ **Integration – Multifaktor-Authentifizierung** “ (com.snc.integration.multifactor.authentication) ist standardmäßig in Ihrer Instanz von aktiviert. Um MFA verwenden zu können, müssen Administratoren MFA mithilfe einer Systemeigenschaft aktivieren. Nach der Aktivierung wählen Administratoren Anwender oder Rollen aus, für die MFA-Anmeldungen erforderlich sind.

Weitere Informationen zur Einrichtung von MFA-Administratoren finden Sie unter Multifaktor-Authentifizierung (MFA).

Benutzer melden sich mit einer Authentifizierungs-App an

Die Benutzer werden aufgefordert, MFA-Optionen für die Anmeldung zu verwenden. Anwender können eine der Optionen auswählen, um die MFA abzuschließen. Wenn ein Anwender das Setup mit einem Faktor abgeschlossen hat, kann er bei Bedarf weiterhin zu seiner Profilseite wechseln und das Setup für die verbleibenden Faktoren abschließen.

Webauthentifizierung

Aktivieren Sie *Integration – Web Authentication* (com.snc.integration.webauthn), um die Authentifizierung mit Hardwareschlüsseln oder biometrischen Lesegeräten in Ihrer Instanz zuzulassen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hardwareschlüssel sind physische Hardware, die Sie zur Authentifizierung verwenden können. Hardwareschlüssel werden zur Authentifizierung in einen Port Ihres Geräts eingefügt. Weitere Informationen zur Registrierung von Hardwareschlüsseln finden Sie unter Registrieren Sie einen Hardware-Sicherheitsschlüssel.

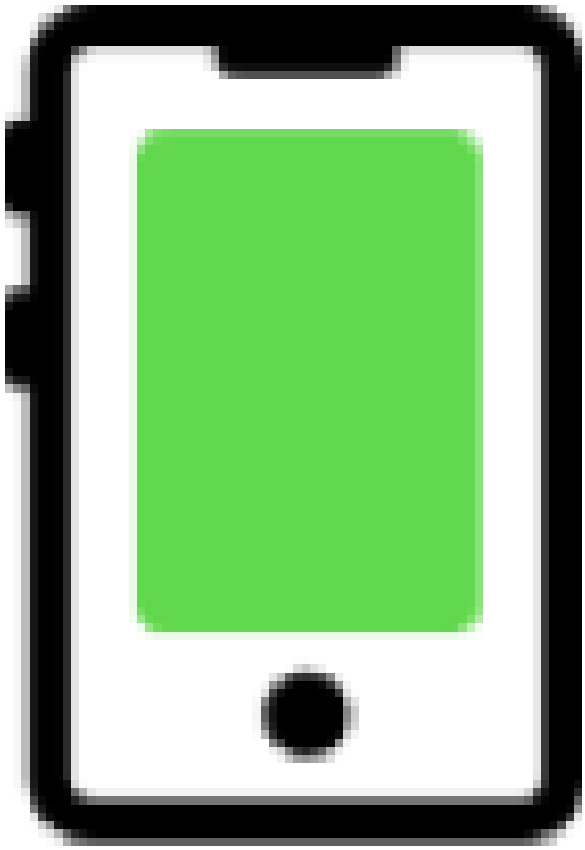


Biometrische Authentifikatoren verwenden Fingerabdruck- oder Gesichtserkennung, um Benutzer zu identifizieren. Ihre Anwender können diese Authentifikatoren auf ihren Geräten als Teil des Multifaktor-Anmeldevorgangs verwenden. Weitere Informationen zur Registrierung biometrischer Authentifikatoren finden Sie unter Registrieren Sie einen biometrischen Authentifikator.

SMS oder E-Mail (Einmalpasswort)

SMS und E-Mail unterstützen MFA, um Benutzern die Anmeldung bei einer Instanz ServiceNow zu ermöglichen und die Experience unterwegs zu verbessern.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Administratoren können die Instanz ServiceNow so konfigurieren, dass Benutzer, die versuchen, sich mit SMS-basiertem OTP bei der Instanz anzumelden.

Wenn Benutzer versuchen, sich bei ServiceNowanzumelden, wird die SMS-OTP an die Mobiltelefonnummer gesendet, die dem Datensatz „sys_user“ zugeordnet ist. Benutzer von können den sechsstelligen Verifizierungscode eingeben, der an das Mobilgerät gesendet wurde, und ihre Identität überprüfen.

Weitere Informationen finden Sie unter Mehrstufige Authentifizierung mit SMS.



Administratoren können die Instanz ServiceNow so konfigurieren, dass Benutzer, die versuchen, sich mit E-Mail-basiertem OTP bei der Instanz anzumelden.

Wenn Benutzer versuchen, sich bei ServiceNowanzumelden, wird die E-Mail-OTP an die E-Mail-Adresse gesendet, die dem Benutzer zugeordnet ist. Benutzer können den sechsstelligen Verifizierungscode eingeben, der an die E-Mail-Adresse gesendet wurde, und ihre Identität überprüfen.

Weitere Informationen finden Sie unter Mehrstufige Authentifizierung mit E-Mail.

Systemeigenschaften der Multifaktor-Authentifizierung

Verwenden Sie die Systemeigenschaften, um MFA zu aktivieren und an Ihre Sicherheitsanforderungen anzupassen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften Multifaktor-Authentifizierung

Eigenschaft	Beschreibung
Multifaktor-Authentifizierung aktivieren (*glide.authenticate.multifactor*)	Option, mit der Benutzer und Administratoren diese Funktion verwenden können. Standardmäßig ist diese Option aktiviert. Weitere Informationen zu dieser Eigenschaft finden Sie unter Multi-Faktor-Authentifizierung (MFA) aktivieren in Härtungseinstellungen für Instanzsicherheit.
Gibt an, wie oft ein Anwender die Multifaktor-Authentifizierung umgehen kann (*glide.authenticate.multifactor.setup.bypass.count*)	Anzahl der Fälle, in denen ein Anwender das Setup von MFA überspringen kann. Ihre Benutzer können sich bei der Instanz anmelden, auch wenn sie ihr Mobilgerät nicht bei sich haben. Wenn Sie diese Funktion deaktivieren und sie dann erneut aktivieren, beginnt der Zähler erneut. Der Standardwert ist 3.
Die Zeit in Minuten, für die der einmalige Code, der an die E-Mail-Adresse des Anwenders gesendet wird, gültig ist, für (*glide.multifactor.onetime.code.validity*)	Anzahl der Minuten, die der Rücksetzungscode gültig ist. Weitere Informationen finden Sie unter Melden Sie sich mit der Multifaktor-Authentifizierung an. Der Standardwert ist 5. **Hinweis:** Diese Eigenschaft gilt für die Validierungszeit des E-Mail-OTP.
Zusätzliche Zeit in Sekunden, für die der Code gültig ist, um den Taktversatz zu berücksichtigen. Der Höchstwert beträgt 60 Sekunden. (*glide.authenticate.multifactor.clock_skew*)	Anzahl der zusätzlichen Sekunden, die der Rücksetzungscode gültig ist. Der Höchstwert ist `60`. Der Standardwert ist `10`. Die Instanz validiert den vom Anwender eingegebenen Code anhand des einzelnen von der App generierten Codes, der zum `aktuellen Zeitpunkt`generiert wird. Sie können das Zeitfenster mit dieser Eigenschaft verzerren und zulassen, dass ein oder mehrere Codes während eines Zeitfensters generiert werden, um als gültig angesehen zu werden. Der Wert der Eigenschaft wird in der folgenden Berechnung verwendet: `aktuelle Uhrzeit - X/2` und `aktuelle Uhrzeit + X/2`, wobei `X` der Wert dieser Eigenschaft ist. Wenn Sie beispielsweise den Wert `10`verwenden, betrachtet die Instanz jeden Code als gültig, den die App innerhalb des Zeitbereichs `[aktuelle Uhrzeit: 5 Sekunden]` und `[aktuelle Uhrzeit + 5 Sekunden]` generiert. Verwenden Sie diese Eigenschaft, um Anmeldeprobleme zu vermeiden, bei denen der Anwender nicht in der Lage ist, den

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften Multifaktor-Authentifizierung (Fortsetzung)

Eigenschaft	Beschreibung
	richtigen Code innerhalb der standardmäßig zugewiesenen Zeit einzugeben.
Aktivieren Sie die Funktion zum Speichern des Browsers für die Multifaktor-Authentifizierung. (*glide.authenticate.multifactor.remember.browser.enable*)	Legen Sie Ihre Instanz so fest, dass ein Anwender zur MFA aufgefordert wird, wenn er sich über ein neues Gerät oder einen neuen Browser anmeldet. Der Standardwert ist „ja“.
Gültigkeit des Browser-Fingerabdrucks in Stunden. (*glide.authenticate.multifactor.browser.fingerprint.validity*)	Nachdem MFA den Browser gespeichert hat, wird der Anwender für diese Dauer nicht aufgefordert, MFA im selben Browser zu verwenden. Der Standardwert ist 8 Stunden.
Maximale Anzahl von Browsern, die ein Anwender speichern kann. (*glide.authenticate.multifactor.remembered.browser.max.count*)	Die Anzahl der Browser, die MFA für diesen Anwender speichert.
Standardwert des Kontrollkästchens „Browser speichern“ auf der Seite „Mehrstufige Validierung“. (*glide.authenticate.multifactor.remember.browser.default*)	Standardwert des Kontrollkästchens „remember-browser“ auf der Seite „Mehrstufige Validierung“.
Aktivieren Sie MFA auf Basis der Webauthentifizierung (FIDO2). (*glide.webauthn.enabled*)	Option zum Aktivieren passwortloser Authentifizierungsmethoden wie Hardwareschlüssel und biometrischer Authentifizierung.
E-Mail-OTP für Multifaktor-Authentifizierung aktivieren (*glide.authenticate.multifactor.email.otp.enable*	Option zum Aktivieren von E-Mail-basierter OTP als Faktor für MFA.
Aktivieren Sie die Setup-UI für die erweiterte Multifaktor-Authentifizierung (MFA), damit Anwender den Faktor unabhängig einrichten können. *glide.auth.mfa.ui.v2.enabled*	Option, um den MFA-Faktor für die Anwender unabhängig zu aktivieren, ohne eine Authentifikator-App einzurichten.

Kriterien für Multifaktor-Authentifizierung

Verwenden Sie Multifaktor-Kriterien, um zu bestimmen, welche Anwender und Rollen die zweistufige Multifaktor-Überprüfung verwenden müssen.

Sie können eines dieser Kriterien oder eine Kombination davon verwenden, um Ihren Geschäftsanforderungen gerecht zu werden.

Hinweis: Es wird empfohlen, MFA auf Basis der Richtlinie „Adaptive Authentifizierung“ zu verwenden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kriterien für Multifaktor-Authentifizierung

Kriterien	Beschreibung
Anwenderbasierte Multifaktor-Kriterien	Verwenden Sie anwenderbasierte Multifaktor-Kriterien, um einzelne Anwender auszuwählen, die sich mit MFA anmelden müssen. Administratoren aktualisieren das Feld **„Multifaktor-Authentifizierung** aktivieren“ in einem Benutzerdatensatz, um die MFA-Anforderungen für einen Benutzer zu aktivieren oder zu deaktivieren. Details zu diesem Vorgang finden Sie unter Konfigurieren Sie anwenderbasierte Multifaktor-Kriterien.
Rollenbasierte Multifaktor-Kriterien	Verwenden Sie rollenbasierte Multifaktor-Kriterien, um die MFA-Anmeldung für alle Anwender zu erfordern, die einer bestimmten Rolle zugewiesen sind. Der Datensatz Rollenbasierte Multifaktor **-Authentifizierung** in der Tabelle Multifaktor **-Kriterien** [multi_factor_criteria] enthält die Liste der Rollen, die eine MFA-Anmeldung erfordern. Einzelheiten zum Verwalten dieser Liste finden Sie unter Konfigurieren Sie rollenbasierte Multifaktor-Kriterien.
Richtlinienbasierte Multifaktor-Kriterien für adaptive Authentifizierung	Verwenden Sie die adaptive Authentifizierung, um zu bestimmen, wann Ihre Instanz MFA erfordert. Die adaptive Authentifizierung verwendet Authentifizierungsrichtlinien, um Kriterien wie die IP-Adresse eines Anwenders oder Anwendergruppen auszuwerten. Weitere Informationen zur Funktion „Adaptive Authentifizierung“ finden Sie unter Adaptive Authentifizierung.

Konfigurieren Sie anwenderbasierte Multifaktor-Kriterien

Verwenden Sie anwenderbasierte Multifaktor-Kriterien, um MFA für einen Anwender zu aktivieren.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Anwenderadministration** > **Anwender**an.
2. Konfigurieren Sie die Liste so, dass die Spalte **Multifaktor-Authentifizierung aktivieren angezeigt** wird.
3. Ändern Sie die Werte der Spalte **Multifaktor-Authentifizierung** aktivieren für die ausgewählten Anwender in **true**.

   Wenn sich der Benutzer mit seinem Anwendernamen und seinem Passwort anmeldet, wird er aufgefordert, die Multifaktor-Authentifizierung einzurichten.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie rollenbasierte Multifaktor-Kriterien

Verwenden Sie rollenbasierte Multifaktor-Kriterien, um die Multifaktor-Authentifizierung für alle Anwender zu erzwingen, die bestimmten Rollen zugewiesen sind.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Multi-Faktor-Authentifizierung** > **Multifaktor-Kriterien**an.
2. Öffnen Sie in der Liste **Multifaktor-Kriterien** den Datensatz **Rollenbasierte Multifaktor-Authentifizierung**.
3. Verwenden Sie die Liste der **Multifaktor-Rollen**, um Rollen hinzuzufügen oder zu entfernen.

Option	Bezeichnung
Eine Rolle hinzufügen	Doppelklicken Sie auf **Neue Zeile einfügen...** und geben Sie einen Rollennamen ein, oder wählen Sie einen entsprechenden Namen aus. Klicken Sie auf das **Speichern-** Symbol ( ), um den Eintrag zu speichern.
Entfernen Sie eine Rolle	Klicken Sie auf das Löschsymbol ( ), um eine Rolle aus der Liste zu entfernen.

4. Klicken Sie auf **Aktualisieren**.

Ergebnisse
Ihre -Instanz erzwingt die Multifaktor-Authentifizierung für alle Benutzer, die Mitglieder der in der Liste **„Multifaktor-Rollen“** aufgeführten Rollen sind.

Wichtig: Der Datensatz muss aktiv sein, um die rollenbasierte Multifaktor-Authentifizierung zu erzwingen.

Konfigurieren Sie richtlinienbasierte Multifaktor-Kriterien für die adaptive Authentifizierung

Verwenden Sie adaptive Richtlinien, um zu bestimmen, welche Benutzer die zweistufige Multifaktor-Überprüfung (MFA) verwenden müssen.

Vorbereitungen
Erforderliche Rolle: admin

Hinweis:

- Wenn die Standardrichtlinie **Step-Up-MFA-Richtlinie**ist, wird Anwendern Multifaktor-Authentifizierung angezeigt, wenn die in der **Step-Up-MFA-** Richtlinie konfigurierte Richtlinie als „wahr“ ausgewertet wird. Richtlinie hat Vorrang vor der anwender- oder rollenbasierten Konfiguration.
- MFA mit SSO-Anmeldung ist nur verfügbar, wenn die Eigenschaft „ `glide.authenticate.mfa.with.multisso.enabled`“ auf „wahr“ festgelegt ist.
- Sie können zum Datensatz „Authentifizierungsrichtlinie“ navigieren, um dem referenzierten Richtlinienfeld (**Step-Up-MFA-Richtlinie** oder **Step-Down-MFA-Richtlinie**) die Richtlinieneingabe(n) hinzuzufügen oder zu bearbeiten.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Kontexte der Authentifizierungsrichtlinie** > **MFA-Kontext**an.
   Der Richtlinienkontext-Datensatz für den **MFA-Kontext** wird geöffnet.
2. Wählen Sie die Standardrichtlinie im Feld **Standardrichtlinie** aus.
   Diese Auswahl bestimmt, wie Ihre Instanz die Richtlinienbedingungen verwendet, um zu bestimmen, ob MFA erforderlich ist.

Standardrichtlinien

Standardrichtlinie	Definition
Step-Up-MFA-Richtlinie	Wählen Sie diese Option aus, um MFA zu erzwingen, wenn die in der **Step-Up-MFA-Richtlinie** definierten Richtlinienbedingungen als „wahr“ ausgewertet werden.
Step-Down-MFA-Richtlinie	Wählen Sie diese Option aus, um MFA zu umgehen, wenn die in der **Step-Down-MFA-Richtlinie** definierten Richtlinienbedingungen als „wahr“ ausgewertet werden.

3. Wählen Sie im Feld **Step-Up-MFA-Richtlinie** eine Richtlinie aus, die mit diesem Kontext verwendet werden soll.
4. Klicken Sie auf **Aktualisieren**.
   Nach dem Speichern des Datensatzes werden die Listen **Richtlinieneingabe** und **Richtlinienbedingungen** aktualisiert, um die Richtlinieneingaben und -bedingungen anzuzeigen, die der im Feld **Step-Up-MFA-Richtlinie** ausgewählten Richtlinie zugeordnet sind.

Webauthentifizierung – MFA

Verwenden Sie **„Integration – Webauthentifizierung“ (com.snc.integration.webauthn)**, um die Authentifizierung mit Hardwareschlüsseln oder biometrischen Lesegeräten in Ihrer Instanz zuzulassen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hardwareschlüssel sind physische Hardware, die Sie zur Authentifizierung verwenden können. Hardwareschlüssel werden zur Authentifizierung in einen Port Ihres Geräts eingefügt. Weitere Informationen zur Registrierung von Hardwareschlüsseln finden Sie unter Registrieren Sie einen Hardware-Sicherheitsschlüssel.



Biometrische Authentifikatoren verwenden Fingerabdruck- oder Gesichtserkennung, um Benutzer zu identifizieren. Ihre Anwender können diese Authentifikatoren auf ihren Geräten als Teil des Multifaktor-Anmeldevorgangs verwenden. Weitere Informationen zur Registrierung biometrischer Authentifikatoren finden Sie unter Registrieren Sie einen biometrischen Authentifikator.

Konfigurieren Sie MFA mit Biometrie

Administratoren können die Liste „Öffentliche Anwenderanmeldeinformationen“ verwenden, um von Anwendern erstellte Anmeldeinformationen anzuzeigen und zu verwalten.

Wenn ein Benutzer eine Authentifikatoranwendung, eine biometrische Authentifizierung oder einen Hardwareschlüssel registriert, erstellt Ihre Instanz einen Datensatz in der Tabelle „

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Öffentliche Anmeldeinformationen des Benutzers“ [sys_user_public_credential]. Verwenden Sie diese Tabelle, um zu sehen, welche Anwender einen Authentifikator registriert haben und welche Typen und wann sie registriert und verwendet wurden. Sie können diese Datensätze auch als inaktiv markieren, um zu verhindern, dass Benutzer diese Anmeldeinformationen verwenden.

Formular für öffentliche Anmeldeinformationen des Anwenders

Feld	Beschreibung
Kurzname der Anmeldeinformationen	Kurzname für die Anmeldeinformationen. Dieser Kurzname wird vom Benutzer bei der Registrierung eines Authentifikators ausgewählt.
Anwender	Benutzer, der den Anmeldeinformationen zugeordnet ist
Aktiv	Gibt an, ob die Anmeldeinformationen aktiv sind. Administratoren können einen Datensatz auf inaktiv setzen, um zu verhindern, dass sich ein Anwender mit diesen Anmeldeinformationen authentifiziert.
Authentifikator	Der Typ des vom Anwender registrierten Authentifikators.
Registrierungszeit	Datum und Uhrzeit der Erstellung dieser Anmeldeinformationen durch den Anwender
Zuletzt verwendet um	Datum und Uhrzeit der letzten Anmeldung des Anwenders mit diesen Anmeldeinformationen.

Eingeschränkte Authentifikatortypen

Wenn Sie eine Authentifizierungsmethode eingeschränkt haben, z. B. biometrische Authentifikatoren, können Anwender keine neuen Anmeldeinformationen dieses Typs erstellen. Alle Anmeldeinformationen, die vor dieser Einschränkung erstellt wurden, funktionieren jedoch weiterhin. Sie können Datensätze in der Tabelle „ **Öffentliche Anwenderanmeldeinformationen** “ deaktivieren, um zu verhindern, dass diese Anmeldeinformationen verwendet werden, nachdem sie erstellt wurden.

Konfigurationsoptionen für den Authentifikator

Verwenden Sie die Seite „Authentifikatorkonfiguration“, um Authentifikatoroptionen für Ihre Instanz zu verwalten.

Navigieren zu **Multi-Faktor-Authentifizierung** > **Webauthentifizierung** > **Konfiguration des Authentifikators** um die Standardkonfigurationsoptionen anzuzeigen und zu bearbeiten.

Formular „Authentifikatorkonfiguration“

Feld	Beschreibung
Zulässiger Authentifikatortyp	Typ der Authentifikatoren, die registriert werden dürfen. Wählen Sie aus:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Authentifikatorkonfiguration“ (Fortsetzung)

Feld	Beschreibung
	• **Plattformauthentifizierer** werden an ein Gerät angehängt oder in dieses integriert. In diese Kategorie fallen Fingerabdrucklesegeräte oder die auf Mobilgeräten verfügbare Gesichtserkennung (z. B. Apple FaceID oder TouchID). • **Roaming** -Authentifikatoren können von einem Computer oder einem anderen Clientgerät entfernt und an anderer Stelle verwendet werden. Hardwareschlüssel fallen unter diese Kategorie.
Nachweistyp	Wenn Sie den Wert auf „direkt“ oder „indirekt“ festlegen, müssen Authentifikatormetadaten importiert werden, um die Herkunft eines Authentifikators während der Registrierung zu bestätigen. • Keine • Direkt • Indirekt
Plattform-Selbstnachweis	Gibt an, ob der Selbstnachweis für Plattformauthentifizierer aktiviert ist.
Plattformübergreifender Selbstnachweis	Gibt an, ob der Selbstnachweis für Roaming-Authentifikatoren aktiviert ist.
Anwenderverifizierung	Wählen Sie **Preferred** oder **Required**aus. Bei Bedarf fordert der Webauthentifizierungs-Flow Anwender zur Verifizierung mit PIN oder anhand von Biometriedaten auf.
Anwenderpräsenz verifizieren	Gibt an, ob der Webauthentifizierungs-Flow die Verifizierung der Anwenderpräsenz erfordert.
Residenter Schlüssel	Wählen Sie **Preferred** oder **Required**aus. Bei Bedarf behält der Authentifikator die Anmeldeinformationen für den öffentlichen Schlüssel im Authentifikatorspeicher bei.
Zeitüberschreitung (in ms)	Maximale Zeitbegrenzung für den Abschluss der Registrierung und Authentifizierung der Webauthentifizierung. Die Zeit wird in Millisekunden angegeben.

Mehrstufige Authentifizierung mit SMS

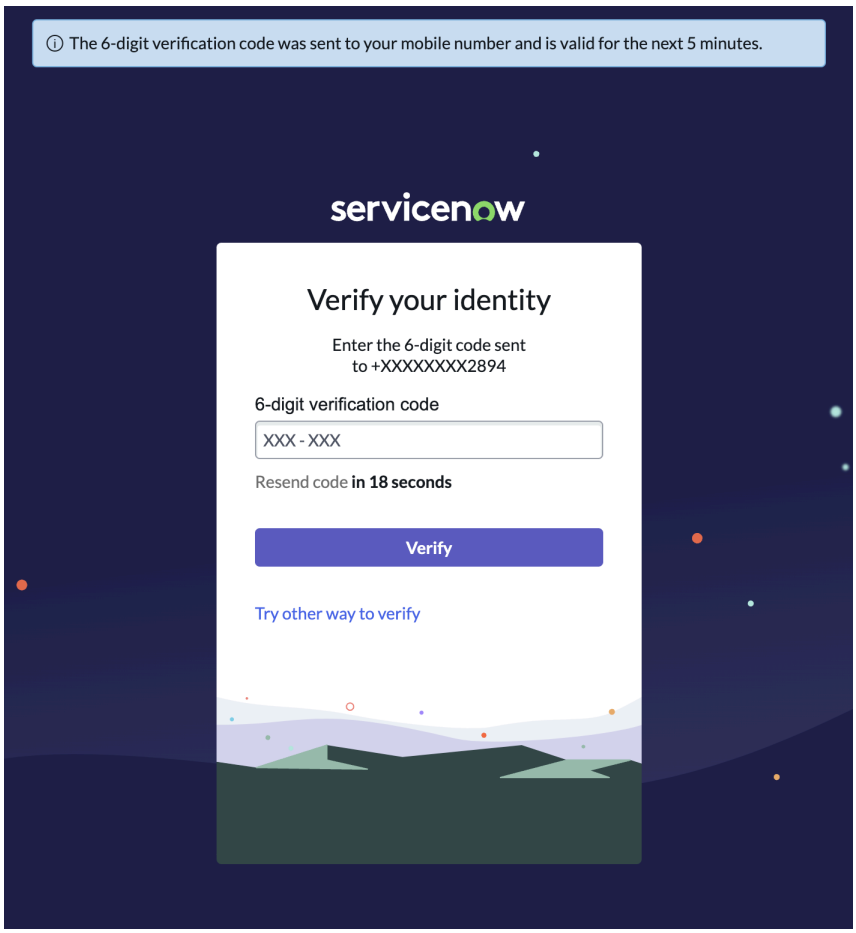
Multifaktor-Authentifizierung (MFA) mit SMS als Faktor für Ihre Authentifizierung.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Administratoren können die Instanz ServiceNow so konfigurieren, dass Benutzer, die versuchen, sich mit SMS-basiertem OTP bei der Instanz anzumelden.

Wenn Benutzer versuchen, sich bei ServiceNowanzumelden, wird die SMS-OTP an die Mobiltelefonnummer gesendet, die dem Datensatz „sys_user“ zugeordnet ist. Benutzer von können den sechsstelligen Verifizierungscode eingeben, der an das Mobilgerät gesendet wurde, und ihre Identität überprüfen.

Sie können MFA mit SMS auch mit der Standardkonfiguration Twilio konfigurieren. Weitere Informationen finden Sie unter Anbieter der Multifaktor-Authentifizierung.



Darüber hinaus kann die MFA mit SMS basierend auf der Richtlinieneingabe und den Bedingungen mithilfe von Filterkriterien gesteuert werden. Es folgen die Arten von Filterkriterien:

- IP-Filterkriterien
- Rollen-Filterkriterien
- Gruppenfilterkriterien

Aktivieren Sie das Plugin „MFA mit SMS“.

Für MFA mit SMS installieren Sie das Plugin Multifaktor-Authentifizierung mit SMS (`com.snc.authentication.sms_mfa`).

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Die folgenden Elemente werden mit der Multifaktor-Authentifizierung mit SMS installiert:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Adaptive Authentifizierung (`com.snc.adaptive_authentication`
- Notify – Twilio Direct-Treiber (`com.snc.notify.twilio_direct`)

Abhängiges Plugin: Integration – Multifaktor-Authentifizierung (`com.snc.integration.multifactor.authentication`)

Hinweis: Sie können die Demodaten bei der Installation des Plugins laden, wenn Sie einen anwenderdefinierten Anbieter für die Generierung der SMS konfigurieren.

Prozedur

1. Navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie das Plugin „Multifaktor-Authentifizierung mit SMS“ (`com.snc.authentication.sms_mfa`) mithilfe der Filterkriterien und der Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: `Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.`

   Nach Abschluss der Installation wird eine Meldung angezeigt.

Konfigurieren Sie SMS als MFA-Faktor

Konfigurieren Sie Richtlinieneingabe und -bedingung, um SMS OTP als MFA-Faktorrichtlinie für die Authentifizierung anzuzeigen.

Vorbereitungen

Erforderliches Plugin: Mehrstufige Authentifizierung mit SMS (`com.snc.authentication.sms_mfa`).

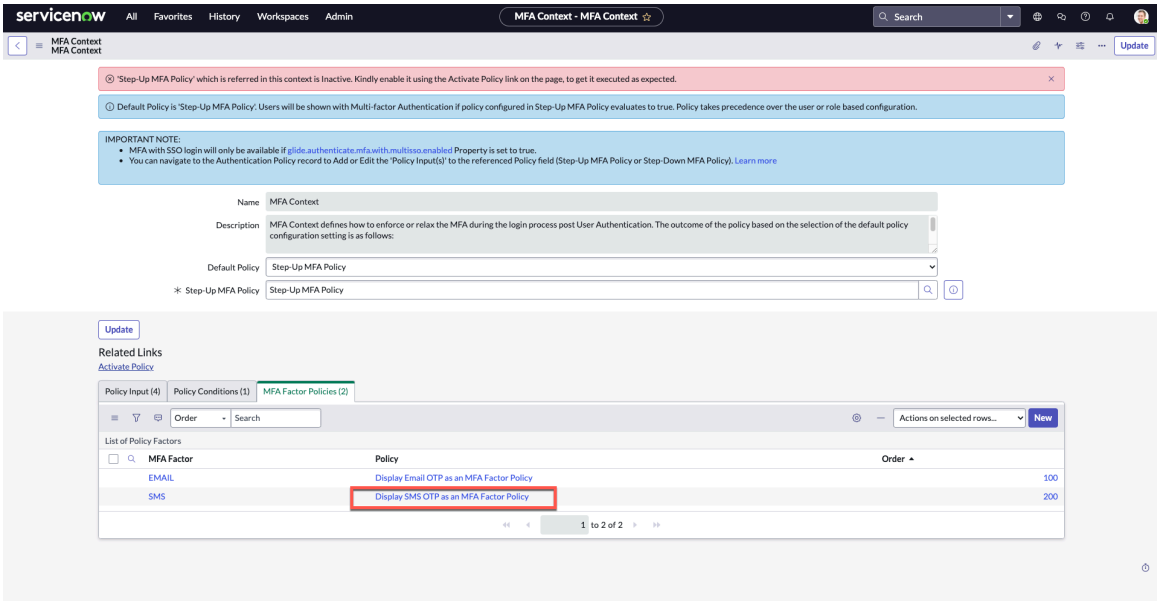
Erforderliche Rolle: admin

Hinweis: Die MFA-Kontextrichtlinie muss als „ `wahr` “ ausgewertet werden, um die SMS-Faktorrichtlinie anzuwenden.

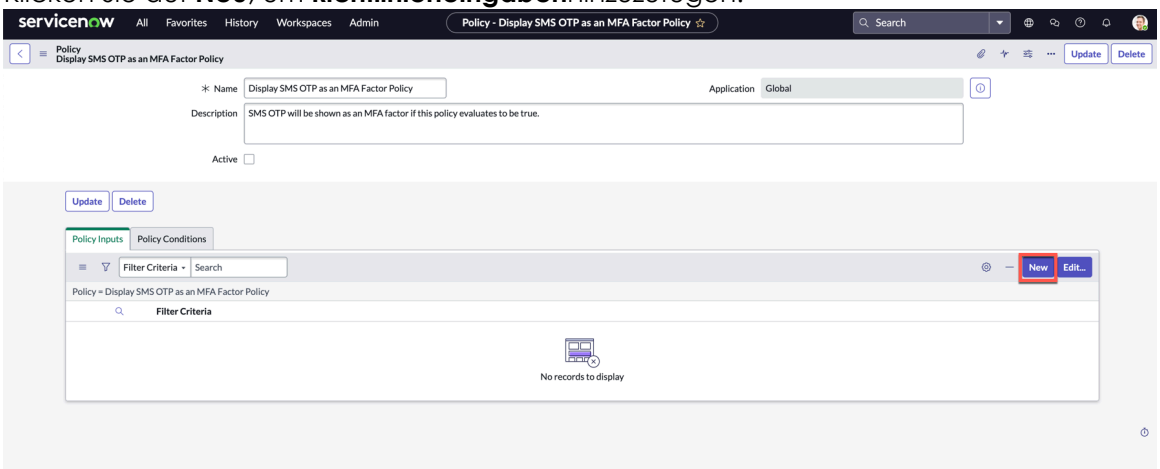
Prozedur

1. Navigieren zu **Alle** > **Multi-Faktor-Authentifizierung** > **MFA-Kontext**an.
2. Klicken Sie auf die Registerkarte **MFA-Faktorrichtlinien**.
3. Wählen Sie **SMS OTP als MFA-Faktorrichtlinie anzeigen aus**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Klicken Sie auf **Neu**, um **Richtlinieneingaben**hinzuzufügen.

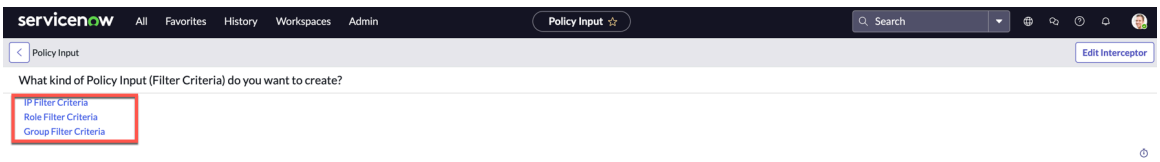


5. Wählen Sie die Filterkriterien aus, die Sie erstellen möchten.

Es folgen die Arten von Filterkriterien:

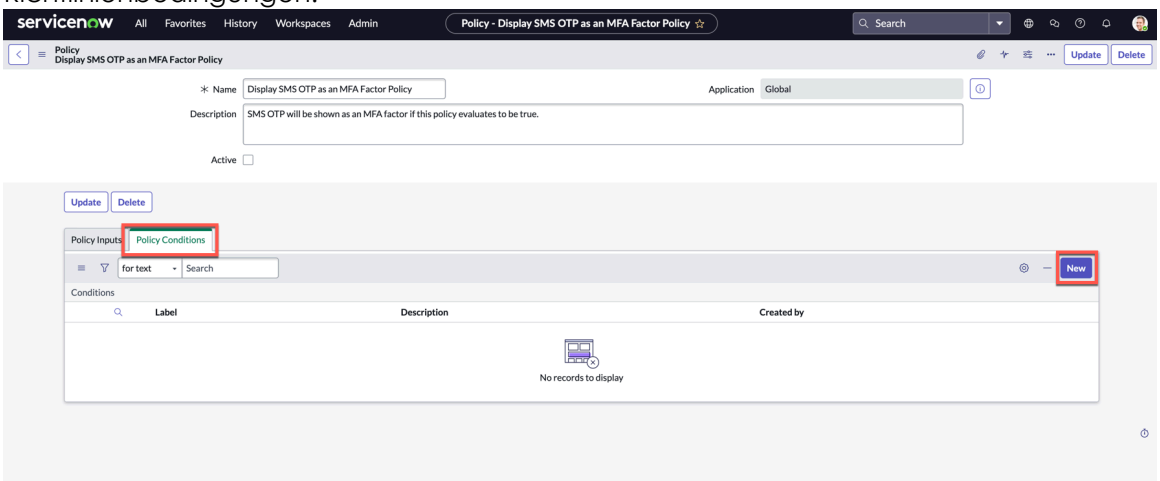
- IP-Filterkriterien
- Rollen-Filterkriterien
- Gruppenfilterkriterien

Beispiel: Rollenfilterkriterien.



© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie auf **Rollenfilterkriterien**, füllen Sie die Felder für die Rollenfilterkriterien aus, und übermitteln Sie den Datensatz.
   Die neue Richtlinie wird erstellt. Weitere Informationen finden Sie unter Rollenfilterkriterien.
7. Klicken Sie auf der Seite Richtlinie – SMS-OTP als MFA-Faktorrichtlinie anzeigen auf Richtlinienbedingungen.



8. Klicken Sie zum Hinzufügen von **Richtlinienbedingungen** auf **Neu**.
9. Füllen Sie die Felder des Formulars aus.

Formular für Bedingungen

Feld	Beschreibung
Bezeichnung	Name zur Identifizierung der Bedingung.
Beschreibung	Beschreibung der Bedingung
Bedingung	Logische Kombination aus mehreren Richtlinieneingaben (Filterkriterien), die zur Auswertung von Authentifizierungsanforderungen verwendet wird. Wählen Sie die Richtlinie für rollenbasierte Filterkriterien aus, die für die Bedingung erstellt wurde.

10. Klicken Sie auf **Absenden**.
11. Wahlweise: Wiederholen Sie Schritt 8, um zusätzliche Richtlinienbedingungen zu erstellen.

> **Hinweis:** Wenn Sie mehrere Richtlinienbedingungen erstellen, hängt die endgültige Ausgabe der Zugriffsrichtlinie von der logischen ODER-Ausgabe aller Richtlinienbedingungen ab. Dies bedeutet, dass die Richtlinie als true ausgewertet wird, wenn eine Ihrer Richtlinienbedingungen erfüllt ist.

Abhängig von der Rollenfilterrichtlinie (Benutzer) und den für die Rolle angegebenen Bedingungen wird den Anwendern der Faktor „SMS als MFA“ als Option für die Authentifizierung angezeigt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anbieter der Multifaktor-Authentifizierung

Verwenden Sie MFA-Anbieter, um die SMS- und E-Mail-basierte Authentifizierung zu konfigurieren und sicherzustellen, dass sich jeder Anwender sicher anmelden kann.

Auf Now Platformkönnen Sie MFA-Anbieter mit dem Mechanismus zur Verwendung von Multifaktor-Authentifizierung wie E-Mail und SMS konfigurieren.

Sie können die folgende für MFA verfügbare Anbieterkonfiguration innerhalb von Now Platformverwenden:

- Konfiguration des E-Mail-Anbieters
- Twilio-Provider-Konfiguration
- Konfiguration des Infobip-Providers.

Hinweis: Twilio und Infobip-Provider-Konfiguration werden automatisch ausgefüllt, indem Demodaten laden bei der Installation der Plugins „Multifaktor-Authentifizierung mit SMS“ (`com.snc.authentication.sms_mfa`) und „Notify – Twilio Direct“ (`com.snc.notify.twilio_direct`) aktiviert wird.

Sie können auch eine eigene Anbieterkonfiguration erstellen, um die Multifaktor-Authentifizierung mit SMS und E-Mail zu aktivieren.

Hinweis: Die Infobip-Provider-Konfiguration wird als Teil der Demodaten bereitgestellt. Sie können die Felder basierend auf Ihren Anforderungen für die Konfiguration Ihres eigenen Providers bearbeiten.

Konfigurieren Sie den MFA-Anbieter

Konfigurieren Sie SMS und E-Mail mit dem Anbieter, um sicherzustellen, dass sich jeder Anwender sicher anmelden kann.

Vorbereitungen

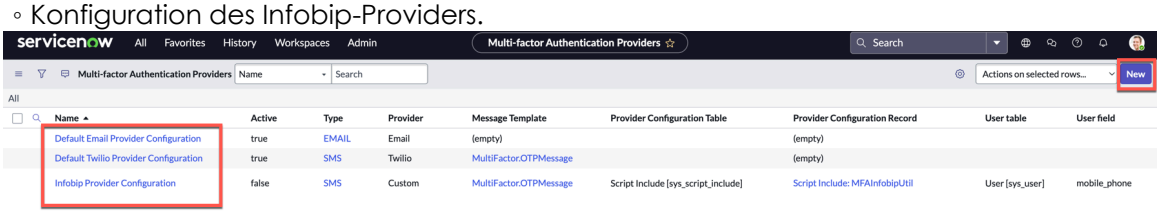
Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Multi-Faktor-Authentifizierung** > **Anbieter**an.

   Die folgenden Anbieterkonfigurationen sind für MFA in Now Platformverfügbar:

   - Konfiguration des E-Mail-Anbieters
   - Twilio-Provider-Konfiguration
   - Konfiguration des Infobip-Providers.



2. Klicken Sie auf **Neu**, um einen neuen Provider zu erstellen.
3. Füllen Sie die Felder im Formular aus.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular für Bedingungen

Feld	Beschreibung
Name	Name des Datensatzes.
Typ	Beschreibung des Datensatzes.
Anbieter	Wählen Sie **Twilio** oder **Anwenderdefiniert**aus. **Hinweis:** Informationen zur Konfiguration von Twilio finden Sie unter Notify mit Twilio konfigurieren . Wenn Sie Anwenderdefiniert **auswählen**, müssen Sie die folgenden Felder angeben: ◦ Konfigurationstabelle des Anbieters ◦ Konfigurationsdatensatz des Anbieters ◦ Skript ◦ Anwendertabelle ◦ Anwenderfeld
Nachrichtenvorlage	Die Nachrichtenvorlage für den Datensatz.
Aktiv	Option zum Aktivieren der Anbieterkonfiguration.

4. Klicken Sie auf **Absenden**.

Je nach Nachrichtenvorlage und Anbieterkonfigurationen wird die SMS oder E-Mail als Faktor für die Authentifizierung während des Anmeldevorgangs an Benutzer gesendet.

Anwenderdefinierte Konfiguration des Vonage-Anbieters (Tutorial)

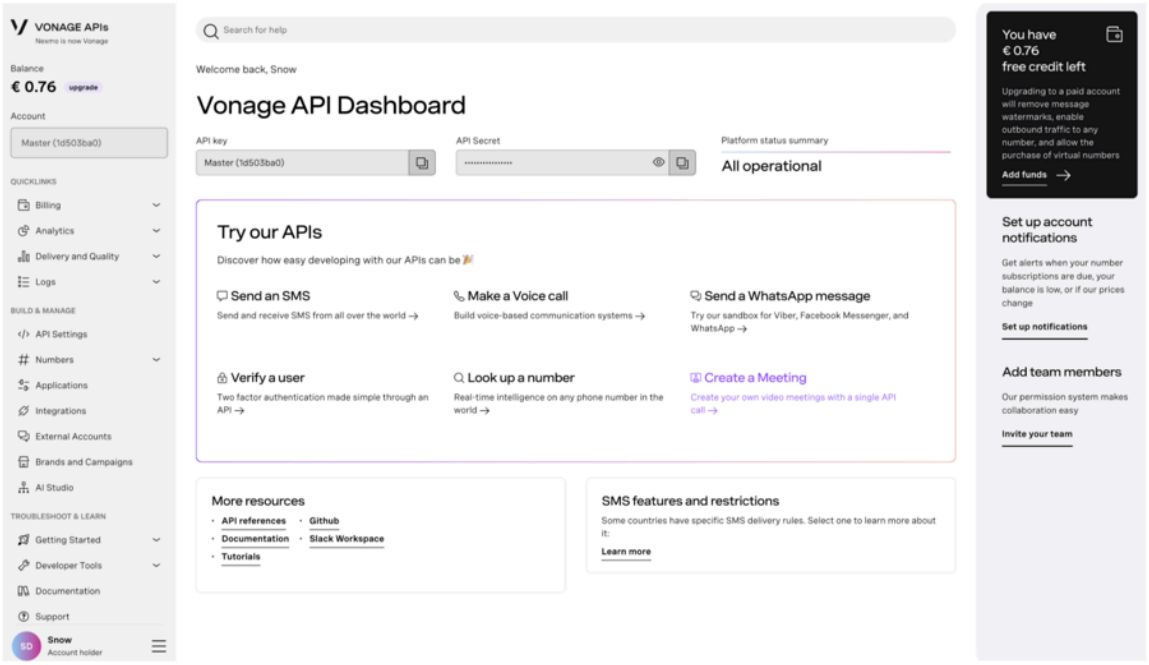
Konfigurieren Sie eine SMS mit dem Vonage-Anbieter, um sicherzustellen, dass sich jeder Anwender sicher anmelden kann.

Vorbereitungen
Erforderliche Rolle: admin

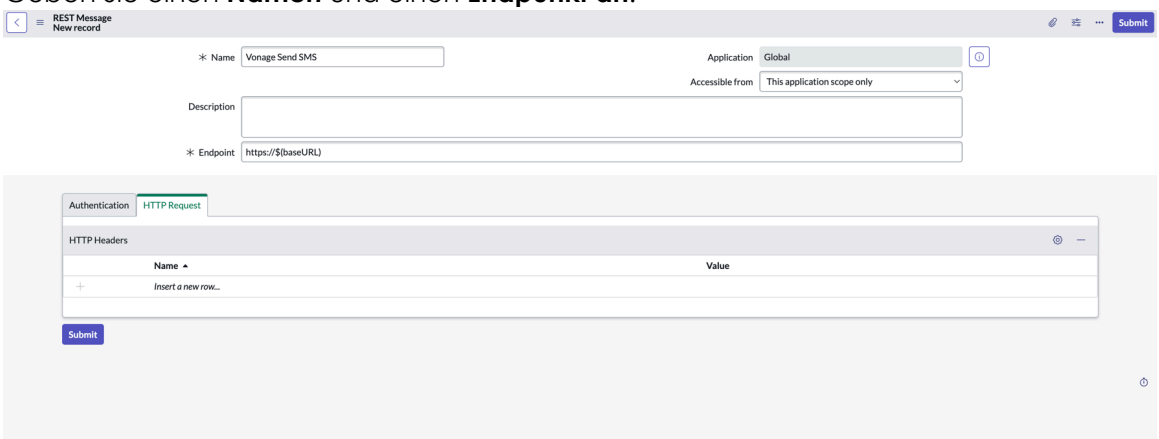
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **Ausgehend** > **REST-Nachricht** und führen Sie die REST-Nachrichtenkonfiguration basierend auf den Informationen aus dem Vonage-API-Dashboard durch.

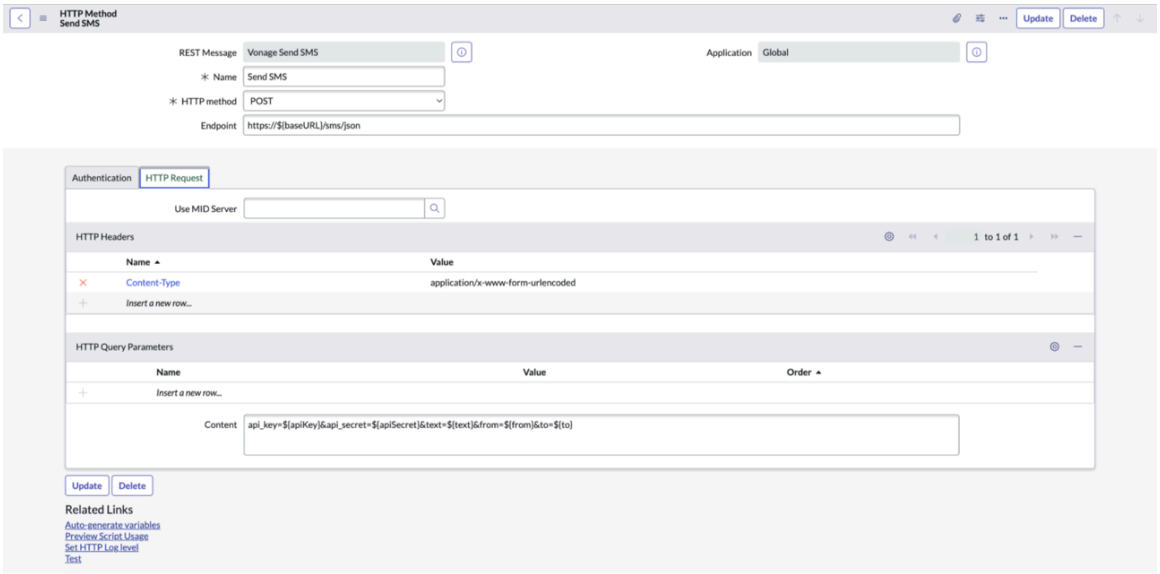


2. Klicken Sie auf **Neu**, um eine neue **REST-Nachricht**zu erstellen.
3. Geben Sie einen **Namen** und einen **Endpunkt an**.



4. Klicken Sie auf **Absenden**.
5. Öffnen Sie den erstellten Datensatz, klicken Sie in der zugehörigen Liste **HTTP-Methoden** auf **Neu**, und wählen Sie **POST**als HTTP-Methode aus.
6. Füllen Sie die folgenden Felder aus:
   - Endpunkt: `https://${baseURL}/sms/json`
   - Inhalt:`api_key=${apiKey}&api_secret=${apiSecret}&text=${text}&from=${from}&to=${to}`
   - Inhaltstyp: `application/x-www-form-urlencoded`

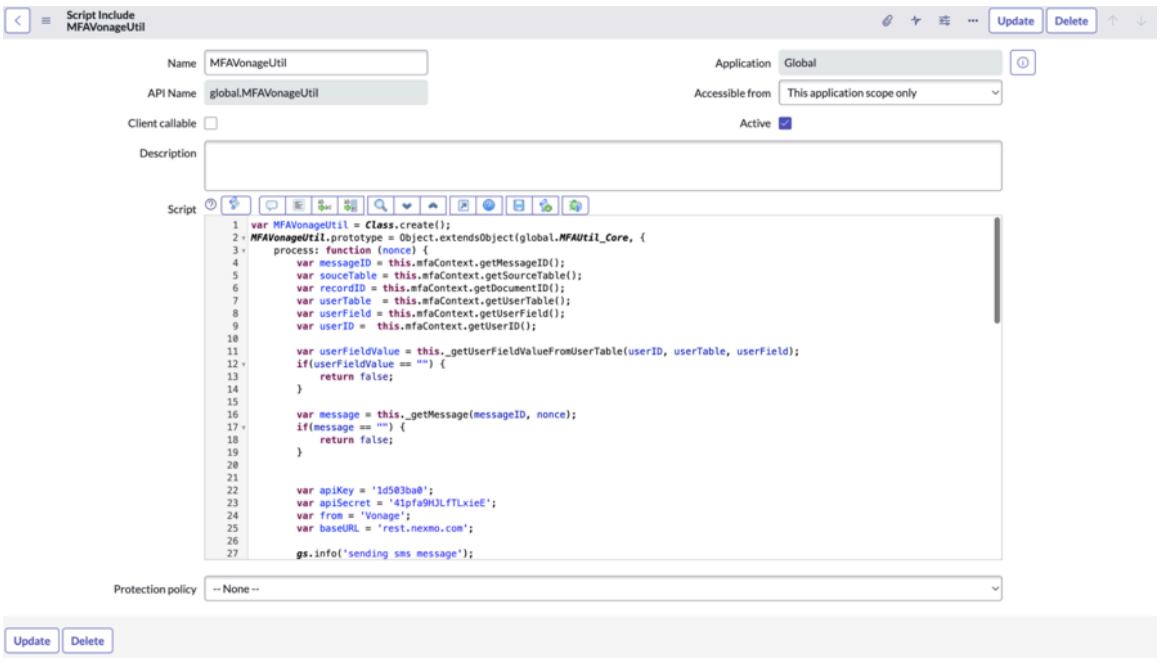
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Aktualisieren Sie den Datensatz.
8. Klicken Sie im Abschnitt „ **Zugehörige Links** “ auf **Variablen automatisch generieren**.
9. Importieren Sie das im Ordner freigegebene SI, und kopieren Sie den apiKey und das Geheimnis aus dem Vonage-API-Dashboard.

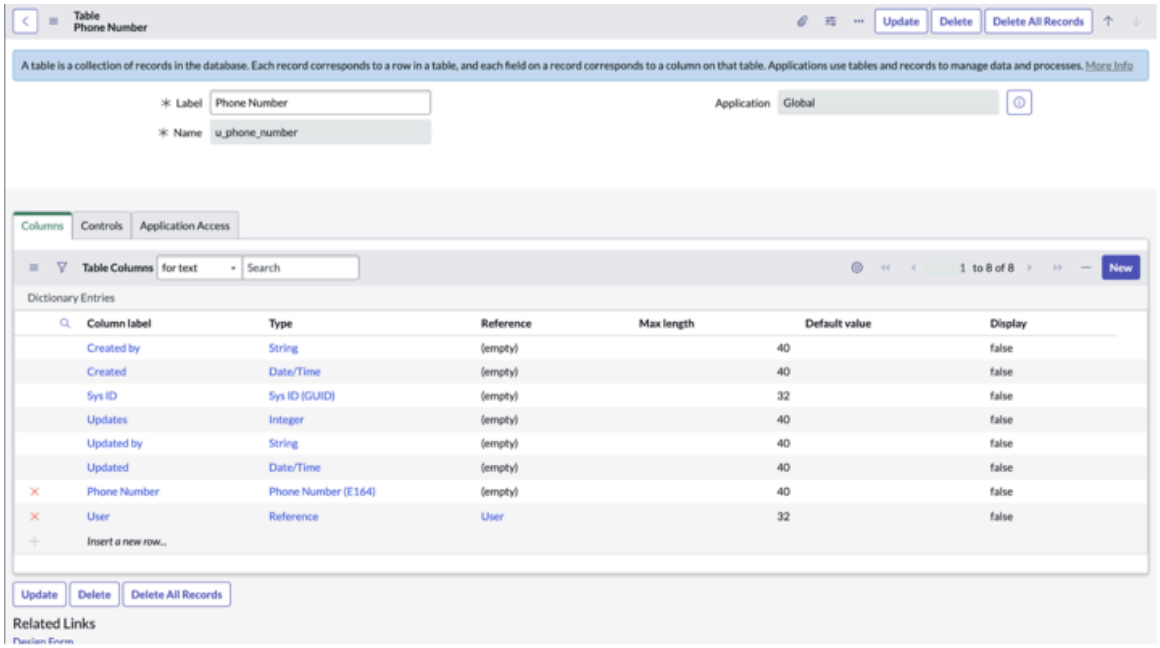
Hinweis:

Den apiKey und das Geheimnis finden Sie in Ihren Vonage-Kontoeinstellungen im Vonage-Dashboard.

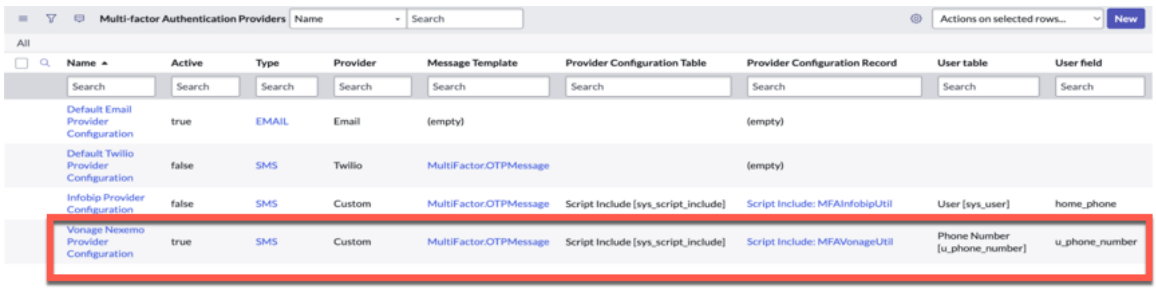


10. Erstellen Sie eine anwenderdefinierte Tabellentelefonnummer mit zwei Spalten. Beispiel:
    - **Spaltenbezeichnung**: Anwender, **Typ**: Referenz, **Referenz**: Anwender (sys_user).
    - **Spaltenbezeichnung**: Telefonnummer, **Typ**: Telefonnummer (E164).

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



11. Erstellen Sie einen anwenderdefinierten Anbieter in der Multifaktor-Anbieter-Tabelle.



Weitere Informationen zur Anbieterkonfiguration finden Sie unter Konfigurieren Sie den MFA-Anbieter.

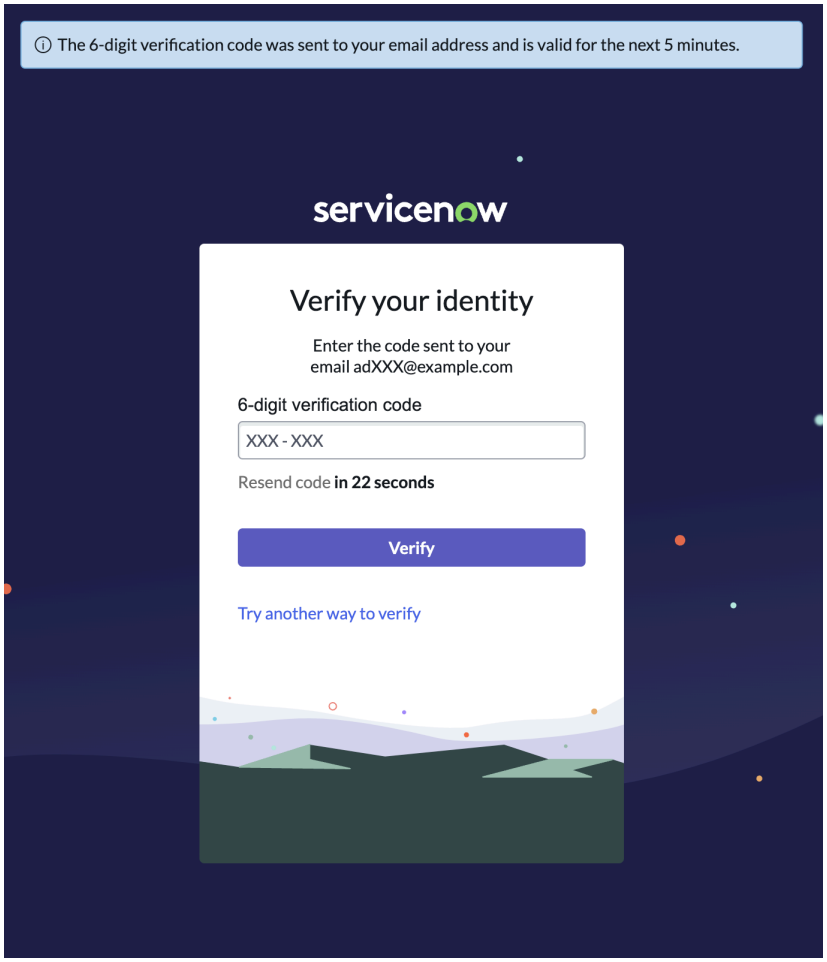
Mehrstufige Authentifizierung mit E-Mail

Multifaktor-Authentifizierung (MFA) mit E-Mail als Faktor für Ihre Authentifizierung.

Administratoren können die Instanz ServiceNow so konfigurieren, dass Benutzer, die versuchen, sich mit E-Mail-basiertem OTP bei der Instanz anzumelden.

Hinweis: MFA mit E-Mail wird standardmäßig mit dem Plugin „Integration – Multifaktor-Authentifizierung“ (`com.snc.integration.multifactor.authentication`) aktiviert. Sie müssen die Richtlinieneingaben und -bedingungen konfigurieren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Wenn Benutzer versuchen, sich bei ServiceNowanzumelden, wird E-Mail-OTP an die zugeordnete E-Mail-Adresse gesendet. Benutzer können den sechsstelligen Verifizierungscode eingeben, der an die E-Mail-Adresse gesendet wurde, und ihre Identität überprüfen.

Konfigurieren Sie E-Mail als MFA-Faktor

Konfigurieren Sie Richtlinieneingabe und -bedingung, um E-Mail-OTP als MFA-Faktorrichtlinie für die Authentifizierung anzuzeigen.

Vorbereitungen

Erforderliche Rolle: admin

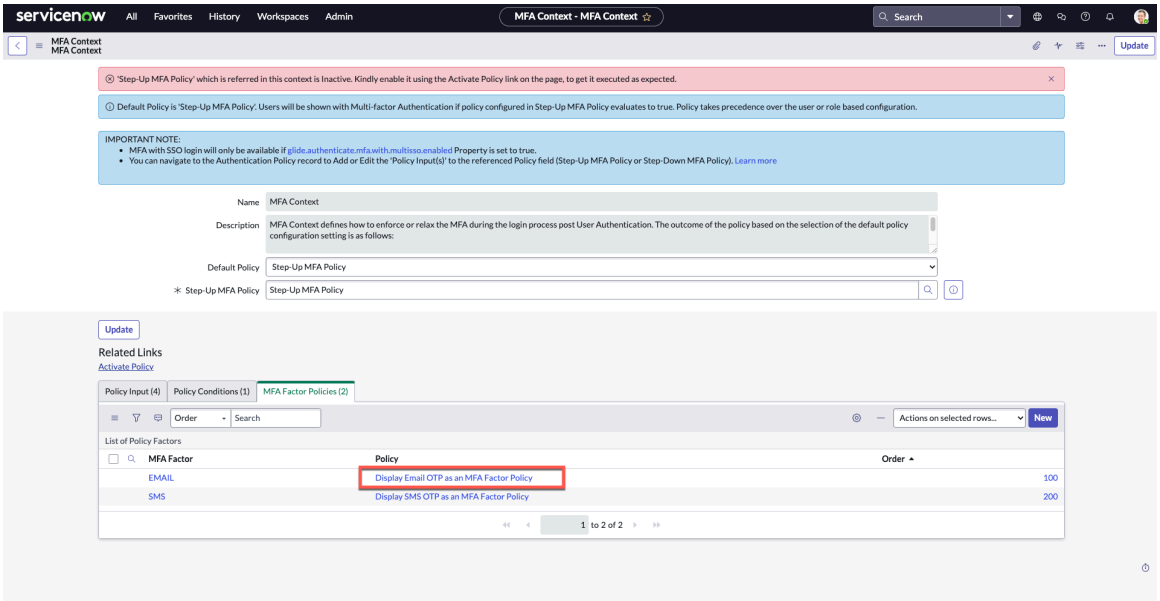
Prozedur

1. Navigieren zu **Alle** > **Multi-Faktor-Authentifizierung** > **MFA-Kontext**an.
2. Klicken Sie auf die Registerkarte Richtlinien für **MFA-Faktor**.

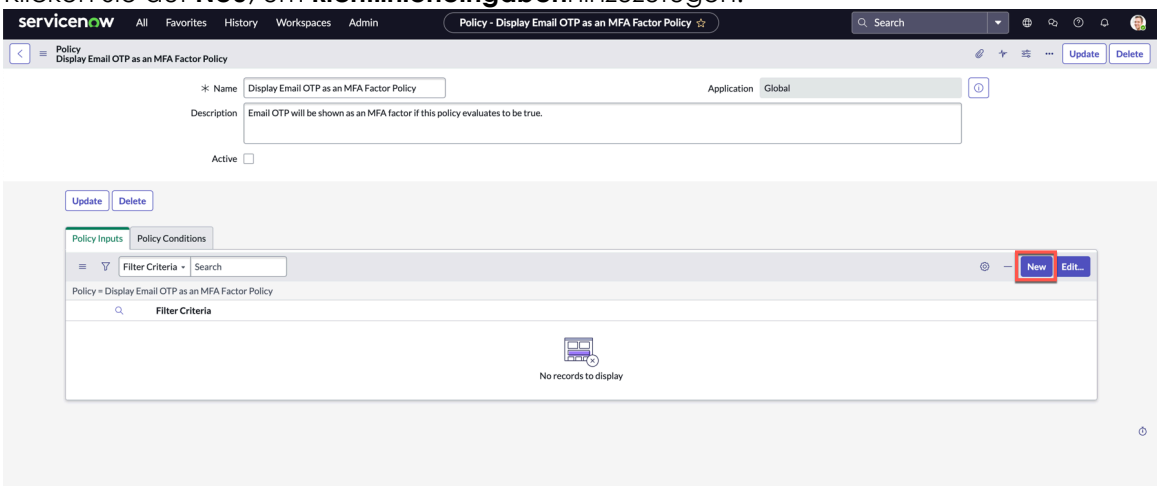
   Hinweis: E- **MAIL** als **MFA-Faktor mit einer Richtlinie** ist standardmäßig verfügbar. Sie können die Richtlinie bearbeiten und die Richtlinieneingaben und -bedingungen angeben.

3. Wählen Sie **E-Mail anzeigen OTP als MFA-Faktorrichtlinie aus**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Klicken Sie auf **Neu**, um **Richtlinieneingaben**hinzuzufügen.

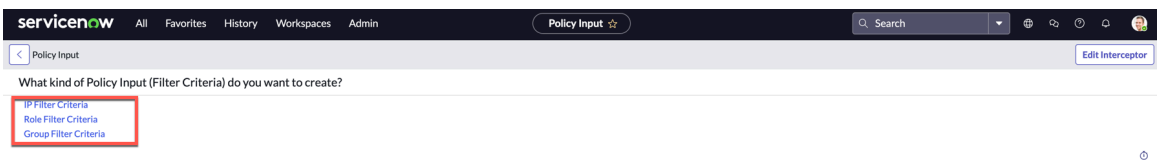


5. Wählen Sie die Filterkriterien aus, die Sie erstellen möchten.

Es folgen die Arten von Filterkriterien:

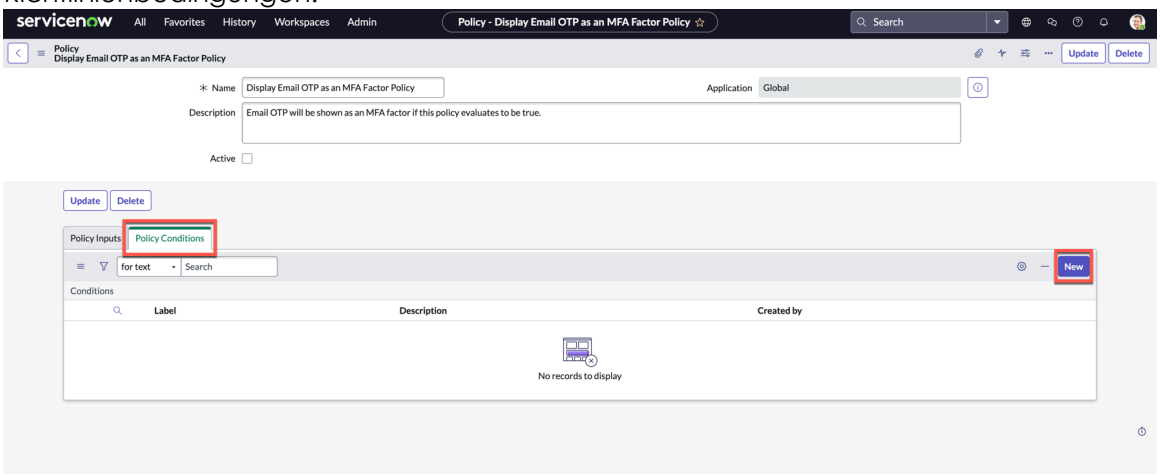
- IP-Filterkriterien
- Rollen-Filterkriterien
- Gruppenfilterkriterien

Beispiel: Rollenfilterkriterien.



© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie auf **Rollenfilterkriterien**, füllen Sie die Felder für die Rollenfilterkriterien aus, und übermitteln Sie den Datensatz. Die neue Richtlinie wird erstellt. Weitere Informationen finden Sie unter Rollenfilterkriterien.
7. Klicken Sie auf der Seite Richtlinie – E-Mail-OTP als MFA-Faktorrichtlinie anzeigen auf Richtlinienbedingungen.



8. Klicken Sie zum Hinzufügen von **Richtlinienbedingungen** auf **Neu**.
9. Füllen Sie die Felder des Formulars aus.

Formular für Bedingungen

Feld	Beschreibung
Bezeichnung	Name zur Identifizierung der Bedingung.
Beschreibung	Beschreibung der Bedingung
Bedingung	Logische Kombination aus mehreren Richtlinieneingaben (Filterkriterien), die zur Auswertung von Authentifizierungsanforderungen verwendet wird. Wählen Sie die rollenbasierte Filterkriterienrichtlinie aus, die für die Bedingung erstellt wurde.

10. Klicken Sie auf **Absenden**.
11. Wahlweise: Wiederholen Sie Schritt 8, um zusätzliche Richtlinienbedingungen zu erstellen.

> **Hinweis:** Wenn Sie mehrere Richtlinienbedingungen erstellen, hängt die endgültige Ausgabe der Zugriffsrichtlinie von der logischen ODER-Ausgabe aller Richtlinienbedingungen ab. Dies bedeutet, dass die Richtlinie als „true“ ausgewertet wird, wenn eine Ihrer Richtlinienbedingungen erfüllt ist.

Abhängig von der Rollenfilterrichtlinie (Benutzer) und den für die Rolle angegebenen Bedingungen wird der Faktor „E-Mail-MFA“ als Option für die Authentifizierung für die Benutzer angezeigt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setzen Sie die Multifaktor-Authentifizierung (MFA) für Anwender zurück

Administratoren können MFA für Anwender zurücksetzen, die die App gelöscht, den Zugriff auf das Gerät verloren haben oder ihrem Gerät keine alternative MFA zugeordnet haben.

Vorbereitungen

Erforderliche Rolle: admin

Das folgende Verfahren beschreibt, wie ein ServiceNow® -Administrator die MFA-Validierung zurücksetzen kann, um Anwender zu entsperren und ihnen die erneute Registrierung von MFA zu ermöglichen.

Prozedur

1. Navigieren zu **Alle** > **Multi-Faktor-Authentifizierung** > **Mehrstufige Anwendereinrichtung**an.
2. Suchen Sie in der Benutzertabelle nach dem Anwender, den Sie entsperren möchten.
3. Legen Sie Validieren auf den Wert **false**fest.
4. Navigieren zu **Alle** > **Multi-Faktor-Authentifizierung** > **Aktuelle Anwenderfaktoren des Anwenders**an.
5. Suchen Sie nach dem gleichen Anwender.
6. Legen Sie „Ist aktueller Faktor“ für den MFA-Typ, den Sie für den Anwender zurücksetzen möchten, auf „ **falsch** “ fest.
   Wenn Sie den Wert in „ **false** “ ändern, wird der Anwender entsperrt und kann MFA erneut registrieren.
   Wenn der entsperrte Benutzer die Anmeldeinformationen eingibt und sich anmeldet, wird die Seite **Multifaktor-Authentifizierung (MFA)** aktivieren angezeigt. Der Benutzer kann die Schritte auf der Seite ausführen, um MFA erneut zu registrieren.

Referenzthema – Multifaktor-Authentifizierung

Referenzthema zur Konfiguration der Multifaktor-Authentifizierung.

Multifaktor-Authentifizierung für Anwender

Um auf die Details zur Multifaktor-Authentifizierung des Benutzers zuzugreifen, navigieren Sie zu **Alle** > **Multi-Faktor-Authentifizierung** > **Mehrstufige Anwendereinrichtung**an.

Multifaktor-Authentifizierung für Anwender

Feld	Beschreibung
Anwender	Der Anwendername des Anwenders
Verbleibende Umgehungen	Die Gesamtzahl der für den Anwender verbleibenden Umgehungen.
Multifaktor-Geheimnis	Die Details des Multifaktor-Geheimnisses.
Überprüft	Ist der Multifaktor validiert. Wenn Sie den Wert in „ **falsch** “ ändern, wird das vorhandene Setup der Authentifikator-App ungültig.

Hinweis: Die zuletzt von den Benutzern verwendeten MFA-Faktoren sind im Modul Zuletzt verwendete Faktoren des Benutzers verfügbar. Navigieren zu **Alle** > **Multi-Faktor-Authentifizierung** > **Aktuelle Anwenderfaktoren des Anwenders**an. Weitere Informationen finden Sie unter Zuletzt verwendete Faktoren des Anwenders.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mehrstufige Browser-Fingerabdrücke

Um auf die Details zu den Browser-Fingerabdrücken des Benutzers zuzugreifen, navigieren Sie zu **Alle** > **Multi-Faktor-Authentifizierung** > **Mehrstufige Browser-Fingerabdrücke**an.

Mehrstufige Browser-Fingerabdrücke

Feld	Beschreibung
Anwender	Der Anwendername des Anwenders
Browser	Der vom Anwender verwendete Browser.
Browser-Fingerabdruck	Details des Browser-Fingerabdrucks
Cookie des Browser-Fingerabdrucks	Die Cookie-Details des Browser-Fingerabdrucks.
Ablauf des Browser-Fingerabdruckcookies	Details zum Ablauf des Browser-Fingerabdruckcookies.

Zuletzt verwendete Faktoren des Anwenders

Um auf die Details zu den zuletzt verwendeten Faktoren des Benutzers zuzugreifen, navigieren Sie zu **Alle** > **Multi-Faktor-Authentifizierung** > **Aktuelle Anwenderfaktoren des Anwenders**an.

Multifaktor-Setups für Anwender

Feld	Beschreibung
Anwender	Der Anwendername des Anwenders
Multifaktor-Typ	Der vom Anwender für die Anmeldung verwendete Multifaktor-Typ.
Ist aktueller Faktor	Die neuesten Multifaktor-Details des Anwenders.

Multifaktor-Authentifizierung (MFA) verwenden

Erfahren Sie, wie Sie mit Tools der Multifaktor-Authentifizierung sicher auf Ihre Instanz zugreifen.

Melden Sie sich mit MFA an

ServiceNow erfordert Authentifikatoranwendungen, die zeitbasierte Einmalpasswörter (Time-based One-time Passwords, TOTP) unterstützen. ServiceNow testet MFA mit den folgenden Authentifikatoren:

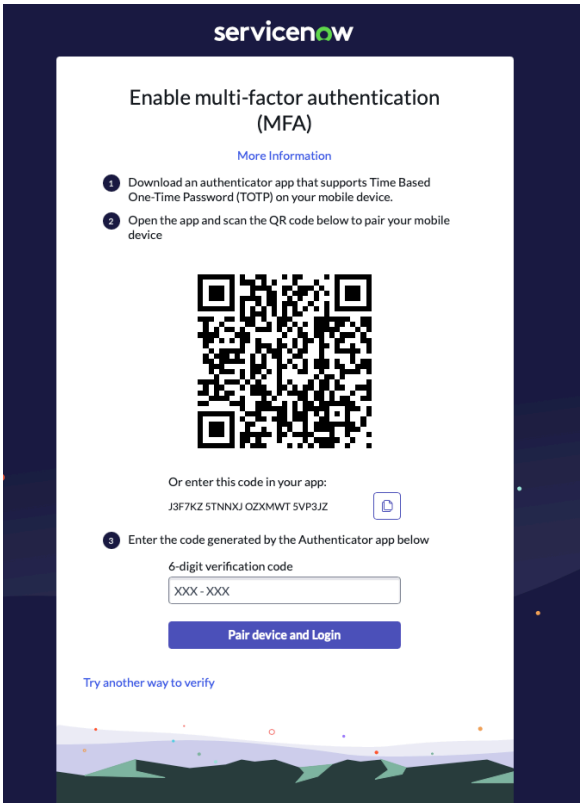
- Google Authentifikator
- Microsoft Authentifikator
- LastPass-Authentifikator
- Autorisieren
- FreeOTP
- duo
- Okta Überprüfen Sie

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Andere, nicht aufgeführte Authentifikatoren sind möglicherweise auch kompatibel, werden jedoch nicht von ServiceNowgetestet.
- Informationen zu browserspezifischen Verhaltensänderungen finden Sie in diesem KB-Artikel

Validierung mit Authentifikator-App



Geben Sie den Code ein, der in Ihrer Authentifikator-App angezeigt wird, um sich anzumelden.

Wenn Ihr Administrator die Multifaktor-Authentifizierung (MFA) für Ihre Instanz aktiviert hat, werden Sie nach Eingabe Ihres Anwendernamens und Passworts zu einer zweiten Authentifizierung aufgefordert. Weitere Informationen zum MFA-Anmeldevorgang finden Sie unter Melden Sie sich mit der Multifaktor-Authentifizierung an

Wenn Sie keine zweite Form der Authentifizierung konfiguriert haben, wird nach der Anmeldung eine Konfigurationsseite angezeigt, die Sie durch den Prozess der Einrichtung einer Authentifizierungs-App führt. Weitere Informationen zu diesem Setup finden Sie unter Richten Sie die Multifaktor-Authentifizierung zum ersten Mal ein.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registrieren Sie ein Authentifizierungsgerät

Nachdem Sie eine Authentifizierungs-App konfiguriert haben, können Sie andere Methoden für die Authentifizierung registrieren.

Biometrische Authentifikatoren

Sie können biometrische Authentifikatoren wie Fingerabdruck- oder Gesichtserkennung als zweite MFA-Authentifizierung verwenden. Wenn Ihr Administrator diese Option zulässt, können Sie mithilfe der Schritte in Registrieren Sie einen biometrischen Authentifikatorbiometrische Authentifikatoren konfigurieren.



Hardwareschlüssel-Authentifikatoren

Hardwareschlüssel sind physische Sicherheitsgeräte, die Sie für die Authentifizierung verwenden können. Sie können ein Hardwaregerät für die Verwendung mit Ihrer Instanz von registrieren, indem Sie die Schritte in Registrieren Sie einen Hardware-Sicherheitsschlüsselausführen .

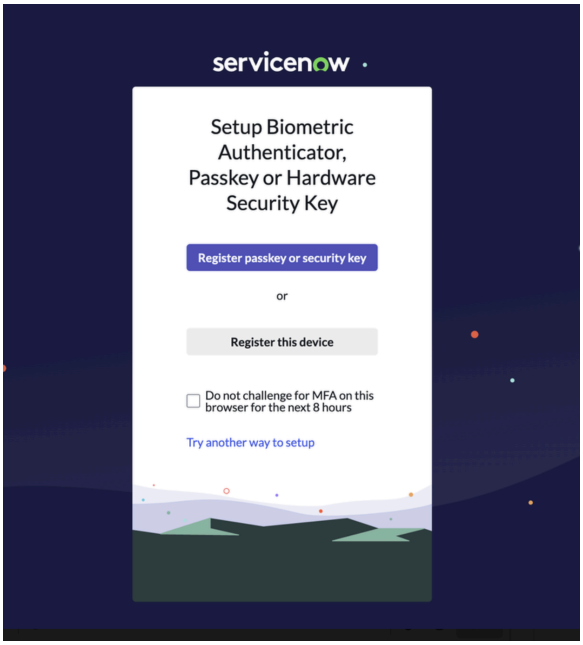


Validierung mit Biometrie oder Hardwareschlüssel

Melden Sie sich mit dem Biometrie- oder Sicherheitsschlüssel an.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

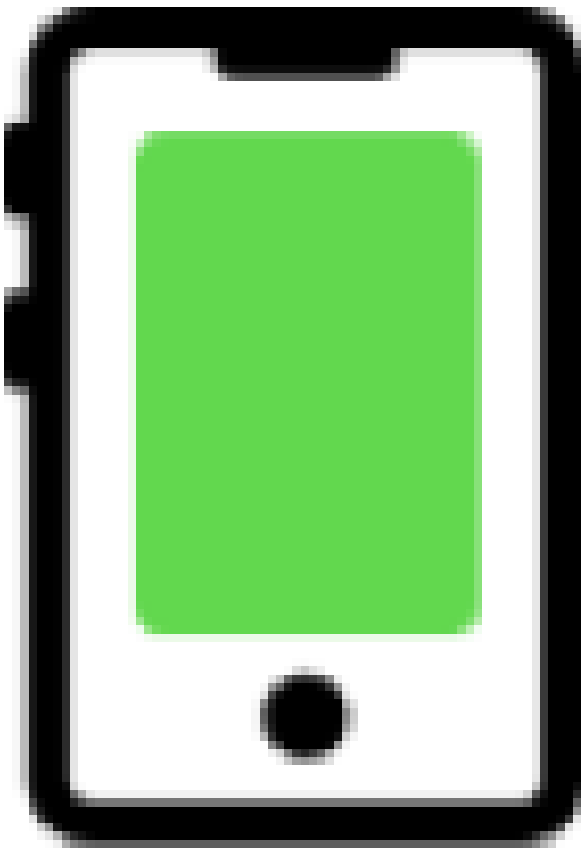


Registrieren Sie eine Telefonnummer für OTP

SMS

Der Administrator konfiguriert die Instanz ServiceNow so, dass Anwender, die versuchen, sich mit SMS-basiertem OTP bei der Instanz anzumelden.

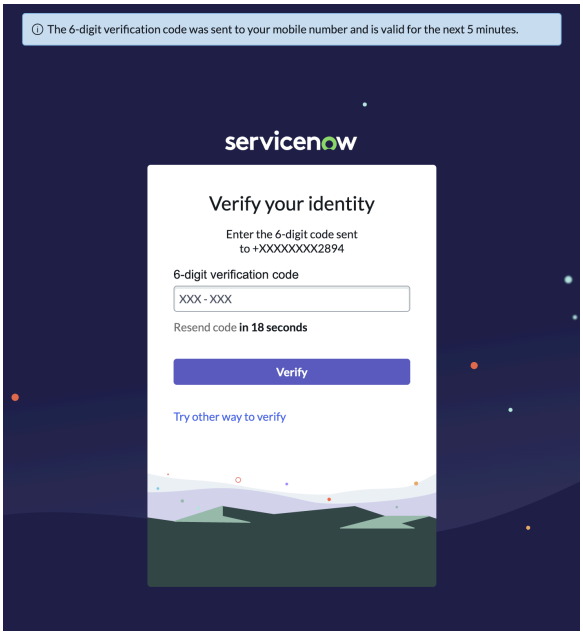
Wenn Benutzer versuchen, sich bei ServiceNowanzumelden, wird die SMS-OTP an die Mobiltelefonnummer gesendet, die dem Datensatz „sys_user“ zugeordnet ist. Benutzer können den sechsstelligen Verifizierungscode eingeben, der an das Mobilgerät gesendet wurde, und ihre Identität überprüfen.



Validierung mit SMS

Geben Sie den 6-stelligen Code ein, der an die Mobiltelefonnummer gesendet wurde, um sich anzumelden. Der gesendete Code ist für die nächsten 5 Minuten gültig. Sie

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



können „Code erneut senden“ verwenden, um den Code erneut zu senden.

Registrieren Sie eine E-Mail-Adresse für OTP

E-Mail-Adresse

Der Administrator konfiguriert die Instanz ServiceNow so, dass Benutzer, die versuchen, sich mit E-Mail-basiertem OTP bei der Instanz anzumelden.

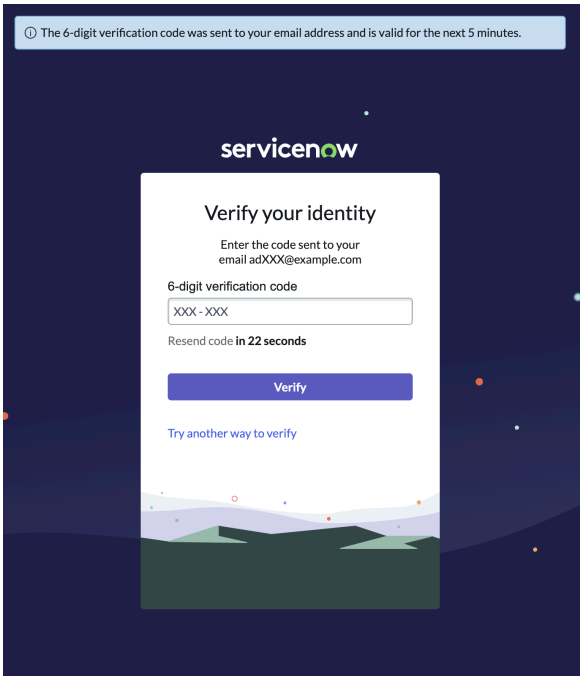
Wenn Benutzer versuchen, sich bei ServiceNowanzumelden, wird die E-Mail-OTP an die E-Mail-Adresse gesendet, die dem Benutzer zugeordnet ist. Benutzer von können den sechsstelligen Verifizierungscode eingeben, der an das Mobilgerät gesendet wurde, und ihre Identität überprüfen.



Validierung per E-Mail

Geben Sie den sechsstelligen Code ein, der an die E-Mail-Adresse gesendet wurde, um sich anzumelden. Der gesendete Code ist für die nächsten 5 Minuten gültig. Sie können „Code erneut senden“ verwenden, um den Code erneut zu senden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Richten Sie die Multifaktor-Authentifizierung zum ersten Mal ein

Wenn Ihr Administrator die Multifaktor-Authentifizierung in Ihrem Profil aktiviert hat, Sie die Anwendung jedoch noch nicht eingerichtet haben, können Sie sie bei der Anmeldung einrichten.

Vorbereitungen

Erforderliche Rolle: keine

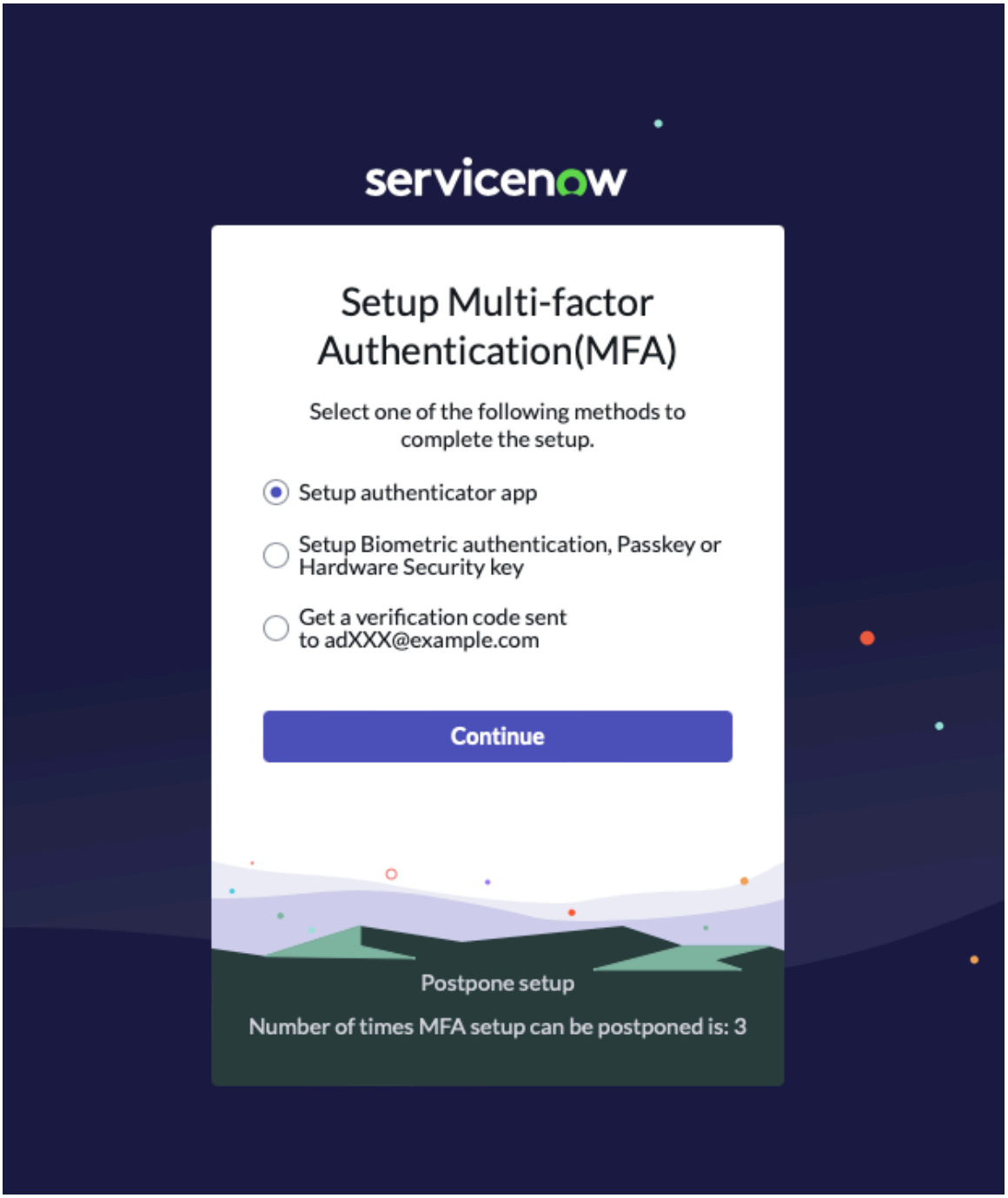
Prozedur

1. Melden Sie sich mit Ihrem Anwendernamen und Passwort bei Ihrer -Instanz an.

   Der Einrichtungsbildschirm für die Multifaktor-Authentifizierung fängt Ihre Anmeldung ab.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



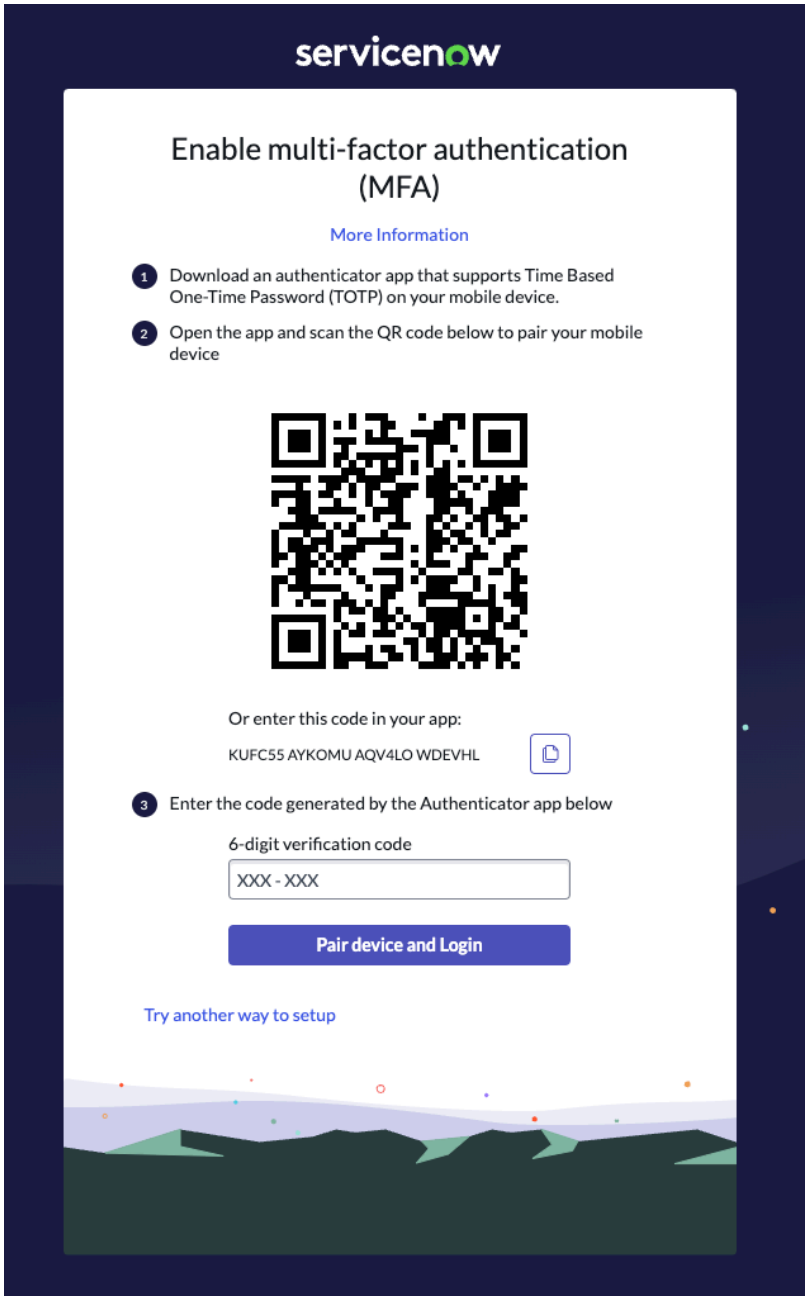
Hinweis: Wenn Sie die jetzt eingerichtete Authentifizierung überspringen möchten, klicken Sie auf **Setup umgehen**. Sie können die Multifaktor-Authentifizierung für eine begrenzte Anzahl von Malen umgehen, die Ihr Administrator zulässt. Schließlich müssen Sie die Multifaktor-Authentifizierung konfigurieren.

2. Wählen Sie eine der folgenden Methoden aus, um das MFA-Setup abzuschließen.

a. Authentifikator-App einrichten

Befolgen Sie die Anweisungen auf dem Bildschirm, um das Gerät zu koppeln und sich anzumelden.

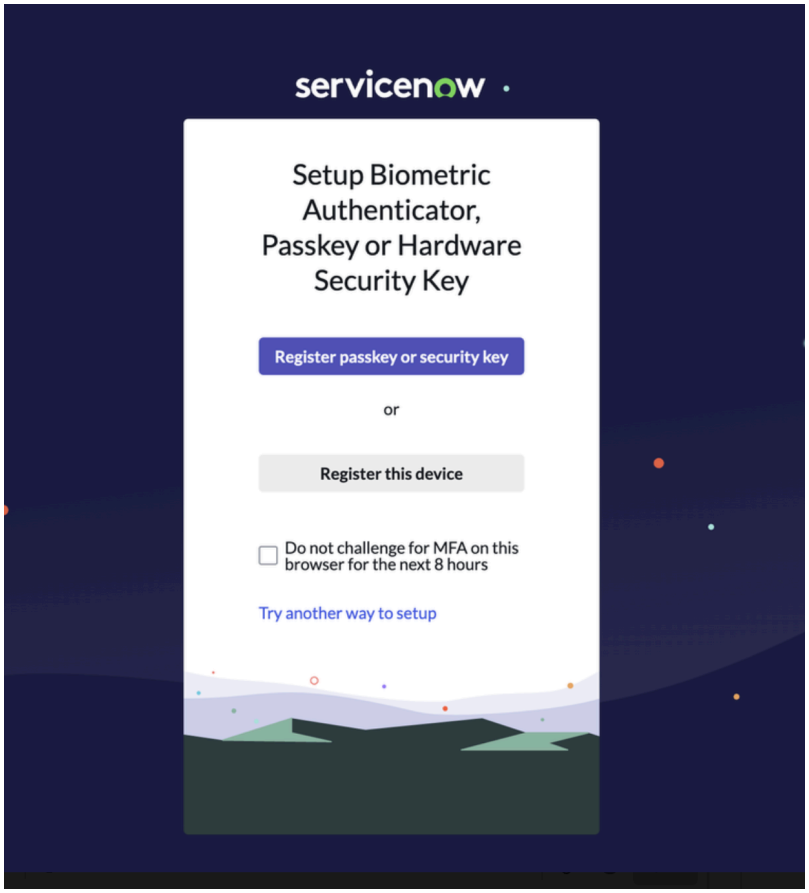
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



b. Biometrischen Authentifikator, Passkey oder Hardware-Sicherheitsschlüssel einrichten

Wählen Sie eine der Optionen aus, um das Setup abzuschließen.

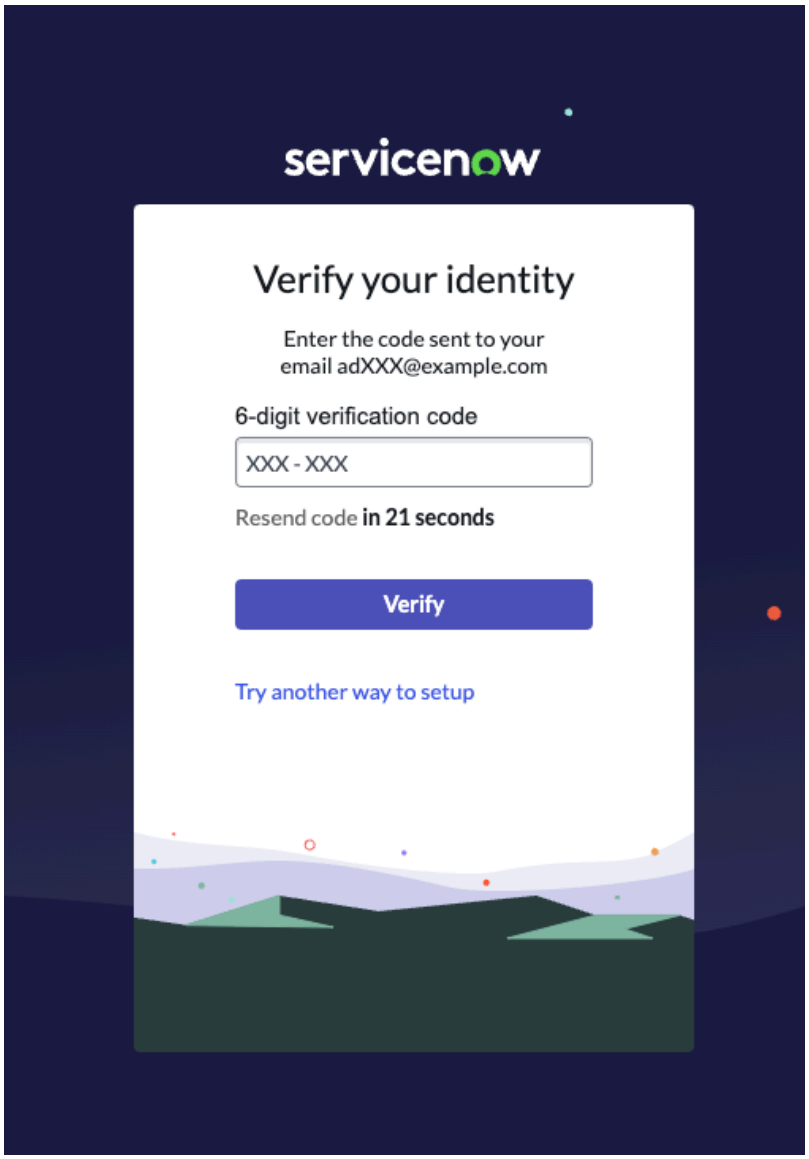
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



c. Lassen Sie sich einen Verifizierungscode per E-Mail zusenden

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geben Sie den Verifizierungscode ein, der per E-Mail gesendet wurde.



Nach erfolgreichem Abschluss einer der Setups werden Sie bei der Instanz angemeldet.

Richten Sie die Multifaktor-Authentifizierung für Ihr Anwenderprofil ein

Aktivieren Sie in den Anwenderprofileinstellungen die Multifaktor-Authentifizierung für Ihren Account.

Vorbereitungen
Erforderliche Rolle: keine

In Ihrer Instanz muss die Multifaktor-Authentifizierung aktiviert sein.

Hinweis: Ihr Administrator kann von Ihnen die Verwendung der Multifaktor-Authentifizierung verlangen. In diesem Fall werden Sie beim Anmelden automatisch dazu aufgefordert. Weitere Informationen finden Sie unter Richten Sie die Multifaktor-Authentifizierung zum ersten Mal ein. Führen Sie das folgende Verfahren aus, wenn Ihr Administrator Ihnen erlaubt, die Multifaktor-Authentifizierung zu aktivieren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

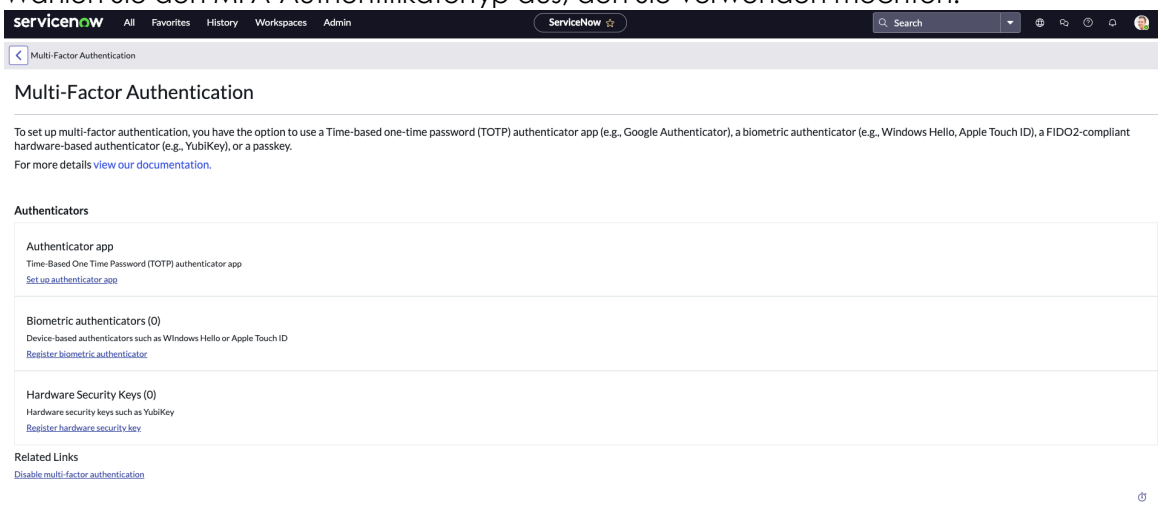
Prozedur

1. Navigieren zu **Alle** > **Self-Service** > **Mein Profil**an.

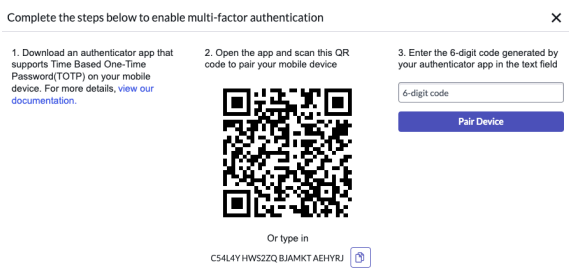
   Hinweis: Sie können Ihr Profil auch aufrufen, indem Sie im Header der Instanz auf Ihren Anwendernamen klicken.

2. Klicken Sie in Ihrem Anwenderprofil im Abschnitt „ **Zugehörige Links** “ auf **Multifaktor-Authentifizierung**.

3. Wählen Sie den MFA-Authentifikatortyp aus, den Sie verwenden möchten.

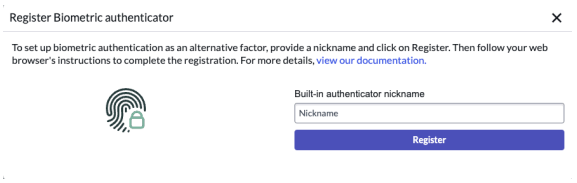
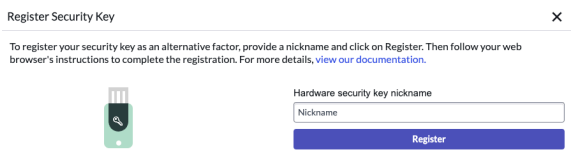


MFA-Authentifikatoren

MFA-Authentifikatoren	Beschreibung
Authentifikator-App	Authentifikator-App auf Basis eines zeitbasierten Einmalpassworts (TOTP) Wählen **Sie Authentifikator-App einrichten**, und befolgen Sie die Anweisungen auf dem Bildschirm, um sich für eine Authentifikator-App als zweiten Faktor für die Authentifizierung zu registrieren. 
Biometrische Authentifikatoren	Gerätebasierte Authentifikatoren wie Windows Hello oder Apple Touch ID Wählen Sie **Biometrische Authentifizierung** registrieren aus, und befolgen Sie die Anweisungen auf dem Bildschirm, um sich für eine Authentifikator-App als

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MFA-Authentifikatoren	Beschreibung
	zweiten Faktor für die Authentifizierung zu registrieren. 
Hardware-Sicherheitsschlüssel	Hardware-Sicherheitsschlüssel wie YubiKey Wählen Sie **Hardware-Sicherheitsschlüssel** registrieren aus, und befolgen Sie die Anweisungen auf dem Bildschirm, um sich für eine Authentifikator-App als zweiten Faktor für die Authentifizierung zu registrieren. 

Ergebnisse

Für Ihren Anwenderaccount ist die Multifaktor-Authentifizierung aktiviert. Sie werden aufgefordert, bei der nächsten Anmeldung die Multifaktor-Authentifizierung zu verwenden.

Hinweis: Sie können die Multifaktor-Authentifizierung für Ihren Account nicht deaktivieren, nachdem Sie sie aktiviert haben. Wenn Sie die Multifaktor-Authentifizierung deaktivieren müssen, wenden Sie sich an Ihren Administrator.

Melden Sie sich mit der Multifaktor-Authentifizierung an

Melden Sie sich mit der Multifaktor-Authentifizierung an, wenn sie von Ihrem Administrator in Ihrer Instanz aktiviert wurde.

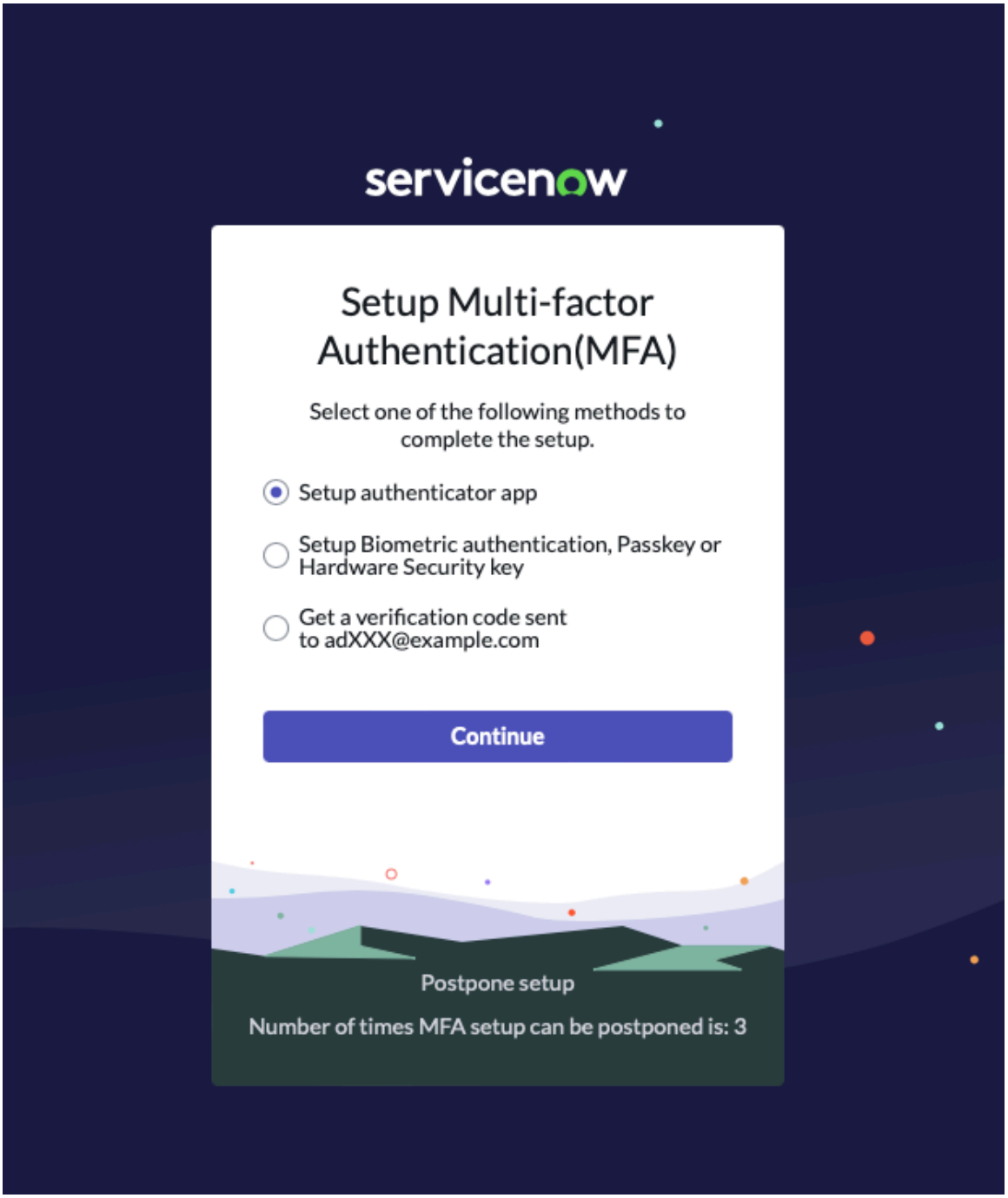
Vorbereitungen

Für Ihr Profil muss die Multifaktor-Authentifizierung aktiviert sein. Sie können sie selbst in Ihrem Anwenderprofil aktivieren, oder Ihr Administrator kann sie für Sie aktivieren.
Erforderliche Rolle: keine

Prozedur

1. Wechseln Sie zur URL Ihrer Instanz, um den Anmeldebildschirm zu öffnen.
2. Geben Sie Ihren Anwendernamen und Ihr Passwort ein.
3. Klicken Sie auf **Anmelden**.
   Der Bildschirm für die Multifaktor-Authentifizierung wird angezeigt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wählen Sie eine der Methoden aus, um das MFA-Setup abzuschließen.
   Weitere Informationen zu den einzelnen Setups finden Sie unter Richten Sie die Multifaktor-Authentifizierung zum ersten Mal ein.

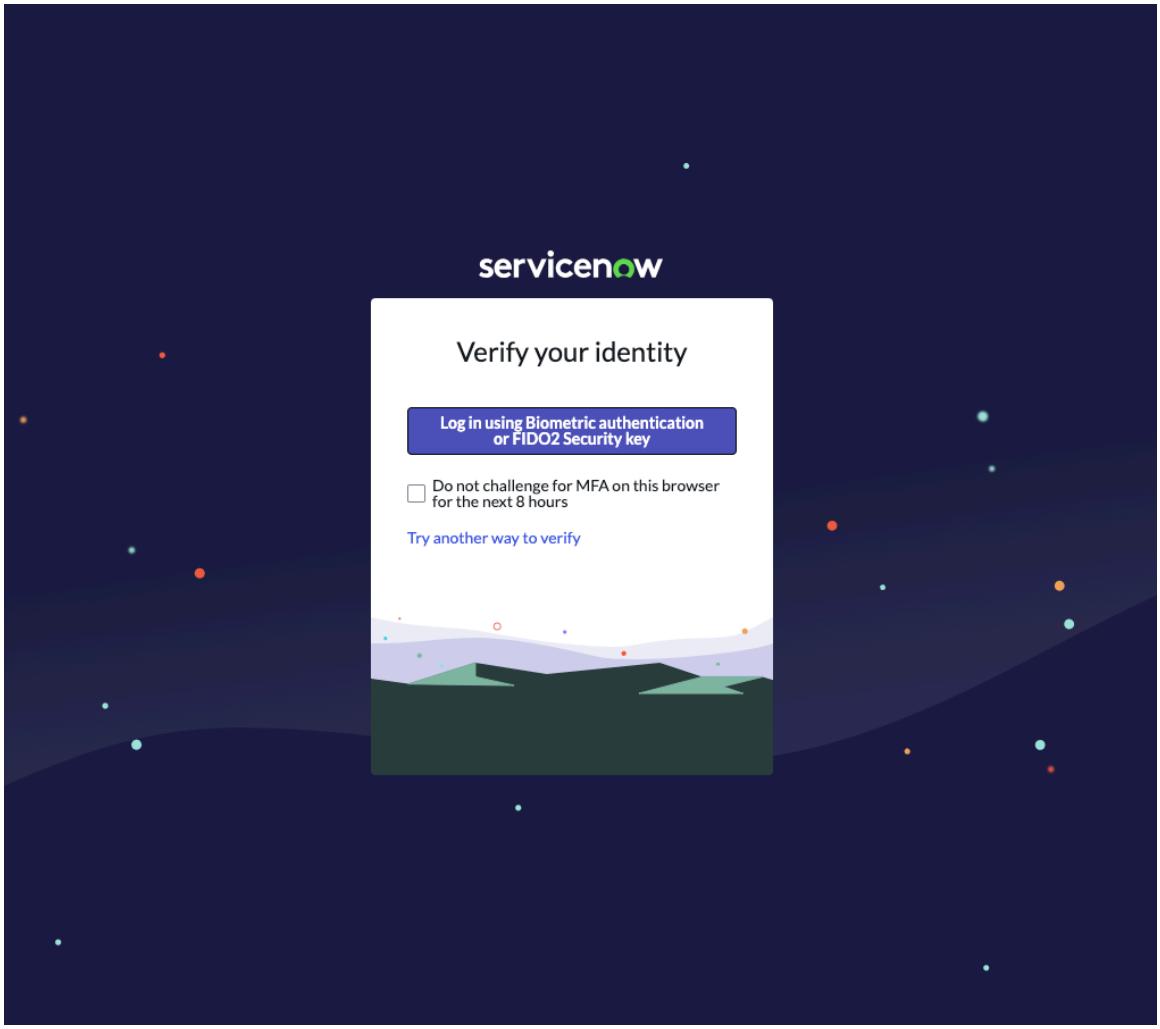
   Wenn Sie das Setup verschieben möchten, wählen Sie **Setup verschieben**aus. Die maximale Anzahl, wie oft Sie das Setup zurückstellen können, wird auf dem Bildschirm angezeigt und dieser Wert wird von Ihrem Administrator konfiguriert.

Ergebnisse
Wenn Sie MFA bereits eingerichtet haben, wird der zuletzt verwendete Faktor angezeigt, wenn Sie sich nach Eingabe Ihres Anwendernamens und Passworts bei Ihrer Instanz anmelden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Example: Zuletzt verwendeter MFA-Faktor

Wenn der zuletzt verwendete Faktor die biometrische Anmeldung war, wird bei der Anmeldung mit Ihrem Anwendernamen und Passwort Ihr direkt mit dem Setup-Bildschirm für die biometrische MFA angezeigt.



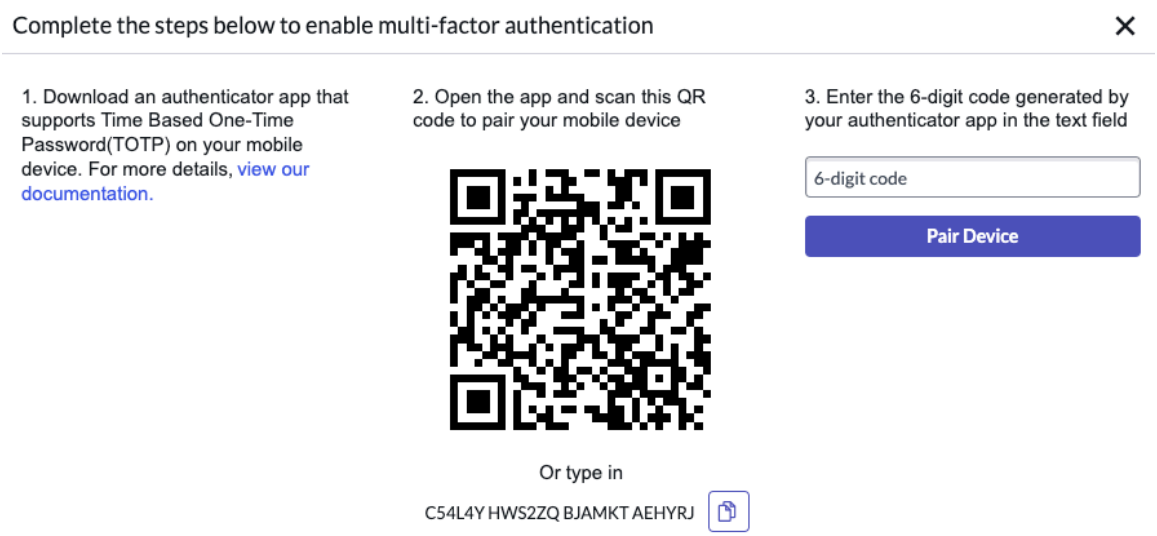
Authentifikatoranwendungen

Verwenden Sie Authentifikatoranwendungen von Drittparteien, um temporäre MFA-Passcodes zu generieren.

Eine Authentifikatoranwendung ist eine Drittanbietersoftware, die temporäre Passcodes generiert. Sie können diese Passcodes zusammen mit Ihrem Passwort verwenden, um sich bei einer Instanz anzumelden, die eine Multifaktor-Authentifizierung (MFA) erfordert.

Wenn Ihr Administrator die MFA für Ihre Instanz aktiviert hat, wird nach der Eingabe von Anwender und Passwort bei der Anmeldung eine Eingabeaufforderung für einen Passcode angezeigt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



ServiceNow erfordert Authentifikatoranwendungen, die zeitbasierte Einmalpasswörter (Time-based One-time Passwords, TOTP) unterstützen.

ServiceNow testet MFA mit den folgenden Authentifikatoren:

- Google Authentifikator
- Microsoft Authentifikator
- LastPass-Authentifikator
- Autorisieren
- FreeOTP
- duo
- Okta Überprüfen Sie

Hinweis: Andere, nicht aufgeführte Authentifikatoren sind möglicherweise auch kompatibel, werden jedoch nicht von ServiceNowgetestet.

Authentifikator-App ändern

Generieren Sie einen neuen Code, um die Authentifikator-App auf Ihrem Gerät zu ändern.

Vorbereitungen

Für Ihr Profil muss die Multifaktor-Authentifizierung aktiviert sein. Sie können sie selbst in Ihrem Anwenderprofil aktivieren, oder Ihr Administrator kann sie für Sie aktivieren.
Erforderliche Rolle: keine

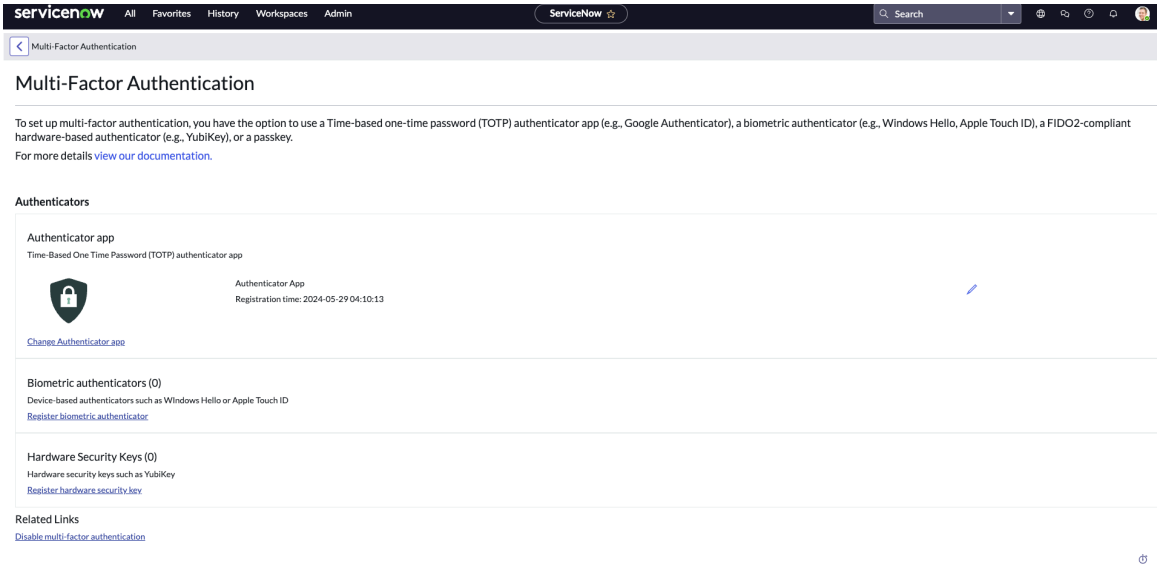
Prozedur

1. Navigieren zu **Alle** > **Self-Service** > **Mein Profil**an.

   Hinweis: Sie können Ihr Profil auch aufrufen, indem Sie im Header der Instanz auf Ihren Anwendernamen klicken.

2. Klicken Sie in Ihrem Anwenderprofil im Abschnitt „ **Zugehörige Links** “ auf **Muti-Faktor-Authentifizierung**.
3. Wählen Sie unter **Authentifikator-App**das Bearbeitungssymbol.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Klicken Sie im Fenster Authentifikatorcode ändern auf **Ändern**.
5. Folgen Sie den Anweisungen auf dem Bildschirm, um die Authentifikator-App auf dem Gerät zu registrieren.

Webauthentifizierung

Ihre Benutzer können Hardwareschlüssel oder die biometrischen Lesegeräte (FIDO2) ihres Geräts verwenden, um sich bei einer Instanz zu authentifizieren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hardwareschlüssel



Hardwareschlüssel sind physische Hardware, die Sie zur Authentifizierung verwenden können. Hardwareschlüssel werden zur Authentifizierung in einen Port Ihres Geräts eingefügt. Weitere Informationen zur Registrierung von Hardwareschlüsseln finden Sie unter Registrieren Sie einen Hardware-Sicherheitsschlüssel.

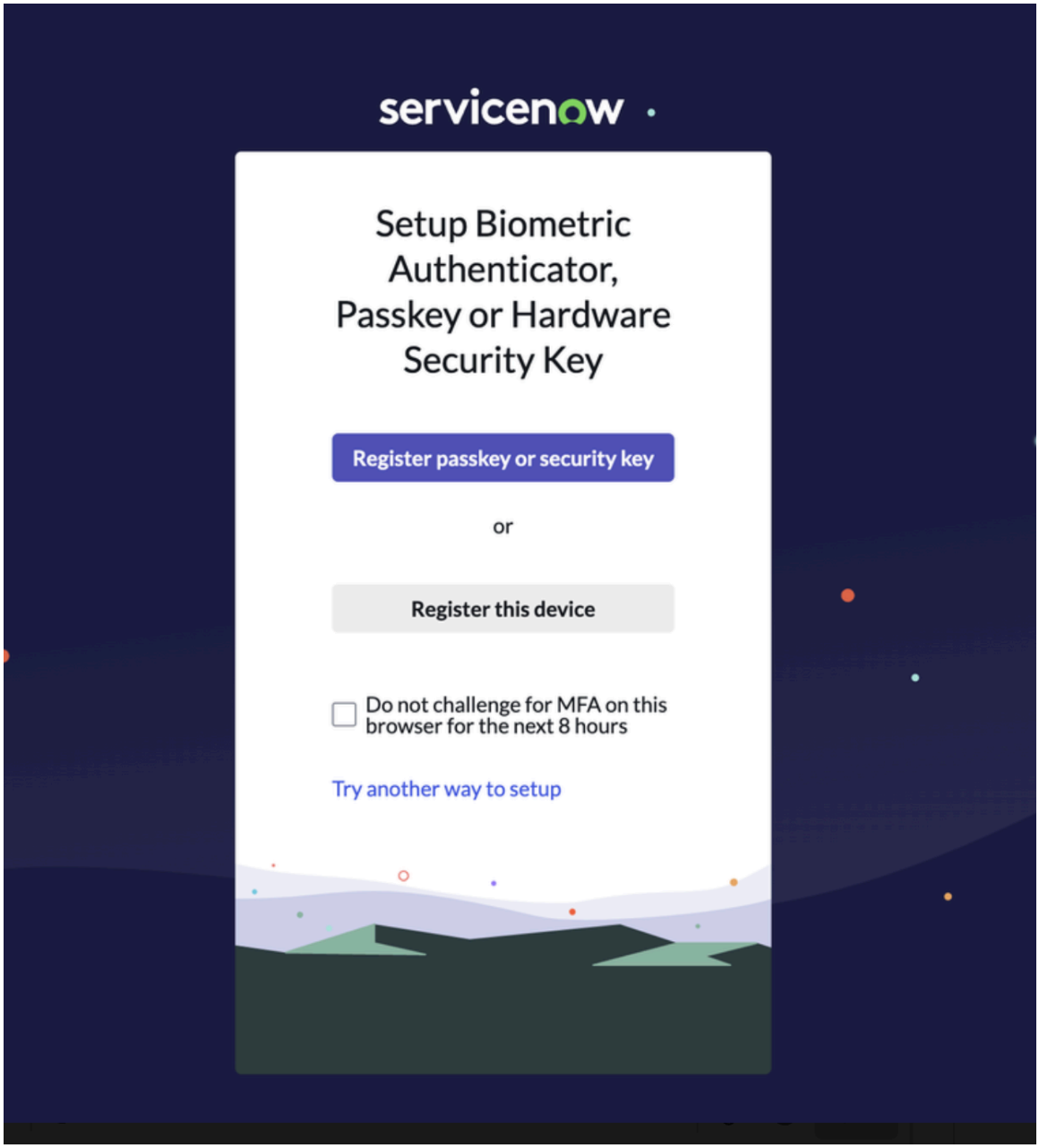
Biometrie



Biometrische Authentifikatoren verwenden Fingerabdruck- oder Gesichtserkennung, um Benutzer zu identifizieren. Ihre Anwender können diese Authentifikatoren auf ihren Geräten als Teil des Multifaktor-Anmeldevorgangs verwenden. Weitere Informationen zur Registrierung biometrischer Authentifikatoren finden Sie unter Registrieren Sie einen biometrischen Authentifikator.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wählen Sie den zweiten Faktor aus, den Sie authentifizieren möchten, und authentifizieren Sie ihn bei Ihrer Instanz.



Informationen zum Konfigurieren des Webauthentifizierungs-Plugins finden Sie unter .

Registrieren Sie einen biometrischen Authentifikator

Registrieren Sie einen biometrischen Authentifikator, der als Teil Ihrer Anmeldung mit Multifaktor-Authentifizierung verwendet werden soll.

Vorbereitungen

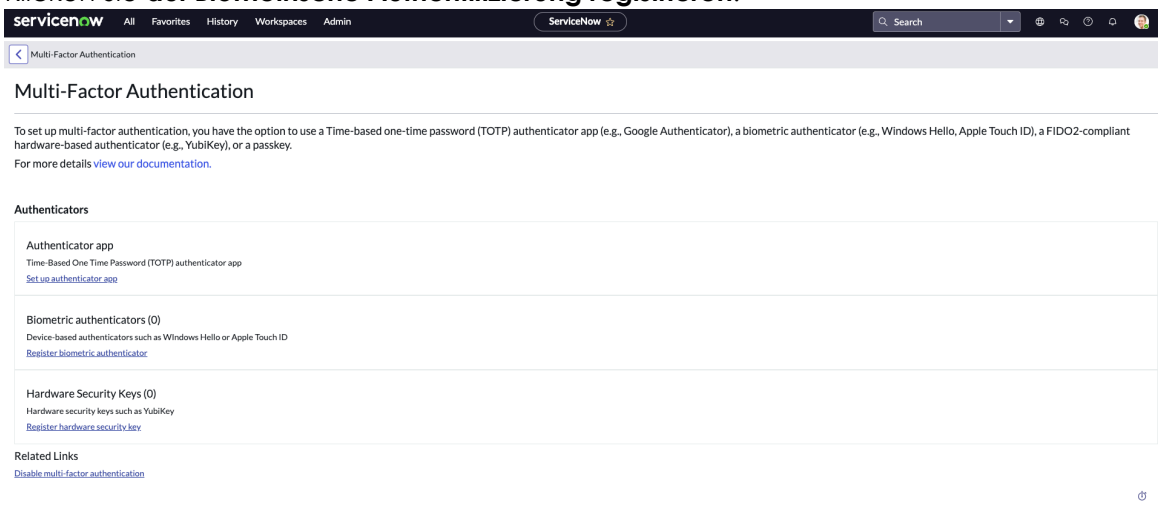
Erforderliche Rolle: keine

Prozedur

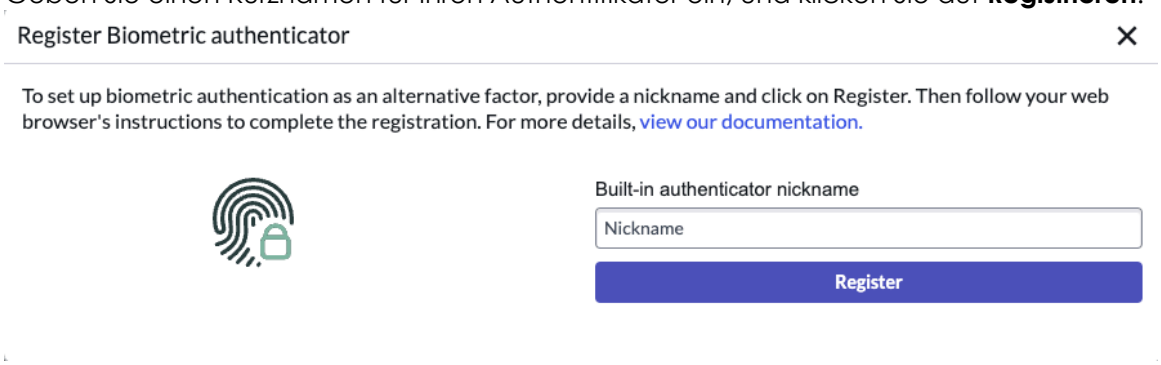
1. Navigieren zu **Alle** > **Self-Service** > **Mein Profil**an.
2. Klicken Sie unter **Zugehörige Links**auf **Multifaktor-Authentifizierung**.
   Die Seite der Multifaktor-Authentifizierung wird geöffnet.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie **auf Biometrische Authentifizierung registrieren**.

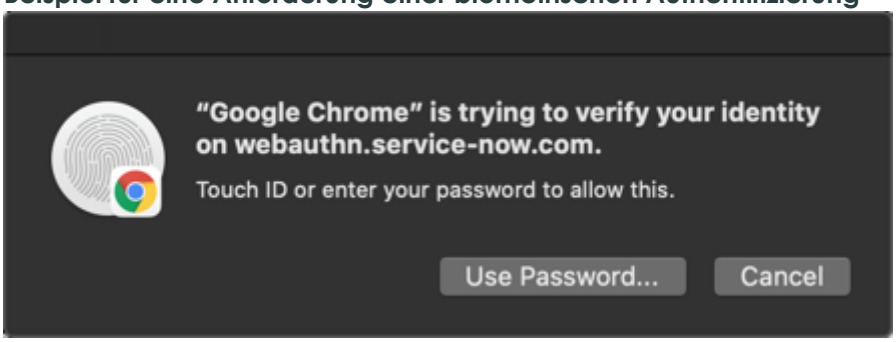


4. Geben Sie einen Kurznamen für Ihren Authentifikator ein, und klicken Sie auf **Registrieren**.



5. Wenn Sie dazu aufgefordert werden, befolgen Sie die Anweisungen auf dem Bildschirm, um sich bei Ihrem biometrischen Authentifikator zu authentifizieren.
Diese Nachricht variiert je nach Authentifikator.

Beispiel für eine Anforderung einer biometrischen Authentifizierung



Nach der erfolgreichen Authentifizierung wird ein Bestätigungsfenster angezeigt. Klicken Sie auf X, um die Bestätigung zu schließen.

Ergebnisse

Ihr biometrischer Authentifikator ist registriert. Der biometrische Authentifikator wird auf der Seite der Multifaktor-Authentifizierung aufgeführt.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registrieren Sie einen Hardware-Sicherheitsschlüssel

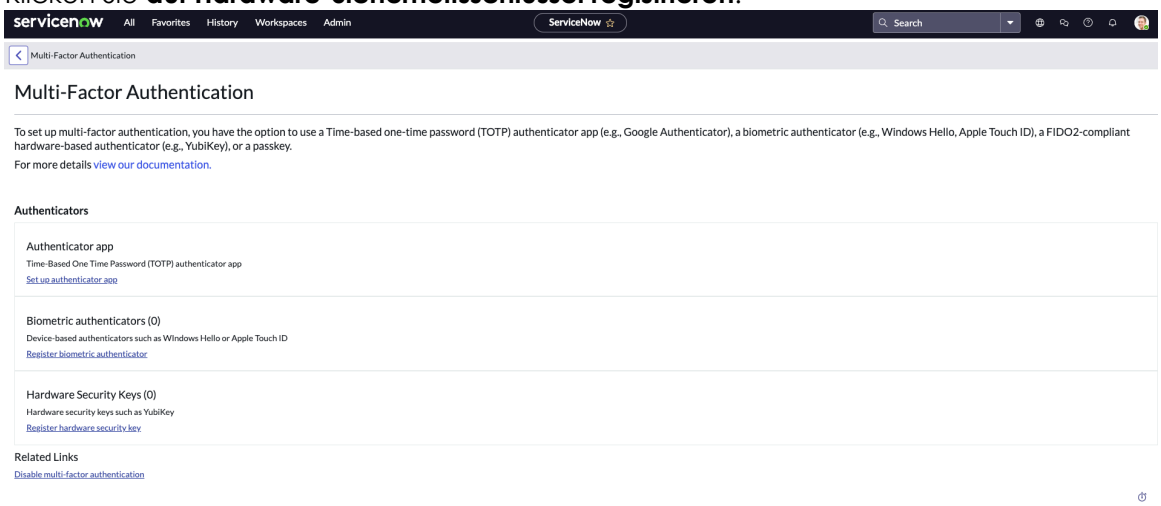
Registrieren Sie einen Hardwareschlüssel, der als Teil Ihrer Anmeldung mit Multifaktor-Authentifizierung verwendet werden soll.

Vorbereitungen

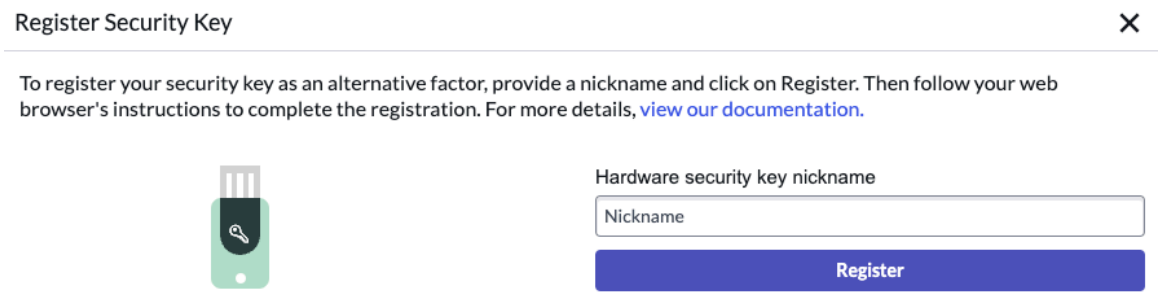
Erforderliche Rolle: keine

Prozedur

1. Navigieren zu **Alle** > **Self-Service** > **Mein Profil**an.
2. Klicken Sie unter **Zugehörige Links**auf **Multifaktor-Authentifizierung**.
   Die Seite der Multifaktor-Authentifizierung wird geöffnet.
3. Klicken Sie **auf Hardware-Sicherheitsschlüssel registrieren**.



4. Geben Sie einen Kurznamen für Ihren Hardwareschlüssel ein, und klicken Sie auf **Registrieren**.



5. Wenn Sie dazu aufgefordert werden, stecken Sie Ihren Hardware-Sicherheitsschlüssel ein, und aktivieren Sie ihn.
   Nach der erfolgreichen Authentifizierung wird ein Bestätigungsfenster angezeigt. Klicken Sie auf X, um die Bestätigung zu schließen.

Ergebnisse

Ihr Hardwareschlüssel ist registriert. Der Hardwareschlüssel wird auf der Seite der Multifaktor-Authentifizierung aufgeführt.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mehrstufige Authentifizierung mit Single Sign-on

Konfigurieren Sie die Multifaktor-Authentifizierung (MFA) mit einem SSO-Anbieter (Single Sign-on) für Ihre Instanz ServiceNow.

Da sich viele Benutzer in Ihrer Organisation bei Ihrem Unternehmensnetzwerk anmelden und auf Ihre Instanz ServiceNow zugreifen, besteht ein größerer Bedarf an einer sicheren Authentifizierung.

MFA bietet in Kombination mit SSO die Sicherheit für Ihre Instanz. Diese Funktion bietet die Flexibilität, MFA für Benutzer bedingt zu aktivieren.

Hinweis:

- ServiceNow MFA wird erzwungen, nachdem der Anwender nach der erfolgreichen Authentifizierung beim Identitätsanbieter weitergeleitet wurde.
- MFA wurde vor dem San Diego-Release nicht mit SSO erzwungen.

Wenn Sie beispielsweise externen Anwendern ein zusätzliches Sicherheitsprotokoll bereitstellen möchten, können Sie MFA nur für diese Anwender erzwingen. Auf diese Weise können Sie zusätzliche Authentifizierungsfunktionen hinzufügen und den Benutzerzugriff steuern.

Für SSO-basierte Anmeldungen wie SAML, OpenID Connect und Digest können Sie MFA für die Authentifizierung erzwingen.

MFA mit SSO kann bei Bedarf basierend auf Ihren Anforderungen konfiguriert werden. Mithilfe von Authentifizierungsschemata und Identitätsanbietern können Sie MFA für bestimmte Anwender mit einem bestimmten Anmeldemechanismus erzwingen.

Sie können MFA für die folgenden Bedingungen erzwingen:

- Authentifizierungsschema
- Identitätsanbieter

MFA mit SSO wird als Teil des Plugins „Adaptive Authentifizierung“ (com.snc.adaptive_authentication) angeboten. Weitere Informationen zum Einrichten der adaptiven Authentifizierung finden Sie unter Adaptive Authentifizierung.

Konfigurieren Sie MFA mit SSO

Erzwingen Sie MFA mit SSO für Ihre Anwender innerhalb oder außerhalb Ihrer Organisation.

Vorbereitungen

Die Funktion „MFA mit SSO“ wird als Teil des Plugins „Adaptive Authentifizierung“ (com.snc.adaptive_authentication) angeboten. Sie müssen die Eigenschaft „Adaptive Authentifizierung“ für die Verwendung von MFA mit SSO aktivieren. Weitere Informationen zum Einrichten der adaptiven Authentifizierung finden Sie unter Adaptive Authentifizierung.

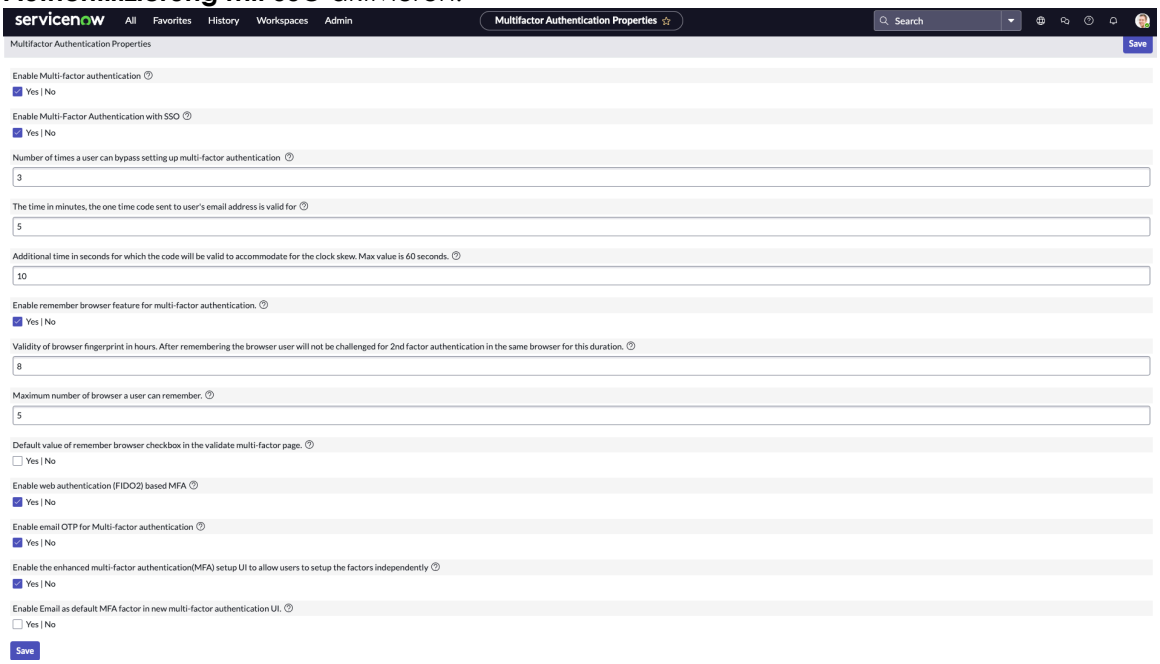
Hinweis: MFA mit SSO-Anmeldung ist verfügbar, wenn die Eigenschaft *glide.authenticate.mfa.with.multisso.enabled* auf **true** festgelegt ist.

Erforderliche Rolle: admin

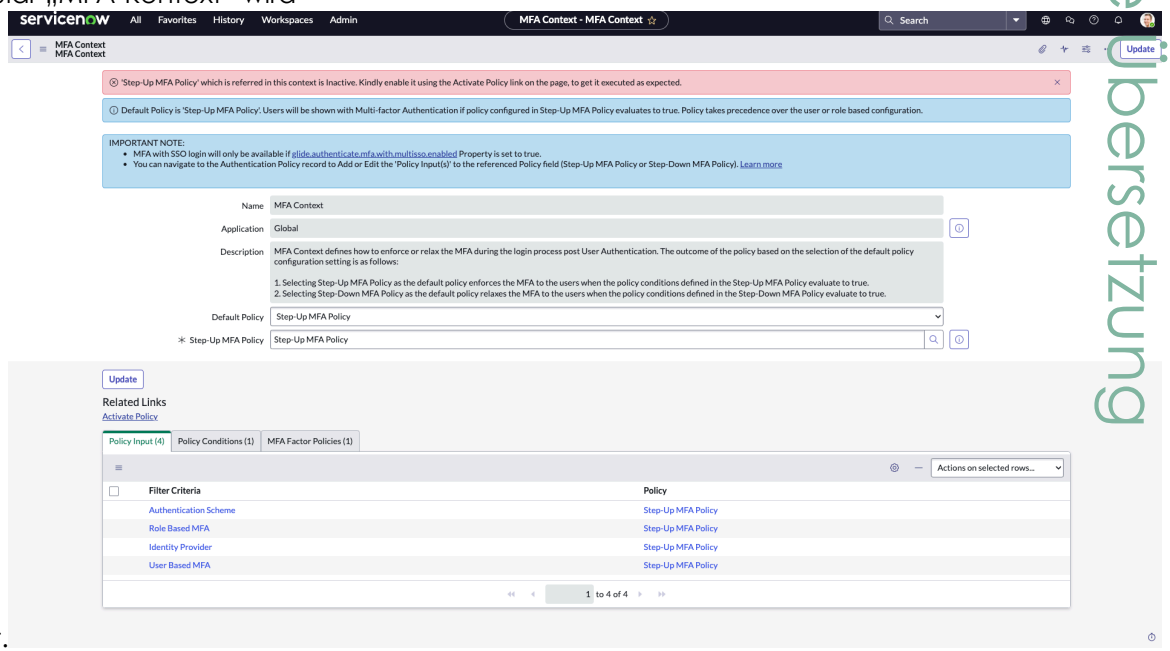
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Multi-Faktor-Authentifizierung** > **Eigenschaften**an.
2. Aktivieren Sie die Kontrollkästchen **Multifaktor-Authentifizierung** aktivieren und **Multifaktor-Authentifizierung mit SSO** aktivieren.



3. Klicken Sie auf **Speichern**.
4. Navigieren zu **Multi-Faktor-Authentifizierung** > **MFA-Kontext**an.
   Das Formular „MFA-Kontext“ wird



angezeigt.

> **Hinweis:** Standardmäßig ist dies die Richtlinie **Step-Up MFA Policy**(Step-Up-MFA-Richtlinie). Anwender werden mit Multifaktor-Authentifizierung angezeigt, wenn eine in der **Step-Up-MFA-Richtlinie** konfigurierte Bedingung als „ **true**“ ausgewertet wird. Die Richtlinie hat Vorrang vor der anwender- oder rollenbasierten Konfiguration.

5. Wahlweise: Um eine Richtlinie zu bearbeiten, gehen Sie zurück zum Datensatz „Authentifizierungsrichtlinie“, ändern Sie die Bedingungen, und kehren Sie zurück.

Automatische Übersetzung

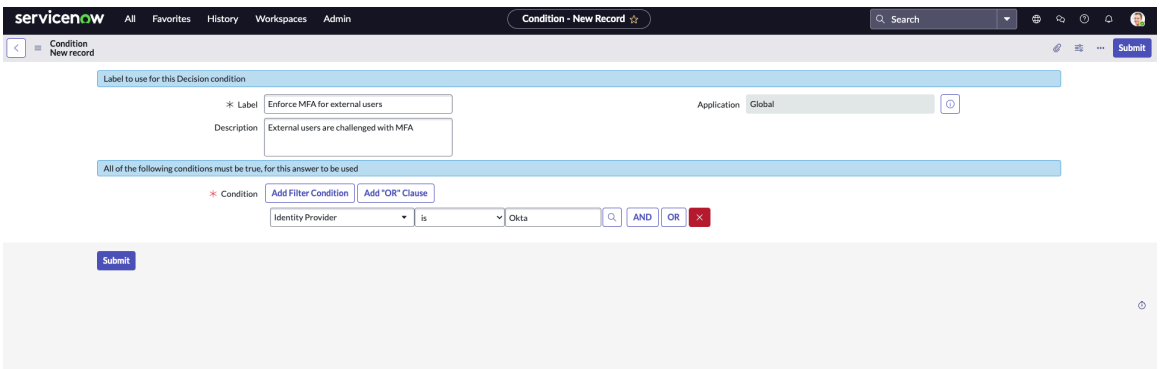
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie zum Datensatz „Authentifizierungsrichtlinie“ navigieren, können Sie den referenzierten Richtlinienfeldern **Step-Up-MFA-Richtlinie** oder **Step-Down-MFA-Richtlinie**„Richtlinieneingaben“ hinzufügen oder bearbeiten.

6. Um eine neue Richtlinienbedingung festzulegen, klicken Sie auf **Richtlinienbedingungen**.
7. Klicken Sie auf **Neu**.
8. Füllen Sie die Felder des Formulars aus.

Formular „Bedingungen“.

Felder	Beschreibung
Bezeichnung	Eindeutiger Name für die Bedingung, die Sie für die Bezeichnung erstellen möchten.
Beschreibung	Die Beschreibung der Richtlinienbedingung.
Bedingungen	Der Typ der Bedingung, die Sie auf die Richtlinie anwenden möchten. Sie können Filterbedingungen und ODER-Klauseln hinzufügen. **Hinweis:** Durch Hinzufügen verschiedener Filterbedingungen und -klauseln können Sie MFA für bestimmte Benutzer hinterfragen.



Example
Um Ihre Bedingungen einzurichten, betrachten Sie das folgende Beispiel. Angenommen, Sie möchten das Authentifizierungsschema mit dem Identitätsanbieter als Bedingung für externe Benutzer. Sie können die Bedingungen wie folgt festlegen:

a. Wählen Sie **Authentifizierungsschema** aus, und legen Sie als Kriterien **Single Sign-on** oder **Anwendername und Passwort**fest.

   Basierend auf dieser Auswahl wird dem Benutzer eine SSO-basierte Anmeldung oder ein Anmeldeformular zur Angabe des Anwendernamens und des Passworts bereitgestellt.

b. Wählen Sie **Identitätsanbieter** aus, und geben Sie den Anbieter als IDP-Datensatz an, für den Sie MFA aktivieren möchten. Beispiel: **Okta**.

Basierend auf dieser Auswahl wird der Anwender, der sich mit SSO anmeldet, nicht mit MFA herausgefordert. Wenn sich der Benutzer hingegen mit Oktaanmeldet, wird er mit MFA herausgefordert.

9. Klicken Sie auf **Absenden**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Adaptive Authentifizierung

Mehrstufige Authentifizierung mit Single Sign-on

Single Sign-on (SSO) für mehrere Anbieter

Mithilfe von externem SSO können Organisationen mehrere SSO-Identitätsanbieter (IdPs) verwenden, um die Authentifizierung zu verwalten und die Standardauthentifizierung der lokalen Datenbank beizubehalten.

Die Integration unterstützt eine beliebige Kombination aus lokalen und externen Authentifizierungsmethoden in einer einzigen Instanz:

- SAML 2.0
- Digest-Authentifizierung
- OpenID Connect

Sie müssen mehrere Schritte zum Einrichten von Mehrfachanbieter-SSO ausführen, einschließlich der Konfiguration von Eigenschaften, des Erstellens von Identitätsanbietern (IdPs) und der Konfiguration von Anwendern für die Verwendung von SSO.

Beispielsweise benötigt ein global verteiltes Unternehmen möglicherweise einen SSO-Anbieter für seine Mitarbeiter, einen anderen für seine Lieferanten und eine lokale Datenbankauthentifizierung für seine Administratoren. Alternativ kann ein Unternehmen SAML 2.0 und Digest-Token-Authentifizierungslösungen in derselben Instanz implementieren.

Aktivieren Sie das Mehrfachanbieter-SSO-Plugin

Diese Integration erfordert das Plugin Integration – Single Sign-on-Installationsprogramm für mehrere Anbieter (com.snc.integration.sso.multi.installer).

Vorbereitungen

Erforderliche Rolle: admin.

Das Plugin „com.snc.integration.sso.multi.installer“ kann auch für OIDC, SAML und Digest verwendet werden.

Erforderliche Rolle: admin

Prozedur

1. Navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie das Plugin Integration – Single Sign-on-Installationsprogramm für mehrere Anbieter (com.snc.integration.sso.multi.installer) mithilfe der Filterkriterien und der Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: `Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.`

Nach Abschluss der Installation wird eine Meldung angezeigt.

Eigenschaften, Tabellen und Skripts für Mehrfachanbieter-SSO

Das Plugin „Integration – Single Sign-on-Installationsprogramm für mehrere Anbieter“ enthält die folgenden Systemeigenschaften, Tabellen und Skripts.

Eigenschaften

Mehrfachanbieter-SSO fügt die folgenden Systemeigenschaften hinzu.

Eigenschaften von Mehrfachanbieter-SSO

Name	Beschreibung
glide.authenticate.multisso.debug	Aktiviert (wahr) oder deaktiviert (falsch) die Debug-Protokollierung für die SSO-Integration mit mehreren Anbietern. • Typ: Wahr | Falsch • Standardwert: falsch
glide.authenticate.multisso.enabled	Aktiviert (wahr) bzw. deaktiviert (falsch) die Mehrfachanbieter-SSO. • Typ: Wahr | Falsch • Standardwert: falsch **Hinweis:** Wenn Sie diese Eigenschaft auf „falsch“ setzen, wird die Mehrfachanbieter-SSO nicht deaktiviert, wenn auch die Accountwiederherstellung (ACR) in der Instanz aktiviert ist. Um sich mit einem Anwendernamen und einem Passwort anzumelden, muss ACR auch mit der Eigenschaft *glide.sso.acr.enabled* deaktiviert werden. Einzelheiten zu dieser Eigenschaft finden Sie unter Eigenschaften für die Accountwiederherstellung.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften von Mehrfachanbieter-SSO (Fortsetzung)

Name	Beschreibung
glide.authenticate.multissov2_feature.enabled	Diese Eigenschaft bestimmt, ob die MultiSSOv2-Version in der Instanz aktiviert ist.

Tabellen

Mehrfachanbieter-SSO fügt die folgenden Tabellen hinzu.

Tabellen für Mehrfachanbieter-SSO

Name	Beschreibung
SSO-Eigenschaften `[sso_properties]`	Speichert Daten für jeden IdP, jedes Schema, allgemeine SSO-Daten usw.
Eigenschaften von SAML 2 Update 1 `[saml2_update1_properties]`	Speichert Daten für SAML 2.0 Update 1-Konfigurationen, wie z. B. SAML-Zertifikate.
Digest-Eigenschaften `[digest_properties]`	Speichert Daten für die Authentifizierungskonfigurationen des Digest-Tokens.
SSO -`Verein [sso_federation]`	Speichert Daten für jeden SSO-Verbund.
OIDC-Identitätsanbieter `[oidc_identity_provider]`	Speichert Daten für auf Open ID Connect basierende Identitätsanbieter.

Skripts

Mehrfachanbieter-SSO fügt die folgenden Skripts hinzu.

SSO-Skripts für mehrere Anbieter

Name	Beschreibung
MultiSSO	Ermöglicht einem Kunden, einen SSO-Typ auf Unternehmensbasis zu definieren.
MultiSSOLogin	Ermöglicht, dass jede Domäne ein eigenes Anmeldeskript hat.
MultiSSOLogout	Ermöglicht, dass jede Domäne ein eigenes Abmeldeskript hat.
MultiSSO_OIDC_benutzerdefiniert	Ermöglicht einem Anwender, ein anwenderdefiniertes Single Sign-on-Skript für die OIDC-Verbindung zu definieren.
MultiSSO_OIDC_logout_custom	Ermöglicht einem Anwender, ein anwenderdefiniertes Abmeldeskript für die OIDC-Verbindung zu definieren.
MultiSSO_Abstract_Core	Stellt eine Basisklasse für alle SSO-Klassen für mehrere Anbieter bereit.
MultiSSO_ClientHelper	Bietet vom Client aufrufbare Dienstprogrammfunktionen für Mehrfachanbieter-SSO.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SSO-Skripts für mehrere Anbieter (Fortsetzung)

Name	Beschreibung
MultiSSO_DigestToken	Stellt eine Basissystemlogik für die Authentifizierung mit Digest-Token bereit.
MultiSSO_SAML2_Update1	Stellt die Logik zur Verarbeitung der SAML 2.0 Update 1-Authentifizierung für Single Sign-on mit mehreren Mandaten bereit.

Konfigurationen für Mehrfachanbieter-SSO

Sie müssen mehrere Schritte zum Einrichten von Mehrfachanbieter-SSO ausführen, einschließlich der Konfiguration von Eigenschaften, des Erstellens von Identitätsanbietern (IdPs) und der Konfiguration von Anwendern für die Verwendung von SSO.

Weitere Informationen zu den einzelnen Konfigurationen finden Sie in den folgenden Themen.

- SAML-IdP-Authentifizierungs-Flow für Multi-Provider-SSO
- Konfigurieren Sie Eigenschaften für Mehrfachanbieter-SSO
- Erstellen Sie einen externen Identitätsanbieter
- Konfigurieren Sie Anwender für Mehrfachanbieter-SSO

Konfigurieren Sie Eigenschaften für Mehrfachanbieter-SSO

Konfigurieren Sie SSO-Eigenschaften, und fügen Sie der Tabelle „Systemeigenschaften“ eine Eigenschaft hinzu, um eine IdP-Aufnahmeliste zu konfigurieren.

Vorbereitungen

Erforderliche Rolle: admin

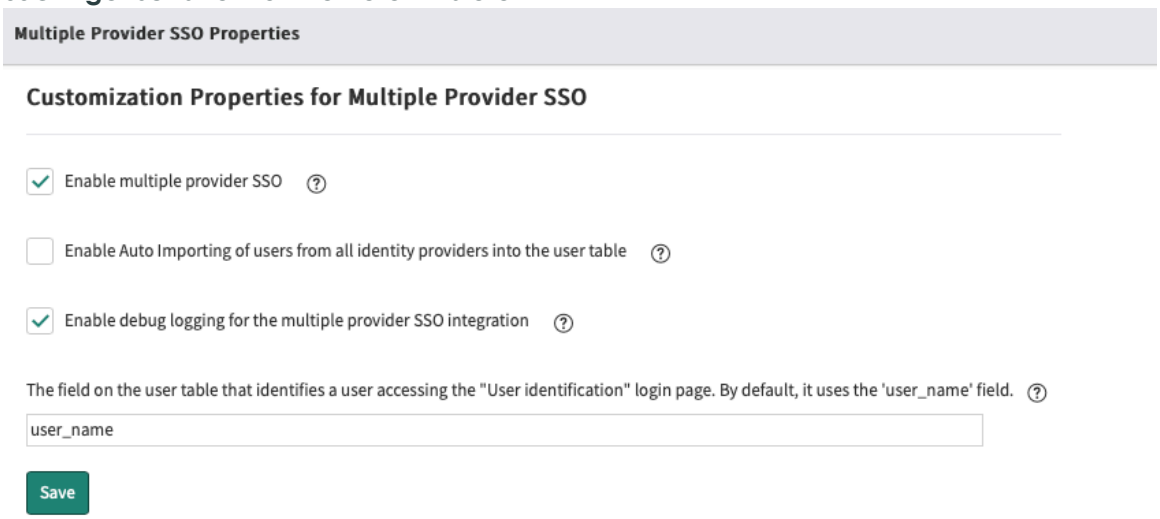
Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Administration** > **Eigenschaften**an.
2. Aktivieren Sie das Kontrollkästchen **Multi-Provider-SSO** aktivieren.
   Diese Auswahl fügt den Link Externe Anmeldung verwenden zur Anmeldeseite hinzu.
3. Um die Benutzertabelle mit den Benutzern im IdP zu aktualisieren, wählen Sie die Option **Automatischen Import** aktivieren aus.
4. Damit die Debug-Nachrichten unten im Inhaltsrahmen angezeigt werden, aktivieren Sie das Kontrollkästchen **Debug-Protokollierung für Multi-Provider-SSO-Integration** aktivieren. Wenn diese Option aktiviert ist, verringert die Debug-Protokollierungsfunktion die Leistung und verbraucht Speicherplatz zum Generieren von Protokollen.
5. Geben Sie in der Eigenschaft **Feld in der Benutzertabelle, das einen Benutzer identifiziert, der auf die Anmeldeseite der Benutzeridentifizierung zugreift das**Feld in der Benutzertabelle ein, das den Wert enthält, den der IdP zur Identifizierung des Benutzers verwendet. Der Standardwert ist **user_name**.

   Der Standardwert ist **user_name**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SSO-Eigenschaften für mehrere Anbieter



6. Klicken Sie auf **Speichern**.
7. Weisen Sie die Benutzer an, auf den Link **Externe Anmeldung verwenden** zu klicken, wenn sie sich bei der Instanz anmelden.

Zugehörige Informationen

SAML-Benutzerbereitstellung

Erstellen Sie einen externen Identitätsanbieter

Nachdem Sie die Mehrfachanbieter-SSO-Eigenschaften konfiguriert haben, können Sie den SAML 2.0- oder Digest-Token-Identitätsanbieter aktualisieren oder einen neuen erstellen.

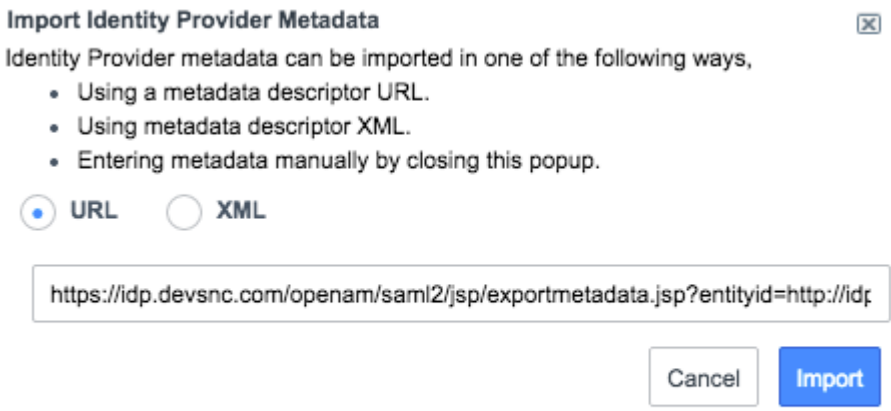
Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identity Provider**an.
2. Um den Datensatz eines Identitätsanbieters zu bearbeiten, klicken Sie auf den Datensatz.
   - Aktualisieren Sie für Digest-Token-Konfigurationen die Eigenschaften manuell.
   - Aktualisieren Sie bei Konfigurationen mit **SAML2** Update 1 die Metadaten des Identitätsanbieters automatisch mit dem zugehörigen Link Metadaten des Identitätsanbieters importieren, oder aktualisieren Sie die Eigenschaften manuell.
   - Aktualisieren Sie für OpenID Connect-Konfigurationen die Eigenschaften manuell.
3. Klicken Sie auf **Neu**, um einen neuen Identitätsanbieter zu erstellen.
   - Für Digest-Token-Konfigurationen: Klicken Sie auf **Digest-SSO**, und geben Sie die Digest-Eigenschaften für Single Sign-on für mehrere Anbieter ein.
   - Für SAML2-Konfigurationen: Klicken Sie **auf MultiSSOV2_SAML2_custom**, und importieren Sie die Identitätsanbieter-Metadaten aus einer URL, als XML, oder geben Sie die Identitätsanbieter-Informationen manuell ein.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



- Für OpenID Connect: Klicken Sie auf **OpenID Connect**, und geben Sie die Client-ID, den geheimen Clientschlüssel und die bekannte Konfigurations-URL ein.

4. Um den IdP zum Failover-IdP festzulegen, der verwendet wird, wenn der Standard-IdP nicht verfügbar ist, aktivieren Sie das Kontrollkästchen **Standard**.

   Wenn SAML 2 Update 1 aktiv ist und Sie ein Upgrade auf das Fuji-Release durchführen, wird der IdP SAML 2 Update 1 als Standard-Failover ausgewählt. Für neue Instanzen oder wenn Sie ein Upgrade von einem Release durchführen, auf dem SAML 2 Update 1 nicht aktiv ist, ist kein standardmäßiger Failover-IdP ausgewählt.

   Hinweis: Beim Importprozess für Metadaten wird automatisch ein Zertifikatdatensatz für den Identitätsanbieter erstellt. Navigieren Sie zum Modul **„x509-Zertifikat“**, um das Zertifikat anzuzeigen.

   Hinweis: Zertifikate für Single Sign-on müssen immer im PEM-Format vorliegen, um mit SAML-Zertifikaten zu funktionieren.

5. Wenn die E-Signatur aktiv ist, konfigurieren Sie das Formular „Identitätsanbieter“, und fügen Sie das Feld **Assertionen-Verbraucher-URL für eSignature-Authentifizierung hinzu**.
   In den meisten Fällen lautet diese URL wie folgt: `https://YOURINSTANCE.service-now.com/consumer.do`. Wenn Sie jedoch eine anwenderdefinierte Methode für die SAML-Authentifizierung für die E-Signatur verwenden, können Sie eine eigene Verbraucher-URL einrichten. Wenn Sie nur SAML 2.0 Update 1 verwenden und kein Single Sign-on für mehrere Anbieter verwenden, konfigurieren Sie die Verbraucher-URL der Assertion mit den SAML-Eigenschaften für die E-Signatur.

Generieren Sie Metadaten des Instanz-Service-Providers (SP) für SAML

Im Rahmen Ihrer SSO-Konfiguration können Sie die SP-Metadaten der Instanz generieren, um sie dem IdP bereitzustellen.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Der IdP benötigt die SP-Metadaten der Instanz, um Anforderungen zu authentifizieren und weiterzuleiten.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wählen Sie Ihr installiertes SSO-Plugin:

Option	Bezeichnung
Mehrfachanbieter-SSO	Navigieren zu **Mehrfachanbieter-SSO** > **Identity Provider**an. Wählen Sie einen IdP aus, und klicken Sie auf die Schaltfläche **Metadaten generieren**. Die Integration generiert die SP-Metadaten der Instanz automatisch aus den Einstellungen für die Systemeigenschaft.
SAML 2 SSO	Navigieren zu **SAML 2 Single Sign-on** > **Metadaten**an. Die Integration generiert die SP-Metadaten der Instanz automatisch aus den Einstellungen für die Systemeigenschaft.

2. Kopieren Sie die SP-Metadaten in das Textfeld.

   Beispiel:

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
 entityID="https://yourinstance.service-now.com">
  <SPSSODescriptor AuthnRequestsSigned="false"
 WantAssertionsSigned="true"
 protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  <SingleLogoutService
 Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
 Location="https://yourinstance.service-now.com/navpage.do" />

 <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddres
s</NameIDFormat>
  <AssertionConsumerService isDefault="true" index="0"
 Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
 Location="https://yourinstance.service-now.com/navpage.do" />
  <AssertionConsumerService index="1"
 Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
 Location="https://yourinstance.service-now.com/consumer.do"/>
 </SPSSODescriptor>
</EntityDescriptor>
```

3. Stellen Sie dem IdP die SP-Metadaten der Instanz bereit.
   Beispielsweise ermöglicht SSOCircle einem Benutzer, die SP-Metadaten online bereitzustellen.

Konfigurieren Sie Anwender für Mehrfachanbieter-SSO

Administratoren können Multi-Provider-SSO für einzelne Benutzer oder für alle Benutzer konfigurieren, die zu einem Unternehmen gehören. Sie können Mehrfachanbieter-SSO für Gruppen nicht konfigurieren.

Vorbereitungen

Erforderliche Rolle: admin

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identity Provider**an.
2. Klicken Sie mit der rechten Maustaste auf den Datensatz eines Identitätsanbieters und wählen Sie **sys_id kopieren**.
3. Kopieren Sie die Daten in die Zwischenablage.
4. Navigieren Sie zu einem Benutzerdatensatz oder einem Unternehmensdatensatz.
5. Konfigurieren Sie das Formular, und fügen Sie das Feld **SSO-Quelle** hinzu.
6. Geben Sie im Feld **SSO-Quelle** eine der folgenden Optionen ein:
   - **SAML-Anwender**: **Geben Sie „sso:“** gefolgt von der sys_id des Datensatzes des Identitätsanbieters ein.
   - **SSO**-Verbundbenutzer: Geben Sie „ **Verbund:** “ gefolgt von der sys_id des Verbunddatensatzes ein.
7. Klicken Sie auf **Aktualisieren**.

IdP-Verbindungen werden getestet

Durch das Testen der Verbindung zu einem IdP werden die Einstellungen validiert, bevor die externe Authentifizierung aktiviert wird.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Das Jakarta-Release unterstützt die Testverbindung in einem Popup-Fenster. Wenn Ihr IdP mit dieser Option nicht ordnungsgemäß funktioniert, können Sie diese Standardeinstellung deaktivieren.
Der Auftrag „MultiSSO-IDP-Metadaten aktualisieren“ ruft das Zertifikat für den IdP ab, während die Verbindung erstellt, aktualisiert oder getestet wird.

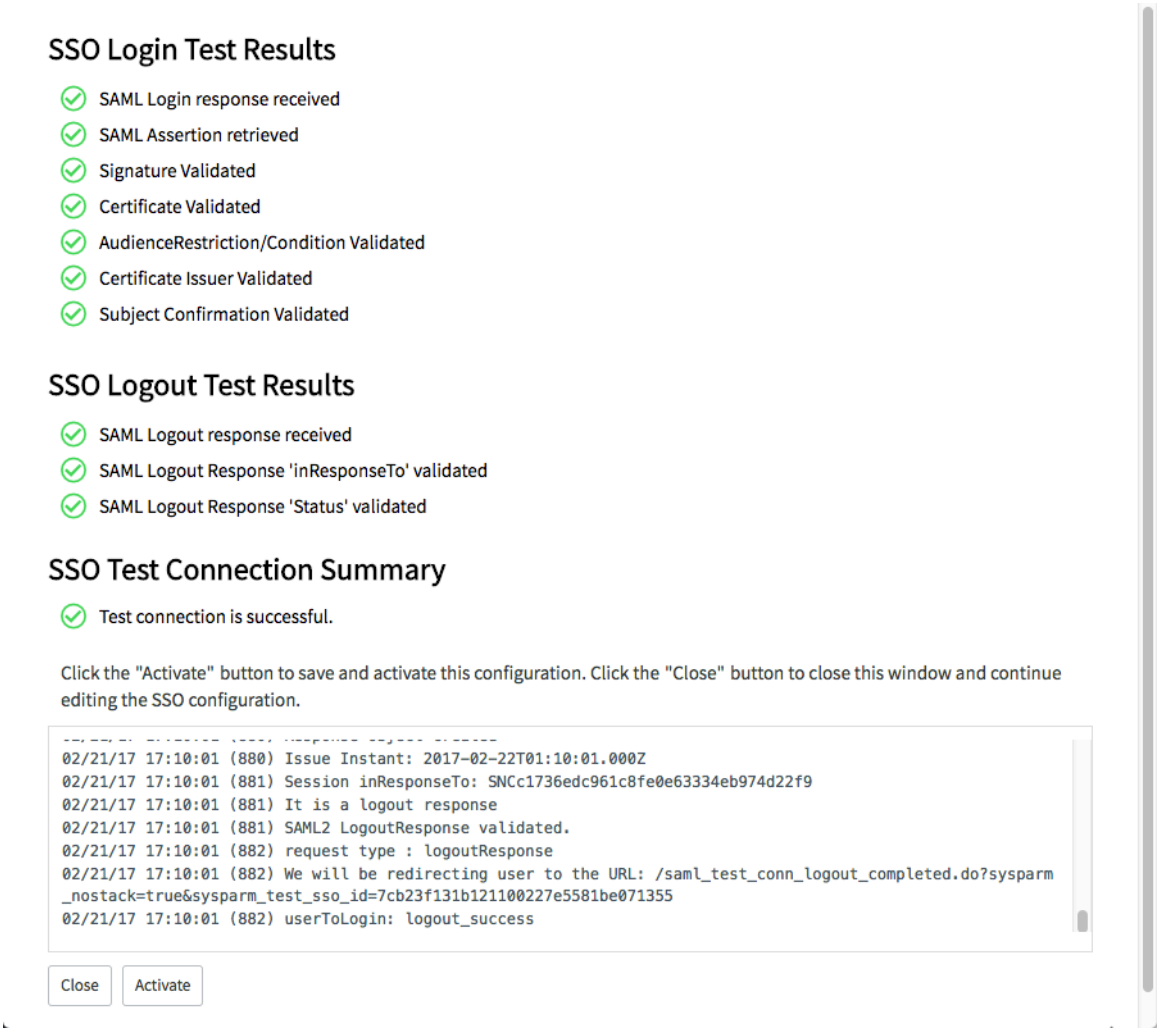
Hinweis: In einigen IDP-Fällen, bei denen die Testverbindung fehlschlägt, muss „glide.authenticate.multisso.test.connection.mandatorisch“ mit dem Wert „falsch“ erstellt werden. Anschließend können Sie den IdP ohne die Testverbindung aktivieren.

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identity Provider**an.
2. Wählen Sie einen definierten IdP aus, oder klicken Sie auf **Neu**, um einen neuen IdP zu definieren.
3. Wahlweise: Konfigurieren Sie einen Identitätsanbieter, wenn Sie einen neuen IdP einrichten.
4. Klicken Sie auf **Verbindung testen**, geben Sie die Anmeldeinformationen für den IdP ein, um die Anmeldung zu überprüfen.
   Sie können den IdP erst aktivieren, wenn Sie eine erfolgreiche Testverbindung haben.
   Wenn der Test fehlschlägt, können Sie aktualisieren, um Ihre Konfigurationsinformationen zu speichern, aber Sie können diese Konfiguration nicht aktivieren.
5. Überprüfen Sie die Ergebnisse mithilfe der **SSO-Testergebnisse/Zusammenfassung** oder des Abschnitts „ **SSO** -Testprotokolle“, um Protokollnachrichten anzuzeigen.
   Wenn Fehler auftreten, lesen Sie die Fehler und Korrekturen für Multi-SSO (SAML 2.0).

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie auf **Abbrechen**, wenn der Test abgeschlossen ist.



Allgemeine IdP-Verbindungsfehler

In der folgenden Tabelle werden einige der häufigsten IdP-Verbindungsfehler und ihre Lösungen beschrieben.

Problembehandlung bei IdP-Testverbindungen

Fehlermeldungen	Lösung
Die Validierung des Anwenderfelds ist fehlgeschlagen. Ungültiges Anwenderfeld<field name> „“ ist kein Feld in der Tabelle „sys_user“.	Stellen Sie sicher, dass der Inhalt des von Ihnen ausgewählten Anwendertabellenfelds mit dem SAML-NameID-Token übereinstimmt.
Der Aussteller der Assertion ist ungültig.	Stellen Sie sicher, dass die **Identitätsanbieter-URL** eine gültige URL zu Ihrem IdP enthält. Jede IdP-URL muss eindeutig sein.
Die Validierung des Elements "AudienceRestriction" ist fehlgeschlagen.	Stellen Sie sicher, dass der Zielgruppen-URI eine gültige URL zu Ihrer **-Instanz** enthält.
Abmeldung von der Sitzung des IdP nicht möglich.	Stellen Sie sicher, dass die **SingleLogoutRequest** -URL eine gültige URL zum Abmeldeservice Ihres IdP enthält.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problembehandlung bei IdP-Testverbindungen (Fortsetzung)

Fehlermeldungen	Lösung
Signatur wurde nicht anhand des Schlüssels der Anmeldeinformationen validiert.	Vergewissern Sie sich, dass für den IdP ein gültiges Zertifikat installiert ist.

Beheben Sie Skriptprobleme mit SAML

Beheben Sie Skriptprobleme mit SAML. Wenn SAML zum Zeitpunkt der Aktivierung von Multiple Single Sign-on bereits aktiv ist und Sie die Installations-Exits bereits angepasst haben, können Skriptprobleme auftreten.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Sichern Sie den geänderten Installations-Exit SAML2SingleSignon_update1 und die Skripteinbindung SAML2_update1.
2. Setzen Sie den Installations-Exit und die Skripteinbindung auf die Version zurück, die mit dem Baselinesystem verfügbar ist.
3. Aktivieren oder aktualisieren Sie das Plugin **Integration – Single Sign-on für mehrere Provider – Installationsprogramm**.
   Das System aktualisiert SAML und alle erforderlichen Dateien auf SAML 2 Update 1.
4. Öffnen Sie die Seite mit den Eigenschaften für Mehrfach-SSO, und aktivieren Sie das Kontrollkästchen **Mehrfach-Anbieter-SSO aktivieren, um die Option** zu aktivieren.
5. Übernehmen Sie die Änderungen am Installationsausgang SAML2SingleSignon_update1 in die Baseline-Skripteinbindung **MultiSSO_SAML2_Update1 und die** Änderungen an der Skripteinbindung SAML2_update1 in die Baseline-Skripteinbindung SAML2_update1.

Melden Sie sich mit Mehrfachanbieter-SSO an

Die empfohlene und effizienteste Methode für Anwender, sich mit Mehrfachanbieter-SSO anzumelden, ist die Verwendung einer speziell konfigurierten URL.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Nachdem die Mehrfachanbieter-SSO konfiguriert wurde, können Sie eine URL an die Benutzer mit dem richtigen IdP in der Parameterzeichenfolge senden. Beispiel:

```
/login_with_sso.do?glide_sso_id=<sys_id of the sso configuration>
```

Nachdem sich ein Benutzer erfolgreich bei der IdP-Seite angemeldet hat, wird dem Browser ein Cookie mit der sys_id des IdP hinzugefügt. Wenn der Benutzer das nächste Mal versucht, sich anzumelden, leitet das System den Benutzer zur Anmeldung beim IdP-Server um, der sich automatisch bei der Instanz anmeldet.

Wenn kein URL-Parameter festgelegt ist oder der Browsercache geleert wurde, können Benutzer außerdem:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Klicken Sie auf der -Anmeldeseite auf den Link **Externe Anmeldung verwenden**.

   Die Seite für die externe Anmeldung wird angezeigt. Benutzer können auf **Lokale Anmeldung** verwenden klicken, um zur Standardanmeldeseite zurückzukehren.

2. Geben Sie den Wert für das angegebene Feld in der Benutzertabelle ein, die Sie in den Eigenschaften für Mehrfachanbieter-SSO konfiguriert haben.

   Der Benutzer wird zum IdP-Server umgeleitet, wo er sich anmeldet.

Ergebnisse

Nachdem sich Benutzer erfolgreich bei einem IdP angemeldet haben, werden sie bei jedem Versuch, auf die Instanz zuzugreifen, automatisch an diesen IdP weitergeleitet. Damit ein Anwender auf einen anderen IdP zugreift, senden Sie dem Anwender eine URL mit den neuen IdP-Informationen im Parameter. Der neue IdP überschreibt den alten IdP im Cookie, wenn sich der Benutzer erfolgreich anmeldet. Wenn sich der Benutzer nicht erfolgreich anmeldet, werden die alten IdP-Informationen im Cookie beibehalten.

Ermöglichen Sie Anwendern, den Identitätsanbieter für die Anmeldung auszuwählen

Mit der Unterstützung von SSO-Verein können Anwender auswählen, bei welchem IdP sie sich anmelden möchten.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

SSO-Verbünde aggregieren Metadaten von mehreren IdPs und Service Providern, einschließlich Ihrer -Instanz. Verbünde veröffentlichen die Metadaten dann als XML-Datei, die Informationen wie IdP-Namen und IdP-Zertifikate enthält. Administratoren können dann die Instanz anweisen, die XML-Datei zu lesen und die SSO-Eigenschaftentabelle automatisch mit allen erforderlichen IdP-Informationen auszufüllen.

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Verbund**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder entsprechend aus (siehe Tabelle).
4. Klicken Sie auf **Absenden**.
5. Nachdem Sie einen Verbund konfiguriert haben, aktivieren Sie die geplante Aufgabe „SSO-Metadaten aktualisieren“, und konfigurieren Sie dann die Benutzer, die auf die Verbund-IdPs zugreifen sollen. Verwenden Sie die sys_ID des soeben erstellten Verbunddatensatzes.

   Verwenden Sie die sys_ID des soeben erstellten Verbunddatensatzes.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die Instanz füllt die Tabelle mit den SSO-Eigenschaften mit den IdP-Informationen. Benutzer, die für die Verwendung des Verbunds konfiguriert sind, werden bei der Anmeldung an die von Ihnen konfigurierte Discovery-Service-URL umgeleitet. Dann wählt er den IdP aus und stellt die erforderlichen Anmeldeinformationen bereit. Alternativ können Sie Anwendern eine URL mit dem IdP im Parameter senden.

Anwendern die Möglichkeit geben, den Identitätsanbieter für die Anmeldung auszuwählen

Feld	Beschreibung
Name	Geben Sie einen beschreibenden Namen für den Verbund ein.
Aktiv	Aktivieren Sie das Kontrollkästchen, damit die Instanz die XML-Datei aus dem Verbund abrufen kann.
Typ	Wählen Sie den Typ der Authentifizierung aus, den dieser Verbund unterstützt.
Discovery Service-URL	Geben Sie die URL des Discovery-Service für diesen Verbund ein. Dies ist der Standort, an den Anwender weitergeleitet werden, um einen IdP auszuwählen und sich anzumelden.
Metadaten-URL	Geben Sie die URL der XML-Datei ein, die die Verbundmetadaten enthält.
x509-Zertifikat	Wählen Sie das Verbundzertifikat aus.
Domäne	Wählen Sie die Domäne aus, zu der die Daten gehören.

Hinweis: Der IdP für die föderierte InCommon-Identitätsverwaltung ist vorkonfiguriert.

Verwenden Sie Serviceportal mit Mehrfachanbieter-SSO, um eine URL umzuleiten

Serviceportal Verwendet eine Kombination aus Systemeigenschaften und Skripteinbindungen, um zu bestimmen, wie das System URL-Weiterleitungen für Benutzer vornimmt, die sich beim Portal anmelden.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn Sie die Systemeigenschaft zur automatischen Umleitung zu Ihrem primären Identitätsanbieter (IdP) verwenden, leitet Serviceportal automatisch zu diesem IdP um. Wenn Sie mehrere IdPs haben, zeigt Serviceportal auf der Anmeldeseite einen Link zur **externen Anmeldung**an.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Service Portal-Anmeldeseite konfigurieren
2. Nach der Anmeldung zum Service Portal weiterleiten

Accountwiederherstellung (ACR)

Administratoren können die Accountwiederherstellung (Account Recovery, ACR) konfigurieren, um Wiederherstellungsaktivitäten durchzuführen, z. B. um SSO-Fehlkonfigurationen oder abgelaufene Zertifikate zu beheben.

Hinweis: Durch das Aktivieren von ACR werden die lokalen interaktiven Anmeldungen (basierend auf Anwendernamen oder Passwörtern) deaktiviert, wenn SSO für Ihre Instanzen aktiviert ist.

ACR bietet die folgenden Funktionen:

- Umgehen Sie Ihre SSO-Anmeldung (Single Sign-on), um Probleme mit der SSO-Konfiguration als Administrator zu beheben.
- Melden Sie sich mit SSO an, um Aufgaben mit einem Administratorkonto auszuführen, das als Accountwiederherstellung konfiguriert ist.
- Mit ACR-Flows können Administratoren Selfservicefunktionen verwenden, um die Accountwiederherstellung zu regeln, wenn ein Bedarf besteht (z. B. bei falscher SSO-Konfiguration oder abgelaufenen Zertifikaten).
- Reduzieren Sie nicht autorisierte Zugriffe auf die Instanz, und stellen Sie eine starke Grundlage für die Verwendung von ACR außerhalb von SSO-Anwendungsfällen bereit.

Neue Instanz

Damit eine neue Instanz ACR verwenden kann, gehen Sie wie folgt vor:

- Mutli-SSO-Plugin aktivieren (`com.snc.integration.sso.multi.installer`)
- ACR aktivieren (`glide.sso.acr.aktiviert`): Ist bei einer neuen Instanz standardmäßig aktiviert.
- Vor dem Aktivieren der SSO-Eigenschaft (`glide.authenticate.multisso.enabled`) muss sich der Administrator als ACR-Benutzer registrieren.

  Hinweis: Wenn Sie diese Eigenschaft auf „falsch“ setzen, wird die Mehrfachanbieter-SSO nicht deaktiviert, wenn auch die Accountwiederherstellung (ACR) in der Instanz aktiviert ist. Um sich mit einem Anwendernamen und einem Passwort anzumelden, muss ACR auch mit der Eigenschaft *`glide.sso.acr.enabled`* deaktiviert werden. Einzelheiten zu dieser Eigenschaft finden Sie unter Eigenschaften für die Accountwiederherstellung.

- Der Administrator muss ein Passwort für die lokale Anmeldung festlegen und MFA registrieren, bevor er sich als ACR-Anwender anmeldet.

Aktualisierte Instanz

Damit eine aktualisierte Instanz ACR verwenden kann, gehen Sie wie folgt vor:

- Mutli-SSO-Plugin aktivieren (`com.snc.integration.sso.multi.installer`)
- ACR aktivieren (`glide.sso.acr.enabled`)

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Im Falle einer aktualisierten Instanz muss der Administrator ACR aktivieren.

- Vor dem Aktivieren der SSO-Eigenschaft (`glide.authenticate.multisso.enabled`) muss sich der Administrator als ACR-Benutzer registrieren.
- Der Administrator muss ein Passwort für die lokale Anmeldung festlegen und MFA registrieren, bevor er sich als ACR-Anwender anmeldet.

Konfigurieren Sie Anwender für die Accountwiederherstellung

Um die Accountwiederherstellung zu verwenden, müssen Sie mindestens einen Administratoraccount als Accountwiederherstellungsbenutzer registrieren. Single Sign-on kann in Ihrer Instanz erst aktiviert werden, wenn mindestens ein Account konfiguriert ist. Details zu diesem Vorgang finden Sie unter Konfigurieren Sie auf der Seite „Eigenschaften der Accountwiederherstellung“ einen Accountwiederherstellungsbenutzer.

Hinweis: Wenn Sie ein Upgrade einer Instanz durchführen, die bereits Single Sign-on auf Rome oder höher verwendet, funktioniert Single Sign-on weiterhin, ohne dass ein Wiederherstellungsbenutzer konfiguriert ist.

Konfiguration der Accountwiederherstellung

Die Funktion zur Accountwiederherstellung ist in den **Plugins Integration – Single Sign-on-Installationsprogramm für mehrere Anbieter (com.snc.integration.sso.multi.installer) enthalten**. Die Funktion ist standardmäßig aktiviert. Sie können diese und andere Einstellungen zur Accountwiederherstellung mithilfe der Systemeigenschaften ändern. Einzelheiten zu diesen Eigenschaften finden Sie unter Eigenschaften für die Accountwiederherstellung.

Kontext der Accountwiederherstellungsrichtlinie

Nachdem Sie einen Anwender für die Accountwiederherstellung registriert und Single Sign-on (SSO) aktiviert haben, schränkt Ihre Instanz alle lokalen Anmeldungen ein. Diese Einschränkung ist im Richtlinienkontext der **SSO – ACR-Kontextauthentifizierung** definiert. Weitere Informationen zum Kontext finden Sie unter Kontext der Accountwiederherstellung.

Einzelheiten dazu, wie Authentifizierungsrichtlinien und Richtlinienkontexte in Ihrer -Instanz funktionieren, finden Sie unter Adaptive Authentifizierung.

Konfigurieren Sie einen Account-Wiederherstellungsbenutzer

Konfigurieren Sie einen Accountwiederherstellungsbenutzer, um Accountwiederherstellungsaktivitäten in Ihrer -Instanz auszuführen.

Ein Accountwiederherstellungsbenutzer ist ein Anwenderaccount, mit dem Administratoren Accountwiederherstellungsaufgaben ausführen können, z. B. das Beheben einer SSO-Fehlkonfiguration oder das Behandeln abgelaufener Zertifikate.

Hinweis: Wenn Sie die Accountwiederherstellung in Ihrer -Instanz verwenden, müssen Sie einen Accountwiederherstellungsbenutzer konfigurieren. Dieser Schritt ist erforderlich, bevor Single Sign-on mit mehreren Anbietern auf einer Instanz aktiviert wird.

Konfigurieren Sie auf der Seite „Eigenschaften der Accountwiederherstellung“ einen Accountwiederherstellungsbenutzer

Konfigurieren Sie eine Accountwiederherstellung auf der Seite mit den Eigenschaften der Accountwiederherstellung.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: admin

Damit eine neue Instanz ACR konfigurieren kann, müssen Sie wie folgt vorgehen:

- Mutli-SSO-Plugin aktivieren (`com.snc.integration.sso.multi.installer`)
- ACR aktivieren (`glide.sso.acr.aktiviert`): Ist bei einer neuen Instanz standardmäßig aktiviert.
- Vor dem Aktivieren der SSO-Eigenschaft (`glide.authenticate.multisso.enabled`) muss sich der Administrator als ACR-Benutzer registrieren.
- Der Administrator muss ein Passwort für die lokale Anmeldung festlegen und MFA registrieren, bevor er sich als ACR-Anwender anmeldet.

Damit eine aktualisierte Instanz ACR verwenden kann, gehen Sie wie folgt vor:

- Mutli-SSO-Plugin aktivieren (`com.snc.integration.sso.multi.installer`)
- ACR aktivieren (`glide.sso.acr.enabled`)

  Hinweis: Im Falle einer aktualisierten Instanz muss der Administrator ACR aktivieren.

- Vor dem Aktivieren der SSO-Eigenschaft (`glide.authenticate.multisso.enabled`) muss sich der Administrator als ACR-Benutzer registrieren.

  Hinweis: Wenn Sie diese Eigenschaft auf „falsch“ setzen, wird die Mehrfachanbieter-SSO nicht deaktiviert, wenn auch die Accountwiederherstellung (ACR) in der Instanz aktiviert ist. Um sich mit einem Anwendernamen und einem Passwort anzumelden, muss ACR auch mit der Eigenschaft *`glide.sso.acr.enabled`* deaktiviert werden. Einzelheiten zu dieser Eigenschaft finden Sie unter Eigenschaften für die Accountwiederherstellung.

- Der Administrator muss ein Passwort für die lokale Anmeldung festlegen und MFA registrieren, bevor er sich als ACR-Anwender anmeldet.

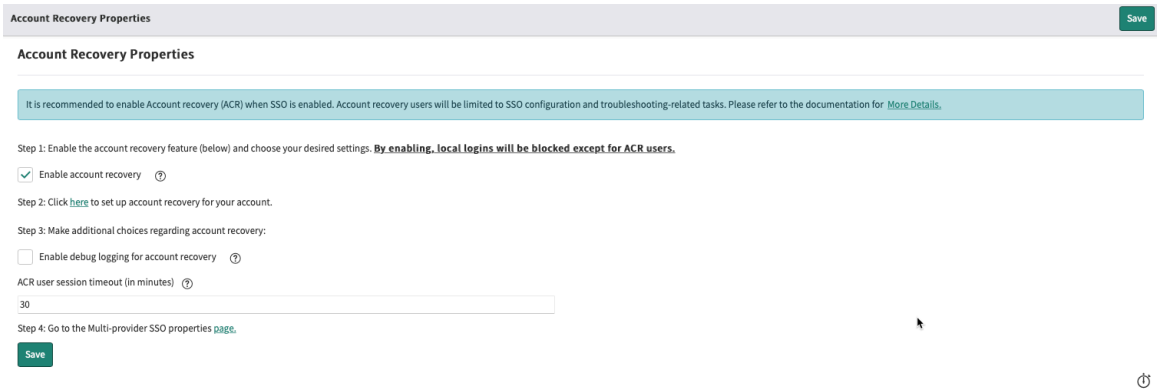
Prozedur

1. Navigieren zu **Alle** > **Accountwiederherstellung** > **Eigenschaften**an.
2. Klicken Sie **auf Accountwiederherstellung aktivieren**.

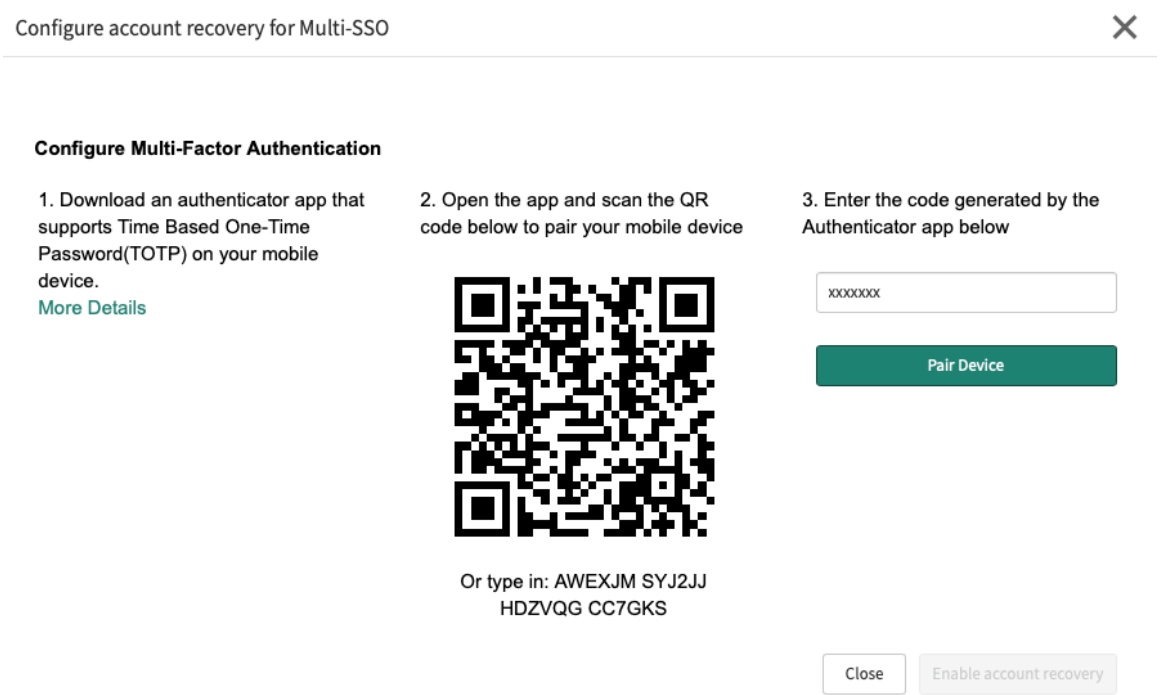
   Hinweis: Sie müssen die Accountwiederherstellung aktivieren, wenn SSO aktiviert ist. Anwender der Accountwiederherstellung sind auf SSO-Konfigurations- und Problembehandlungsaufgaben beschränkt.

3. Klicken Sie **hier** auf den Text in Schritt 2.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Befolgen Sie die Bildschirmanweisungen im Modal **„Accountwiederherstellung für Multi-SSO konfigurieren“**.



Nach Abschluss der Schritte auf dem Bildschirm wird die **Option Accountwiederherstellung** aktivieren aktiviert.

5. Klicken Sie **auf Accountwiederherstellung aktivieren**.

Ergebnisse

Sie haben Ihren Anwenderaccount als Accountwiederherstellungsanwender konfiguriert. Sie können diesen Account verifizieren und alle anderen konfigurierten Anwender für die Accountwiederherstellung anzeigen, indem Sie zu navigieren **Mehrfachanbieter-SSO** > **Accountwiederherstellung** > **Anwender**an.

Konfigurieren Sie einen Accountwiederherstellungsbenutzer über ein Administratorbenutzerprofil

Konfigurieren Sie im Administratorbenutzerprofil einen -Administrator als Accountwiederherstellungsbenutzer.

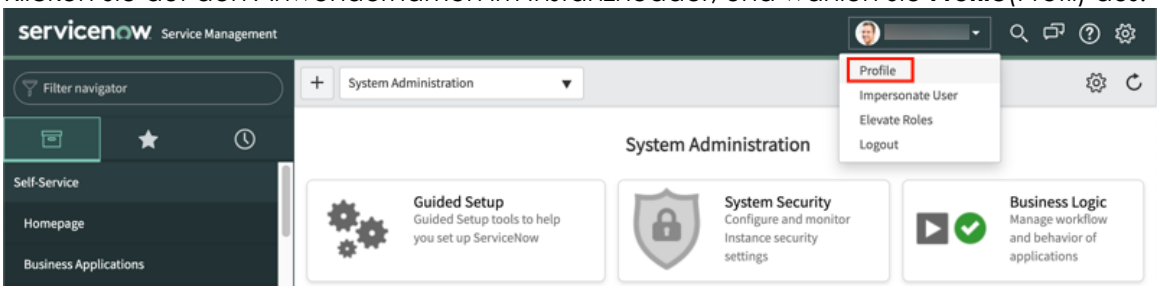
Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

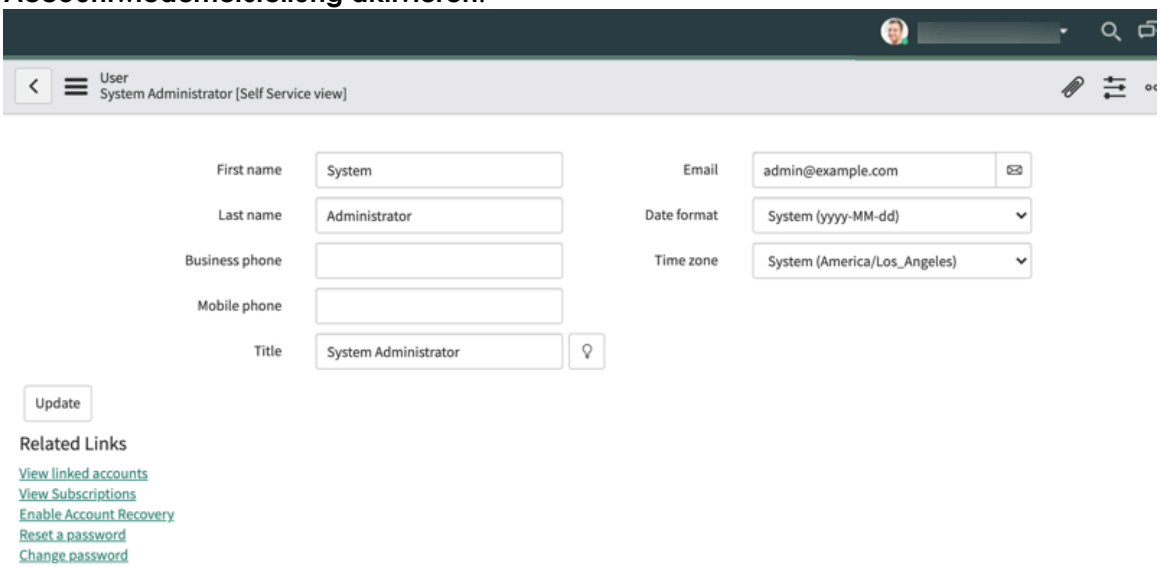
Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Melden Sie sich mit einem Administratorkonto bei Ihrer -Instanz an.
2. Klicken Sie auf den Anwendernamen im Instanzheader, und wählen Sie **Profile**(Profil) aus.



3. Klicken Sie im Formular „ **Benutzer** “ im Abschnitt „ **Zugehörige Links** “ auf **Accountwiederherstellung aktivieren**.

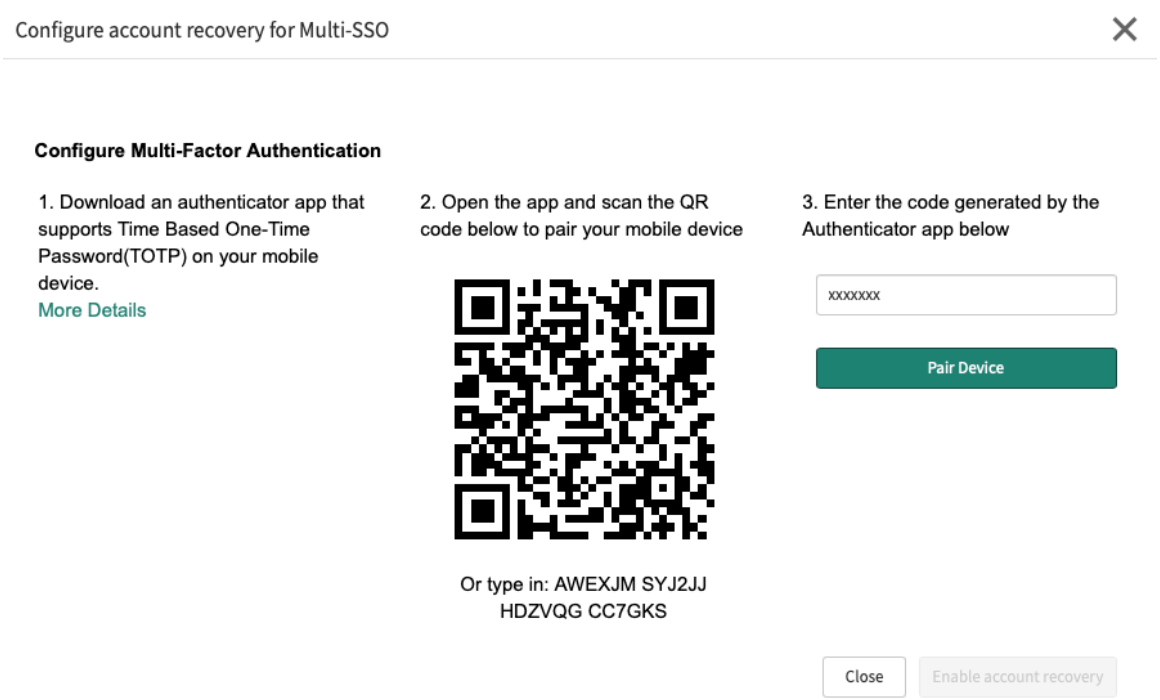


Hinweis:

Wenn für den ausgewählten Anwender bereits die Accountwiederherstellung aktiviert ist, wird **Accountwiederherstellung** aktivieren nicht in den zugehörigen Links angezeigt. Stattdessen wird die Option **Accountwiederherstellung deaktivieren angezeigt**.

4. Befolgen Sie die Bildschirmanweisungen im Modal **„Accountwiederherstellung für Multi-SSO konfigurieren“**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Nach Abschluss der Schritte auf dem Bildschirm wird die **Option Accountwiederherstellung** aktivieren aktiviert.

5. Klicken Sie **auf Accountwiederherstellung aktivieren**.

Ergebnisse

Sie haben Ihren Anwenderaccount als Accountwiederherstellungsanwender konfiguriert. Sie können diesen Account verifizieren und alle anderen konfigurierten Anwender für die Accountwiederherstellung anzeigen, indem Sie zu navigieren **Mehrfachanbieter-SSO** > **Accountwiederherstellung** > **Anwender**an.

Eigenschaften für die Accountwiederherstellung

Verwenden Sie die Systemeigenschaften, um die Accountwiederherstellung (Account Recovery, ACR) in Ihrer -Instanz zu konfigurieren.

Greifen Sie auf die Eigenschaften zur Accountwiederherstellung in Ihrer Instanz zu, indem Sie zu navigieren **Mehrfachanbieter-SSO** > **Accountwiederherstellung** > **Eigenschaften**an.

Systemeigenschaften für die Accountwiederherstellung

Eigenschaft	Beschreibung
Funktion zur Accountwiederherstellung aktivieren [glide.sso.acr.aktiviert]	Gibt an, ob die Funktion zur Accountwiederherstellung in Ihrer Instanz aktiviert ist. Diese Eigenschaft ist standardmäßig aktiviert.
Debug-Protokollierung für Account-Wiederherstellung aktivieren [glide.sso.acr.debug.log.enabled]	Gibt an, ob Ihre -Instanz Informationen zur Accountwiederherstellung in die Debug-Protokollierung einbezieht. Diese Eigenschaft ist standardmäßig deaktiviert.
Zeitüberschreitung bei ACR-Anwendersitzung (in Minuten) [glide.sso.acr.ui.session.timeout]	Minuten der Inaktivität, bevor Ihre Instanz eine Benutzersitzung zur

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Systemeigenschaften für die Accountwiederherstellung (Fortsetzung)

Eigenschaft	Beschreibung
	Accountwiederherstellung beendet. Diese Eigenschaft hat einen Standardwert von 30.

E-Signatur für Mehrfachanbieter-SSO

Mit der E-Signatur mit Mehrfachanbieter-SSO können Sie die E-Signatur-Eigenschaften anstelle der SAML- oder OIDC-Eigenschaften für die Authentifizierung verwenden.

Zur Verifizierung des Single Sign-on (SSO) während der Authentifizierung und um von Anwendern die Angabe von Anmeldeinformationen vor dem Senden ihrer elektronischen Signatur zu verlangen, können Sie die Authentifizierung so konfigurieren, dass vor dem Senden einer Signatur die Eingabe von Anmeldeinformationen abgefragt wird.

Sie können das Plugin Approvals with e-signature (`com.glide.e_signature_approvals`) installieren, um die E-Signatur-Konfiguration für SSO-Anmeldungen zu erhalten.

Hinweis: Sie müssen Codesignatur Signaturen (`com.glide.code_signing.signatures`) installieren, um das E-Signatur-Plugin zu installieren.

Die Genehmigung mit dem E-Signatur-Plugin aktivieren

Die Genehmigung mit dem E-Signatur-Plugin (com.glide.e_signature_approvals) ermöglicht es Benutzern, Anforderungen zu genehmigen, indem sie ihre Anmeldeinformationen erneut eingeben.

Vorbereitungen

Erforderliche Rolle: admin

Hinweis: Sie müssen Codesignatur Signaturen (`com.glide.code_signing.signatures`) installieren, um das E-Signatur-Plugin zu installieren.

Prozedur

1. Navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie das Plugin über die Filterkriterien und die Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: `Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.`

   Nach Abschluss der Installation wird eine Meldung angezeigt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Multi-Provider SSO verwenden, um eine SSO-Genehmigung für eine SAML 2.0-Authentifizierung einzurichten

Eine SSO-Genehmigung mit E-Signatur erfordert die Konfiguration der SAML-IdP und der ServiceNow-Instanz.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Das SAML-IdP muss das forceAuthn-Attribut in SAML-Bestätigungsanforderungen unterstützen und berücksichtigen. Die E-Signatur funktioniert ohne diese IdP-Einstellung nicht. Richten Sie eine Genehmigung mit E-Signatur ein, indem Sie Anmeldeinformationen aus einer SAML 2.0-Authentifizierung verwenden.

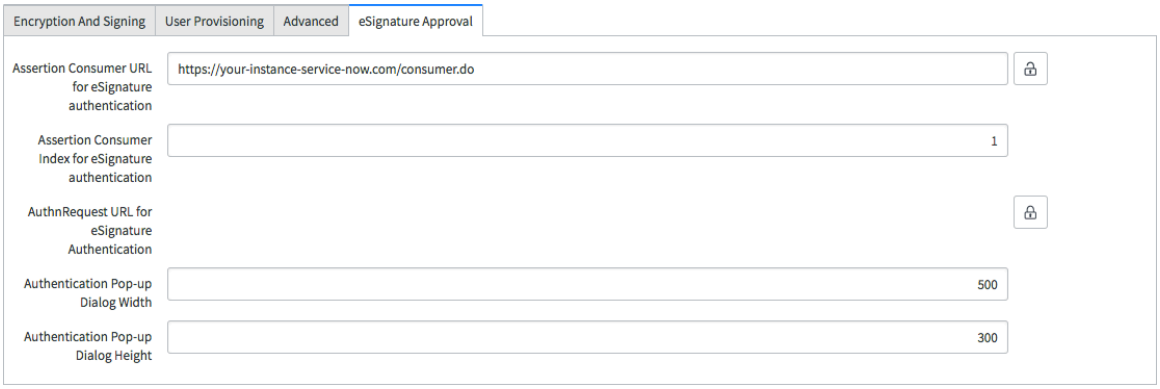
Prozedur

1. Aktivieren Sie SAML 2.0 mit dem Plugin Multi-Provider-SSOaktivieren, oder führen Sie ein Upgrade auf SAML 2.0 durch.
2. Aktivieren Sie das Plugin für die Genehmigung mit E-Signatur.
3. Navigieren zu **Mehrfachanbieter-SSO** > **Identity Provider** und verifizieren Sie, dass auf der Registerkarte „Erweitert“ das Attribut **„AuthnRequest erzwingen“ aktiviert ist**.
   Ihr SAML 2.0-IdP muss das Attribut **„AuthnRequest erzwingen“** unterstützen. Andernfalls wird die E-Signatur nicht unterstützt.
4. Geben Sie auf der Registerkarte eSignature-Genehmigung die folgenden SAML-Eigenschaften für die eSignature ein.

Option	Bezeichnung
Assertionen-Verbraucher-URL für eSignatur-Authentifizierung	Diese Eigenschaft ist standardmäßig auf die entsprechende URL voreingestellt. Um diese Eigenschaft zu konfigurieren, wählen Sie das Sperrsymbol, um dieses Feld bearbeitbar zu machen. Wählen Sie nach der Bearbeitung das Symbol aus, um das Feld zu sperren.
Assertionen-Verbraucher-Index für eSignatur-Authentifizierung	Wenn für Ihren Dienstanbieter mehr als eine URL für die AssertionConsumerURL festgelegt ist, können Sie den Index für die E-Signatur beginnend mit Index 1 oder höher festlegen.
AuthnRequest-URL für die E-Signatur-Authentifizierung	Sie können die URL eingeben, die auf die SAML 2.0 IdP AuthnRequest-URL für die E-Signatur-Authentifizierung verweist. Wenn die URL mit der Assertionen-Verbraucher-URL identisch ist, können Sie diese Einstellung leer lassen.
Breite des Popup-Dialogfelds zur Authentifizierung	Wenn ein Benutzer eine Anforderung mit E-Signatur genehmigt, wird ein Dialogfeld geöffnet und ein Benutzer kann Anmeldeinformationen eingeben. Diese Einstellung steuert die Breite dieses Dialogfelds. Der Standardwert ist 500.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
Höhe des Popup-Dialogfelds zur Authentifizierung	Wenn ein Benutzer eine Anforderung mit E-Signatur genehmigt, wird ein Dialogfeld geöffnet und ein Benutzer kann Anmeldeinformationen eingeben. Diese Einstellung steuert die Höhe dieses Dialogfelds. Der Standardwert ist 300.



5. Wählen Sie die Schaltfläche **Metadaten generieren** unter den Registerkarten aus, um die Metadaten des Service Providers neu zu generieren.
6. Kopieren Sie die Metadaten des Service Providers, und aktualisieren Sie sie auf dem SAML-IdP.

Verwenden Sie Mehrfachanbieter-SSO, um eine SSO-Genehmigung für eine OIDC-Authentifizierung einzurichten

Eine SSO-Genehmigung mit E-Signatur erfordert die Konfiguration der SAML-IdP und der ServiceNow-Instanz.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Das SAML-IdP muss das forceAuthn-Attribut in SAML-Bestätigungsanforderungen unterstützen und berücksichtigen. Die E-Signatur funktioniert ohne diese IdP-Einstellung nicht. Richten Sie eine Genehmigung mit E-Signatur ein, indem Sie Anmeldeinformationen aus einer SAML 2.0-Authentifizierung verwenden.

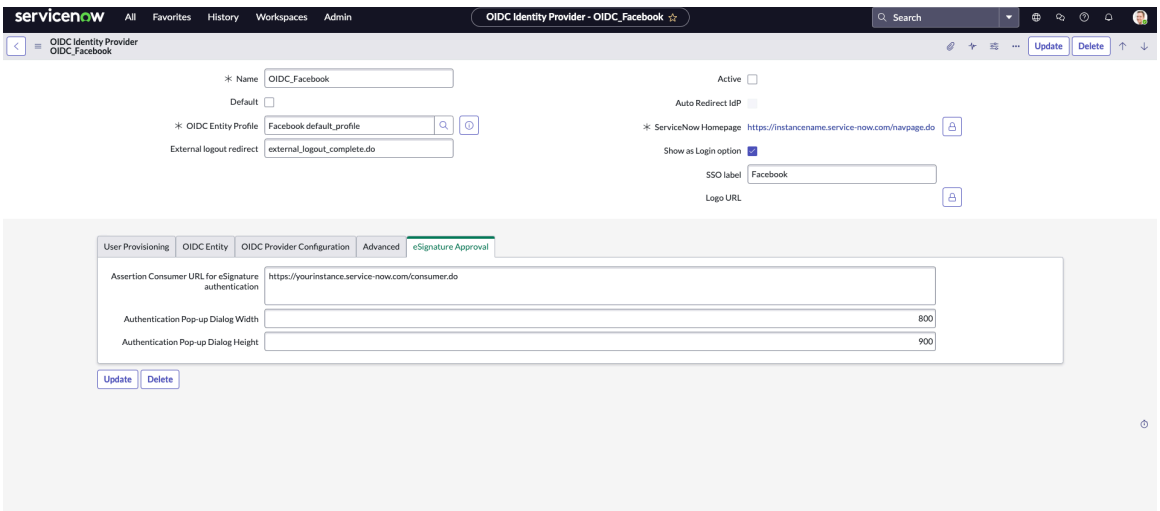
Prozedur

1. Aktivieren Sie das Plugin für die Genehmigung mit E-Signatur.
2. Navigieren zu **Mehrfachanbieter-SSO** > **Identity Provider** und überprüfen Sie Ihre OIDC-Providerkonfigurationen
3. Geben Sie auf der Registerkarte eSignature-Genehmigung die folgenden SAML-Eigenschaften für die eSignature ein.

Option	Bezeichnung
Assertionen-Verbraucher-URL für eSignatur-Authentifizierung	Diese Eigenschaft ist standardmäßig auf die entsprechende URL voreingestellt. Um diese Eigenschaft zu konfigurieren, wählen Sie das Sperrsymbol, um dieses Feld bearbeitbar zu

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	machen. Wählen Sie nach der Bearbeitung das Symbol aus, um das Feld zu sperren.
Breite des Popup-Dialogfelds zur Authentifizierung	Wenn ein Benutzer eine Anforderung mit E-Signatur genehmigt, wird ein Dialogfeld geöffnet und ein Benutzer kann Anmeldeinformationen eingeben. Diese Einstellung steuert die Breite dieses Dialogfelds. Der Standardwert ist 800.
Höhe des Popup-Dialogfelds zur Authentifizierung	Wenn ein Benutzer eine Anforderung mit E-Signatur genehmigt, wird ein Dialogfeld geöffnet und ein Benutzer kann Anmeldeinformationen eingeben. Diese Einstellung steuert die Höhe dieses Dialogfelds. Der Standardwert ist 900.



4. Wählen Sie Absenden, wenn Sie die E-Signatur während des ersten **OIDC** -Setups konfigurieren, oder **Aktualisieren**, wenn Sie die Details in der E-Signatur aktualisieren möchten.

OpenID Connect (OIDC) als Identitätsanbieter (IdP) mit Single Sign-On (SSO)

OpenID Connect (OIDC) ist eine Identitätsebene, die auf dem OAuth-Protokoll aufbaut und Ihnen und Ihren Endanwendern eine moderne und intuitive SSO-Experience (Single Sign-on) bietet. OIDC verbessert auch die Anmelde-Experience für mobile Anwendungen, indem Benutzer die Möglichkeit erhalten, sich bei ServiceNow -Anwendungen mit ihrem Social Identity Provider anzumelden. Beispielsweise können Administratoren Single Sign-on mit einem Drittpartei-Identitätsanbieter konfigurieren, der OpenID Connect unterstützt. Benutzer haben dann die Möglichkeit, sich bei Ihrer anwenderdefinierten Anwendung ServiceNow mit den Anmeldeinformationen ihres Identitätsanbieters anzumelden.

Sie können soziale Identitätsanbieter wie Google für Ihre Business-to-Customer-Benutzer (B2C) und Unternehmensidentitätsanbieter wie Okta , Microsoft Azure AD für Ihre Business-to-Business-Benutzer verwenden.

Eine OpenID Connect-Konfiguration (OIDC) für Single Sign-on (SSO) erstellen

Erstellen oder aktualisieren Sie eine OpenID Connect(OIDC)-Konfiguration mithilfe des Mehrfachanbieter-SSO-Plugins.

OpenID Connect-Konfiguration (OIDC) für Single Sign-on (SSO)

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Registrieren Sie eine OIDC-Anwendung bei Ihrem Identitätsanbieter (IdP), und notieren Sie sich die Client-ID, den geheimen Clientschlüssel und die bekannte Konfigurations-URL.
- Aktivieren Sie das Mehrfachanbieter-SSO-Plugin
- Konfigurieren Sie Eigenschaften für Mehrfachanbieter-SSO
- Aktivieren Sie das Plugin „Genehmigung mit e-Signature “, um eSignature für den OIDC-IdP zu aktivieren.
- Erforderliche Rolle: admin

Wenn Sie über eine Client-ID, einen geheimen Clientschlüssel und eine bekannte Konfigurations-URL des Identitätsanbieters verfügen, können Sie die OIDC-Konfiguration für SSO direkt importieren.

Hinweis: Die Anmeldeoption mit OIDC-IdP wird nicht unterstützt, wenn das Plugin „Domain Separation“ installiert ist.

Wenn Sie nicht über die erforderlichen Informationen zum Identitätsanbieter verfügen, können Sie OIDC für SSO manuell konfigurieren. Nach Abschluss der Konfiguration können sich Benutzer mit externen Identitätsanbietern für soziale Medien wie Google OktaServiceNow] bei den Anwendungen anmelden.

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identity Provider**an.
2. Wählen Sie eine der folgenden Optionen aus.
   - Klicken Sie auf einen Datensatz eines OIDC-Identitätsanbieters, um eine vorhandene Konfiguration zu aktualisieren.
   - Um eine neue Konfiguration zu erstellen, klicken Sie auf **Neu**, und wählen Sie **OpenID Connect**aus.
3. Geben Sie für eine neue Konfiguration die OIDC-Konfigurationsinformationen mit einer der folgenden Methoden ein.

Option	Bezeichnung
Importieren Sie die bekannte OpenID Connect-Konfiguration	Wenn Sie die bekannte Konfigurations-URL zusammen mit den zugehörigen Client-Anmeldeinformationen haben, können Sie eine OIDC-Konfiguration direkt importieren. **Hinweis:** Wenn Sie die bekannte OIDC-Konfiguration importieren, werden alle zugehörigen Felder automatisch ausgefüllt.
Konfigurieren Sie das Formular „OIDC-Identitätsanbieter“ manuell	Wenn keine OAuth-OIDC-Entität vorhanden ist, schließen Sie das Popup-Fenster Import OpenID Connect Known Configuration (Bekannte OpenID Connect-Konfiguration importieren) und füllen Sie die Felder im Formular OIDC-Identitätsanbieter manuell aus.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Importieren Sie die Felder „OpenID Connect Known Configuration“.

Eigenschaft	Beschreibung
Name	Eindeutiger Name für die Konfiguration des OIDC-Identitätsanbieters.
Client-ID	Client-ID der Anwendung, die beim OIDC-Drittpartei-Identitätsanbieter registriert ist.
Geheimer Clientschlüssel	Geheimer Clientschlüssel der Anwendung, die beim OIDC-Identitätsanbieter der Drittpartei registriert ist.
Bekannte Konfigurations-URL	URL, die Metadaten zum Drittpartei-OIDC-Identitätsanbieter enthält.

Alle Pflichtfelder müssen im Formular „OIDC-Identitätsanbieter“ ausgefüllt werden.

Bevor Sie das Formular „OIDC-Identitätsanbieter“ manuell ausfüllen, vergewissern Sie sich, dass Sie bereits ein OAuth-Entitätsprofil für den OIDC-IdP haben.

Wenn Sie kein OAuth-Entitätsprofil haben, können Sie es mit den Standardvorlagen für externe OIDC-Anbieter wie Okta, Azure und anderen erstellen.

Der Gewährungstyp des OAuth-Entitätsprofils muss mit einem Autorisierungscode lauten. Weitere Informationen finden Sie unter Einen OAuth-OIDC-Anbieter auf der Now Platform konfigurieren.

Hinweis: Sie können die Vorlagen von Drittanbieter-Identitätsanbietern verwenden. Auth0, Azure AD, Google und Okta sind in den Demodaten des Plugins „Single Sign-on-Installationsprogramm für mehrere Anbieter“ verfügbar.

OIDC-Identitätsanbieter-Felder

Eigenschaft	Beschreibung
Name	Name des OIDC-Identitätsanbieter-Datensatzes.
Aktiv	Option zum Aktivieren der OIDC-IdP-Konfiguration. **Hinweis:** Diese Option kann erst nach einer erfolgreichen Testverbindung aktiviert werden.
Standard	Option zum Festlegen der OIDC-IdP-Konfiguration als Standard, wenn mehr als eine OIDC-Konfiguration vorhanden ist.
Automatische IdP-Weiterleitung	Option zum Aktivieren der automatischen Umleitung der Anwender zur Anmeldeseite des Identitätsanbieters. Dieses Feld zeigt an, wenn im Abschnitt „Zugehörige Links“ die Option **Als automatische IdP** -Weiterleitung festlegen festgelegt ist. **Hinweis:** Wenn Sie eine neue IdP-Konfiguration für die automatische Weiterleitung aktivieren, wird das Cookie *glide_sso_id* automatisch mit dem neuen IdP für die automatische Weiterleitung aktualisiert. Die Systemeigenschaft *glide.authenticate.sso.update.idp.cookie* steuert diese Funktion.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
OIDC-Entitätsprofil	OAuth-Entitätsprofil für die OIDC-Konfiguration.
ServiceNow Homepage	Die URL der für die Authentifizierung verwendeten Anmeldeseite. Dieses Feld wird automatisch auf Ihre Instanz-URL festgelegt. Das Format der URL lautet: `https://yourinstance.service-now.com/navpage.do`
Weiterleitung für externe Abmeldung	Die URL, an die Anwender von der Integration nach der Abmeldung weitergeleitet werden. Normalerweise das -Portal, das für SSO verwendet wird. Dieses Feld wird automatisch auf „ `external_logout_complete.do` “ festgelegt. Beispiel: `https://IhreInstanz.service-now.com/external_logout_complete.do`
Als Anmeldeoption anzeigen	Option zum Anzeigen des OIDC-IdP als Anmeldeoption auf der Anmeldeseite. Als Anmeldeoption wird die **Anmeldung mit der Schaltfläche „Identitätsanbieter** “ angezeigt.
SSO-Bezeichnung	Bezeichnung des OIDC-IdP, die auf der Anmeldeseite angezeigt wird. Dieses Feld wird nur angezeigt, wenn **die Option Als Anmeldung anzeigen** aktiviert ist.
Logo-URL	Öffentlich verfügbare URL, die das Logo des OIDC-IdP-Anbieters enthält. Dieses Feld wird nur angezeigt, wenn **die Option Als Anmeldung anzeigen** aktiviert ist.

4. Wahlweise: Aktivieren Sie die automatische Anwenderbereitstellung auf der Registerkarte Anwenderbereitstellung>Registerkarte Anwenderbereitstellung.

   (Optional) Sie können die automatische Anwenderbereitstellung während der Anwenderanmeldung aktivieren. Wenn die automatische Anwenderbereitstellung aktiviert ist, wird in der ServiceNow-Instanz automatisch ein Anwenderdatensatz erstellt, wenn dieser Anwenderdatensatz nicht vorhanden ist.

Felder für die Anwenderbereitstellung

Eigenschaft	Beschreibung
Anwender automatisch bereitstellen	Option zum Aktivieren der automatischen Anwenderbereitstellung. Diese Eigenschaft erstellt einen Anwender in der Instanzanwendertabelle (sys_user), wenn der Anwender den IdP beendet, aber nicht in der Anwendertabelle vorhanden ist.
Bereitstellen mit	Datenquelle, die zum Transformieren eines `ID-Tokens`, eines `Anwenderinformations` -Endpunkts oder von `ID-Token und Anwenderinformationen` in einen ServiceNow-Anwender verwendet werden soll. Verwenden Sie die Liste „Nachschlagen“, um die vordefinierte Datenquellenvorlage auszuwählen, und öffnen Sie dann den Datensatz, um die Tabellenzuordnung für Transformationen zu konfigurieren.
Bereitstellungsdatenquelle	ID-Token-Datenquelle, die für die Anwenderbereitstellung verwendet wird.
Datenquelle von Anwenderinformationen	Die Endpunkt-Datenquelle für Anwenderinformationen, die für die Anwenderbereitstellung verwendet wird. Dieses Feld wird angezeigt, wenn `Anwenderinformationen` oder

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	`ID-Token und Anwenderinformationen` für das Feld **Bereitstellen mit** ausgewählt sind.
Anwender bei der nächsten Anmeldung aktualisieren	Option zum Aktivieren der Anwenderaktualisierung während der nächsten Anmeldung.
Anwenderintervallzeit aktualisieren (Sekunden)	Mindestzeitraum in Sekunden für die Aktualisierung eines Anwenderdatensatzes zwischen nachfolgenden Anmeldungen. Dieses Feld wird automatisch auf 3.600 Sekunden festgelegt. Beispiel: Nachdem sich ein Anwender angemeldet hat, wird der Anwenderdatensatz nach 3.600 Sekunden bis zur nächsten Anmeldung aktualisiert. Dieses Feld ist nur verfügbar, wenn das Feld **Anwender bei nächster Anmeldung** aktualisieren aktiviert ist.
Auf bereitgestellte Anwender angewendete Anwenderrollen	Liste der Rollen, die auf die neu bereitgestellten Anwender angewendet werden.

5. Registerkarte „OIDC-Entität“.
   Sie können die OIDC-Clientkonfiguration und den OIDC-Verbindungs-Flow mithilfe des Entitätsdatensatzes anzeigen und ändern.
6. Registerkarte OIDC-Providerkonfiguration
   Sie können die bekannte Konfigurations-URL der Validierung der OIDC-IdP- oder ID-Token-Anforderung anzeigen und ändern.
7. Wahlweise: Registerkarte „Erweitert“

   (Optional) Skripts, die während des Single Sign-on und der Abmeldung ausgeführt werden.

Erweiterte Felder

Eigenschaft	Beschreibung
Single Sign-on-Skript	Skript, das während Single Sign-on ausgeführt wird. Dieses Feld wird automatisch auf `MultiSSO_OIDC_custom festgelegt`.
Abmeldeskript	Skript, das ausgeführt wird, nachdem sich der Anwender abgemeldet hat. Dieses Feld wird automatisch auf `MultiSSO_OIDC_logout_custom festgelegt`.

8. Wahlweise: Konfigurieren Sie auf der Registerkarte eSignature-Genehmigung die eSignature für den OIDC-IDP.

   Hinweis: Die Registerkarte „eSignature-Genehmigung“ wird nur angezeigt, wenn Sie das Plugin „ **Genehmigung mit e-Signature** “ (com.glide.e_signature_approvals) installieren.

eSignature-Genehmigungsfelder

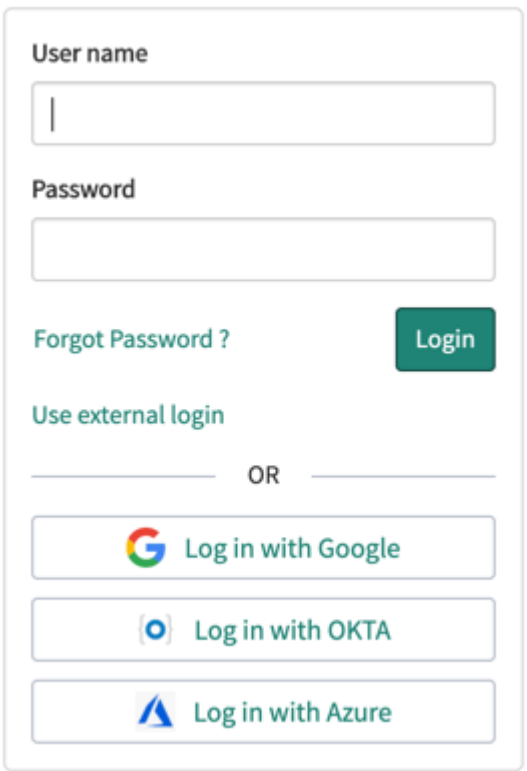
Eigenschaft	Beschreibung
Assertionen-Verbraucher-URL für eSignatur-Authentifizierung	Wenn Sie eine anwenderdefinierte Methode für die Handhabung der OIDC-Authentifizierung für eSignature verwenden, können Sie eine eigene Verbraucher-

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	URL einrichten. Wenn Sie beispielsweise Mehrfachanbieter-SSO verwenden, müssen Sie diese Eigenschaft nicht verwenden. Das Format der URL ist `https://Ihre-instanz.service-now.com/consumer.do`
Breite des Popup-Dialogfelds zur Authentifizierung	Breite des Popup-Dialogfelds zur Authentifizierung. Dieses Feld wird automatisch auf `800`festgelegt.
Höhe des Popup-Dialogfelds zur Authentifizierung	Höhe des Popup-Dialogfelds zur Authentifizierung. Dieses Feld wird automatisch auf `900`festgelegt.

9. Wahlweise: Navigieren Sie zur Anmeldeseite der Instanz, um zu überprüfen, ob IdP als Anmeldeoption angezeigt wird.
   Die URL muss das folgende Format haben: `https://IhreInstanz/login_mit_sso.do?glide_sso_id=sysId_IdP`

   Hinweis: Wenn Sie **Ausgewählt als Anmeldeoption**aktiviert haben, können Sie zur Anmelde-URL der Instanz wechseln.



Facebook-basiertes Single Sign-on (SSO) verwenden

Melden Sie sich bei der Instanz ServiceNow mit Ihren Facebook -Anmeldeinformationen über die Facebook-basierte SSO an.

Vorbereitungen

Facebook-basiertes SSO ist im Lieferumfang Ihrer Instanz ServiceNow enthalten.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können die Identity Provider-Konfigurationen (Idp) für den IdP **OIDC_Facebook** als Ihre **Identitätsanbieter**definieren. Weitere Informationen zu IDP-Konfigurationen finden Sie unter Ein Facebook-basiertes Single Sign-On (SSO) konfigurieren.

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identity Provider**an.
2. Wählen **Sie OIDC_Facebook aus**.
3. Geben Sie auf der Seite „OIDC_Facebook“ die folgenden Felder an:

Hinweis:

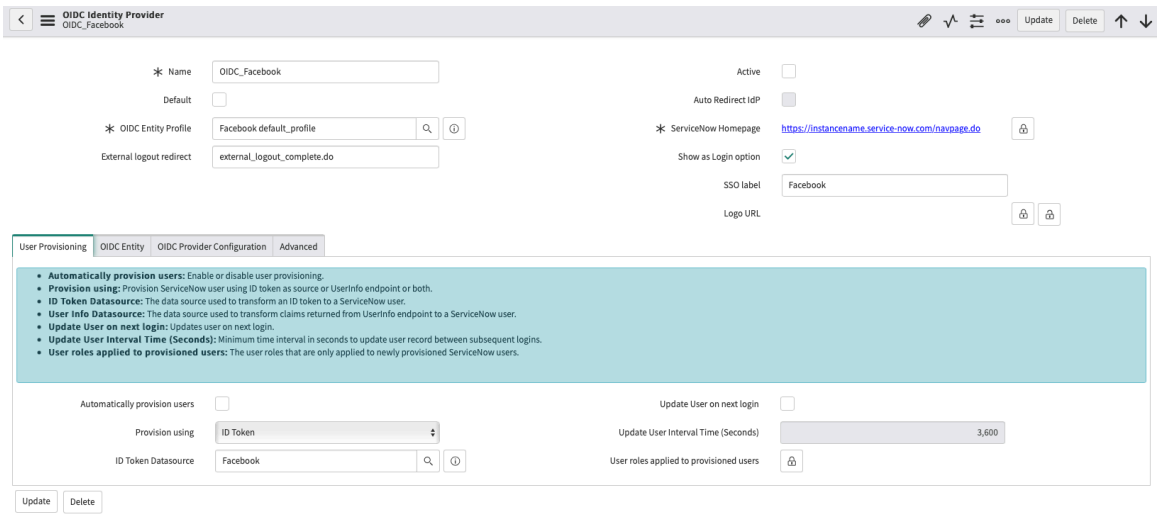
- Die meisten Felder werden bei Verwendung des Standard-IdP automatisch ausgefüllt.
- Details der Homepage ServiceNow müssen angegeben werden.
- Anwenderbezogene Details wie Client-ID und geheimer Clientschlüssel von Facebook müssen innerhalb des IdP angegeben werden.

OIDC_Facebook Details zum Identitätsanbieter

Feld	Beschreibung
Name	Name des OIDC-IdP-Datensatzes. Geben Sie `OIDC_Facebook ein`.
Standard	Option zum Festlegen der OIDC-IdP-Konfiguration als Standard.
OIDC-Entitätsprofil	OAuth-Entitätsprofil für die OIDC-Konfiguration. Geben Sie `Facebook default_profile ein`.
Weiterleitung für externe Abmeldung	Die URL, an die Anwender von der Integration nach der Abmeldung weitergeleitet werden. Normalerweise ist diese URL das Portal, das für SSO verwendet wird. Dieses Feld wird automatisch auf **external_logout_complete.do**festgelegt. Beispiel: `https://`<yourinstance> .service-now.com/external_logout_complete.do
Aktiv	Option zum Aktivieren der OIDC-IdP-Konfiguration. **Hinweis:** Diese Option kann erst nach einer erfolgreichen Testverbindung aktiviert werden.
Automatische IdP-Weiterleitung	Option zum Aktivieren der automatischen Umleitung der Anwender zur Anmeldeseite des Identitätsanbieters.
ServiceNow Homepage	URL der Anmeldeseite, die für die Authentifizierung verwendet wird. Dieses Feld wird automatisch auf Ihre Instanz-URL festgelegt. Das Format der URL ist

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	`https://.`<yourinstance> .service-now.com/navpage.do
Als Anmeldeoption anzeigen	Option zum Anzeigen des OIDC-IdP als Anmeldeoption auf der Anmeldeseite. In diesem Fall wird die Anmeldeoption als Schaltfläche **Mit Facebook** anmelden angezeigt.
SSO-Bezeichnung	Bezeichnung des OIDC-IdP, die auf der Anmeldeseite angezeigt wird. Dieses Feld wird nur angezeigt, wenn **die Option Als Anmeldung anzeigen** aktiviert ist.
Logo-URL	Öffentlich verfügbare URL, die das Logo des OIDC-IdP-Anbieters enthält. Dieses Feld wird nur angezeigt, wenn **die Option Als Anmeldung anzeigen** aktiviert ist.



4. Wahlweise: Öffnen Sie die Registerkarte **Anwenderbereitstellung**, und füllen Sie die Felder aus.

Hinweis: Sie müssen die OIDC-bezogenen Informationen wie Client-ID und Client-Geheimnis Ihrer Benutzer aus Facebookkonfigurieren.

Registerkarte Anwenderbereitstellung

Feld	Beschreibung
Anwender automatisch bereitstellen	Option zum Aktivieren der automatischen Anwenderbereitstellung. Diese Eigenschaft erstellt einen Anwender in der Instanzanwendertabelle [sys_user], wenn der Anwender auf dem IdP vorhanden ist, aber nicht in der Anwendertabelle.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Sie können die automatische Anwenderbereitstellung während der Anwenderanmeldung aktivieren. Wenn die automatische Anwenderbereitstellung aktiviert ist, wird automatisch ein Anwenderdatensatz in der Instanz ServiceNow erstellt, wenn dieser Anwenderdatensatz nicht vorhanden ist.
Bereitstellen mit	Die Datenquelle, die für die Transformation in einen ServiceNow -Benutzer verwendet werden soll. Die Auswahlmöglichkeiten lauten wie folgt: ◦ **Ein ID-Token** ◦ **Endpunkt für Benutzerinformationen** ◦ **Sowohl ID-Token als auch Anwenderinformationen** Verwenden Sie die Liste „Nachschlagen“, um die vordefinierte Datenquellenvorlage auszuwählen, und öffnen Sie dann den Datensatz, um die Tabellenzuordnung für Transformationen zu konfigurieren.
Bereitstellungsdatenquelle	Die Datenquelle des ID-Tokens, die für die Benutzerbereitstellung verwendet wird.
Datenquelle von Anwenderinformationen	Die Endpunkt-Datenquelle für Anwenderinformationen, die für die Anwenderbereitstellung verwendet wird. Dieses Feld wird nur angezeigt, wenn im Feld **Bereitstellen mit** die Option **Benutzerinformationen** oder **ID-Token und Benutzerinformationen gleichzeitig** ausgewählt ist.
Anwender bei der nächsten Anmeldung aktualisieren	Option zum Aktivieren von Anwender-Updates während der nächsten Anmeldung.
Anwenderintervallzeit aktualisieren (Sekunden)	Mindestzeitraum (in Sekunden) für die Aktualisierung eines Anwenderdatensatzes zwischen nachfolgenden Anmeldungen. Dieses Feld wird automatisch auf 3600 Sekunden festgelegt. Beispiel: Nachdem sich ein Anwender angemeldet hat, wird der Anwenderdatensatz nach 3.600 Sekunden bis zur nächsten Anmeldung aktualisiert. Dieses Feld ist nur verfügbar, wenn das Feld **Anwender bei nächster Anmeldung** aktualisieren aktiviert ist.
Auf bereitgestellte Anwender angewendete Anwenderrollen	Liste der Rollen, die auf die neu bereitgestellten Anwender angewendet werden.

5. Auf der Registerkarte **OIDC-Entität** können Sie die OIDC-Clientkonfiguration und den OIDC-Verbindungs-Flow mithilfe des Entitätsdatensatzes anzeigen und ändern.
   Weitere Informationen zur OIDC-basierten Konfiguration finden Sie unter Konfigurieren Sie einen OAuth-OIDC-Provider für die Annahme von Drittanbieter-Token
6. Zeigen Sie auf der Registerkarte **OIDC-Provider-Konfiguration** die bekannte Konfigurations-URL des OIDC-IdP an, und ändern Sie sie.
7. Wahlweise: Öffnen Sie die Registerkarte **Erweitert**, und füllen Sie die Felder aus.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Erweitert“

Eigenschaft	Beschreibung
Single Sign-on-Skript	Das Skript, das während Single Sign-on ausgeführt wird.
Abmeldeskript	Das Skript, das nach dem Abmelden des Anwenders ausgeführt wird.

Hinweis: Skripts werden während des Single Sign-on und der Abmeldung ausgeführt.

8. Klicken Sie auf **Aktiv**, um die Konfiguration zu aktivieren und zu testen.
9. Klicken Sie auf **Aktualisieren**, um den Datensatz zu aktualisieren.
   Im Anmeldeformular wird die Facebook-basierte Anmeldeoption angezeigt.
10. Wenn Sie sich im Anmeldeformular anmelden, gehen Sie wie folgt vor:
    a. Wählen Sie die Option Facebook aus.
    b. Um sich bei der Instanz ServiceNow anzumelden, geben Sie Ihre Facebook -Anmeldeinformationen an.

Ein Facebook-basiertes Single Sign-On (SSO) konfigurieren

Konfigurieren Sie ein Facebook-basiertes SSO für Ihre ServiceNow -Instanz.

Vorbereitungen

Verfügen über eine gültige Client-ID, die als IdP von Facebookkonfiguriert ist.

Aktivieren Sie die folgenden Eigenschaften:

- Aktivieren Sie SSO mit mehreren Providern.
- Aktivieren Sie die Debug-Protokollierung für SSO-Integrationen mit mehreren Anbietern.

Erforderliche Rolle: admin

Prozedur

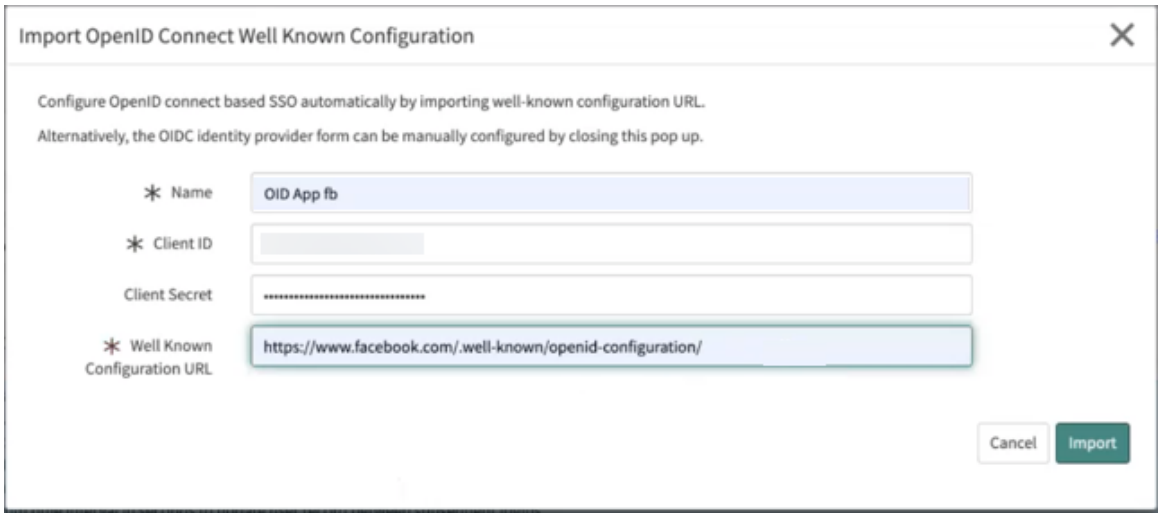
1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identity Provider**an.
2. Um einen neuen Identitätsanbieter Facebook zu erstellen, klicken Sie auf **Neu**.
3. Klicken Sie **auf OpenID Connect**.
4. Füllen Sie die Felder des Formulars aus.

Formular „OpenID Connect – Known Configuration importieren“.

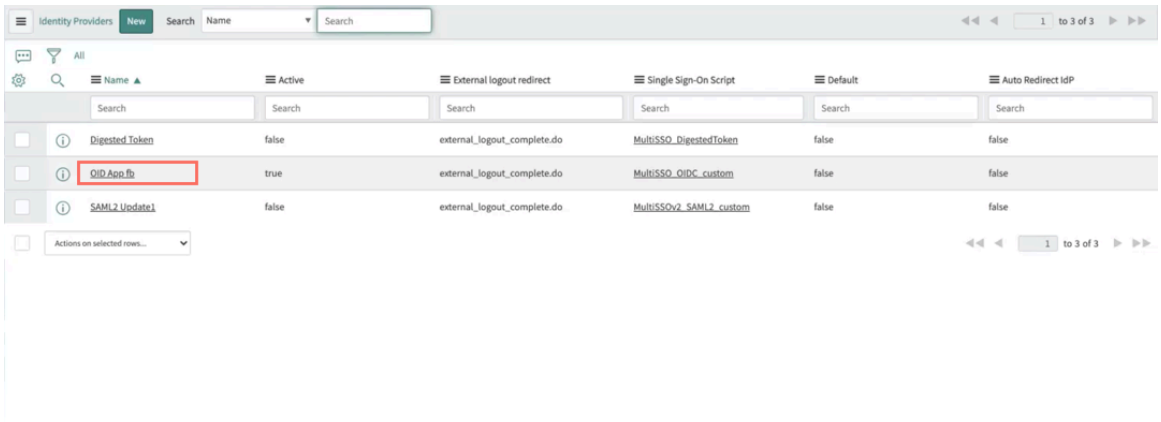
Felder	Beschreibung
Name	Eindeutiger Name für die Konfiguration des OIDC-Identitätsanbieters.
Client-ID	Die Client-ID der Anwendung, die beim OIDC-Identitätsanbieter der Drittpartei registriert ist.
Geheimer Clientschlüssel	Der geheime Clientschlüssel der Anwendung, die beim OIDC-

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder	Beschreibung
	Identitätsanbieter der Drittpartei registriert ist.
Bekannte Konfigurations-URL	Die URL, die Metadaten zum Drittpartei-OIDC-Identitätsanbieter enthält.



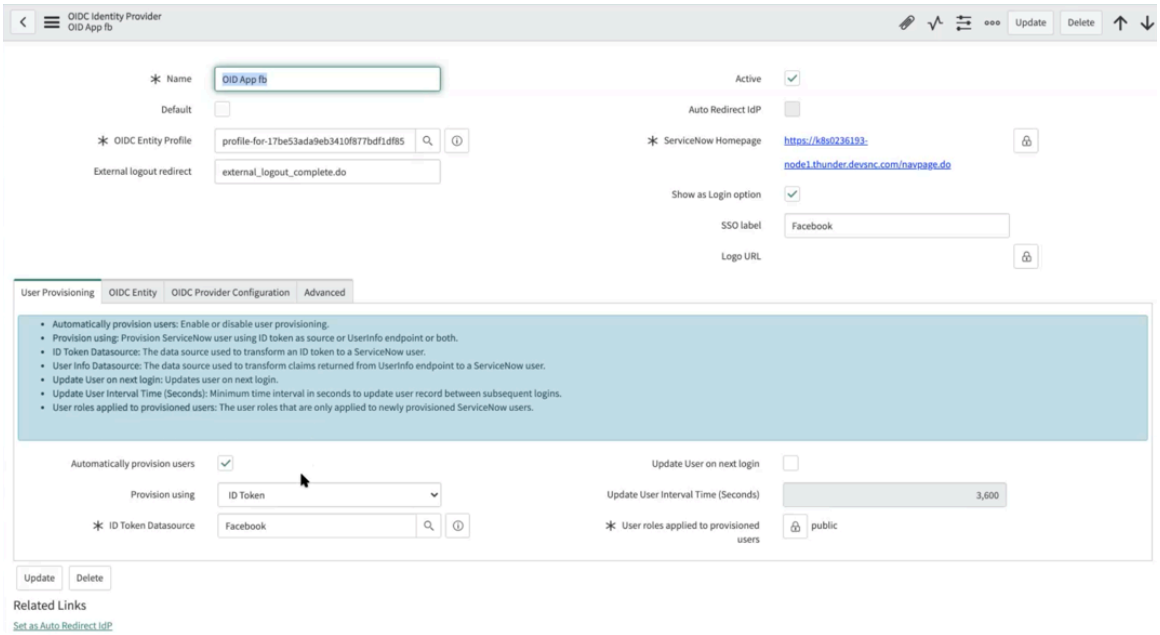
5. Klicken Sie auf **Importieren**.
   Der Facebook-basierte IdP wird erstellt.



6. Wählen Sie den IdP Facebook aus.
7. Gehen Sie im IdP Facebook wie folgt vor:
   a. Validieren Sie alle Felder wie **Name**, **OIDC-Entitätsprofil**, **Weiterleitung**für externe Abmeldung und **ServiceNow Homepage**.
   b. Geben Sie Ihre **SSO-Bezeichnung an**.
8. Geben Sie auf der Registerkarte **Anwenderbereitstellung** die Felder an, die Sie benötigen, um Anwender für bestimmte Anwenderbereitstellungen und Rollen zu konfigurieren.

   Nur die Pflichtfelder sind erforderlich. Die verbleibenden Felder können Sie je nach Bedarf angeben.

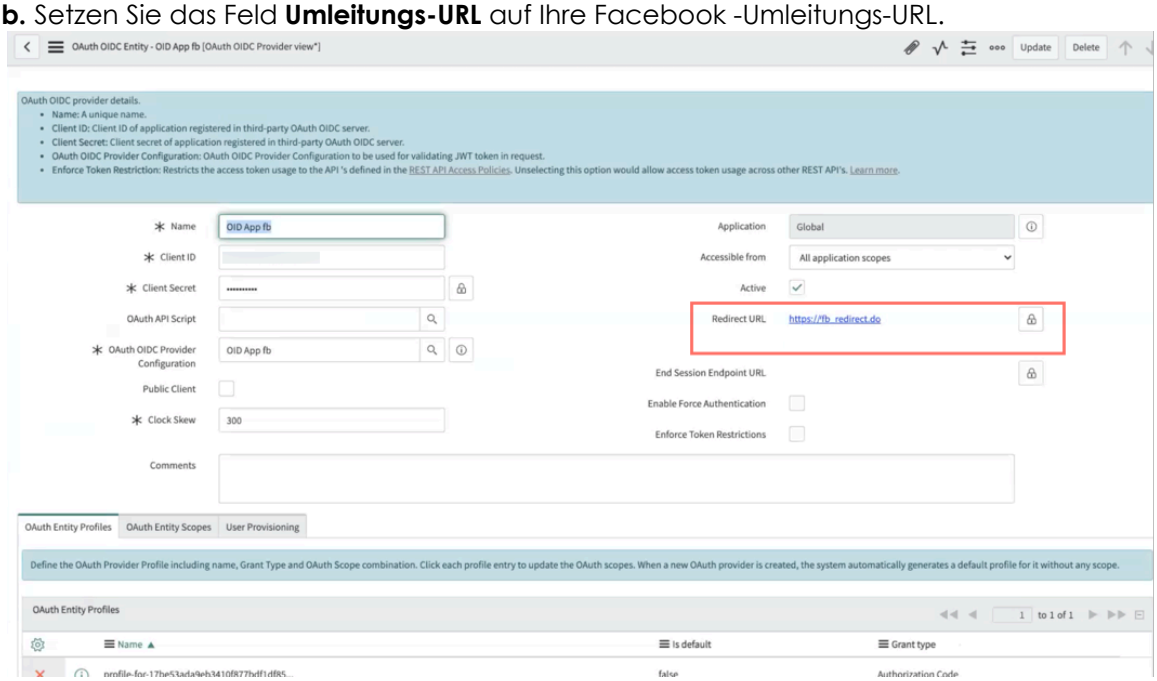
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



9. Gehen Sie auf der Registerkarte **OIDC-Entität** wie folgt vor:

a. Klicken Sie auf die Entität.

b. Setzen Sie das Feld **Umleitungs-URL** auf Ihre Facebook -Umleitungs-URL.

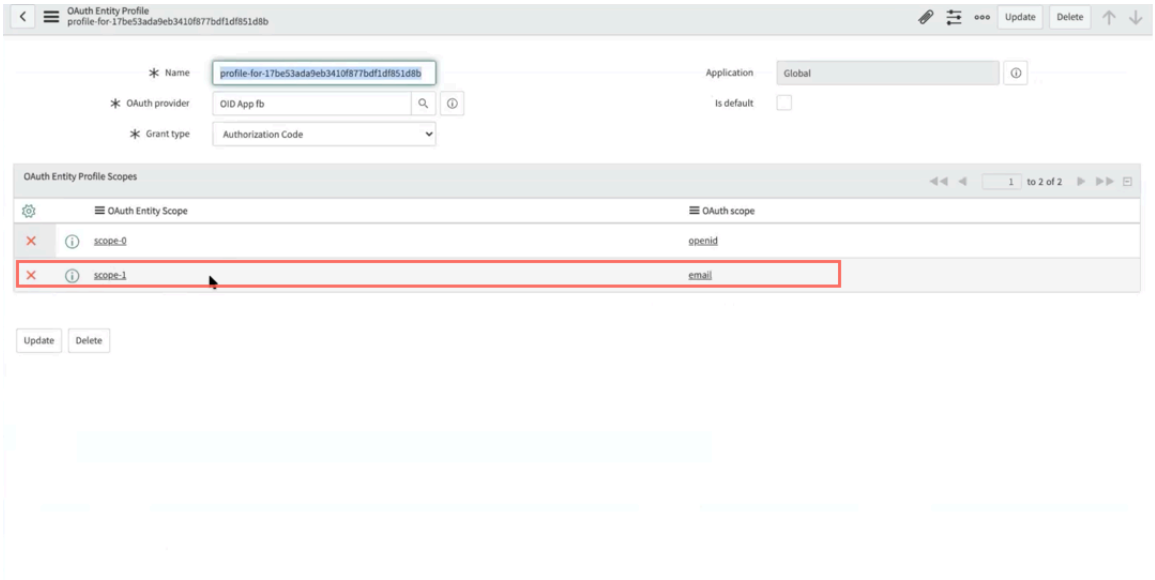


10. Gehen Sie auf der Registerkarte **OAuth-Entitätsprofile** wie folgt vor:

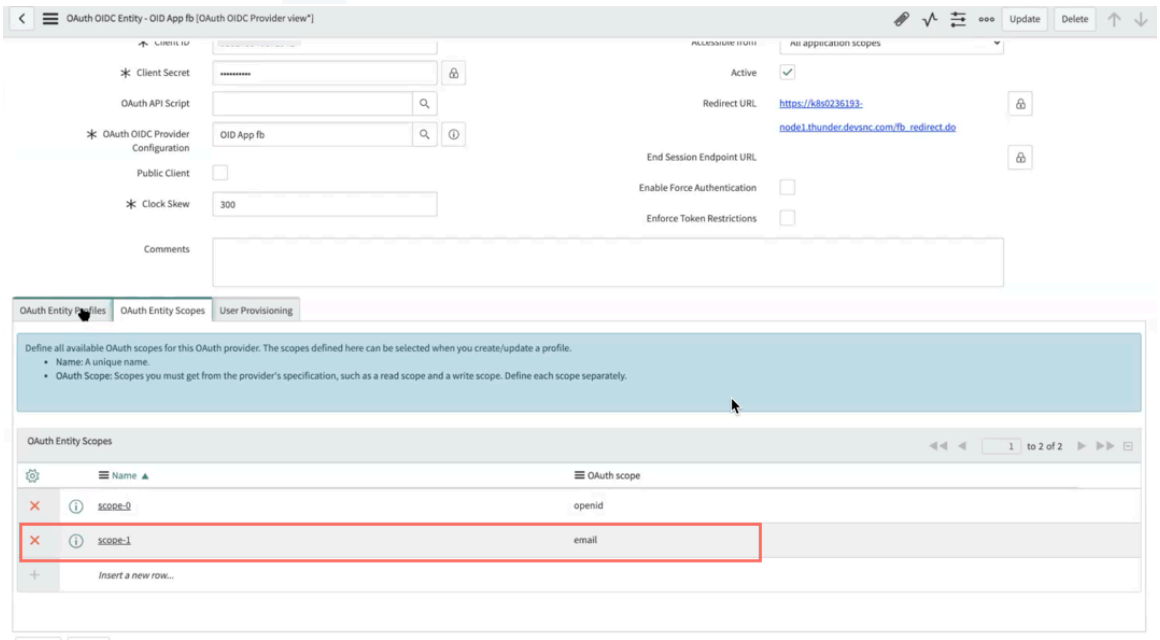
a. Klicken Sie in den Profildetails auf ein Profil.

b. Wählen Sie einen Bereich aus, und überprüfen Sie die Details.
Wählen Sie beispielsweise **scope-1**aus

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



11. Klicken Sie auf der Registerkarte **OAuth-Entitätsbereiche** auf den Link **scope-1**, und fügen Sie den Bereich als E-`Mail`hinzu.

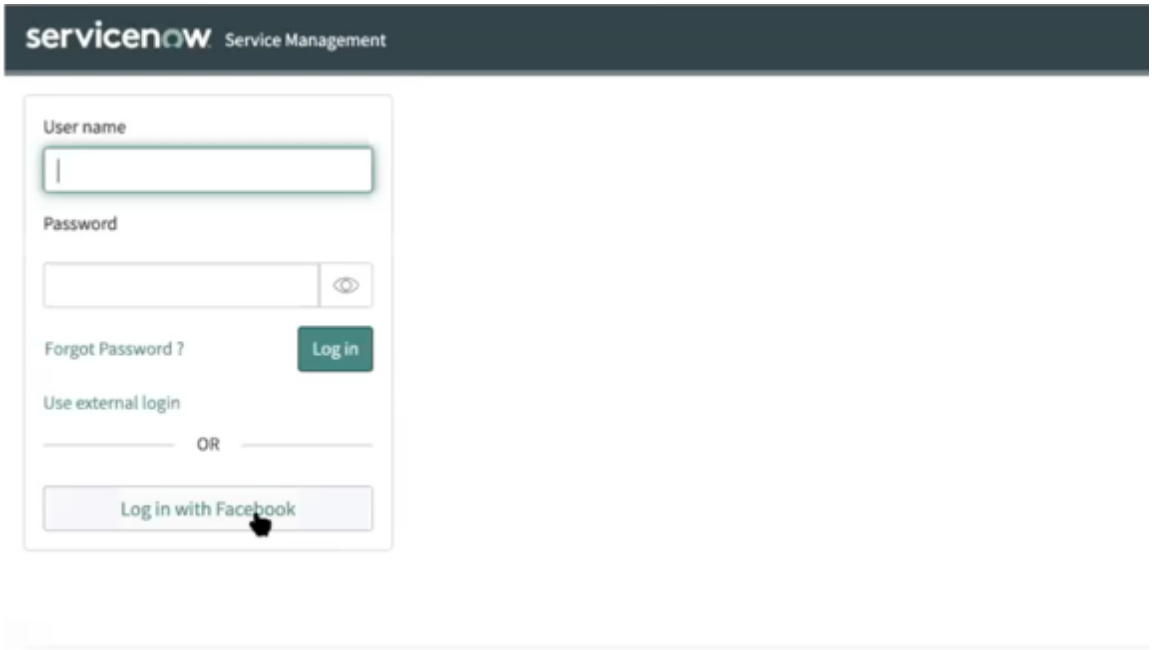


12. Klicken Sie zum Speichern der Konfiguration mit der rechten Maustaste auf den Header, und wählen Sie **Speichern**aus.
13. Um die Konfiguration als aktiv festzulegen, wählen Sie **Aktiv**aus.

Ergebnisse

Benutzer werden mit der SSO-Option Facebook im Anmeldeformular angezeigt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



SAML

Die Security Assertion Markup Language (SAML) ist ein XML-basierter Standard für den Austausch von Authentifizierungs- und Autorisierungsdaten zwischen Sicherheitsdomänen.

SAML tauscht Sicherheitsinformationen zwischen einem Identitätsanbieter (einem Ersteller von Assertionen) und einem Service Provider (einem Verbraucher von Assertionen) aus. SAML ist ein Produkt des Technischen Ausschusses für Sicherheitsservices von OASIS. Bei korrekter Implementierung ist SAML eine der sichersten verfügbaren Single Sign-on-Methoden (Single Sign-on, SSO).

Die SAML 2.0 -Integration ermöglicht SSO durch den Austausch von XML-Token mit einem externen Identitätsanbieter (IdP). Der IdP authentifiziert den Benutzer und übergibt ein NameID-Token an das System. Wenn das System einen Benutzer mit einem übereinstimmenden NameID-Token findet (z. B. die E-Mail-Adresse), meldet die Instanz diesen Benutzer an.

Wenn Sie das SAML 2.0-Plugin für die SSO-Authentifizierung verwenden, müssen Sie die Eigenschaft „glide.ui.rotate_sessions“ auf „falsch“ setzen. Andernfalls wird die Freigabe von Sitzungsinformationen zwischen der -Instanz und dem Identitätsanbieter beeinträchtigt. Benutzer mit der erhöhten Berechtigung „security_admin“ können auf diese Eigenschaft zugreifen.

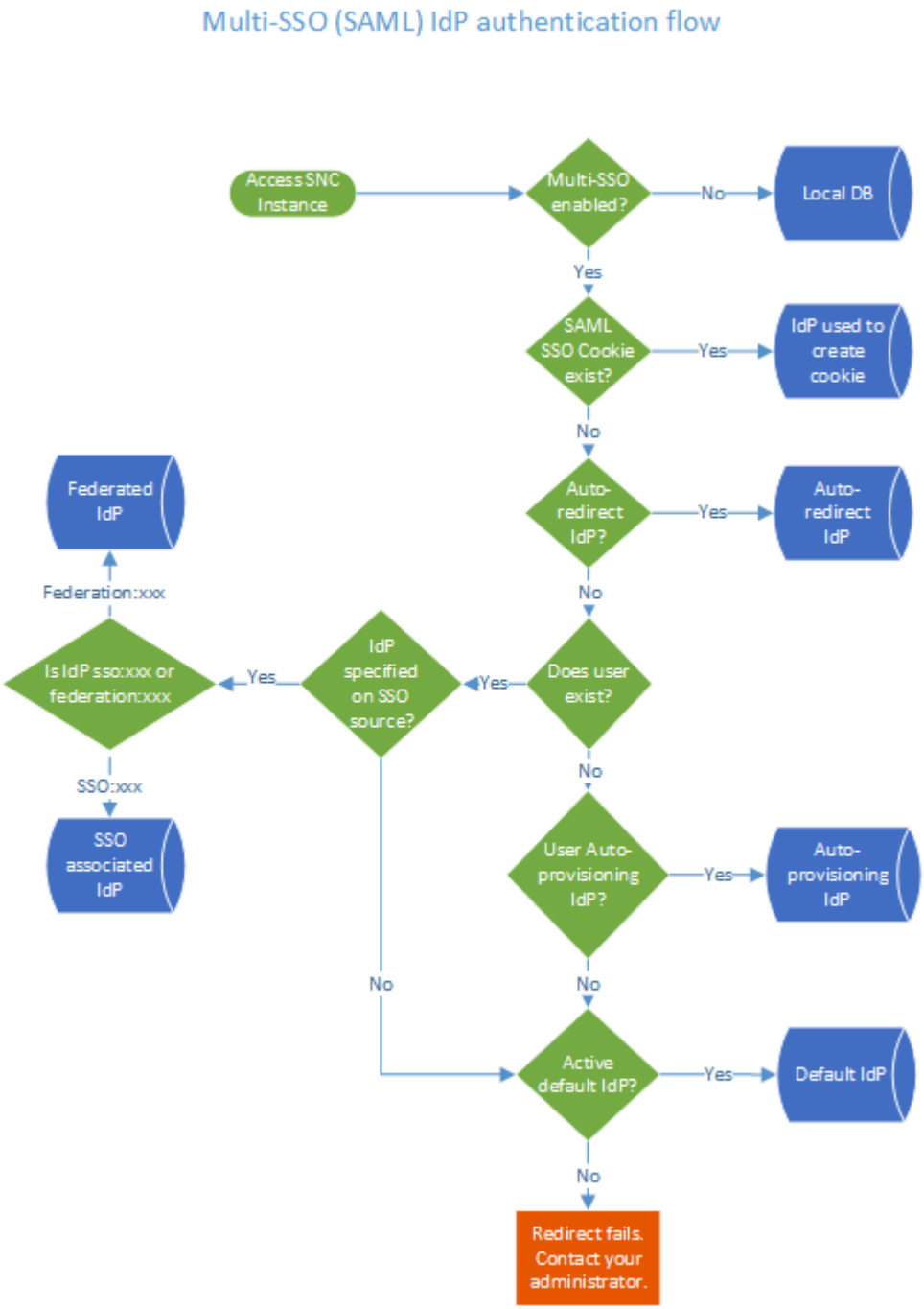
Hinweis: Kunden, die eine vorhandene SAML 2.0-Integration verwenden, wird empfohlen, ein Upgrade auf das Multi-Provider-SSO-Plugin durchzuführen.

SAML-IdP-Authentifizierungs-Flow für Multi-Provider-SSO

Beschreibt die verschiedenen Entitäten, die einen Anwender über SAML-Multi-SSO authentifizieren können.

Sie können dem Authentifizierungs-Flow folgen, um zu verstehen, wann eine Entität einen Benutzer mithilfe von Multi-SSO authentifiziert.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Lokale Datenbank

Wenn Multi-SSO nicht aktiviert ist, wird die Authentifizierung an eine lokale DB weitergeleitet.

SAML-SSO-Cookie-IDP

Wenn ein SAML-SSO-Cookie vorhanden ist, authentifiziert der mit diesem Cookie angegebene IdP den Anwender.

IdP automatisch umleiten

Wenn die automatische IdP-Weiterleitung aktiviert ist, authentifiziert dieser IdP den Anwender.

Föderierter IdP

Wenn der Benutzerbrowser zum Anmeldebildschirm für die externe Autorisierung (login_locate_sso.do) umgeleitet wird und der Benutzer in der Benutzertabelle

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

mit dem im Feld „ **SSO-Quelle** “ festgelegten IdP als „Verbund:xxx“ vorhanden ist, authentifiziert der föderierte IdP den Benutzer.

Zugeordneter IdP

Wenn der Benutzerbrowser zum Anmeldebildschirm für die externe Autorisierung (login_locate_sso.do) umgeleitet wird und der Benutzer in der Benutzertabelle mit dem im Feld **SSO-Quelle** als IdP festgelegten sso:xxx vorhanden ist, authentifiziert der zugeordnete IdP den Benutzer.

IdP mit automatischer Bereitstellung

Wenn der Benutzerbrowser zum Anmeldebildschirm der externen Autorisierung (login_locate_sso.do) umgeleitet wird und der Benutzer nicht in der Benutzertabelle vorhanden ist, die automatische Bereitstellung jedoch aktiviert ist, authentifiziert der IdP mit automatischer Bereitstellung den Benutzer.

Hinweis: Wenn mehr als ein IdP mit automatischer Bereitstellung aktiviert ist, kann der Benutzer den zu verwendenden automatischen Bereitstellungs-IdP auswählen.

Standard-IdP

Wenn der Browser des Benutzers zum Anmeldebildschirm der externen Autorisierung (login_locate_sso.do) umgeleitet wird und der Benutzer entweder:

- Ist in der Benutzertabelle nicht vorhanden, automatische Bereitstellung ist nicht aktiviert, und es ist ein aktiver Standard-IdP vorhanden
- In der Benutzertabelle ist vorhanden, im SSO-Quellanwender- oder Unternehmensdatensatz ist kein IdP angegeben, und es ist ein aktiver Standard-IdP vorhanden

dann authentifiziert der Standard-IdP den Benutzer.

Systemeigenschaften des Identitätsanbieters (IdP).

Ein IdP bietet im Allgemeinen ein XML-Dokument an, das seine Authentifizierungs- und Abmeldemetadaten enthält.

Beispielsweise veröffentlicht SSOCircle seine Metadaten online.

Durchsuchen Sie die IdP-Metadaten, um diese Einträge zu finden:

- Das `SingleSignOnService` -Element mit dem Attribut „ `Binding` “, das den Wert „`HTTP-Redirect`“enthält. Das `Standortattribut` listet die URL auf, die die Integration für den AuthnRequest-Service benötigt.
- Das `SingleLogoutService` -Element mit einem `Bindungsattribut`, das den Wert „`HTTP-Redirect`“ enthält. Das `Standortattribut` gibt die URL an, die die Integration für den SingleLogoutRequest-Service benötigt.

Hinweis: Die SAML 2.0-Integration unterstützt nur die Bindung an IdP-Services per HTTP-Umleitung.

Beispiel:

```
<SingleSignOnServiceBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"Location="https://
idp.ssocircle.com:443/sso/SSORedirect/metaAlias/ssocircle"/>
```

```
<SingleLogoutServiceBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"Location="https://
idp.ssocircle.com:443/sso/IDPSloRedirect/metaAlias/ssocircle"ResponseLoca
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
tion="https://
idp.ssocircle.com:443/sso/IDPSloRedirect/metaAlias/ssocircle"/>
```

Legen Sie die URL des IdP-Ausstellers fest

Stellen Sie die URL für die IdPs bereit, die das Sicherheitstoken ausstellen.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Die Integration verifiziert, dass jede SAML-Antwort dieselbe URL enthält, die in dieser Systemeigenschaft aufgeführt ist und die im *Aussteller* -Element aufgeführte URL enthält. Beispiel:

```
<samlp:Responsexmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  Destination="https://demoi2.service-now.com/navpage.do"
  ID="s28da6774c88ae1eab292bf25fe625db81919d8e1e"
 InResponseTo="SNC841720c227c81948cfd68cadcad235c6"
 IssueInstant="2012-01-30T20:07:10Z"  Version="2.0"><saml:Issuer
 xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">http://
idp.ssocircle.com</saml:Issuer>
   ...
   <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
     ID="s2f347f973c063836cf70ea38302d94976f9c5b851"
     IssueInstant="2012-01-30T20:07:10Z"
 Version="2.0"><saml:Issuer>http://idp.ssocircle.com</saml:Issuer>
      ...
   </saml:Assertion></samlp:Response>
```

Prozedur

1. Navigieren zu **Alle** > **SAML 2 Single Sign-on** > **Eigenschaften**an.
2. In der Eigenschaft *„URL des Identitätsanbieters", die das SAML2-Sicherheitstoken mit Anwenderinformationen ausstellt.*, geben Sie die URL zu Ihrem IdP ein.

   Jede IdP-URL muss eindeutig sein. Standardmäßig enthält die Integration die URL zu SSOCircle. Weitere Informationen finden Sie unter http://idp.ssoCircle.com .

Legen Sie die AuthnRequest-Service-URL fest

Legen Sie mithilfe der Metadaten des IdP die Anforderungsservice-URLs für den IdP der Integration fest.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. In der Eigenschaft *die Basis-URL zum AuthnRequest-Service des Identitätsanbieters. AuthnRequest wird als SAMLRequest-Parameter*an diese URL gesendet. Geben Sie die URL für die HTTP-Redirect-Bindung ein, die Sie vom Element „ `SingleSignOnService` " erhalten haben.
2. Aktivieren Sie das Kontrollkästchen neben *AuthnRequest signieren*, damit der Single Sign-on-Service des Identitätsanbieters eine signierte AuthnRequest erhält.
3. In der Eigenschaft *Wenn das SAML 2.0-Single Sign-on fehlschlägt, weil die Sitzung nicht authentifiziert ist oder dies die erste Anmeldung ist, führen Sie eine Weiterleitung zu dieser URL durch. Dies ist die Basis-URL, an die die ursprüngliche SAML 2.0 AuthnRequest mit dem*

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

*SAMLRequest-Parameter*gesendet wird. Geben Sie die URL für die HTTP-Redirect-Bindung ein, die Sie vom Element „ `SingleSignOnService` “ erhalten haben.

Standardmäßig enthält die Integration die URL zum SSOCircle-Service.

Legen Sie die SingleLogoutRequest-Service-URL fest

Legen Sie die Anforderungsservice-URLs für den IdP der Integration fest, indem Sie die -Metadaten des IdP verwenden.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. In *Die Basis-URL zum SingleLogoutRequest-Service des Identitätsanbieters. Der LogoutRequest wird an diese URL als SAMLRequest-Parameter* -Eigenschaft gesendet. Geben Sie die URL ein, die Sie aus dem `SingleLogoutService-` Element erhalten haben. Der LogoutRequest wird als SAMLRequest-Parameter an diese URL gesendet. Standardmäßig enthält die Integration die URL zum SSOCircle-Service.
2. Geben Sie *unter URL für die Weiterleitung von Anwendern nach der Abmeldung, in der Regel zurück zu dem Portal, das die SSO-Eigenschaft aktiviert hat (z. B. http://portal.unternehmena.com/logout)*, die URL ein, an die Anwender nach der erfolgreichen Abmeldung weitergeleitet werden sollen.

   Wenn Ihr IdP formularbasierte Authentifizierung verwendet, geben Sie die URL zum Anmeldeformular Ihres IdP ein. Wenn Ihr IdP eine nicht formularbasierte Authentifizierungsmethode wie Kerberos verwendet, sollten Sie die URL auf eine statische Abmeldeseite festlegen. Auf diese Weise werden Benutzer, die sich abmelden, nicht sofort zum IdP weitergeleitet und melden sich erneut an. Standardmäßig enthält die Integration die URL zur statischen UI-Seite `external_logout_complete.do`.

(Optional) Signierte Abmeldeanforderungen aktivieren

Bei einigen IdPs muss der Service Provider Abmeldeanforderungen mit einem Zertifikat signieren.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn für Ihren IdP signierte Abmeldeanforderungen erforderlich sind, verwenden Sie die Metadaten des IdP, um die folgenden Systemeigenschaften festzulegen.

Prozedur

1. Auf der Registerkarte **Erweitert** über die Eigenschaft *LogoutRequest signieren. Legen Sie diese Eigenschaft auf „true“ fest, wenn der SingleLogoutRequest-Service des Identitätsanbieters signierte LogoutRequest*erfordert. Wählen Sie „ **Ja** “, um anzugeben, dass Ihr IdP eine signierte Abmeldeanforderung erfordert, oder wählen Sie „ **Nein** “, um nicht signierte Abmeldeanforderungen zu verwenden.
2. Wenn Sie „ **Ja** zum Signieren des *LogoutRequest*“ ausgewählt haben, ist in *die Protokollbindung für den SingleLogoutRequest-Service des Identitätsanbieters festgelegt. (Der Wert kann entweder „urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect“ oder „urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST“ lauten.) Eigenschaft*, Geben Sie einen der unterstützten Werte ein, die im `Bindungsattribut` des Elements `SingleLogoutService` aufgeführt sind.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardmäßig verwendet die Integration eine HTTP-Redirect-Bindung.

3. Klicken Sie auf **Aktualisieren**.
4. Installieren Sie einen Service Provider-Schlüsselspeicher (SP).

Systemeigenschaften des Service Providers (SP).

Diese Systemeigenschaften definieren, wie die Instanz mit dem IdP als Service Provider interagiert.

Befolgen Sie den sequenziellen Prozess, um IdP als Service Provider zu definieren.

Legen Sie die Instanz-URL für SAML fest

Legen Sie die instanzspezifischen URLs so fest, dass der IdP Benutzer authentifizieren kann.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Geben Sie in der Eigenschaft *URL der ServiceNow-Instanz (normalerweise diese Instanz)* die URL (einschließlich Anmeldeseite) der Instanz ein, für die sich der IdP authentifiziert.
   Beispiel: https://IhreInstanz.service-now.com/navpage.do
2. Geben Sie in der Eigenschaft *Die Entitätsidentifizierung oder der Aussteller* die Basis-URL (ohne Anmeldeseite) der Instanz ein, für die sich der IdP authentifiziert.
   Beispiel: https://IhreInstanz.service-now.com/

Legen Sie die Zielgruppen-URL für SAML fest

Aktivieren Sie Ihre -Instanz, um mithilfe der Eigenschaft „Zielgruppe“ zu überprüfen, ob sie der beabsichtigte Empfänger einer SAML-Antwort ist.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Die Integration verifiziert, dass jede SAML-Antwort dieselbe URL enthält, die in dieser Systemeigenschaft aufgeführt ist und die im *Zielgruppen* -Element aufgeführte URL enthält. Beispiel:

```
<samlp:Responsexmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  ID="s2cdc74f37f923e26fe1aeec42b70a93d24230334f"
  InResponseTo="90AA6073F01567BFB0DF194F596314E2"
 Version="2.0"  IssueInstant="2010-04-29T23:21:51Z"
 Destination="https://dloomac.service-now.com/navpage.do">
...
<saml:Conditions NotBefore="2012-01-30T19:57:10Z"
 NotOnOrAfter="2012-01-30T20:17:10Z"><saml:AudienceRestriction><saml:Audi
ence>https://
demoi2.service-now.com</saml:Audience></saml:AudienceRestriction></saml:C
onditions>
...
</samlp:Response>
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **SAML 2 Single Sign-on** > **Eigenschaften**an.
2. In der Eigenschaft *die Zielgruppen-URI, die das SAML2-Token akzeptiert. (Normalerweise ist dies der Instanz-URI. Beispiel: https://<instance name> .service-now.com.)*, geben Sie die URL Ihrer Instanz ein.
   Beispiel: https://demoi2.service-now.com. Diese URL muss mit dem Wert des *Zielgruppenelements* in der SAML-Antwort übereinstimmen.
3. Klicken Sie auf **Aktualisieren**.

Richten Sie eine NameID-Richtlinie für SAML ein

Richten Sie eine NameID-Richtlinie für SAML ein. SAML 2.0 erfordert, dass der IdP ein NameID-Token mit dem Service Provider austauscht.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Für die SAML 2.0-Integration muss das NameID-Token einem bestimmten Feld in der Benutzertabelle zugeordnet werden. Die Integration verwendet den Wert des NameID-Tokens, um zu bestimmen, welchen Anwender der IdP authentifiziert.

Prozedur

1. Durchsuchen Sie die IdP-Metadaten, um das `NameIDFormat`- Element zu finden, das den Wert `emailAddress`enthält.
   Der Wert dieses Elements ist das Standardformat, das die Integration verwendet.
2. Überprüfen Sie andere `NameIDFormat`- Elemente, um festzustellen, ob Formate vorhanden sind, die mit anderen Feldern in der Anwendertabelle übereinstimmen.

Ermitteln Sie, welches Anwendertabellenfeld mit dem NameID-Token übereinstimmt

Identitätsanbieter geben an, welches Format das `NameID`- Token hat.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Das Einrichten von SAML 2.0 erfordert die Auswahl eines Felds aus der Benutzertabelle, das dem Format des `NameID`- Tokens entspricht. Normalerweise bieten IdPs die Möglichkeit, eine E-Mail-Adresse als `NameID`- Token zu verwenden. Da die Tabelle „Anwender“ ein Feld „E-Mail“ enthält, ist dieses Feld eine logische Auswahl für die Verwendung als `NameID`- Token. Um ein anderes Feld aus der Anwendertabelle als `NameID`- Token zu verwenden, überprüfen Sie zunächst, ob der IdP ein `NameID` -Format bereitstellt, das dem Wert eines Anwendertabellenfelds entspricht. Dies erfordert möglicherweise das Hinzufügen des Felds zur Benutzertabelle.

Prozedur

1. Vergleichen Sie die verfügbaren Formate im `NameIDFormat` -Element des IdP mit Feldern in der Benutzertabelle.
2. Wählen Sie ein `NameID` -Format aus, in dem sich ein übereinstimmender Wert in der Anwendertabelle befindet.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Geben Sie im Feld *Die Anwendertabelle, die mit dem NameID-Element des Antragstellers im Feld SAMLResponse übereinstimmen* soll, den Namen des Anwendertabellenfelds ein, um nach übereinstimmenden Werten im `NameID`- Token zu suchen.

   Standardmäßig verwendet die Integration das Feld „E-Mail“.

Legen Sie die Richtlinie für den IdP-NameID fest

Geben Sie an, welches Format der IdP für das `NameID`- Token verwendet.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Dieses Format wird als Teil der Metadaten des IdP aufgeführt.

Prozedur

1. In der Eigenschaft *die NameID-Richtlinie, die für die Rückgabe der NameID des Antragstellers in der SAML-Antwort verwendet werden soll. Ihr SAML-Identitätsanbieter muss dies unterstützen, indem er die Richtlinie in seinen Metadaten deklariert. Der NameID-Wert wird zum Abgleich mit dem angegebenen Feld in der Anwendertabelle verwendet, um den Anwender zu suchen.*, geben Sie den Wert des `NameIDFormat`- Elements ein, das die Integration verwendet.

   Standardmäßig verwendet die Integration das SSOCircle `NameID` -Format für E-Mail-Adressen.

2. Klicken Sie auf **Speichern**.

Werte im Tabellenfeld „Anwender“ für SAML

Stellen Sie sicher, dass das Feld Anwendertabelle der Integration entsprechende übereinstimmende Werte enthält.

Wenn die Integration beispielsweise das Feld „E-Mail“ als `NameID`- Token verwendet, stellen Sie sicher, dass die Instanz dieselbe E-Mail-Adresse auflistet wie der IdP. Die Integration kann keinen Anwender authentifizieren, der keinen übereinstimmenden Wert für das `NameID`- Token hat.

(Optional) Aktivieren Sie die Bereitstellung einer Authentifizierungskontextklasse für SAML

Sie können die Instanz so konfigurieren, dass eine Authentifizierungskontextklasse-Anforderung an den IdP gesendet wird, die das bevorzugte Format für die Authentifizierungsanforderung Ihrer Instanz enthält.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn Sie das Erstellen einer AuthContextClass-Nachricht aktivieren, müssen Sie auch ein Referenzformat für die Authentifizierungskontextklasse angeben.

Hinweis: Bei einigen IdPs kann der Service Provider die Authentifizierungskontextklasse nicht festlegen. Durch Deaktivieren dieser Einstellung kann der IdP die Authentifizierungskontextklasse auswählen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wählen Sie in der Eigenschaft *Eine AuthnContextClass-Anforderung erstellen in der AuthnRequest-Anweisung die Option***Ja** aus, um eine bestimmte Kontextklasse anzugeben, z. B. Passwortgeschützter Transport, oder wählen Sie **Nein**, damit der IdP die am besten geeignete Kontextklasse auswählt.
2. Wenn Sie in der **AuthnRequest**-*Anweisung die Option zum Erstellen einer AuthnContextClass-Anforderung*ausgewählt haben, geben Sie im Feld *AuthnContextClassRef-Methode, die in unserer SAML 2.0-AuthnRequest-Eigenschaft für die* Eigenschaft „Identitätsanbieter“ angefordert wird, die URN der Kontextklasse ein, die Sie für die Authentifizierung verwenden möchten (siehe Tabelle).).

   AuthnContextClass-URN-Optionen

Authentifizierungstyp	Authentifizierungskontextklasse URN
Formularbasierte Authentifizierung	`urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport`
Kerberos-basierte Authentifizierung	`urn:federation:authentication:windows`

   Standardmäßig verwendet die Integration eine Passwortgeschützte Transportauthentifizierungsmethode.
3. Klicken Sie auf **Aktualisieren**.

(Optional) Legen Sie Schlüsselspeichereigenschaften für das Signieren von Abmeldeanforderungen für SAML fest

Legen Sie die Schlüsselspeichereigenschaften so fest, dass die Integration Abmeldeanforderungen mithilfe Ihres signierten Servers und Ihrer signierten CA-Zertifikate signieren kann.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Geben Sie in der Eigenschaft *Alias der im SAML 2.0 SP-Schlüsselspeicher gespeicherten Schlüsseleingabe zum Signieren von SAML 2-Anforderungen*den Aliasnamen ein, den Sie für den SAML 2.0-Schlüsselspeicher erstellt haben.
   Standardmäßig sucht die Integration nach dem Alias *saml2sp*.
2. Geben Sie in der Eigenschaft *Das Passwort der im SAML 2.0 SP-Schlüsselspeicher gespeicherten Schlüsseleingabe zum Signieren von SAML 2-Anforderungen*das Passwort für Ihren SAML 2.0-Schlüsselspeicher ein.
   Standardmäßig entspricht das Passwort dem Standardaliasnamen.
3. Klicken Sie auf **Aktualisieren**.
4. Generieren Sie Ihre SP-Metadaten erneut.
   Weitere Informationen finden Sie unter SP-Metadaten.

Erstellt einen Service Provider-Schlüsselspeicher für SAML

Erstellen Sie einen Java-Schlüsselspeicher, der die folgenden Elemente enthält, damit Ihre Instanz Abmeldeanforderungen signieren kann.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

- Signiertes Serverzertifikat für die Instanz
- Signiertes CA-Zertifikat
- Paar aus öffentlichem und privatem Schlüssel

Sie können Ihr eigenes signiertes Zertifikat mit einer privaten Zertifizierungsstelle erstellen oder eines von einer öffentlichen Zertifizierungsstelle erwerben.

Die folgenden Schritte veranschaulichen, wie Sie eine neue Java Keytool-Schlüsselspeicherdatei generieren, eine Zertifikatsignaturanforderung (Certificate Signing Request, CSR) erstellen und Zertifikate importieren. Alle Stamm- oder Zwischenzertifikate müssen importiert werden, bevor das primäre Zertifikat für Ihre Domäne importiert wird. Geben Sie diese Befehle in eine Befehlszeilenschnittstelle ein.

Hinweis: Diese Anweisungen sind nicht spezifisch für die Plattform und erfordern technische Kenntnisse über Sicherheitszertifikate. Der technische Support kann bei der Erstellung der Zertifikate nicht helfen.

Prozedur

1. Generieren Sie einen Java-Schlüsselspeicher und ein Schlüsselpaar.

```
keytool -genkey -alias mydomain -keyalg RSA -keystore my.keystore
```

2. Generieren Sie eine CSR für einen vorhandenen Java-Schlüsselspeicher.

```
keytool -certreq -alias mydomain -keystore my.keystore -file
 mydomain.csr
```

3. Importieren Sie ein CA-Zertifikat einer Stamm- oder Zwischenzertifizierungsstelle in einen vorhandenen Java-Schlüsselspeicher.

```
keytool -import -trustcacerts -alias root -file Thawte.crt -keystore
 my.keystore
```

4. Importieren Sie ein signiertes primäres Zertifikat in einen vorhandenen Java-Schlüsselspeicher.

```
keytool -import -trustcacerts -alias mydomain -file mydomain.crt
 -keystore my.keystore
```

Installieren Sie einen Service Provider-Schlüsselspeicher zum Signieren von SAML-Anforderungen

Führen Sie die folgenden Schritte aus, um den vorhandenen Beispielschlüsselspeicher zu entfernen und einen eigenen Service Provider-Schlüsselspeicher zu installieren, der Ihr öffentliches und privates Schlüsselpaar enthält.

Vorbereitungen
Erforderliche Rolle: admin

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Erstellen Sie einen Service Provider-Schlüsselspeicher.
2. Navigieren zu **SAML 2 Single Sign-on** > **Zertifikat** oder **Mehrere Anbieter** > **Administrator** > **x509-Zertifikat**an.
3. Klicken Sie **auf SAML 2.0 Keystore_Key2048_SHA256**.
4. Klicken Sie auf den Link **Anhänge verwalten**.
5. Aktivieren Sie das Kontrollkästchen Löschen neben *saml2sp_key2048withsha256.jks*.
6. Klicken Sie auf **Entfernen**.
7. Klicken Sie auf **Dateien** auswählen, und wählen Sie den Schlüsselspeicher aus, der Ihre signierten Zertifikate enthält.
8. Klicken Sie auf **Anhängen**.
9. Schließen Sie das Popup „Anhänge“.

   Hinweis: Es wird empfohlen, einen anderen Namen für das neu angehängte Zertifikat anzugeben.

10. Geben Sie im Feld *Schlüsselspeicher-Passwort*das Passwort für den Zugriff auf den SAML 2-Alias ein.
11. Klicken Sie auf **Aktualisieren**.

(Optional) Erweiterte SAML-Eigenschaften

Mit den folgenden erweiterten Einstellungen können Sie die Sicherheit weiter erhöhen und die Integration debuggen.

Erweiterte Einstellungen

Navigieren zu **Alle** > **SAML 2 Single Sign-on** > **Eigenschaften**an.

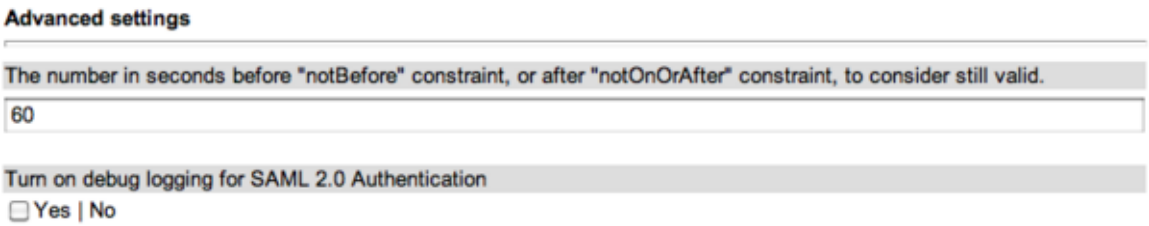


Tabelle „Erweiterte Systemeigenschaften“.

Eigenschaft	Beschreibung
Die Anzahl der Sekunden der Einschränkung „notBefore“ oder nach der Einschränkung „notOnOrAfter“, die als noch gültig gilt	Geben Sie die Anzahl der Sekunden ein, die den Einschränkungen *NotBefore* und *NotOnOrAfter* hinzugefügt werden sollen, um Zeitunterschiede zwischen der IdP-Uhr und der SP-Uhr zu berücksichtigen. Diese Einschränkungen verhindern Replay-Angriffe, indem Anforderungen abgelehnt werden, die nicht innerhalb des angegebenen Zeitrahmens gestellt werden. Wenn sich die IdP-Uhr und die SP-Uhr erheblich unterscheiden, kann die Netzwerklatenz dazu führen, dass die SAML-Anforderung nicht autorisiert ist. Diese Eigenschaft fügt einen Toleranzzeitraum hinzu, während dessen SAML-Anforderungen und -Antworten noch als gültig betrachtet werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle „Erweiterte Systemeigenschaften“. (Fortsetzung)

Eigenschaft	Beschreibung
Debug-Protokollierung für SAML 2.0-Authentifizierung aktivieren	Wählen Sie „ **Ja** “, um zusätzliche Protokollierungsinformationen für SAML 2.0-Ereignisse zu aktivieren.

Installieren Sie das Zertifikat des Identitätsanbieters

Sie können ein PEM-Zertifikat in ein X.509-Zertifikatformular einfügen, damit der Identitätsanbieter die Kommunikation mit dem Service Provider überprüfen kann.

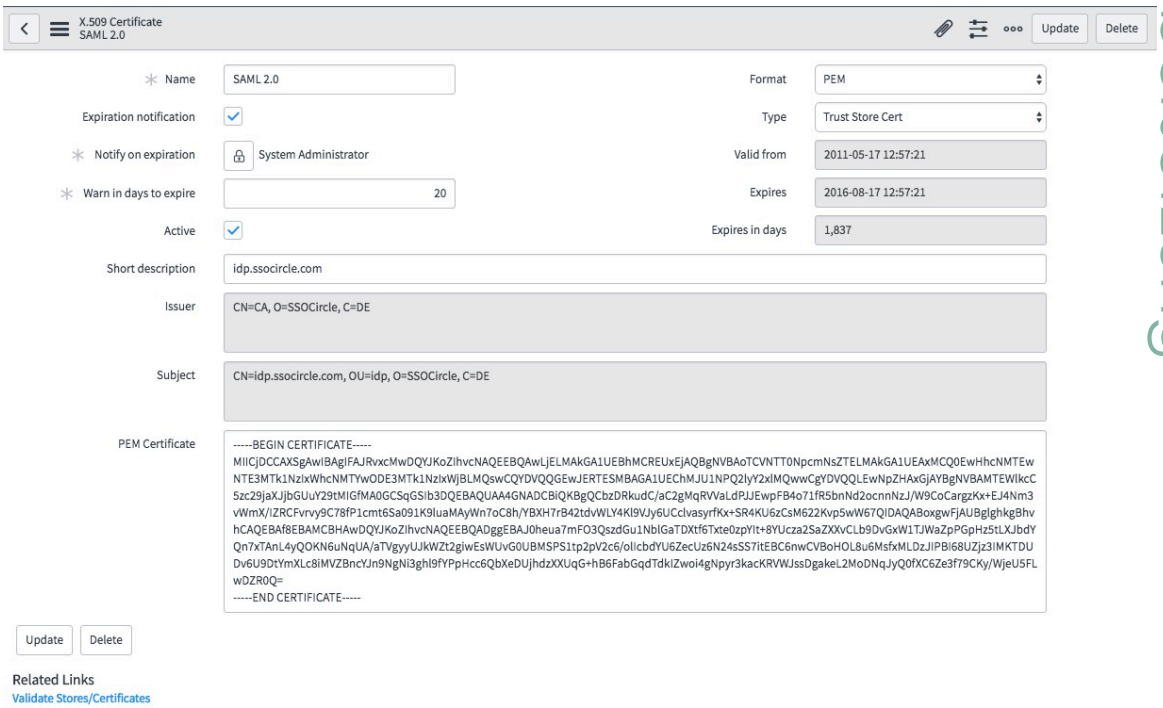
Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Das Zertifikat des IdP befindet sich in den Metadaten des IdP. Der IdP-Entwickler bestimmt, wo sich die Zertifikatmetadaten befinden, wenn er den lokalen IdP erstellt.

Hinweis: Zertifikate für Single Sign-on müssen immer im PEM-Format vorliegen, um mit SAML-Zertifikaten zu funktionieren.

Prozedur

1. Navigieren zu **Alle** > **SAML Single Sign-on** > **Zertifikat**an.
2. Füllen Sie die Formularfelder aus (siehe Tabelle).
3. Klicken Sie auf **Speichern**.



Hinweis: Die Integration signiert das Zertifikat derzeit nicht in der Kommunikation zwischen der Instanz und dem IdP.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Der Zertifikatname. Ändern Sie den *Namenseintrag* nicht. Der Name des X.509-Zertifikats muss *SAML 2.0* lauten, damit die Integration es verwenden kann. Diese Anforderung ist nur erfüllt, wenn Sie Single Sign-on (SSO) für mehrere Anbieternicht verwenden.
Ablaufbenachrichtigung	Wählen Sie diese Option aus, um eine Benachrichtigung an die Anwender zu senden, die im Feld Bei **Ablauf benachrichtigen** ausgewählt sind. Dies ist standardmäßig aktiviert.
Benachrichtigung bei Ablauf	Wählen Sie die Anwender aus, um die Benachrichtigung über den Ablauf des Zertifikats wiederzugeben. Wenn keine Benutzer ausgewählt sind, wird der angemeldete Benutzer standardmäßig zusammen mit den letzten beiden angemeldeten Benutzern mit der Administratorrolle hinzugefügt.
Tage vor Ablauf benachrichtigen	Die Anzahl der Tage vor Ablauf, in der die Instanz die Benachrichtigung sendet. Geben Sie einen Wert von mindestens 20 ein. Bei Instanzen, die auf Istanbul und höher aktualisiert wurden, ist dieser Wert auf 20 festgelegt, sofern kein größerer Wert angegeben ist.
Aktiv	Ein Kontrollkästchen, das angibt, dass dieses Zertifikat aktiv ist.
Format	Das Format des Zertifikats. SAML verwendet das PEM-Format.
Typ	Der Zertifikatcontainer. Die Instanz von erkennt Zertifikate aus Truststores, Java-Schlüsselspeichern und PKCS#12-Schlüsselspeichern.
Gültig ab	Die Instanz fügt diesem Feld automatisch das Gültigkeitsdatum des Zertifikats hinzu. Hängen Sie das Zertifikat an den X.509-Zertifikatdatensatz an, um dieses Feld auszufüllen.
Läuft ab	Die Instanz fügt automatisch das Ablaufdatum des Zertifikats zu diesem Feld hinzu. Hängen Sie das Zertifikat an den X.509-Zertifikatdatensatz an, um dieses Feld auszufüllen.
Läuft in Tagen ab	Die berechnete Anzahl von Tagen bis zum Ablauf.
Kurzbeschreibung	Eine Beschreibung für das Zertifikat.
Problem	Die Instanz fügt den Zertifikataussteller diesem Feld automatisch hinzu. Hängen Sie das Zertifikat an den X.509-Zertifikatdatensatz an, um dieses Feld auszufüllen.
Betreff	Die Instanz fügt den Zertifikatantragsteller automatisch zu diesem Feld hinzu. Hängen Sie das Zertifikat an den X.509-Zertifikatdatensatz an, um dieses Feld auszufüllen.
PEM-Zertifikat	Geben Sie den Wert des X509-Zertifikats ein.

Nächste Maßnahme

Klicken Sie auf **Stores/Zertifikate validieren**, um den Truststore und das Zertifikat zu testen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fehlendes Zertifikat für SAML wird ersetzt

Wenn das **Zertifikatmodul** eine leere Seite anzeigt, wurde der SAML 2.0-Zertifikatdatensatz gelöscht. Sie können das fehlende Zertifikat ersetzen, indem Sie manuell einen Zertifikatdatensatz erstellen.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Zertifikate**an.
2. Erstellen Sie einen neuen Datensatz mit dem Namen `SAML 2.0`.

   Wichtig: Sie MÜSSEN diesen Namen verwenden. Diese Anforderung ist nur erfüllt, wenn Sie Single Sign-on (SSO) für mehrere Anbieternicht verwenden.

3. Klicken **SAML 2 Single Sign-on** > **Zertifikat**an.
4. Geben Sie im Feld *PEM-Zertifikat* den Wert des Elements „`ds:X509Certificate`“ aus den Metadaten Ihres IdP ein.
5. Klicken Sie auf **Speichern**.

Testen Sie die SAML-Integration

Testen Sie die SAML-Integration, nachdem Sie alle anderen Setupaufgaben abgeschlossen haben.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Melden Sie sich bei der Instanz als Benutzer mit der Administratorrolle an.
2. Navigieren zu **SAML 2 Single Sign-on** > **Eigenschaften**an.
3. Wählen Sie in der Eigenschaft *Externe Authentifizierung aktivieren*die Option **Ja**aus.

   Hinweis:

   Zum Aktivieren der externen Authentifizierung müssen alle Benutzer SAML 2.0 Single Sign-on verwenden. Wenn ein Benutzer versucht, ohne Authentifizierung auf die Anwendung zuzugreifen, sendet die Instanz automatisch eine Authentifizierungsanforderung an (IdP) und leitet den Benutzer zur Seite für die SAML-IdP-Authentifizierung weiter.

4. Klicken Sie auf **Speichern**.
5. Melden Sie sich von der Instanz ab.
6. Navigieren Sie zur Instanz-URL.
   Wenn die Integration ordnungsgemäß funktioniert, sollte der IdP nach den Anmeldeinformationen des Benutzers fragen.

Zugehörige Informationen

Fehler und Korrekturen für Multi-SSO (SAML 2.0).

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fehler und Korrekturen für Multi-SSO (SAML 2.0).

Eine Liste häufiger Fehler und zugehöriger Korrekturen für das Setup und die Konfiguration von Multi-SSO (SAML 2.0).

Fehler beim Setup von Multi-SSO (SAML 2.0).

Fehler in Instanzprotokollen	Testverbindu	SAML-Eigenschaft	Diagnose	Beheben
NotAfter:<Thu Jun 05 22:57:44 PDT 2014> .	Stellen Sie sicher, dass das x509-IDP-Zertifikat vorhanden, gültig und aktiv ist.	N/V	Das aktuelle Zertifikat oder die SAML-Assertion ist abgelaufen.	• Synchronisieren Sie die SNC-Uhr mit der Uhr des SAML-IdP-Servers. • Aktualisiert den SAML 2.0-Zertifikatdatensatz.
• SAML 2.0-Zertifikat wurde nicht gefunden. • In der ServiceNow-Instanz wurde keine digitale Signatur gefunden.	Stellen Sie sicher, dass das x509-IDP-Zertifikat vorhanden, gültig und aktiv ist	Die PEM-formatierte Zeichenfolge muss in das Feld PEM-Zertifikat eingegeben werden.	Das SAML-Zertifikat ist nicht vorhanden. Möglicherweise ist sie inaktiv.	Stellen Sie sicher, dass das richtige Zertifikat im PEM-Format in die Instanz hochgeladen wird.
Zertifikate stimmen nicht überein. Erwartet:<certStr> , Istwert:<inboundCert>	Stellen Sie sicher, dass das .x509-IDP-Zertifikat vorhanden, gültig und aktiv ist.	N/V	Das verfügbare Zertifikat in SNC stimmt nicht mit dem Zertifikat in der Assertion überein. Ursachen: • Das Zertifikat wird auf dem IdP aktualisiert, aber nicht in der ServiceNow-Instanz. • Das Zertifikat hat das falsche Format.	Bestätigen Sie, dass die PEM-formatierte Zeichenfolge im SAML 2.0-Zertifikatdatensatz mit dem X509-Zertifikat in der SAML-Antwort für den Anwender-IdP übereinstimmt.
Fehler beim Überprüfen der Gültigkeit des Zertifikats.	Stellen Sie sicher, dass das x509-IDP-Zertifikat vorhanden, gültig und aktiv ist	N/V	Das aktuelle Zertifikat ist möglicherweise abgelaufen.	Aktualisiert den SAML 2.0-Zertifikatdatensatz.
Signaturprofil konnte nicht validiert werden.	Stellen Sie sicher, dass das	N/V	Die Assertion wurde möglicherweise	Überprüfen Sie, ob der IdP über dasselbe

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fehler beim Setup von Multi-SSO (SAML 2.0). (Fortsetzung)

Fehler in Instanzprotokollen	Testverbindu	SAML-Eigenschaft	Diagnose	Beheben
	x509-IDP-Zertifikat vorhanden, gültig und aktiv ist.		mit einem anderen Zertifikat signiert.	Zertifikat verfügt wie die SNC-Instanz.
InResponseTo-Attribut in SubjectConfirmationDa stimmt nicht überein. Erwartet:<inResponseTo> Istwert: .	Die Validierung des Antragstellers ist fehlgeschlagen.	N/V	Dieser Fehler wird angezeigt, wenn eine der folgenden Situationen auftritt: • Der IdP gibt eine SAML-Antwort für eine andere SAML-Anforderung zurück • Ein Anwender setzt ein Lesezeichen für die URL mit der SAMLRequest anstatt nur für die Instanz-URL • Wenn ein Nullwert erwartet wird, wird die Antwort möglicherweise an einen anderen Knoten gesendet, wenn die Instanz über mehrere Knoten verfügt.	Der IdP-Administrator muss bestätigen, dass die erwartete SAML-Antwort zurückgegeben wird. Diese Situation kann ein Problem mit dem Lastenausgleichsmodul oder der Infrastruktur sein.
SessionIndex-Wert nicht gefunden:<message>	SessionIndex ungültig. ...	N/V	Der SessionIndex ist in der SNC-Instanz erforderlich. Der IdP gibt ihn in der SAML-Antwort zurück, um eine erfolgreiche Authentifizierung zu gewährleisten.	Der IdP-Administrator muss bestätigen, dass der SessionIndex in der SAML-Antwort definiert ist.
Es konnte kein gültiges SubjectConfirmation-Element gefunden werden.	Die Validierung des Antragstellers ist fehlgeschlagen.	N/V	Bedingungen könnten aufgrund eines Fehlers beim IdP fehlen. Der StatusCode in der Antwort würde Beantworter anstelle des erwarteten Erfolgs enthalten.	Überprüfen Sie die SAML-Antwort, um zu bestimmen, ob Bedingungen in der SAML-Antwort enthalten sind. Die gültigen Betreffbestätigungsdaten können für die richtige Zielgruppe

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fehler beim Setup von Multi-SSO (SAML 2.0). (Fortsetzung)

Fehler in Instanzprotokollen	Testverbindu	SAML-Eigenschaft	Diagnose	Beheben
				abgelaufen sein oder nicht.
Assertionszielgruppe stimmt nicht überein. Erwartet:<propAudience> Istwert:<audienceUri> . oder Die Validierung des Elements "AudienceRestriction" ist fehlgeschlagen. Keine übereinstimmende Zielgruppe gefunden.	Stellen Sie sicher, dass das Feld „Audience URI“ richtig eingestellt ist	Der Zielgruppen-URI, der das SAML2-Token akzeptiert. (Normalerweise ist dies der Instanz-URI. Beispiel: `https://demo.service-now.com`.)	Der in der SNC-Instanz konfigurierte Zielgruppen-URI muss mit dem Wert im IdP übereinstimmen.	Suchen<saml2:Audience> in der SAML-Antwort in den Protokollen, und vergewissern Sie sich, dass der Wert mit dem in der Instanz übereinstimmt.
Der Aussteller der Assertion ist ungültig. Erwartet:<value on instance> , Istwert:<value returned by IdP>	Der Aussteller der Assertion ist ungültig.	Die Identitätsanbieter-URL, die das SAML2-Sicherheitstoken mit Anwenderinformationen ausstellt.	Die ID der IdP-Entität (Aussteller) stimmt nicht mit dem in der SNC-Instanz definierten Wert überein.	• Überprüfen Sie, ob IdP oder SP nicht ordnungsgemäß konfiguriert ist. • Stellen Sie sicher, dass die SAML-Eigenschaft (die Identitätsanbieter-URL, die das SAML2-Sicherheitstoken mit Anwenderinformationen ausstellt) richtig eingestellt ist.
Betreff ist in der Zukunft gültig. Jetzt:<now> , NotBefore:<notBefore> oder Betreff ist abgelaufen. Jetzt:<now> , NotOnOrAfter:<notOnOrAfter>	Die Bestätigung der Antragstellerbeschränkung ist fehlgeschlagen.	Die Zeit in Sekunden vor der Beschränkung „notBefore“ oder nach der Beschränkung „notOnOrAfter“, die als noch gültig gilt.	Die IdP-Uhr wird nicht mit der SP-Uhr synchronisiert.	Aktualisieren Sie die SAML-Eigenschaft „glide.authenticate.sso.saml2.Clocksk auf einen größeren Wert. Der Standardwert ist 180 Sekunden. Einige Fälle erfordern eine Einstellung von 300 oder höher. Unter Umständen müssen Sie auch die Uhrzeit auf Ihrem IdP-Server überprüfen.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fehler beim Setup von Multi-SSO (SAML 2.0). (Fortsetzung)

Fehler in Instanzprotokollen	Testverbindu	SAML-Eigenschaft	Diagnose	Beheben
Assertion ist erst in der Zukunft gültig:<now> , notBefore:<notBefore> oder Assertion ist abgelaufen, jetzt:<now> , notOnOrAfter:<notOnOrAfter>	Assertion ist ungültig.	Die Zeit in Sekunden vor der Beschränkung „notBefore“ oder nach der Beschränkung „notOnOrAfter“, die als noch gültig gilt.	Die IdP-Uhr wird nicht mit der SP-Uhr synchronisiert	Aktualisieren Sie die SAML-Eigenschaft auf einen größeren Wert. Standard: 60 Sekunden. Einige Fälle erfordern eine Einstellung von 300 oder höher. Unter Umständen müssen Sie auch die Uhrzeit auf Ihrem IdP-Server überprüfen.

Häufige Anmelde- und IdP-Fehler

Fehler oder Symptom	Diagnose	Beheben
Anmeldeanforderungen erzeugen eine Endlosschleife zwischen dem System und dem IdP, wenn „Hochsicherheit“ aktiviert ist.	• Normalerweise ist der URL-Endpunkt eine Fehlerseite oder Abmeldeseite. • Mit „logout_redirect.do“ kann diese Schleife erstellt werden, wenn Sie *glide.security.url.whitelist* definieren, ohne den IdP-Hostnamen zum Eigenschaftswert hinzuzufügen. **Hinweis:** Weitere Informationen zu dieser Eigenschaft finden Sie unter URL-Allow-Liste für Abmeldeumleitungen in Härtungseinstellungen für Instanzsicherheit.	Legen Sie die Systemeigenschaft „glide.authenticate.failed_redirect“ fest (oder erstellen Sie sie), um fehlgeschlagene Authentifizierungsanforderungen an diese URL umzuleiten.
Das zur Authentifizierung des Anwenders oder der Anforderung verwendete Token ist mit dem Signaturalgorithmus http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 signiert, was nicht der erwartete Signaturalgorithmus http://	Ereignisdetails finden Sie auf der Registerkarte Warnungskontext.	Navigieren Sie zur Registerkarte Erweitert des Konfigurationsdialogfelds „Relying Partei Trust“, und vergewissern Sie sich, dass der Algorithmus auf SHA-1 und nicht auf SHA-256 festgelegt ist.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Häufige Anmelde- und IdP-Fehler (Fortsetzung)

Fehler oder Symptom	Diagnose	Beheben
www ist. w3.org/2000/09/xmldsig#rsa-sha1		
In der Systemprotokolltabelle (syslog) wird die Fehlermeldung `urn:oasis:names:tc:SAML:2.0:status:Requester` angezeigt.	Wenn Ihr IdP (z. B. ADFS) mit dem Status `oasis:names:tc:SAML:2.0:status:Requester` auf eine Anmeldung aufgrund eines Problems mit der an ihn gesendeten Anforderung abgelehnt. Leider enthält die vom IdP erhaltene SAML-Antwort in den meisten Fällen keine weiteren Details für den Fehler.	Überprüfen Sie die an den IdP gesendete SAML-Anforderung und arbeiten Sie mit Ihrem IdP-Administrator zusammen, um die SAML-Einstellungen Ihrer Instanz zu aktualisieren und so den Fehler zu vermeiden. Unter Umständen müssen Sie sich an Ihren IDP-Provider wenden, um den Grund für den Anmeldefehler zu erfahren.

SSO-Anmeldungen (Single Sign-on) umleiten

Wenn SSO aktiviert ist, können Sie Anwender zu bestimmten Seiten umleiten oder sich lokal anmelden.

Wenn ein Benutzer beispielsweise versucht, zu `https://customerX.service-now.com`zu wechseln, kann anstelle der Standardanmeldeseite ein internes Unternehmensportal angezeigt werden. Oder wenn sich ein Benutzer von einer Anwendung abmeldet, kann der Browser ihn zu einer bestimmten internen Seite umleiten. Sie können Umleitungseigenschaften innerhalb der -Instanz festlegen, um sicherzustellen, dass Benutzer eine SSO-Anmeldeseite anstelle der Standardanmeldeseite sehen.

Hinweis: Die folgenden Eigenschaften erzwingen SSO nicht. Die Seite „login.do“ ist weiterhin zugänglich, und Anwender können sich beim System anmelden, wenn sie ein lokales Passwort festgelegt haben.

Umleitungseigenschaften

Wenn sich ein Anwender abmeldet oder ein Versuch fehlschlägt, sich mit SSO anzumelden, können Sie definieren, wohin der Anwender als Nächstes weitergeleitet wird, z. B. auf eine Hauptportalseite oder zu einem Knowledge Base-Artikel mit SSO-Anmeldeinformationen. Verwenden Sie die folgenden Eigenschaften, um die URLs anzugeben. Wenn eine dieser Eigenschaften in Ihrer Instanz nicht vorhanden ist, können Sie sie erstellen.

glide.authenticate.failed_requirement_redirect

URL für die Umleitung von Benutzern, wenn diese versuchen, auf eine private Seite zuzugreifen (z. B. um einen Incident anzuzeigen) und keine SSO-Anmeldeinformationen angeben. Die Eigenschaft ist normalerweise auf das Anmeldeportal eines Kunden festgelegt (z. B. `http://portal.unternehmena.com/`).

glide.authenticate.failed_redirect

URL für die Umleitung von Anwendern nach fehlgeschlagenem SSO-Versuch. Sie können zu einem öffentlichen Wissensartikel umleiten, der den Fehler beschreibt und hilfreiche Links enthält (z. B. `http://portal.unternehmena.com/fehler`).

glide.authenticate.external.logout_redirect

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

URL für die Umleitung von Anwendern nach dem Abmelden, normalerweise zurück zu dem Portal, das die Single Sign-on-Anmeldung aktiviert hat (z. B. `http://portal.unternehmena.com/logout`).

glide.authentication.external.disable_local_login

Bei Festlegung auf „wahr“ sind SSO-Anmeldeinformationen für die Hauptanmeldeseite erforderlich. Der Standardwert ist „false“. Diese Eigenschaft muss in Verbindung mit der Eigenschaft *glide.authenticate.failed_requirement_redirect* verwendet werden.

Die folgende Tabelle zeigt die Beziehung zwischen den Rückgabewerten für den Installationsausgang, den Eigenschaften und dem erwarteten Verhalten.

Anmeldung nur mit SSO wird erzwungen

Rückgabewert	Eigenschaft	Verhalten
„failed_missing_requirement“	*glide.authenticate.failed_requirement_redirect*	Wenn dieser wird, gibt die die erforderli Anmeldeinfo Sitzung nicht Die Anmeldu die Sitzung w Eigenschaft umgeleitet. D die URL für d der die Anm Anmeldeinfo werden.
„failed_authentication“	*glide.authenticate.failed_redirect*	Wenn dieser wird, gibt er Authentifizier SSO-Anmeld fehlgeschlag nicht vorhan ist. Die Anme und die Sitzu die Eigensch umgeleitet. D die URL für d der die Anm Anmeldeinfo werden.
<user_id>	N/V	Anmeldung *<user_id>* Anwender a Wert stimmt überein, der *glide.auth* definiert ist („ Abgleich mit

Automatisierte Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die lokale Anmeldung wird eingeschränkt

Aus Sicherheitsgründen sollten Sie sich nicht nur auf Umleitungseigenschaften verlassen, um die lokale Anmeldung zu verhindern. Wenn sich ein Benutzer niemals lokal anmelden darf und immer von Ihrem internen Single Sign-on-System authentifiziert wird, muss jedem Benutzer, der in die Instanz importiert wird, ein zufälliges Passwort zugewiesen werden. Das zufällige Passwort kann am einfachsten zum Zeitpunkt des Anwenderimports festgelegt werden. Wenn die Anwenderdaten über einen Importsatz in Ihr System importiert werden, können Sie mit dem folgenden Code ein onBefore-Transformationsskript erstellen.

```
var r  = new Packages. java. util. Random ( ) ;

 var str1  = Packages. java. lang. Long. toString (Packages. java. lang.
 Math. abs (r. nextLong ( ) ) , 36 ) ; var str2  = Packages. java. lang.
 Long. toString (Packages. java. lang. Math. abs (r. nextLong ( ) ) , 36
 ) ;

 var newPass  = str1  + str2 ;

target. user_password = newPass ;

 //password now set to a random string like this:
 //qvm81zdrn7cwwylpvw94eebk
```

Klonen Sie eine -Instanz mit einer SAML-Integration

Klonen Sie eine -Instanz mit einer SAML-Integration. Bevor Sie eine Instanz klonen, die SAML 2.0 verwendet, behalten Sie die SAML-SSO-bezogenen Einstellungen in der Zielinstanz bei. Andernfalls können Sie die Zielinstanz unzugänglich machen.

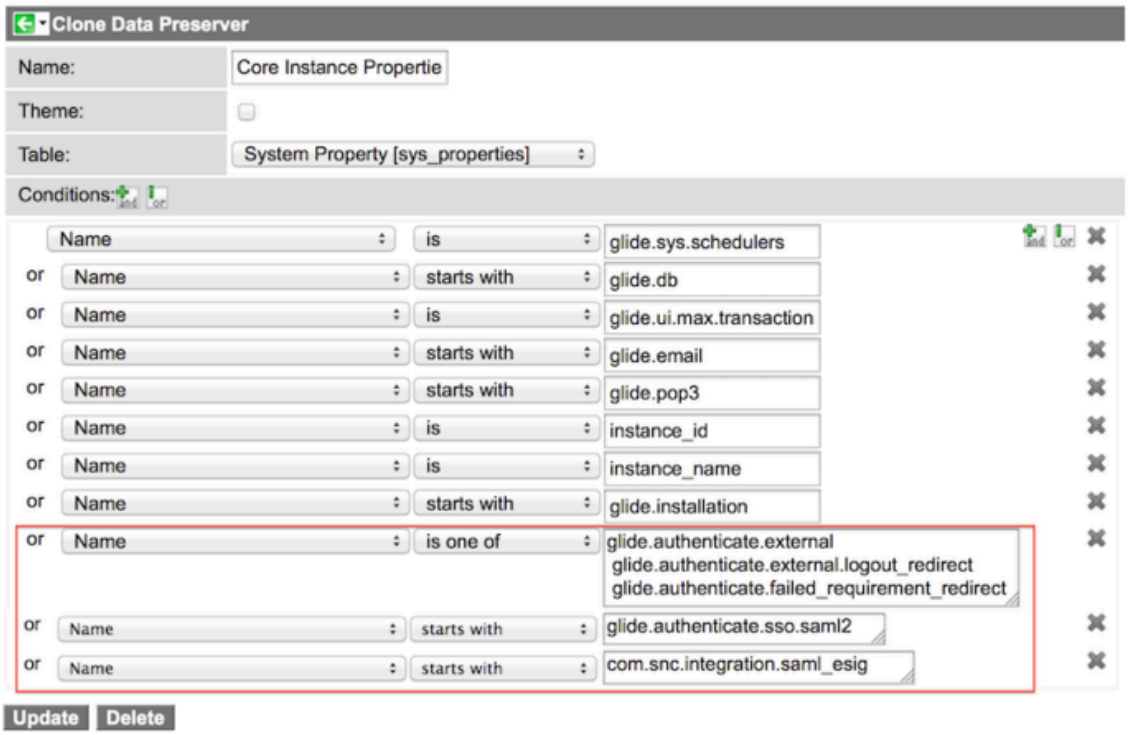
Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren Sie in der Quellinstanz zu **Systemklon** > **Daten erhalten** > **Eigenschaften der Core-Instanz**an.
2. Stellen Sie sicher, dass die folgenden Eigenschaften im Zusammenhang mit SAML-SSO mithilfe von Bedingungen erhalten bleiben.
   - glide.authenticate
   - glide.security
   - glide.entry
   - glide.script
   - glide.session
   - glide.saml2
   - com.glide.communications
   - com.snc.integration.saml_esig

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis: Wenn Sie den Klon erstellen, fügen Sie Anhänge hinzu, damit Zertifikate auf die Zielinstanz übertragen werden. Stellen Sie außerdem sicher, dass das Kontrollkästchen Design deaktiviert ist, damit diese Eigenschaften beibehalten werden, unabhängig davon, ob Sie das **Instanzdesign** beibehalten.

3. Navigieren Sie in der Quellinstanz zu **Systemklon** > **Daten erhalten** um die SAML-Zertifikate in „sys_certificate“ und die SAML-Anwender in „sys_user“ im Zusammenhang mit SAML/SSO/Multi-SSO beizubehalten.

   Wenn Sie sie benötigen, exportieren Sie sie in XML, und importieren Sie sie dann manuell auf dem Ziel.

   Warnung: Versuchen Sie nicht, das SAML/SSO/Multi-SSO-Setup von einem System auf ein anderes zu klonen. Die meisten Übertragungen von SAML/SSO- oder Multi-SSO-Einstellungen funktionieren NICHT, da sie beim Identitätsanbieter konfiguriert werden müssen. Wenn Sie ein funktionierendes Setup überschreiben, kann die Zielinstanz nicht authentifiziert werden, sodass auf Ihre Zielinstanz nicht zugegriffen werden kann. Ändern Sie auch nicht die sys_id Ihres Multi-SSO-Anbieter-Datensatzes. Dadurch werden Ihre Anwender gezwungen, ihre Cookies zu leeren. Weitere Informationen zu Vorsichtsmaßnahmen beim Klonen finden Sie unter Prüfliste vor dem Klonen einer Instanz .

4. Multi-SSO-Tabellen „sso_properties“, „Digest_properties“ und „saml2_update1_properties“ ausschließen.
5. Erstellen Sie die SAML/SSO/Multi-SSO-Datensätze manuell für jede Instanz unabhängig, und richten Sie die Datensätze auch für Ihren Identitätsanbieter ein.
6. Stellen Sie sicher, dass Sie manuell ein LOCAL-Administratorkonto im Datensatz „sys_user“ (nicht in LDAP oder SAML) in der Zielinstanz und mit einer sys_id erstellen, die in der Quellinstanz nicht vorhanden ist.
7. Klicken Sie auf **Aktualisieren**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

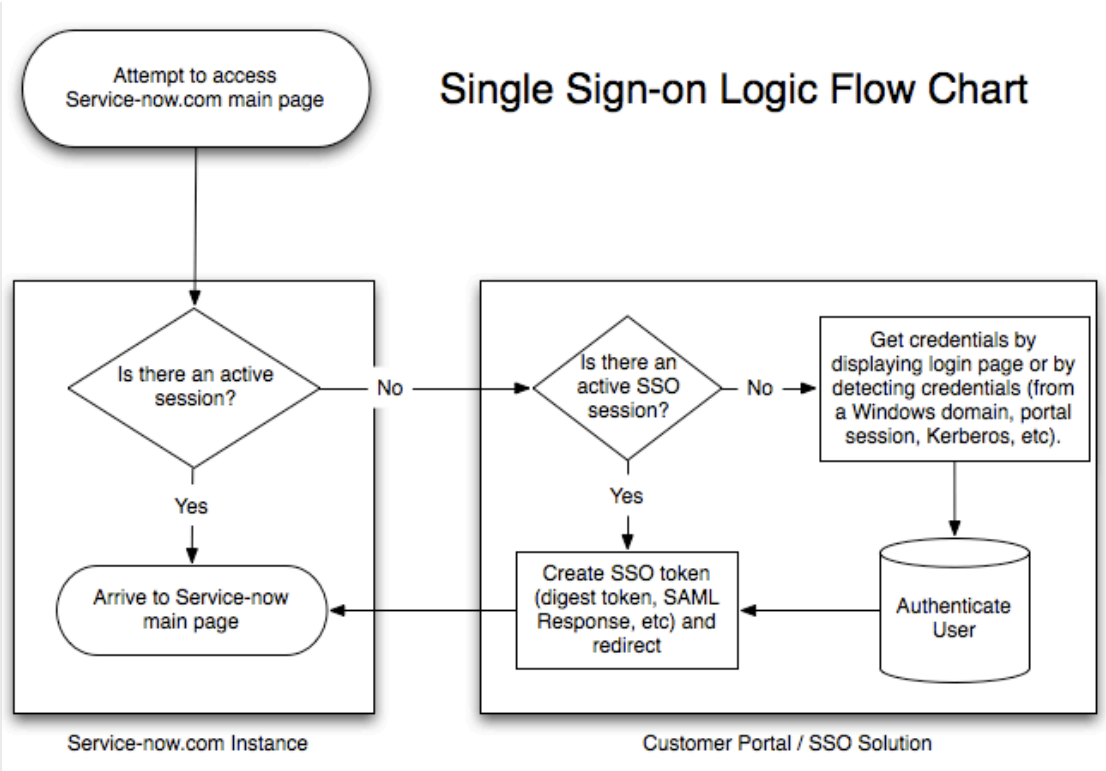
SAML 2.0-Konzepte

Machen Sie sich mit diesen SAML-Konzepten vertraut.

Typischer SAML-Prozess-Flow (Diagramm)

Ein typischer SSO-Logik-Flow umfasst die Suche nach einer aktiven Sitzung, die Überprüfung der Anmeldeinformationen und die Erstellung des erforderlichen Tokens.

SSO-Standard



Prozess-Flow für Anmeldung (AuthnRequest).

SAML 2.0 spezifiziert ein Webbrowser-SSO-Profil, das den Austausch von Informationen zwischen einem Identitätsanbieter (IdP), einem Service Provider (SP) und einem Prinzipal (Benutzer) in einem Webbrowser umfasst.

Der Identitätsanbieter kann ein beliebiger SSO-Service sein, der SAML-Authentifizierungsservices anbietet (z. B. SSOCircle). Der Service Provider ist immer eine Instanz. Der Nachrichten-Flow beginnt mit einer Anforderung für eine gesicherte Ressource beim Service Provider.

Fordern Sie die Zielressource beim SP an

Der Prinzipal fordert eine Zielressource beim Service Provider an:

https://instanz.service-now.de/

Die Instanz prüft die Anforderung darauf, ob die URL-Parameter SAMLRequest und RelayState vorhanden sind. Wenn sie vorhanden sind, hat der Benutzer bereits die Validierung beim IdP durchgeführt und kann die Schritte 2 bis 6 überspringen.

AuthnRequest an Identitätsanbieter ausgeben

Die Instanz erstellt eine `AuthnRequest`, die mithilfe des `SAMLRequest` -Werts an den IdP gesendet wird. Die Instanz erstellt und sendet auch einen `RelayState`- URL-Parameterwert.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das `RelayState-` Token ist ein undurchsichtiger Verweis auf Statusinformationen, die beim Service Provider verwaltet werden. Der Wert des Parameters `„SAMLRequest"` ist der dekomprimierte und base64-codierte Wert von<samlp:AuthnRequest> Element:

```
<samlp:AuthnRequest    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="identifier_1"    Version="2.0"
 IssueInstant="2004-12-05T09:21:59Z"
 AssertionConsumerServiceIndex="0"><saml:Issuer>https://
sp.example.com/SAML2</saml:Issuer><samlp:NameIDPolicy
 AllowCreate="true"
 Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"/></samlp:Au
thnRequest>
```

Die Integration URL-codiert dann die<samlp:AuthnRequest> Element und sendet es als `SAMLRequest-` URL-Parameter.

Der SSO-Service verarbeitet den<samlp:AuthnRequest> -Element durch URL-Decodierung, Base64-Decodierung und Erweiterung der Anforderung, in dieser Reihenfolge. Anschließend wird eine Sicherheitsprüfung durchgeführt. Wenn der Benutzer keinen gültigen Sicherheitskontext hat, identifiziert der IdP den Benutzer, indem er zur Eingabe von Anmeldeinformationen auffordert. Wenn der Benutzer bereits angemeldet ist, antwortet der IdP einfach mit den URL-Parametern `SAMLResponse<tt> und <tt>RelayState` (siehe Schritt 3).

Antworten Sie mit einer SAMLResponse und RelayState

Nach dem Sammeln der erforderlichen Anmeldeinformationen validiert der SSO-Service die Anforderung und antwortet mit einem Dokument, das ein XHTML-Formular enthält:

```
<formmethod="post"action="https://
instance.service-now.com/navpage.do" ...><input type="hidden"
 name="SAMLResponse" value="response ..." /><input type="hidden"
 name="RelayState" value="token ..." />
    ...
    <input type="submit" value="Submit" /></form>
```

Der Wert des `RelaisState-` Parameters stammt aus diesem Schritt. Der Wert des Parameters `„SAMLResponse"` ist die base64-Codierung von<samlp:Response> Element:

```
<samlp:Responsexmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  ID="s2cdc74f37f923e26fe1aeec42b70a93d24230334f"
  InResponseTo="90AA6073F01567BFB0DF194F596314E2"
 Version="2.0"  IssueInstant="2010-04-29T23:21:51Z"
 Destination="https://dloomac.service-now.com/navpage.do"><saml:Issuer
 xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">http://
idp.ssocircle.com</saml:Issuer><samlp:Status
 xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"><samlp:StatusCode
 xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
 Value="urn:oasis:names:tc:SAML:2.0:status:Success"></samlp:StatusCode
></samlp:Status><saml:Assertion
 xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="s23e536bfc51b8487d4d3299dec162d9c2e338823b"
    IssueInstant="2010-04-29T23:21:51Z"
 Version="2.0"><saml:Issuer>http://
idp.ssocircle.com</saml:Issuer><Signature
 xmlns="http://www.w3.org/2000/09/xmldsig#">
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
...
      </Signature><saml:Subject><saml:NameID
 Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
            NameQualifier="http://idp.ssocircle.com"
 SPNameQualifier="https://
dloomac.service-now.com/navpage.do">david.loo@service-now.com</saml:NameI
D><saml:SubjectConfirmation
 Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"><saml:SubjectConfirmation
Data              InResponseTo="90AA6073F01567BFB0DF194F596314E2"
             NotOnOrAfter="2010-04-29T23:31:51Z"
 Recipient="https://dloomac.service-now.com/navpage.do" /
></saml:SubjectConfirmation></saml:Subject><saml:Conditions
 NotBefore="2010-04-29T23:11:51Z"
 NotOnOrAfter="2010-04-29T23:31:51Z"><saml:AudienceRestriction><saml:Audi
ence>https://
dloomac.service-now.com</saml:Audience></saml:AudienceRestriction></saml:
Conditions><saml:AuthnStatement AuthnInstant="2010-04-29T23:21:51Z"

 SessionIndex="s2dbf89ab99001e0e8cdaed67266d9d4b21b968a04"><saml:AuthnCon
text><saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Pa
sswordProtectedTransport</saml:AuthnContextClassRef></saml:AuthnContext
></saml:AuthnStatement></saml:Assertion></samlp:Response>
```

Validieren Sie die SAML-Antwort

Der Wert „`SAMLResponse`“ wird base64-decodiert und erweitert, um das XML-Dokument in Schritt 3 anzuzeigen. Das Anmeldeskript extrahiert den XML-Wert aus dem Element „`//Subject/NameID`“ und verwendet ihn, um in der Benutzertabelle nach einem vorhandenen Anwender zu suchen.

Das Anmeldeskript extrahiert auch die Sitzungs-ID aus dem Element `//AuthnStatement/@SessionIndex` und speichert sie für den `LogoutRequest`.

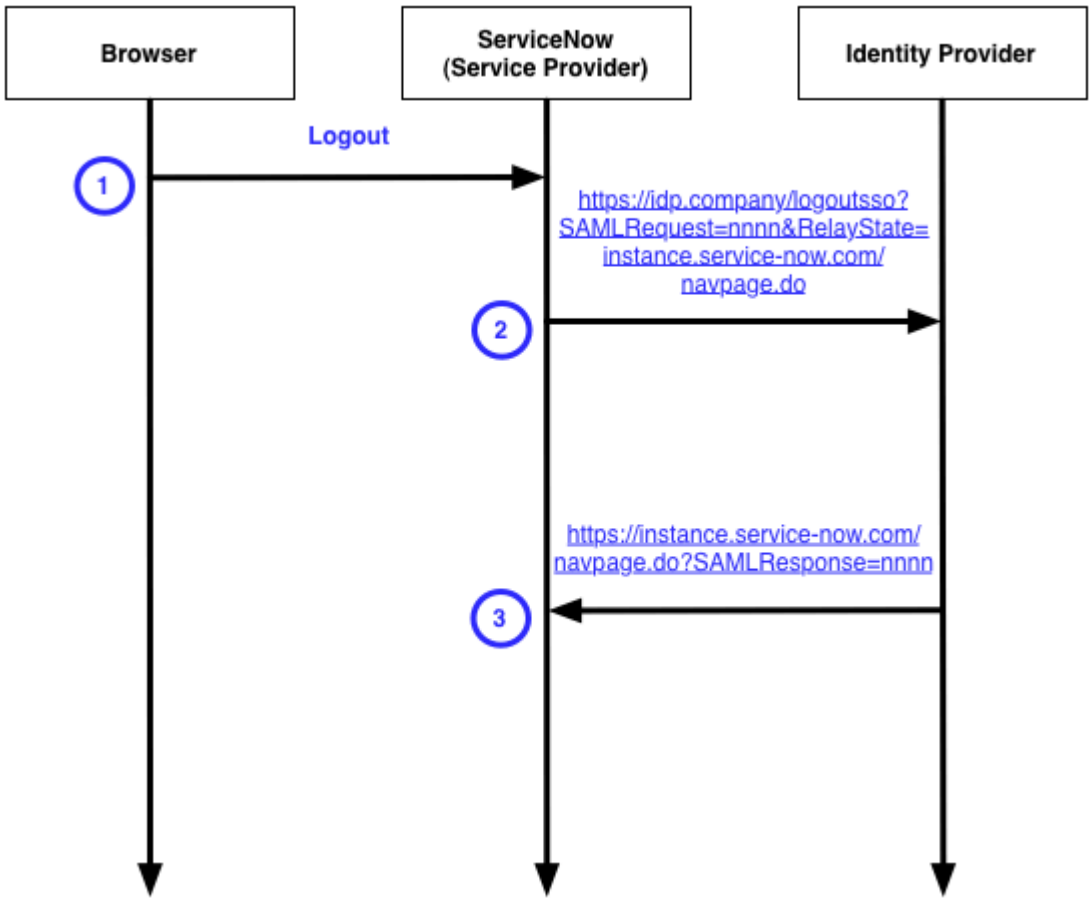
Prozess-Flow zum Abmelden (LogoutRequest).

Während der Abmeldung sendet die Instanz den SAML 2.0 *LogoutRequest* -Serviceaufruf an den IdP.

Dieser Service meldet den Anwender ab und leitet ihn dann zurück zur angegebenen Abmelde-URL.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SAML 2-Abmeldung



Anwender klickt auf die Schaltfläche „Abmelden“.

Der Benutzer klickt auf die Schaltfläche Abmelden, und die Instanz führt das **Abmeldeskript** aus.

LogoutRequest ausgegeben

Das Abmeldeskript erstellt einen SAML 2.0 `LogoutRequest` und sendet ihn an den vorkonfigurierten SingleLogoutRequest SAML 2.0-Service beim IdP. Der IdP dekomprimiert die Anforderung und wird anschließend base64-codiert. Ein Beispiel für einen `LogoutRequest` sieht wie folgt aus:

```
<saml2p:LogoutRequestxmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
 ID="21B78E9C6C8ECF16F01E4A0F15AB2D46"
 IssueInstant="2010-04-28T21:36:11.230Z"  Version="2.0"><saml2:Issuer
 xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">https://
dloomac.service-now.com
 </saml2:Issuer><saml2:NameID
 xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
 Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
          NameQualifier="http://idp.ssocircle.com"
 SPNameQualifier="https://
dloomac.service-now.com/navpage.do">david.loo@service-now.com</saml2:Name
ID><saml2p:SessionIndex>s211b2f811485b2a1d2cc4db2b271933c286771104
 </saml2p:SessionIndex></saml2p:LogoutRequest>
```

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

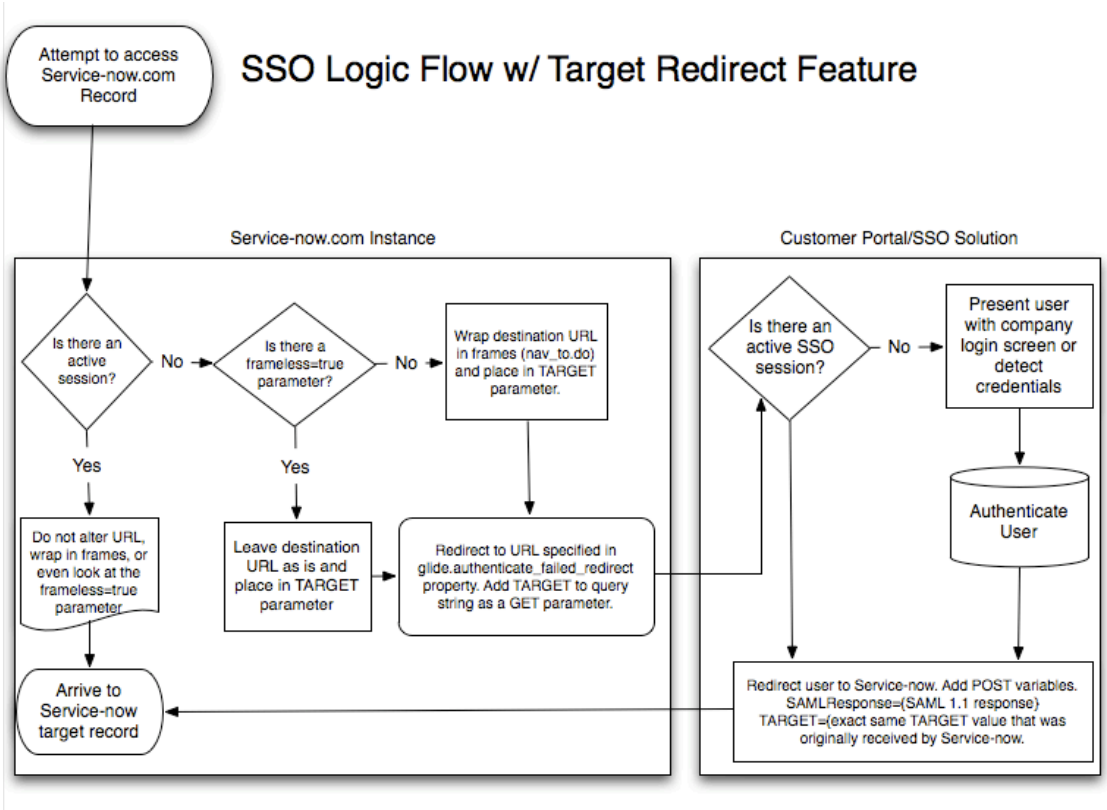
Anwender meldet sich ab

Der Anwender meldet sich vom IdP ab. Der IdP leitet zurück zur Instanz, die wiederum zurück zum IdP umleitet, da der Benutzer nicht angemeldet ist.

URL-Informationen für einen SSO-Anbieter

Während einer Anmeldeabfrage, die aus einem URL-Link in die Instanz resultiert, die eine SSO-Sitzung erfordert, muss die verweisende URL möglicherweise an den SSO-Anbieter übergeben werden, damit die URL nach der Authentifizierung an die Instanz zurückgegeben und mit der richtigen Ressource verknüpft werden kann .

SSO-Zielumleitung



Rückgabewerte für den Installationsausgang wurden verbessert, um eine URL anstelle oder zusätzlich zu der in den Eigenschaften definierten URL zu übergeben. Normalerweise geben Sie einen Anwendernamen oder einen vordefinierten Zeichenfolgenwert zurück, um die Autorisierung oder Abfrage der SSO-Sitzung zu steuern. Die folgenden Beispiele zeigen das erweiterte Verhalten der Übergabe einer URL.

```
return
 "failed_missing_requirement:%26amp;TARGET=https://
instance.service-now.com/nav_to.do?uri=incident.do?sys_id=12345";
```

Im obigen Beispiel wird die URL `https://instance.service-now.com/nav_to.do?uri=incident.do?sys_id=12345` in Form eines URL-Parameters namens TARGET an den SSO-Anbieter übergeben.

Hinweis: Es wird davon ausgegangen, dass der SSO-Anbieter diese Informationen im Parameter TARGET verwendet, um zur Instanz zurückzukehren, wenn die Anmeldeinformationen des Benutzers gesammelt und die Authentifizierung bestanden wurden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein Doppelpunkt : trennt die beiden Rückgabewerte, und ein codiertes & (%26amp;) verkettet die in der Eigenschaft *glide.authenticate.failed_missing_requirement* und dem TARGET-Parameter definierte URL.

SAML 2.0-Konfiguration mit Mehrfachanbieter-SSO

Sie können eine SAML 2.0-SSO-Konfiguration mit der Mehrfachanbieter-SSO-Funktion erstellen oder aktualisieren.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Hinweis: Neu im Release Jakarta : Bevor Sie Ihre IdP-Konfiguration aktivieren können, müssen Sie Ihre Konfiguration mithilfe der Testverbindungsfunktion validieren. Sie können die Aktualisierungsfunktion weiterhin verwenden, um Ihre Konfigurationsdaten zu speichern. Ohne eine erfolgreiche Testverbindung ist dies jedoch keine aktive Konfiguration.

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identity Provider**an.
2. Sie haben folgende Möglichkeiten.
   - Klicken Sie auf einen SSO-Konfigurationsdatensatz, um eine Konfiguration zu aktualisieren.
   - Klicken Sie auf, um eine neue Konfiguration zu erstellen **Neu** > **SAML**an.
3. Geben Sie die IdP-Informationen mit einer der folgenden Methoden ein.

Option	Bezeichnung
Unter Verwendung einer Metadaten-Deskriptor-URL	Aktivieren Sie das Kontrollkästchen URL, und geben Sie die URL des von Ihnen verwendeten IdP ein.
Verwenden der Metadaten-Deskriptor-XML-Datei	Klicken Sie auf das Kontrollkästchen XML, und fügen Sie die XML-Daten ein, die von dem von Ihnen verwendeten IdP generiert wurden.
Metadaten werden manuell eingegeben	Schließen Sie das Popup-Fenster, und geben Sie die Daten manuell in die Eigenschaftsfelder ein.

Alle Pflichtfelder müssen im Formular „Identitätsanbieter“ ausgefüllt werden.



Single Sign-on-Felder für mehrere Provider

Eigenschaft	Erforderlich	Beschreibung
Name	Ja	Geben Sie den Namen für den IdP ein. Dieser IdP ist die Sys-ID für die automatische Umleitung.
Aktiv	Ja	„Aktiv“ muss für den IdP, der für die Authentifizierung verwendet werden soll, auf „wahr“ festgelegt werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Erforderlich	Beschreibung
		Hinweis: Die Option zum Festlegen dieser Eigenschaft ist nur nach einer erfolgreichen Testverbindung verfügbar.
Standard	Nein	Der IdP mit automatischer Weiterleitung (früher als primärer IdP bezeichnet) leitet Benutzer automatisch zum Zugriff auf die Basisinstanz-URL um. Diese Eigenschaft legt diese IdP-Konfiguration als Standard fest.
Automatische IdP-Weiterleitung	Nein	Legt diese IdP-Konfiguration als automatische IdP-Weiterleitung fest. **Hinweis:** Wenn Sie eine neue IdP-Konfiguration für die automatische Weiterleitung aktivieren, wird das Cookie *glide_sso_id* mit dem neuen IdP für die automatische Weiterleitung aktualisiert. Die Systemeigenschaft *glide.authenticate.sso.update.idp.cookie*, die automatisch aktiviert ist, steuert diese Funktion.
URL des Identitätsanbieters	Ja	Geben Sie die URL zu Ihrem IdP ein. Jede IdP-URL muss eindeutig sein.
AuthnRequest des Identitätsanbieters	Ja	Geben Sie die URL für die HTTP-Redirect-Bindung ein, die Sie vom Element „SingleSignOnService“ erhalten haben.
SingleLogoutRequest des Identitätsanbieters	Nein	Geben Sie die URL ein, die Sie vom Element SingleLogoutService erhalten haben.
ServiceNow Homepage	Ja	Geben Sie die URL, einschließlich Anmeldeseite, der Instanz ein, für die sich der IdP authentifiziert. Beispiel: https://IhreInstanz.service-now.com/navpage.do
Entitäts-ID/Aussteller	Ja	Geben Sie die Basis-URL ohne Anmeldeseite ein. der Instanz, für die sich der IdP authentifiziert. Beispiel: https://IhreInstanz.service-now.com/
Zielgruppen-URI	Ja	Geben Sie die Basis-URL ohne Anmeldeseite ein. der Instanz, für die sich der IdP authentifiziert. Beispiel: https://IhreInstanz.service-now.com/
NameID-Richtlinie	Ja	Geben Sie den Wert des NameIDFormat-Elements ein, das die Integration verwendet.
Weiterleitung für externe Abmeldung	Nein	Geben Sie die URL ein, an die die Integration Anwender nach der Abmeldung weiterleitet.
Fehlerhafte Anforderungsumleitung	Nein	Geben Sie die URL für die Umleitung von fehlgeschlagenen Authentifizierungsanforderungen ein. Standardmäßig ist dies der URL-Endpunkt einer im IdP konfigurierten Fehlerseite oder Abmeldeseite. Sie können diesen Wert im Feld glide.authenticate.failed_requirement_redirect ausfüllen.

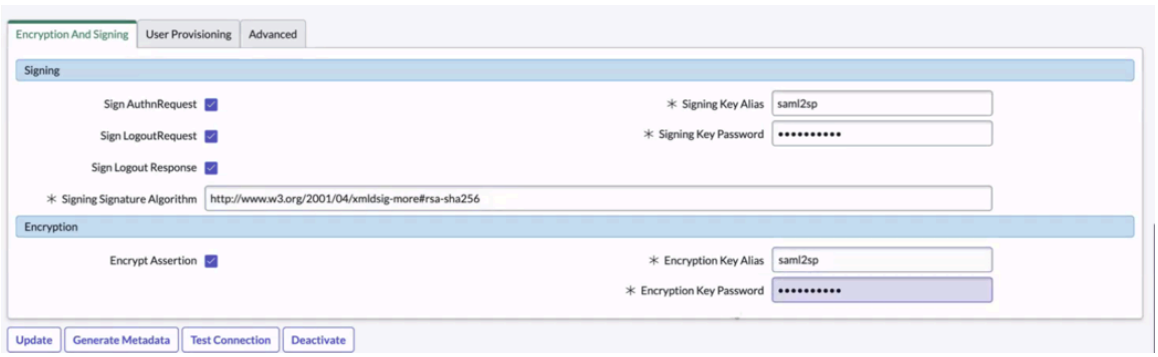
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Erforderlich	Beschreibung
Clienttyp	Nein	Wählen Sie den Clienttyp basierend auf dem Typ Ihres Clients aus. Optionen:**IFrame Eingebettet**. **Hinweis:** Wenn das Feld „Clienttyp“ für Ihre Konfiguration erforderlich ist, können Sie das Formular bearbeiten und das Feld hinzufügen. Weitere Informationen finden Sie unter Konfigurieren Sie den Clienttyp für OAuth- und SSO-Datensätze.

4. Wahlweise: Registerkarte „Verschlüsselung und Signierung“.

Hinweis:

- Es wird empfohlen, eigene Zertifikate für die Verschlüsselung und Signierung zu verwenden.
- Der **von FIPS genehmigte Modus** erfordert unterschiedliche Zertifikate für **Verschlüsselung** und **Signatur**
- Stellen Sie bei der Verwendung der Zertifikate sicher, dass Sie die folgenden Systemeigenschaften mit der sys_id der Zertifikate (x.509-Zertifikate) aktualisieren:
  - `Signieren (glide.authenticate.sso.saml2.keystore`)
  - **Verschlüsselung** (`glide.authenticate.sso.saml2.encryption.keystore`)
- Stellen Sie sicher, dass Sie den Schlüsselalias und das Schlüsselpasswort der **Signier-** und **Verschlüsselungsschlüsselspeicher** im Identitätsanbieter-Datensatz aktualisieren, und generieren Sie die Metadaten (Wählen **Sie Metadaten generieren**aus).
- Laden Sie die in den generierten Metadaten (XML) vorhandenen Signatur- und Verschlüsselungszertifikate zum Identitätsanbieter hoch.



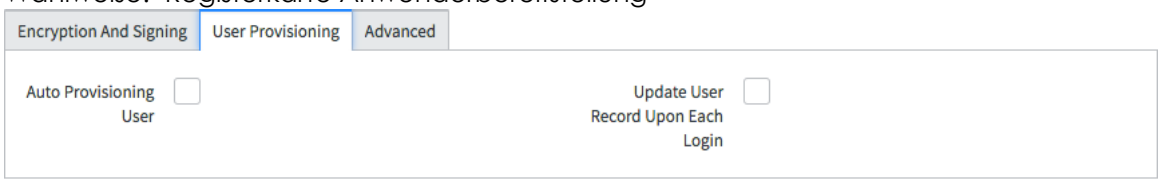
Felder für Verschlüsselung und Signatur

Eigenschaft	Beschreibung
Signaturschlüsselalias	Geben Sie den Signaturalias des im SAML 2.0 SP-Schlüsselspeicher gespeicherten Schlüsseleintrags ein.
Signaturschlüssel-Passwort	Geben Sie das Signaturpasswort des im SAML 2.0 SP-Schlüsselspeicher gespeicherten Schlüsseleintrags ein.
Verschlüsselungsschlüsselalias	Geben Sie den Verschlüsselungsalias des im SAML 2.0 SP-Schlüsselspeicher gespeicherten Schlüsseleintrags ein.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
Passwort des Verschlüsselungsschlüssels	Geben Sie das Verschlüsselungspasswort des im SAML 2.0 SP-Schlüsselspeicher gespeicherten Schlüsseleintrags ein.
Assertion verschlüsseln	Aktivieren Sie das Kontrollkästchen, um die Assertion in der SAML-Antwort zu verschlüsseln. In den für den IdP generierten Metadaten ist das x509-Zertifikat eingebettet, das der IdP zum Verschlüsseln der Assertion in der von ihm generierten SAML-Antwort verwendet.
Signaturalgorithmus für Signieren	Geben Sie die URL ein, die auf den AuthnRequest-Verbraucher des SAML 2.0-Identitätsanbieters für die eSignature-Authentifizierung verweist.
AuthnRequest signieren	Aktivieren Sie das Kontrollkästchen, um den Empfang des signierten AuthnRequest für den IdP-Single Sign-on-Service zu aktivieren.
LogoutRequest signieren	Aktivieren Sie das Kontrollkästchen, um den Empfang des signierten LogoutRequest für den IdP-Single Sign-on-Service zu aktivieren.
Abmeldeantwort signieren	Aktivieren Sie das Kontrollkästchen, um dem IdP-Single-Sign-on-Service den Empfang einer signierten Abmeldeantwort zu ermöglichen.

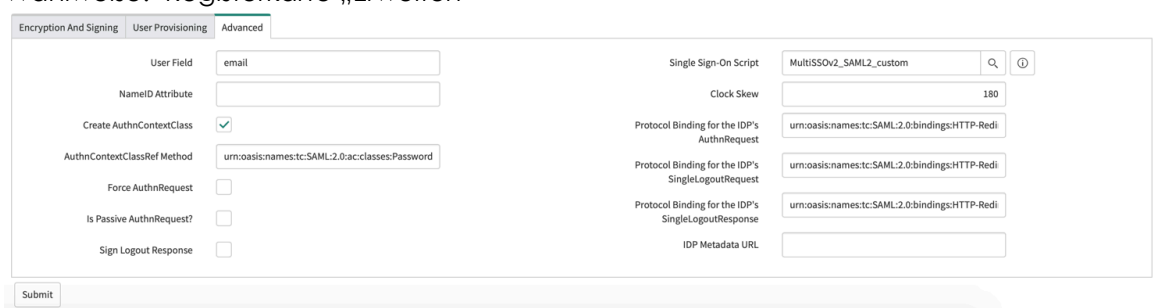
5. Wahlweise: Registerkarte Anwenderbereitstellung



Felder für die Anwenderbereitstellung

Eigenschaft	Beschreibung
Automatische Bereitstellung von Anwender	Aktiviert die automatische Anwenderbereitstellung und erstellt die Anwender, wenn der Anwender in der Instanzanwendertabelle basierend auf den vom IdP bereitgestellten Informationen nicht vorhanden ist.
Anwenderdatensatz bei jeder Anmeldung aktualisiere	Aktualisiert jedes Mal, wenn sich der Anwender mit SAML anmeldet, die Anwenderinformationen in der Instanzanwendertabelle mit den Informationen im IdP.

6. Wahlweise: Registerkarte „Erweitert“



© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Felder

Eigenschaft	Beschreibung
Anwenderfeld	Geben Sie das Feld in der Anwendertabelle ein, das den Wert enthält, den der IdP zum Identifizieren des Anwenders benötigt. Dies ist eine eindeutige ID als Teil der Antwort. Zum Beispiel Anwendername, Mitarbeiter-ID usw. In der Sys-Benutzertabelle wird diese eindeutige ID mit den Benutzerdetails abgeglichen.
Attribut NameID	Lassen Sie dieses Feld leer, es sei denn, Sie konfigurieren eine neue NameID-Richtlinie. Wenn Sie eine neue Richtlinie konfigurieren, benötigt das System die Benutzertabelle, die es verwenden muss, um den Benutzer zu identifizieren, der sich anmeldet. Das System gleicht das NameID-Token mit dem Namen des entsprechenden Benutzertabellenfelds ab.
AuthnContextClass erstellen	Aktivieren Sie das Kontrollkästchen, um eine bestimmte Kontextklasse anzugeben, z. B. Passwortgeschützter Transport. Wenn das Kontrollkästchen deaktiviert ist, wählt der IdP die am besten geeignete Kontextklasse aus.
AuthnContextClassRef-Methode	Geben Sie die URN des Anmeldemechanismus ein, den der IdP zur Authentifizierung von Anwendern verwenden soll.
AuthnRequest erzwingen	Aktivieren Sie das Kontrollkästchen, um AuthnRequests zu erzwingen.
Ist passive AuthnRequest	Aktivieren Sie das Kontrollkästchen, wenn AuthnRequest passiv ist.
Single Sign-on-Skript	Wählen Sie das Single Sign-on-Skript aus. Der Standardwert ist *MultiSSOV2_SAML2_custom*.
Abmeldeantwort signieren	Geben Sie in dieses Feld die Details für die Abmeldeantwort ein.
Taktversatz	Geben Sie die Anzahl der Sekunden zwischen den beiden Attributen ein, die die SAMLResponse-Nonce bilden. Der Standardwert ist 60. Eine gültige SAML-Antwort muss zwischen den Datums-/Zeit-Werten von „*notBefore*“ und „*notOnOrAfter*“ liegen. Eine Beispiel-SAML-Antwortnachricht finden Sie unter Beispiel-SAML-2-Antwort mit den Elementen SubjectConfirmation und SubjectConfirmationData sowie Beispiel-SAML-2-Antwort mit den Elementen AudienceRestrictions und Audience.
Protokollbindung für „SingleLogoutReuqest“ des IdP	Geben Sie einen der unterstützten Werte ein, die im Bindungsattribut des Elements SingleLogoutService aufgeführt sind.
Metadaten-URL, aus der IDP-Eigenschaften importiert werden	Die IdP-Eigenschaften werden von dieser URL importiert. Wenn festgelegt, wird der automatische Import des SAML-Zertifikats vom IdP aktiviert, wenn das vorherige Zertifikat abgelaufen ist. **Hinweis:** Wenn Sie ein Upgrade von SAML2 Update 1 auf Multi-Provider-SSO durchführen oder Ihre SSO-Verbindung manuell einrichten, wird die URL für die IdP-Metadaten nicht automatisch ausgefüllt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

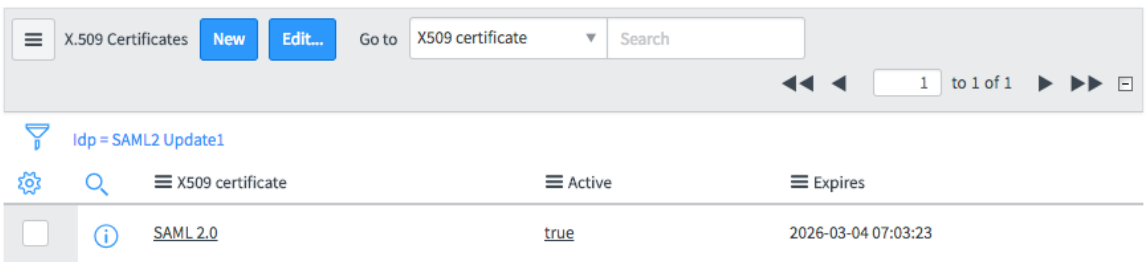
Eigenschaft	Beschreibung
Anforderung	Eine eindeutige ID als Teil der Anforderung. Die ID kann ein Anwendername, eine Mitarbeiter-ID usw. sein. **Hinweis:** Sowohl die Weiterleitung als auch die Nachbindung werden für die Anforderung unterstützt. Die Option zum Festlegen dieses Felds wird nur nach einer erfolgreichen Testverbindung angezeigt. Weitere Informationen finden Sie unter IdP-Verbindungen werden getestet.
Antwort	Eine eindeutige ID als Teil der Antwort. Die ID kann ein Anwendername, eine Mitarbeiter-ID usw. sein. **Hinweis:** Sowohl die Umleitung als auch die Nachbindung werden für die Antwort unterstützt. Die Option zum Festlegen dieses Felds wird nur nach einer erfolgreichen Testverbindung angezeigt. Weitere Informationen finden Sie unter IdP-Verbindungen werden getestet.

X.509-Zertifikate für SAML

Speichern und aktivieren Sie die erforderlichen IdP-Zertifikate für Ihre SAML-Konfiguration.

Die X.509-Zertifikate sind die IdP-Zertifikate, die von einer SAML-Konfiguration verwendet werden. Nachdem Sie ein Zertifikat installiert haben, können Sie beliebig viele Zertifikate hinzufügen. Wenn mehrere Zertifikate vorhanden sind, verwendet das System das erste gefundene aktive Zertifikat. Wenn Sie die URL für das **Feld „Metadaten-URL, aus der IDP-Eigenschaften importiert werden**“ festlegen, fragt das System automatisch den IdP nach einem aktuellen, gültigen Zertifikat ab, wenn Ihr Zertifikat nicht mehr gültig ist. Dieses Zertifikat wird an Ihre -Instanz angehängt und für Ihre aktive SAML-Konfiguration verwendet.

Hinweis: Die Abfrage erfolgt, wenn der IdP außerhalb Ihres Netzwerks zugänglich ist.



Geführte Tour für SAML

Verwenden Sie die geführte Tour zu SAML, um SAML für Single Sign-on zu konfigurieren.

Die geführte Tour für SAML hilft Ihnen, sich zu schulen und SSO für Ihre Instanz ServiceNow® zu konfigurieren. Administratoren können die geführte Tour auswählen, um schnell zu erfahren, welche Aktionen bei der Konfiguration von SSO für die Instanzen erforderlich sind.

Bevor Sie die geführte Tour verwenden, müssen Sie eine SAML-Anwendung in Ihrem bevorzugten Identitätsanbieter konfigurieren, z. B. Okta, Microsoft Azure, ADFS usw. Informationen zum Konfigurieren einer SAML-Anwendung finden Sie in der folgenden Dokumentation:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Okta: Für Okta müssen Sie Folgendes ausführen:
  - Fügen Sie eine Okta-SAML-Anwendung hinzu
  - Konfigurieren Sie SAML 2.0 für ServiceNow®
- Microsoft Azure: Integration von Single Sign-on (SSO) mit ServiceNow®
- Ping: SAML-SSO mit konfigurieren ServiceNow®
- ADFS: Integration mit SAML 2.0

Um die geführte Tour für SAML zu verwenden, aktivieren Sie das Plugin Integration – Single Sign-on-Installationsprogramm für mehrere Anbieter. Weitere Informationen finden Sie unter Aktivieren Sie das Mehrfachanbieter-SSO-Plugin.

Um die geführte Tour für SAML zu verwenden, gehen Sie wie folgt vor:

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identitätsanbieter**an.
2. Klicken Sie auf **Neu**.
3. Wählen Sie **SAML aus**.
4. Klicken Sie auf das **Hilfesymbol**.
5. Klicken Sie auf **Tour**starten .

Die geführte Tour für SAML verwendet eine Reihe von Schritten, die sich über mehrere Seiten erstrecken, um die Konfiguration abzuschließen. Befolgen Sie die Schritte und Anweisungen, die als Teil der Tour bereitgestellt wurden, und schließen Sie die Tour ab. Weitere Informationen zur SAML-Konfiguration finden Sie unter SAML 2.0-Konfiguration mit Mehrfachanbieter-SSO.

Integration von SAML 2.0 mit anderen Funktionen

Sie können Ihre SAML 2.0-Lösung mit anderen Funktionen wie E-Signatur, Deep Linking und ADFS integrieren.

Fügen Sie Deep Linking-Unterstützung für SAML hinzu

Mit Deep Links können Instanzen direkte E-Mail-Links zu einem bestimmten Datensatz im System unterstützen.

Wenn die SAML 2.0-Integration aktiviert ist, müssen Deeplinking-URLs eine Authentifizierungsprüfung bestehen, bevor der IdP den Benutzer zur ursprünglich angeforderten URL umleitet. Betrachten Sie beispielsweise eine E-Mail, die diese URL enthält: `https://`<instance name> .service-now.com/nav_to.do?uri=incident.do?sys_id=46c88ac1a9fe1981014de1c831fbcf6d

Die Instanz sendet eine Authentifizierungsanforderung an den IdP und verwendet den URL-Parameter `RelayState`, um die ursprünglich angeforderte Ressource beizubehalten (in diesem Fall `uri=incident.do?sys_id=46c88ac1a9fe1981014de1c831fbcf6d`). Nachdem der IdP den Benutzer authentifiziert hat, liest die Instanz den Wert des RelaisState-URL-Parameters und leitet den Benutzer zur angeforderten Ressource weiter (falls in der Instanz vorhanden).

Um Unterstützung für Deep Linking hinzuzufügen, vergewissern Sie sich, dass der Identitätsanbieter den URL-Parameter `RelayState` unterstützt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integration von ADFS mit SAML 2.0

Das ServiceNow Multi-Provider-SSO-Plugin unterstützt eine SAML 2. Single Sign-on-Integration (Single Sign-on, SSO) mit Microsoft ADFS.

Informationen zum Installieren und Konfigurieren von ADFS finden Sie unter Übersicht über die Active Directory-Verbundservices . Das Multi-Provider-SSO-Plugin wurde mit einer SAML 2.0-SSO-Integration mit ADFS 2.0, 3.0, Azure AD konfiguriert und getestet. Die SAML-Antwort wird in nicht unterstützt

Richten Sie ADFS für SAML ein

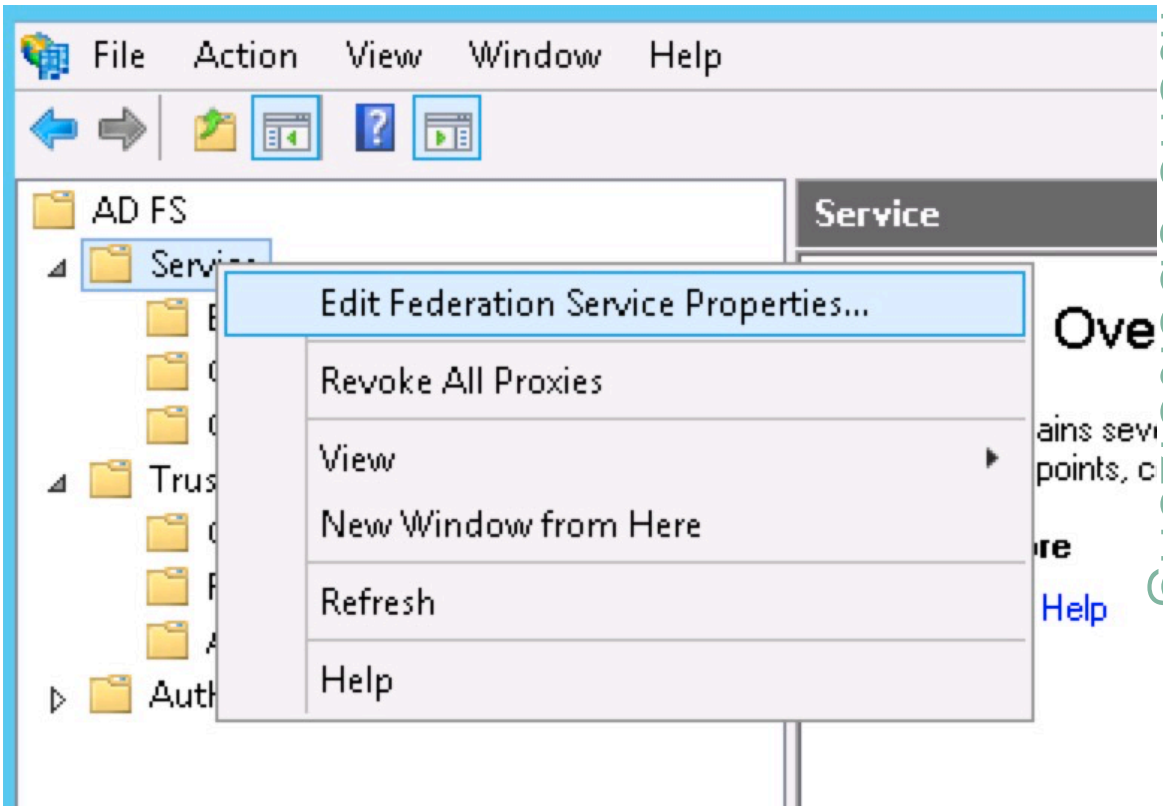
Richten Sie ADFS für SAML ein. Dieses Verfahren verwendet ADFS 2.0 und zeigt samportal.example.com als ADFS-Website an. Ersetzen Sie diese durch Ihre ADFS-Websiteadresse.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

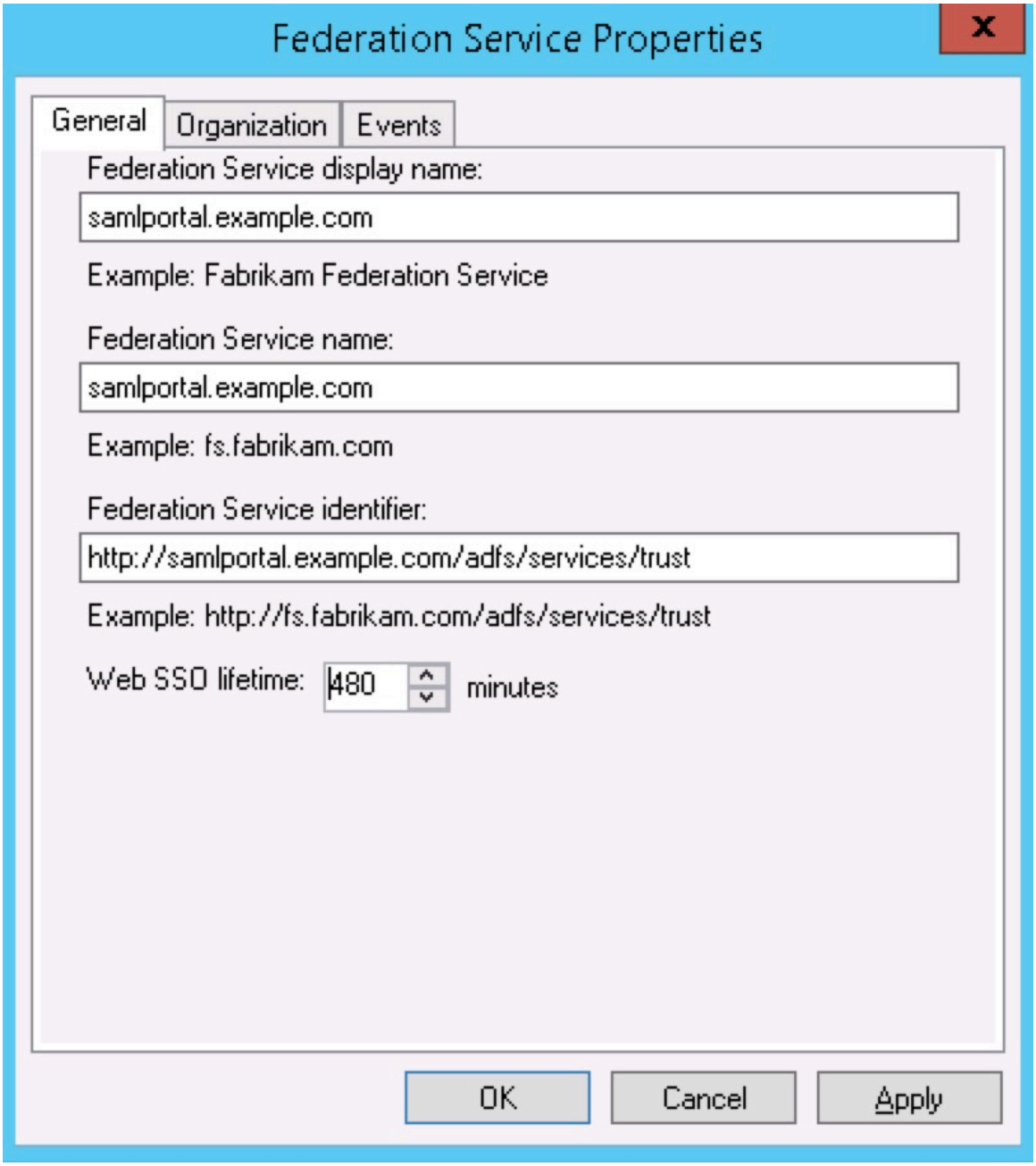
1. Melden Sie sich beim ADFS 3.0-Server an, und öffnen Sie die -Verwaltungskonsole.
2. Klicken Sie mit der rechten Maustaste auf **Service**, und wählen Sie **Eigenschaften des Verbundservice bearbeiten**aus.



3. Stellen Sie sicher, dass die allgemeinen Einstellungen mit Ihren DNS-Einträgen und Zertifikatnamen übereinstimmen.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Automatische Übersetzung

4. Navigieren Sie zu den Zertifikaten, und exportieren Sie das Token-Signaturzertifikat.

a. Klicken Sie mit der rechten Maustaste auf das Zertifikat, und wählen Sie **Zertifikat anzeigen**aus.

b. Wählen Sie die Registerkarte **Details** aus.

c. Klicken Sie **auf In Datei kopieren**.
Der Assistent zum Exportieren von Zertifikaten wird geöffnet.

d. Wählen Sie **Weiter**.

e. Vergewissern Sie sich, dass die Option **No, do not export the private Key** (Privaten Schlüssel nicht exportieren) ausgewählt ist, und klicken Sie dann auf **Next**(Weiter).

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

f. Wählen Sie **DER codierte Binärobjekt X.509 (.cer)**aus, und klicken Sie dann auf **Weiter**.

g. Wählen Sie aus, wo Sie die Datei speichern möchten, geben Sie ihr einen Namen, und klicken Sie auf **Weiter**.

h. Wählen Sie **Fertigstellen** aus.
Die Instanz erfordert, dass dieses Zertifikat im PEM-Format vorliegt. Sie können dieses Zertifikat mit Client-Tools oder Online-Tools wie SSL Shopper konvertieren.

5. Verwenden Sie das DER/Binär-Zertifikat, das Sie gerade erstellt haben, und exportieren Sie es im Standard-PEM-Format.

Richten Sie die -Instanz für ADFS ein

Konfigurieren Sie Ihre -Instanz und die SAML 2.0-Einstellungen für die Verwendung mit ADFS.

Vorbereitungen

Führen Sie diese Schritte nur aus, nachdem Sie ADFS für SAML eingerichtet haben. Weitere Informationen zu diesem Prozess finden Sie unter ADFS für SAML einrichten.

Erforderliche Rolle: admin

Prozedur

1. Falls noch nicht aktiv, Aktivieren Sie das Mehrfachanbieter-SSO-Plugin.
2. Konfigurieren Sie SAML, aber wenn Sie das IdP-Zertifikat installieren, hängen Sie das PEM-Zertifikat an, das Sie bei der Ausführung von Richten Sie ADFS für SAML einerstellt haben.
3. Klicken Sie auf **Speichern**.
4. Stellen Sie sicher, dass die **Felder** Problem und **Betreff** Werte enthalten und keine Fehler vorliegen.
Wenn ein Fehler auftritt, öffnen Sie das gespeicherte Zertifikat im PEM-Format im Editor, kopieren Sie das Zertifikat und fügen Sie es in das Feld PEM-Zertifikat ein.
5. Stellen Sie sicher, dass der Installations-Exit SAML2SingleSignon_update1 aktiv ist.
6. Setzen Sie die SAML 2.0-Konfiguration fort.

Hinweis: Wenn ein Zertifikat auf dem ADFS-Server aktualisiert wird, müssen Sie auch ein aktualisiertes Zertifikat in die Instanz hochladen.

Konfigurieren Sie eine abhängige ADFS-Seite

Importieren Sie die Instanzmetadaten in Ihren ADFS-Server. Die manuelle Konfiguration der vertrauenden Partei scheint jedoch einfacher zu implementieren zu sein.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identity Provider** > **SAML2-Update1** > **Verschlüsselung und Signatur** und stellen Sie sicher, dass die SAML-Eigenschaft AuthnRequest signieren (*glide.authenticate.sso.saml2.require_signed_authnrequest*) nicht aktiv ist.
Lassen Sie diese Eigenschaft nur aktiv, wenn Ihr ADFS-Administrator überprüfen kann, ob Sie signierte Anforderungen benötigen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Kopieren Sie die Metadaten, die Sie über den SAML 2-Metadatenlink generiert haben, und speichern Sie sie in einer Datei.
3. Melden Sie sich beim ADFS-Server an, und öffnen Sie die Verwaltungskonsole.
4. Wählen Sie **Trusts der vertrauenden Partei aus**.
5. Wählen Sie in der oberen rechten Ecke des Fensters die **Option Trust der vertrauenden Partei hinzufügen** aus.

   Der Assistent zum Hinzufügen wird angezeigt.
6. Klicken Sie auf **Start**, um zu beginnen.
7. Verwenden Sie die Option **Datei** importieren, um die Metadatendatei zu importieren.
8. Geben Sie einen Anzeigenamen wie „ `ServiceNow` “ ein, und geben Sie die gewünschten Notizen ein.
9. Wählen Sie **das ADFS 3.0-Profil aus**.
10. Wählen Sie kein Tokenverschlüsselungszertifikat aus.
    Dabei wird das Zertifikat verwendet, das für den bereits exportierten Service definiert ist. Das Definieren eines Zertifikats verhindert eine ordnungsgemäße Kommunikation mit der Instanz.
11. Aktivieren Sie keine Einstellungen für die **Konfigurations-URL**.
12. Geben Sie den Instanzstandort, mit dem Sie eine Verbindung hergestellt haben, als Trust-Bezeichner der vertrauenden Partei ein.
    Verwenden Sie in diesem Fall `https://company.service-now.com`, und klicken Sie auf **Hinzufügen**.
13. allen Anwendern den Zugriff auf diese abhängige Partei zulassen.
14. Klicken Sie auf **Weiter**, und deaktivieren Sie das Kontrollkästchen **Ansprüche öffnen, wenn dies abgeschlossen** ist.
15. Schließen Sie diese Seite.
    Der neue Trust der vertrauenden Partei wird im Fenster angezeigt.
16. Klicken Sie mit der rechten Maustaste auf den Trust der vertrauenden Seite, und wählen Sie **Eigenschaften**aus.
17. Navigieren Sie zur Registerkarte **Erweitert**, und legen Sie für den **sicheren Hash-Algorithmus** entweder SHA-256 oder SHA-1 fest.
18. Navigieren Sie zur Registerkarte Endpunkte, und fügen Sie einen **SAML-Assertionsverbraucher** mit einer **Post** -Bindung und der URL `https://company.service-now.com/navpage.do`hinzu.

Konfigurieren Sie die Anspruchsregeln der abhängigen Partei in ADFS

Bearbeiten Sie die Anspruchsregeln, um eine ordnungsgemäße Kommunikation mit der Instanz zu ermöglichen.

Vorbereitungen

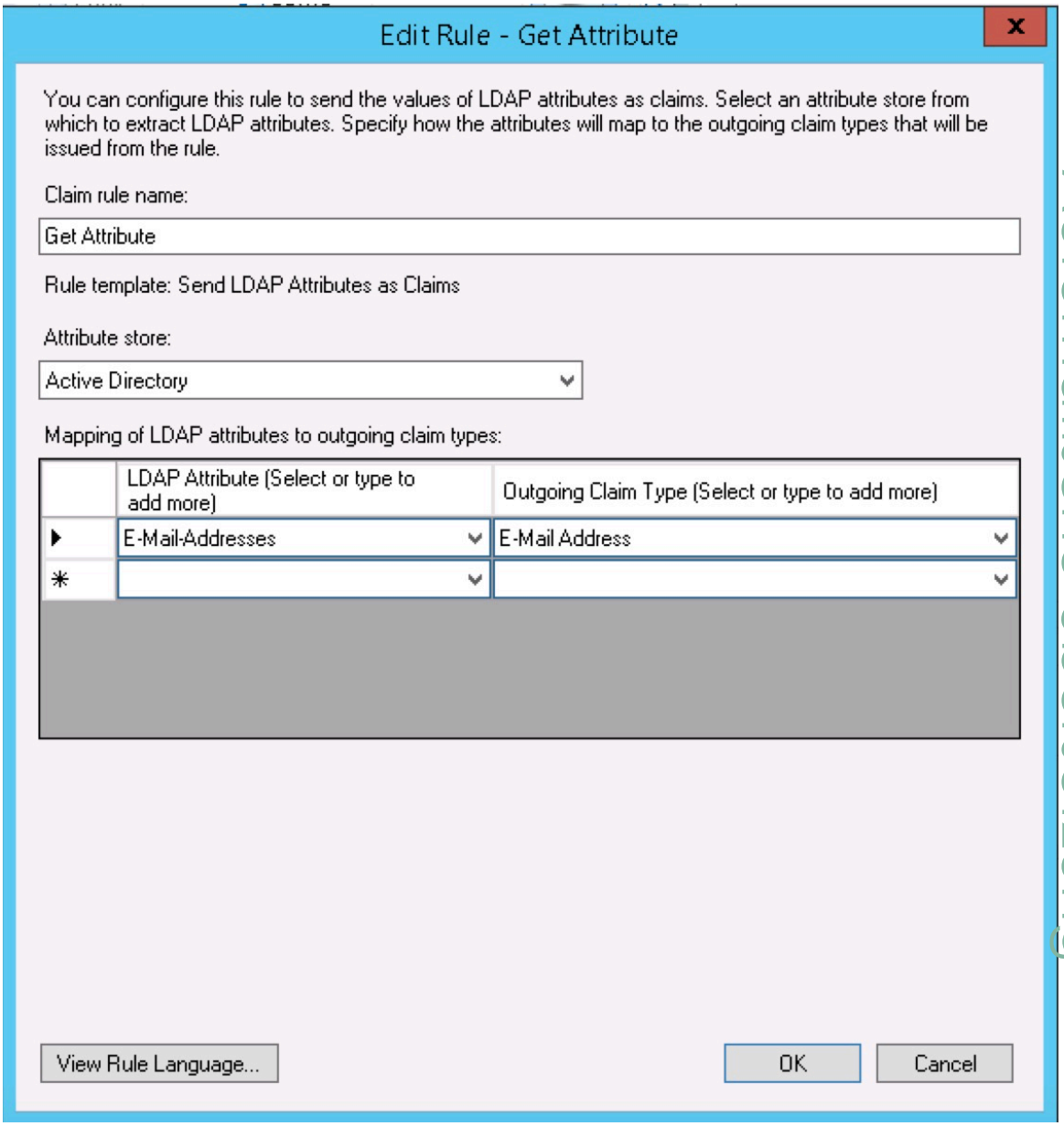
Erforderliche Rolle: admin

Prozedur

1. Melden Sie sich beim ADFS-Server an, und öffnen Sie die Verwaltungskonsole.
2. Klicken Sie mit der rechten Maustaste auf den Trust der vertrauenden Partei, und wählen Sie **Anspruchsregeln bearbeiten**aus.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf die Registerkarte **Ausgabe Transformationsregeln**.
4. Wählen **Sie Regeln hinzufügen**.
5. Wählen **Sie „LDAP-Attribut als Ansprüche senden“ als** zu verwendende Anspruchsregelvorlage aus.
6. Geben Sie der Forderung einen Namen wie z. B. `LDAP-Attribute abrufen`.
7. Legen Sie den **Attributspeicher** auf `Active Directory`, das **LDAP-Attribut** auf `E-Mail-Adressen`und den **Typ des ausgehenden Anspruchs** auf `E-Mail-Adresse fest`.




```
c:[Type ==
 "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccoun
tname", Issuer == "AD AUTHORITY"]
=> issue(store = "Active Directory",
types =
 ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
"),
query = ";mail;{0}", param = c.Value);
```

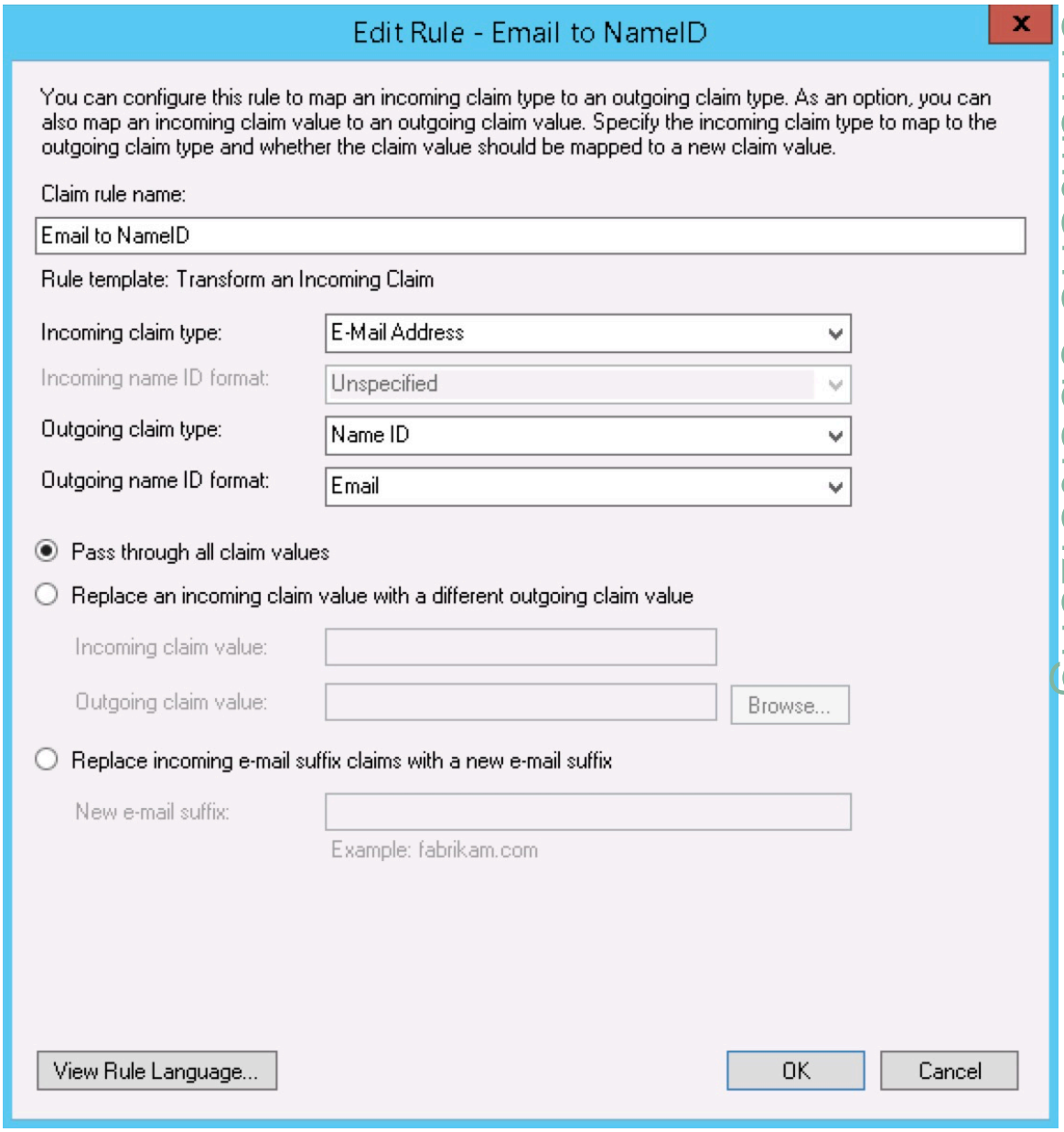
Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Wählen Sie **Fertigstellen** aus.
9. Wählen **Sie Regeln hinzufügen**.
10. Wählen Sie **Eingehenden Anspruch transformieren** als zu verwendende Anspruchsregelvorlage aus.
11. Geben Sie dem Anspruch einen Namen, z. B. `E-Mail an Namens-ID`.
12. Legen Sie in der vorherigen Regel den Typ des **eingehenden Anspruchs auf den Typ** des **ausgehenden Anspruchs fest**.
    Beispiel: `E-Mail-Adresse`.
13. Legen Sie den **Typ des ausgehenden Anspruchs** auf `Namens-ID` und das **Format der ausgehenden Namens-ID** auf E- `Mail fest`.

    Hinweis: Diese Werte müssen mit der Namens-ID-Richtlinie übereinstimmen, die Sie während der SAML 2.0-Konfiguration definieren.

14. Wählen Sie **Alle Anspruchswerte übergeben aus**.



Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Anspruchsregel sollte ähnlich wie die folgende Regelsprache aussehen.

```
c:[Type ==
 "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
 => issue(Type =
 "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifie
r",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value,
 ValueType = c.ValueType,
Properties["http://
schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"]
= "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress");
```

15. Klicken Sie auf **Fertigstellen**.

Erstellen Sie einen SAML-Logout-Endpunkt

Erstellen Sie einen SAML-Logout-Endpunkt, um eine Einzelabmeldung zu ermöglichen.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Weitere Informationen finden Sie in diesem Artikel zur ADFS-Signatur .

Prozedur

1. Gehe zu **ADFS-Manager** > **Trust-Beziehungen** > **Trusts der vertrauenden Partei** > **Eigenschaften**an.
2. Klicken Sie auf der Registerkarte Endpunkte auf **SAML hinzufügen**.
3. Konfigurieren Sie die Einstellungen:
   - **Endpunkttyp**: SAML-Logout
   - **Bindung**: POST
   - **Vertrauenswürdige URL**: Die URL Ihres ADFS-Servers. Beispiel:

     ```
     https://myadfsserver.domain.net/adfs/ls/?wa=wsignout1.0
     ```

   - **Antwort-URL**: Die Abmelde-URL der Anwendung. Beispiel:

     ```
     https://{instancename}.service-now.com/external_logout_complete.do
     ```

Testen Sie die ADFS-Konfiguration

Testen Sie Ihre ADFS-Konfiguration, um sicherzustellen, dass sie ordnungsgemäß als Identitätsanbieter funktioniert.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Öffnen Sie einen Internet Explorer-Browser.
2. Navigieren Sie zu Ihrem ADFS-Portal.

   Beispiel: `https://samportal.example.com/adfs/ls/idpinitiatedsignon.aspx`. Diese Seite enthält eine Dropdown-Liste aller konfigurierten Trusts der vertrauenden Partei.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie die vertrauende Partei aus, die Ihrer Instanz zugeordnet ist.
4. Klicken **Sie auf Sign-in fortsetzen**.

   Wenn Sie die externe SAML 2.0-Authentifizierung ordnungsgemäß konfiguriert haben, sollten Sie automatisch bei der Instanz angemeldet werden.

5. Testen Sie eine URL für die direkte Anmeldung, indem Sie zu `https://samportal.example.com/adfs/ls/idpinitiatedsignon.aspx?logintoRP=https://company.service-now.com`navigieren.

(Workaround) Aktivieren Sie die vom Service Provider initiierte Authentifizierung

Verwenden Sie diese Problemumgehung, wenn die Authentifizierung fehlschlägt, da Sie nicht über SAML 2.0 Update 1 verfügen. Dieses Problem kann auftreten, wenn Anwender versuchen, die IdP-Authentifizierung zu überspringen und direkt zur Instanz zu navigieren.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Dieser Fehler tritt auf, wenn die Instanz ADFS nicht mit der erforderlichen Definition und Semantik für das Attribut „SPNameQualifier“ in der SAMLResponse bereitstellt.

Aktivieren Sie die vom Service Provider initiierte Authentifizierung, indem Sie eine der folgenden Aktionen ausführen:

Prozedur

- Führen Sie ein Upgrade auf SAML 2.0 Update 1 durch, und deaktivieren Sie die Option zum Erstellen einer AuthnContextClass-Anforderung.
- Ändern Sie die **SAML2-Skripteinbindung**, um die Definitionen des Attributs `SPNameQualifier` zu kommentieren, wenn SAML 2.0 aktiv ist (nicht SAML 2.0 Update 1).

  Kommentieren Sie diese Zeilen in den Funktionen createNameID und createNameIDPolicy aus:

```
//nid.setSPNameQualifier (serviceURL ) ;

 //nameIdPolicy. setSPNameQualifier (serviceURLStr ) ;
```

Nächste Maßnahme
Wenn Sie nicht möchten, dass die Anmeldeaufforderung von Ihrem ADFS-Server angezeigt wird, wenn Sie auf die Instanz zugreifen, legen Sie die folgende Eigenschaft für SAML 2.0 Update 1 auf false fest: **Erstellen Sie eine AuthnContextClass-Anforderung in der AuthnRequest-** Anweisung (*`glide.authenticate.sso.saml2.createrequestedauthncontext`*).

(Workaround) Unterstützt die Kerberos-Authentifizierung

Für die SAML 2.0-Integration ist ein Workaround verfügbar, der den Authentifizierungskontext von formularbasierter Authentifizierung in Windows-basierte Authentifizierung ändert.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Derzeit verwendet die SAML 2-Integration einen Authentifizierungskontext mit PasswordProtectedTransport oder „formularbasierte Authentifizierung“. Dieser Authentifizierungskontext erfordert, dass der Identitätsanbieter Anwendern ein Formular

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zur Authentifizierung von Anmeldeinformationen vorlegt. Bei Kerberos ist eine SAML-Sitzung bereits über eine hergestellte Windows-Anmeldung aktiv, sodass sich der Benutzer nicht beim IdP authentifizieren muss.

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identity Provider**an.
2. Öffnen Sie den **SAML2 Update1** IdP-Datensatz.
3. Legen Sie die **Methode AuthnContextClassRef, die in die SAML 2.0 AuthnRequest für den Identitätsanbieter aufgenommen wird**, auf eine der folgenden Optionen fest:

Werte der AuthnContextClassRef-Methode
`urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport` (Standard)
`urn:federation:authentication:windows`

4. Klicken Sie auf **Aktualisieren**.

Integration von Azure AD mit SAML 2.0

Integrieren Sie ServiceNow in Azure Active Directory (Azure AD).

Durch die Integration von ServiceNow in Azure AD können Sie:

- Steuern Sie in Azure AD, wer Zugriff auf ServiceNowhat.
- Ermöglicht Benutzern die automatische Anmeldung bei ServiceNow mit ihren Azure AD-Konten.
- Verwalten Sie Ihre Accounts im Azure-Portal.

Voraussetzungen

Um zu beginnen, müssen Sie Folgendes ausführen:

- Ein Azure AD-Abonnement. Wenn Sie kein Abonnement haben, können Sie einen kostenlosen Account erhalten.
- Ein ServiceNow Single Sign-on (SSO) aktiviert.
- Eine ServiceNow -Instanz oder ein Mandant von ServiceNow, die bzw. der San Diego-Versionen oder höher unterstützt.
- Für einen ServiceNow -Mandanten muss das Single Sign-on-Plugin für mehrere Anbieter aktiviert sein.
- Aktivieren Sie für die automatische Konfiguration das Plugin für mehrere Anbieter für ServiceNow.

Satz von Aktionen für die Konfiguration

Im Folgenden finden Sie die Aktionen, die zum Konfigurieren von Azure AD ausgeführt werden müssen:

- Fügen Sie ServiceNow aus der Galerie zu Azure AD hinzu.
- Konfigurieren Sie Azure AD SSO
- Erstellen Sie einen Azure AD-Testanwender

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Weisen Sie den Azure AD-Testanwender zu
- ServiceNow konfigurieren

Fügen Sie ServiceNow aus der Galerie hinzu

Fügen Sie ServiceNow aus der Galerie Ihrer Liste der verwalteten SaaS-Apps in Azure AD hinzu.

Vorbereitungen

Erforderliche Rolle: Azure-Administrator

Prozedur

1. Melden Sie sich mit einem Microsoft-Konto beim Azure-Portal an.
2. Wählen Sie im linken Bereich den Service **Azure Active Directory** aus.
3. Navigieren zu **Unternehmensanwendungen** > **Alle Anwendungen**an.
4. Um eine neue Anwendung hinzuzufügen, wählen Sie **New** application (Neue Anwendung).
5. Geben Sie im Abschnitt Aus Galerie hinzufügen im Suchfeld ServiceNow ein.
6. Wählen Sie im Ergebnisbereich ServiceNow aus, und fügen Sie dann die App hinzu.
7. Warten Sie einige Sekunden, während die App Ihrem Mandanten hinzugefügt wird.

Konfigurieren Sie Azure AD SSO

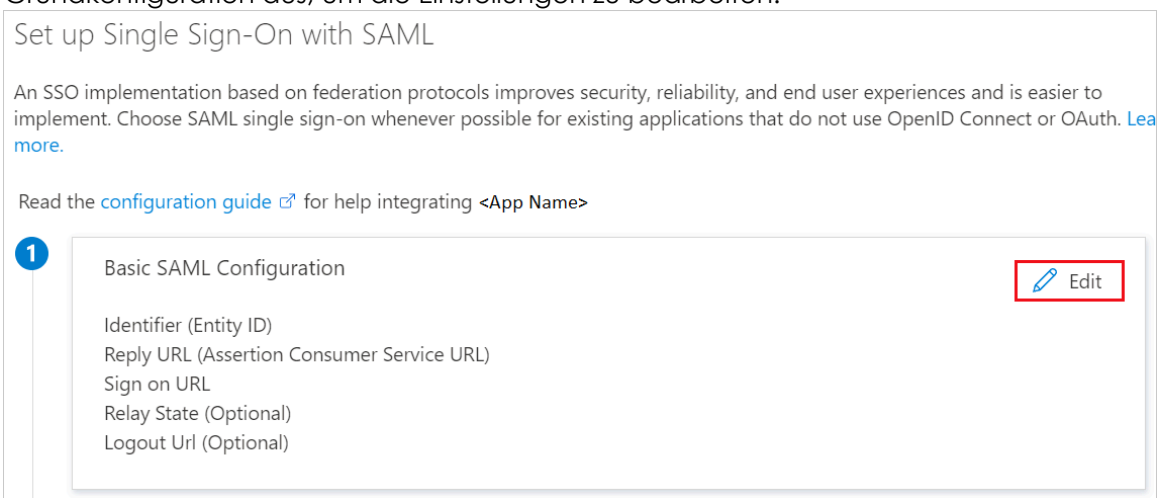
Konfigurieren Sie Azure AD SSO im Azure-Portal.

Vorbereitungen

Erforderliche Rolle: Azure-Administrator

Prozedur

1. Suchen Sie im Azure-Portal auf der Seite zur Integration der Anwendung ServiceNow den Abschnitt Verwalten.
2. Wählen Sie Single Sign-on aus.
   Wählen Sie auf der Seite Single Sign-on-Methode auswählen die Option SAML aus.
3. Wählen Sie auf der Seite „Single Sign-on mit SAML einrichten“ das Stiftsymbol für SAML-Grundkonfiguration aus, um die Einstellungen zu bearbeiten.



4. Führen Sie im Abschnitt Grundlegende SAML-Konfiguration Folgendes aus:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. **Geben Sie im Feld Signatur-URL**eines der folgenden URL-Muster ein:

```
https://<instancename>.service-now.com/navpage.do
https://<instance-name>.service-now.com/login_with_sso.do?glide_sso_id
=<sys_id of the sso configuration>
```

Hinweis: Sie müssen die sys_id innerhalb dieser URL angeben.

b. Geben Sie unter Bezeichner (Entitäts-ID) eine URL mit folgendem Muster ein:
`https://`<instance-name> .service-now.com .

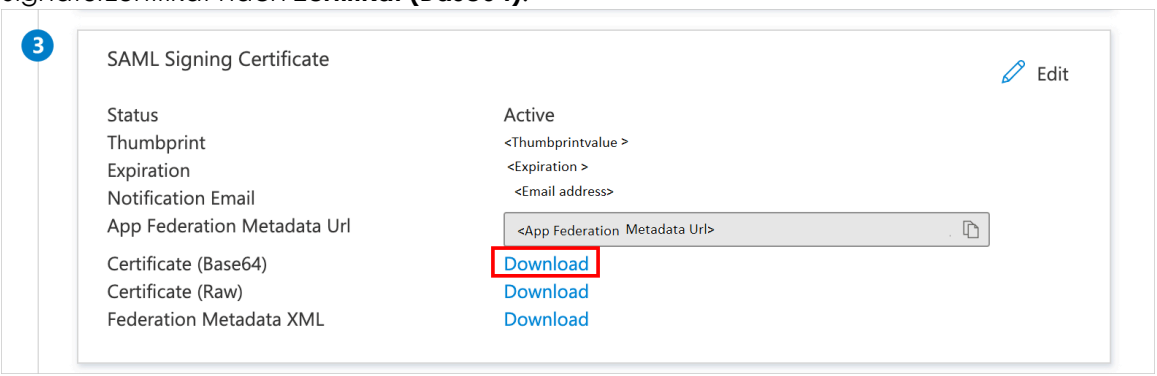
c. Geben Sie für **Antwort-URL**eines der folgenden URL-Muster ein:

```
https://<instancename>.service-now.com/navpage.do
https://<instancename>.service-now.com/customer.do
```

d. Geben Sie unter Abmelde-URL eine URL mit dem folgenden Muster ein:
`https://`<instancename> .service-now.com/navpage.do

Hinweis: Sie müssen die tatsächliche Anmelde-URL, Antwort-URL, Abmelde-URL und den Bezeichner aktualisieren. Die in diesen URLs angezeigten Werte dienen zu Demozwecken.

5. Suchen Sie auf der Seite Single Sign-on mit SAML einrichten im Abschnitt SAML-Signaturzertifikat nach **Zertifikat (Base64)**.

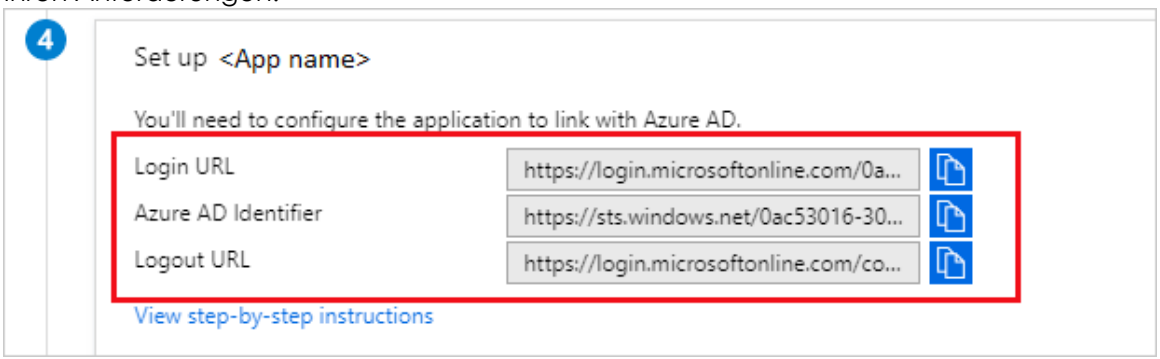


a. Wählen Sie die Schaltfläche Kopieren aus, um die **App-Verbund-Metadaten-URL**zu kopieren und in den Editor einzufügen.
Diese URL ist für die weitere Konfiguration erforderlich.

b. Wählen Sie **Download** aus, um das Zertifikat (Base64) herunterzuladen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Kopieren Sie im Abschnitt „Setup ServiceNow “ die entsprechenden URLs entsprechend Ihren Anforderungen.



Erstellen Sie einen Azure AD-Testanwender

Erstellen Sie einen Testanwender in Azure AD.

Vorbereitungen

Erforderliche Rolle: Azure-Administrator

Prozedur

1. Navigieren Sie im Azure-Portal zu **Alle** > **Azure Active Directory** > **Anwender** > **Alle Anwender**an.
2. Wählen Sie **Neuer Anwender aus**.
3. Geben Sie in den Benutzereigenschaften die folgenden Informationen an:
   - Name
   - Benutzername
   - Passwort
4. Klicken Sie auf **Erstellen**.

Weisen Sie den Azure AD-Testanwender zu

Weisen Sie den Azure AD-Testanwender, der für die Verwendung des Azure-Single Sign-ons erstellt wird, zu, indem Sie Zugriff auf ServiceNowgewähren.

Vorbereitungen

Erforderliche Rolle: Azure-Administrator

Prozedur

1. Navigieren Sie im Azure-Portal zu **Alle** > **Unternehmensanwendungen** > **Alle Anwendungen**an.
2. Wählen Sie in der Anwendungsliste ServiceNowaus.
3. Wählen Sie auf der Seite der App im Abschnitt Verwalten die Option **Anwender und Gruppen aus**.
4. Wählen Sie **Anwender hinzufügen** aus.
5. Wählen Sie im Fenster **„Zuweisung** hinzufügen“ die Option **Benutzer und Gruppen aus**.
6. Wählen Sie im Fenster **Benutzer und Gruppen** den Testbenutzer aus, der aus der `Benutzerliste` erstellt wurde.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Wählen Sie bei Bedarf in der Dropdown-Liste **Rolle** auswählen die Rolle für den zugewiesenen Anwender aus.
8. Wählen Sie im Fenster „ **Zuweisung** hinzufügen " **Zuweisen**aus.

ServiceNow konfigurieren

Konfigurieren Sie ServiceNow mit Azure AD-Details, um SSO zu verwenden.

Vorbereitungen

Plugin: `Integration – Single Sign-on für mehrere Anbieter – Installationsprogramm`

Aktivieren Sie die Mehrfachanbieter-SSO-Eigenschaften:

- ◦ Wählen Sie **SSO mit mehreren Providern aktivieren aus**.
  - ◦ Wählen Sie Aktivieren Sie **das automatische Importieren von Benutzern von allen Identitätsanbietern in die Benutzertabelle**.
  - ◦ Wählen Sie **Debug-Protokollierung für SSO-Integration mit mehreren Anbietern aktivieren aus**.
  - ◦ Geben Sie „ **email**" ein, das Feld in der Benutzertabelle, das….

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identity Provider**an.
2. Wählen Sie auf der Seite „Identitätsanbieter" **Neu**.
3. Wählen Sie im Fenster „Identitätsanbieter" **SAML**aus.
4. Beim Importieren von Identity Provider-Metadaten haben Sie folgende Möglichkeiten:
   - ◦ **URL**: App-Verbund-Metadaten-URL zum automatischen Ausfüllen der Details auf der Konfigurationsseite des Identitätsanbieters.
   - ◦ **Import**: Importieren Sie die XML-Datei, um die Details auf der Konfigurationsseite des Identitätsanbieters zu importieren.
5. Klicken Sie mit der rechten Maustaste oben auf dem Bildschirm, klicken Sie auf **sys_id kopieren**und verwenden Sie diesen Wert für die **Sign-on-URL** im Abschnitt **Grundlegende SAML-Konfiguration**.
6. Füllen Sie die Felder des Formulars aus.

Single Sign-on-Felder für mehrere Provider

Eigenschaft	Erforderlich	Beschreibung
Name	Ja	Name für den IdP Dieser IdP ist die Sys-ID für die automatische Umleitung.
Aktiv	Ja	„Aktiv" muss für den IdP, der für die Authentifizierung verwendet werden soll, auf „wahr" festgelegt werden. **Hinweis:** Die Option zum Festlegen dieser Eigenschaft ist nur nach einer erfolgreichen Testverbindung verfügbar.

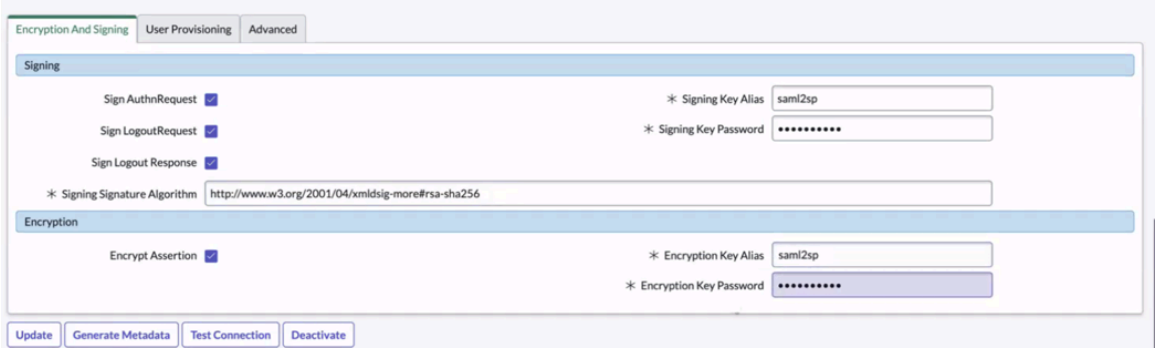
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Erforderlich	Beschreibung
Standard	Nein	Der IdP mit automatischer Weiterleitung (früher als primärer IdP bezeichnet) leitet Benutzer automatisch zum Zugriff auf die Basisinstanz-URL um. Diese Eigenschaft legt diese IdP-Konfiguration als Standard fest.
Automatische IdP-Weiterleitung	Nein	IdP-Konfiguration, die Sie als automatische IdP-Weiterleitung festlegen können. **Hinweis:** Wenn Sie eine neue IdP-Konfiguration für die automatische Weiterleitung aktivieren, wird das Cookie *glide_sso_id* mit dem neuen IdP für die automatische Weiterleitung aktualisiert. Die Systemeigenschaft *glide.authenticate.sso.update.idp.cookie*, die automatisch aktiviert ist, steuert diese Funktion.
URL des Identitätsanbieters	Ja	URL zu Ihrem IdP. Jede IdP-URL muss eindeutig sein.
AuthnRequest des Identitätsanbieters	Ja	URL zur HTTP-Redirect-Bindung, die vom SingleSignOnService-Element abgerufen wird.
SingleLogoutRequest des Identitätsanbieters	Nein	URL, die vom SingleLogoutService-Element abgerufen wird.
ServiceNow Homepage	Ja	URL, einschließlich Anmeldeseite, der Instanz, für die sich der IdP authentifiziert. Beispiel: https://IhreInstanz.service-now.com/navpage.do
Entitäts-ID/Aussteller	Ja	Basis-URL, ohne die Anmeldeseite der Instanz, für die sich der IdP authentifiziert. Beispiel: https://IhreInstanz.service-now.com/
Zielgruppen-URI	Ja	Basis-URL, ohne die Anmeldeseite der Instanz, für die sich der IdP authentifiziert. Beispiel: https://IhreInstanz.service-now.com/
NameID-Richtlinie	Ja	Wert des NameIDFormat-Elements, das die Integration verwendet.
Weiterleitung für externe Abmeldung	Nein	URL, an die die Integration Anwender nach der Abmeldung weiterleitet.
Fehlerhafte Anforderungsumleitung	Nein	URL für die Umleitung fehlgeschlagener Authentifizierungsanforderungen. Standardmäßig ist dies der URL-Endpunkt einer im IdP konfigurierten Fehlerseite oder Abmeldeseite. Sie können diesen Wert im Feld glide.authenticate.failed_requirement_redirect ausfüllen.

7. Wahlweise: Registerkarte „Verschlüsselung und Signierung“.

Hinweis: Verwenden Sie Ihre eigenen Zertifikate für die Verschlüsselung und Signatur.

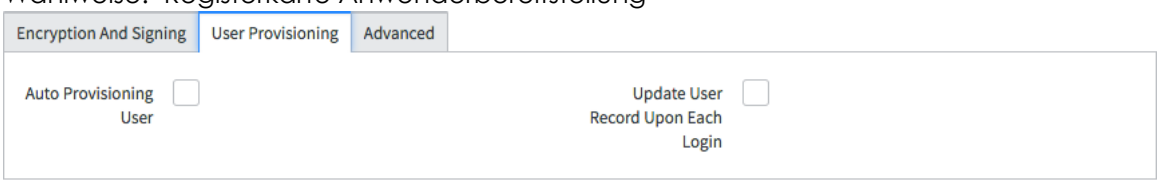
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Verschlüsselungs- und Signaturfelder

Eigenschaft	Beschreibung
Alias zum Signieren/für Verschlüsselungsschlüssel	Alias des im SAML 2.0 SP-Schlüsselspeicher gespeicherten Schlüsseleintrags.
Signaturschlüssel-Passwort	Passwort des im SAML 2.0 SP-Schlüsselspeicher gespeicherten Schlüsseleintrags.
Assertion verschlüsseln	Aktivieren Sie die Checkbox, um die Assertion in der SAML-Antwort zu verschlüsseln. In den für den IdP generierten Metadaten ist das x509-Zertifikat eingebettet, das der IdP zum Verschlüsseln der Assertion in der von ihm generierten SAML-Antwort verwendet.
Signaturalgorithmus für Signieren	URL, die auf den AuthnRequest-Verbraucher des SAML 2.0-Identitätsanbieters für die eSignature-Authentifizierung verweist.
AuthnRequest signieren	Aktivieren Sie die Checkbox, damit der IdP-Single-Sign-on-Service eine signierte AuthnRequest empfängt.
LogoutRequest signieren	Aktivieren Sie die Checkbox, damit der IdP-Single-Sign-on-Service eine signierte LogoutRequest empfängt.

8. Wahlweise: Registerkarte Anwenderbereitstellung

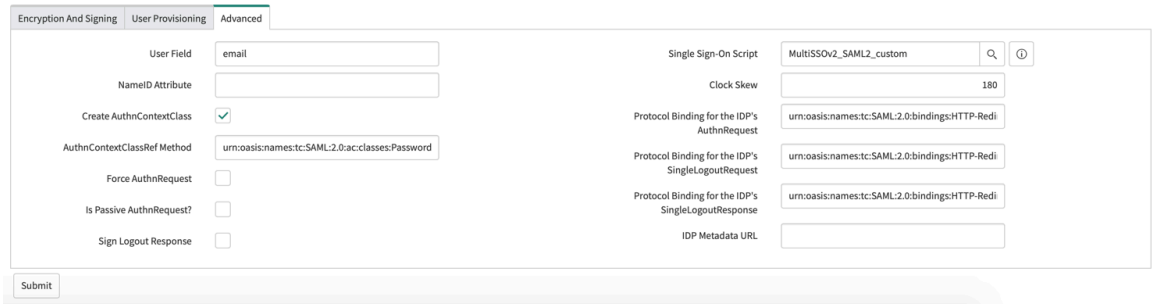


Felder für die Anwenderbereitstellung

Eigenschaft	Beschreibung
Automatische Bereitstellung von Anwender	Bei der automatischen Anwenderbereitstellung werden die Anwender basierend auf den vom IdP bereitgestellten Informationen erstellt, wenn der Anwender in der Instanzanwendertabelle nicht vorhanden ist.
Anwenderdatensatz bei jeder Anmeldung aktualisiere	Jedes Mal, wenn sich der Anwender mit SAML anmeldet, werden die Anwenderinformationen in der Instanzanwendertabelle mit den Informationen im IdP aktualisiert.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Wahlweise: Registerkarte „Erweitert“



Erweiterte Felder

Eigenschaft	Beschreibung
Anwenderfeld	Feld in der Benutzertabelle, das den Wert enthält, den der IdP zum Identifizieren des Benutzers benötigt. Diese eindeutige ID ist Teil der Antwort. Zum Beispiel ein Anwendername, eine Mitarbeiter-ID usw. In der Sys-Benutzertabelle wird diese eindeutige ID mit den Benutzerdetails abgeglichen.
Attribut NameID	Feld, das Sie leer lassen, es sei denn, Sie konfigurieren eine neue NameID-Richtlinie. Wenn Sie eine neue Richtlinie konfigurieren, benötigt das System die Benutzertabelle, die es verwenden muss, um den Benutzer zu identifizieren, der sich anmeldet. Das System gleicht das NameID-Token mit dem Namen des betreffenden Benutzertabellenfelds ab.
AuthnContextClass erstellen	Aktivieren Sie die Checkbox, um eine bestimmte Kontextklasse anzugeben, wie z. B. Passwortgeschützter Transport. Wenn das Kontrollkästchen deaktiviert ist, wählt der IdP die am besten geeignete Kontextklasse aus.
AuthnContextClassRef-Methode	URN des Anmeldemechanismus, den der IdP zur Authentifizierung von Anwendern verwenden soll.
AuthnRequest erzwingen	Aktivieren Sie die Checkbox, um das Auftreten von AuthnRequests zu erzwingen.
Ist passive AuthnRequest	Checkbox, wenn AuthnRequest passiv ist.
Single Sign-on-Skript	Single Sign-on-Skript. Der Standardwert ist *MultiSSOV2_SAML2_custom*.
Abmeldeantwort signieren	Details zur Abmeldeantwort in diesem Feld.
Taktversatz	Anzahl der Sekunden zwischen den beiden Attributen, aus denen die SAML-Antwort-Nonce besteht. Der Standardwert ist 60. Eine gültige SAML-Antwort muss zwischen den Datums-/Zeit-Werten von „*notBefore*“ und „*notOnOrAfter*“ liegen. Eine Beispiel-SAML-Antwortnachricht finden Sie unter Beispiel-SAML-2-Antwort mit den Elementen SubjectConfirmation und SubjectConfirmationData sowie Beispiel-SAML-2-Antwort mit den Elementen AudienceRestrictions und Audience.
Protokollbindung für „SingleLogoutReuqest“ des IdP	Einer der unterstützten Werte, die im Bindungsattribut des SingleLogoutService-Elements aufgeführt sind.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
Metadaten-URL, aus der IDP-Eigenschaften importiert werden	Von dieser URL werden IdP-Eigenschaften importiert. Wenn festgelegt, wird der automatische Import des SAML-Zertifikats vom IdP aktiviert, wenn das vorherige Zertifikat abgelaufen ist. **Hinweis:** Wenn Sie ein Upgrade von SAML2 Update 1 auf Multi-Provider-SSO durchführen oder Ihre SSO-Verbindung manuell einrichten, wird die URL für die IdP-Metadaten nicht automatisch ausgefüllt.
Anforderung	Eindeutige ID als Teil der Anforderung. Die ID kann ein Anwendername, eine Mitarbeiter-ID usw. sein. **Hinweis:** Sowohl die Weiterleitung als auch die Nachbindung werden für die Anforderung unterstützt. Die Option zum Festlegen dieses Felds wird nur nach einer erfolgreichen Testverbindung angezeigt. Weitere Informationen finden Sie unter IdP-Verbindungen werden getestet.
Antwort	Eindeutige ID als Teil der Antwort. Die ID kann ein Anwendername, eine Mitarbeiter-ID usw. sein. **Hinweis:** Sowohl die Umleitung als auch die Nachbindung werden für die Antwort unterstützt. Die Option zum Festlegen dieses Felds wird nur nach einer erfolgreichen Testverbindung angezeigt. Weitere Informationen finden Sie unter IdP-Verbindungen werden getestet.

10. Wählen Sie **Verbindung testen** in der oberen rechten Ecke der Seite.
11. Geben Sie Ihre Anmeldeinformationen ein.
    Die Ergebnisse des SSO-Logouttests werden angezeigt.
12. Wählen Sie **Aktivieren** aus, um die Konfiguration zu aktivieren.

E-Mail-Links mit externer Authentifizierung

Sie können E-Mail-Links verwenden, wenn Sie die externe Authentifizierung mit Digest-Token verwenden. Sie müssen jedoch festlegen, wie Links in E-Mail-Benachrichtigungen behandelt werden sollen.

Die Standardlinks enthalten eine URL, die Sie zu einem bestimmten Ort in der Instanz wie einem Incident oder einer Change-Anforderung leitet, ohne SSO-Anmeldeinformationen zu integrieren. Nachfolgend finden Sie Beispiele dafür, wie Sie den Benutzer an den Speicherort in der Instanz leiten, ohne sich auf der Anmeldeseite der Instanz anzumelden.

- Unverschlüsselte HTTP-Technik zum Herstellen einer Verbindung mit der /demo-Instanz (navigiert nicht zu einem bestimmten Datensatz):

```
https://<instance
 name>.service-now.com/?SM_USER=user_name&DE_USER=lQjIVp7aRJtyPx5+2O/vg
U24tbE=
```

- Link (in einer E-Mail-Benachrichtigung) zu einem bestimmten Datensatz, damit der Benutzer zuerst zum Anmeldeportal des Unternehmens wechselt:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
https://login.company_portal_page.com/nav_to.do?uri=incident.do?sys_id=
009f8eda0a0a0b2b01ab4eb094223466%26sysparm_stack=incident_list.do%3Fsys
parm_query=active=true
```

Sie müssen die Eigenschaft *glide.email.override.url* in Ihrer Instanz so festlegen, dass sie die URL der Unternehmensportalseite enthält. Wenn diese Eigenschaft nicht vorhanden ist, können Sie sie erstellen.

- Das Unternehmensportal muss dann diese URL verwenden und die Umleitungs-URL an die Instanz erstellen, wobei das Segment beibehalten wird, das für den Zugriff auf den spezifischen Datensatz erforderlich ist, und die SSO-Anmeldeinformationen am Ende der URL hinzuzufügen:

```
https://<instance
 name>.service-now.com/nav_to.do?uri=incident.do?sys_id=009f8eda0a0a0b2
b01ab4eb094223466%26sysparm_stack=incident_list.do%3Fsysparm_query=acti
ve=true&SM_USER=user_name&DE_USER=lQjIVp7aRJtyPx5+2O/vgU24tbE=
```

Fügen Sie E-Signatur-Unterstützung für SAML hinzu

Konfigurieren Sie die folgenden Eigenschaften für die E-Signatur mit Security Assertion Markup Language (SAML) 2.0 Update 1.

Wenn die E-Signatur mit Multi-SSO aktiv ist, werden die SAML-Eigenschaften nicht verwendet. Das System fügt der Tabelle „SAML2 Update1-Eigenschaften“ [saml2_update1_properties] Eigenschaften für die E-Signatur hinzu:

Eigenschaft	Beschreibung	Standard
Assertionen-Verbraucher-Index für eSignatur-Authentifizierung	Eine Indexnummer, die den Endpunkt identifiziert.	1
Assertionen-Verbraucher-URL für eSignatur-Authentifizierung	Die URL, die den Verbraucher identifiziert	`https://Ihre-instanz.service-now.com/consumer.do`
AuthnRequest-URL für eSignature-Authentifizierung	Die URL für die Authentifizierung	Keine

Wenn Sie die E-Signatur mit SAML 1.0 oder SAML 2.0 (ohne Update 1) verwenden, lesen Sie die speziellen Konfigurationsanweisungen: E-Signatur für Mehrfachanbieter-SSO.

Hinweis: Wenn Sie ein Life-Science-Kunde sind, der E-Signatur verwendet, deaktivieren Sie die Business-Regel zur Verhinderung der Selbstsperre des Anwenders.

Migrieren einer vorhandenen SAML 1.1-Integration zu SAML 2.0

Wenden Sie sich an den Kundensupport, um von einer SAML 1.1-Integration zu einer SAML 2.0-Integration zu migrieren.

Aktualisieren Sie Ihre vorhandene SAML 2.0-Integration

Aktualisieren Sie Ihre vorhandene SAML 2.0-Integration.

Vorbereitungen

Erforderliche Rolle: admin

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Fordern Sie das SAML 2.0 Update 1-Plugin an. Wenden Sie sich an Kundenservice und Support, um das *Sicherheitsverbesserungs-Plugin „SAML 2.0 Single Sign-On - Update 1: “* anzufordern. Das Plugin wendet aktualisierte Versionen des *SAML2SingleSign*- Installations-Exits (Anmeldeskript), des *SAML2Logout*- Installations-Exits (Abmeldeskript) und der *SAML2-Skripteinbindung* (Skriptobjekt) an.

Führen Sie Anpassungen aus vorhandenen Installations-Exit-Skripts in neuen Skripts zusammen. Das Update speichert eine inaktive Kopie der ursprünglichen Installations-Exit-Skripts der Integration. Sie können diese Kopien verwenden, um alle Anpassungen, die Sie an den An- und Abmeldeskripts vorgenommen haben, mit den neuen Versionen dieser Installations-Exits zusammenzuführen.

Führt Anpassungen aus vorhandenen Installationsendskripts in neue Skripts zusammen

Name des ursprünglichen Installations-Exit-Skripts	Ursprünglicher Skriptstatus	Name des neuen Installations-Endskripts	Neuer Skriptstatus
SAML2SingleSign	Inaktiv	SAML2SingleSign_Update1	Aktiv
SAML2	Inaktiv	SAML2_Update1	Aktiv
SAML2Logout	Inaktiv	SAML2Logout_update1	Aktiv

Sie können zu den SAML 2.0-Anmelde- und Abmeldeskripts navigieren, indem Sie die folgenden Pfade verwenden, um die Installation zu beenden:

- **SAML 2 Single Sign-on** > **Anmeldeskript**an.
- **SAML 2 Single Sign-on** > **Abmeldeskript**an.
- **Systemdefinition** > **Installationsausgänge**an.

Sie können über die folgenden Pfade zur Skripteinbindung SAML 2.0 Update 1 navigieren:

- **SAML 2 Single Sign-on** > **Skriptobjekt**an.
- **Systemdefinition** > **Skripteinbindungen**an.

Testen Sie das Update.

Prozedur

1. Fügen Sie eine Systemeigenschaft namens `glide.authenticate.sso.saml2.debug` mit dem Wert *true*hinzu.
2. Versuchen Sie, sich bei SAML 2.0 anzumelden.
3. Überprüfen Sie das Systemprotokoll.
   SAML2-Validierungsfehler beginnen mit dem Text *SAML2ValidationError*.
4. Typische Anmeldefehler erkennen und beheben
   Weitere Informationen finden Sie unter Fehler und Korrekturen für Multi-SSO (SAML 2.0)..

Beispiel für SAML 2-Antworten nach dem Update

Die folgenden Abschnitte veranschaulichen die neuen erforderlichen Elemente und Attribute, die der IdP in der SAML-Antwort bereitstellen muss.

Beispiel für SAML 2-Antwort mit Ausstellerelement

In der folgenden SAML 2-Antwort wird das Element *Aussteller* verwendet.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
<samlp:Responsexmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  Destination="https://demoi2.service-now.com/navpage.do"
  ID="s28da6774c88ae1eab292bf25fe625db81919d8e1e"
 InResponseTo="SNC841720c227c81948cfd68cadcad235c6"
 IssueInstant="2012-01-30T20:07:10Z"  Version="2.0"><saml:Issuer
 xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">http://
idp.ssocircle.com</saml:Issuer>
   ...
   <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
     ID="s2f347f973c063836cf70ea38302d94976f9c5b851"
     IssueInstant="2012-01-30T20:07:10Z"
 Version="2.0"><saml:Issuer>http://idp.ssocircle.com</saml:Issuer>
      ...
   </saml:Assertion></samlp:Response>
```

SAML 2-Beispielantwort mit den Elementen SubjectConfirmation und SubjectConfirmationData

In der folgenden SAML 2-Antwort werden die Elemente *SubjectConfirmation* und *SubjectConfirmationData* mit den Attributen *NotOnOrAfter* und *Recipient* verwendet.

```
<saml:SubjectConfirmationMethod="urn:oasis:names:tc:SAML:2.0:cm:bearer"><
saml:SubjectConfirmationData
 InResponseTo="SNC841720c227c81948cfd68cadcad235c6"
     NotOnOrAfter="2012-01-30T20:17:10Z"
 Recipient="https://
demoi2.service-now.com/navpage.do"/></saml:SubjectConfirmation>
```

SAML 2-Beispielantwort mit den Elementen AudienceRestrictions und Audience

In der folgenden SAML 2-Antwort werden die Elemente *AudienceRestrictions* und *Auditence* mit den Attributen *NotBefore* und *NotOnOrAfter verwendet*.

```
<saml:ConditionsNotBefore="2012-01-30T19:57:10Z"
 NotOnOrAfter="2012-01-30T20:17:10Z"><saml:AudienceRestriction><saml:Audi
ence>https://
demoi2.service-now.com</saml:Audience></saml:AudienceRestriction></saml:C
onditions>
```

SAML-Benutzerbereitstellung

Wenn in Ihrem IdP Benutzer vorhanden sind, in Ihrer Instanz jedoch nicht, kann die SAML-Benutzerbereitstellung automatisch Benutzer in der Benutzertabelle [sys_user] Ihrer Instanz erstellen.

Die SAML-Anwenderbereitstellung wird für SAML 2.0 Update 1 unterstützt, wenn Multi-SSO aktiviert ist.

Funktionsweise der SAML-Benutzerbereitstellung

Wenn die SAML-Anwenderbereitstellung aktiviert ist und das System auf einen neuen Anwender trifft, der sich nicht in der Instanz befindet, erstellt die Instanz automatisch einen Datensatz in einer temporären Tabelle mit dem Namen `u_imp_saml_user_`.<suffix> , wobei ist ein automatisch generierter Textbezeichner. Das System erstellt auch eine Transformationszuordnung, die die Datenbeziehungen zwischen der Importtabelle und der Benutzertabelle angibt. Jeder im System identifizierte IdP in hat eine eigene Transformationszuordnung. Die Transformationszuordnung wird für jeden IdP einmal erstellt. Administratoren können sie nach Bedarf aktualisieren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn sich der Benutzer anmeldet, greift er auf einen IdP zu, um sich anzumelden.

- Das System zeigt eine Liste aller IdPs an, die die SAML-Benutzerbereitstellung verwenden können. Wenn nur ein IdP die SAML-Benutzerbereitstellung verwenden kann, wird dieser automatisch verwendet.
- Wenn keine der obigen Bedingungen zutrifft, verwendet das System die automatische IdP-Weiterleitung.

Verwalten Sie die SAML-Benutzerbereitstellung

Aktualisieren Sie die Tabelle „User“ mit den Anwendern in Ihrem IdP, indem Sie zuerst die Feldzuordnung einrichten und dann die Anwenderbereitstellung über die Multi-SSO-IdP-Einstellungen aktivieren.

Vorbereitungen

Richten Sie Ihre IdP-Zuordnung ein, um zu ermitteln, welche Felder im IdP den richtigen Feldern in der Benutzertabelle zugeordnet sind.

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Eigenschaften**an.
2. Wählen Sie „Aktivieren Sie das **automatische Importieren von Anwendern von allen Identitätsanbietern in die Anwendertabelle** “ (*glide.authenticate.multisso.user.autoprovision*), um diese Funktion zu aktivieren.
3. Klicken Sie auf **Speichern**.
4. Navigieren zu **Mehrfachanbieter-SSO** > **Identity Provider**an.
5. Öffnen Sie den Identitätsanbieter-Datensatz, den Sie verwenden möchten.
6. Erstellen Sie einen Datensatz in der Benutzertabelle, wenn der Benutzer noch nicht vorhanden ist, indem Sie **Benutzer automatisch bereitstellen**auswählen.
   Wenn Sie ein Upgrade auf diesen Release durchgeführt haben, müssen Sie das Formular konfigurieren und dieses Feld hinzufügen.
7. Aktivieren Sie die Aktualisierung von Anwenderdatensätzen, wenn sich Anwender beim IdP anmelden und die Informationen auf dem IdP mit den Informationen in der Anwendertabelle veraltet sind, indem Sie **Anwenderdatensatz bei jeder**Anmeldung aktualisieren auswählen.
   Wenn Sie ein Upgrade auf diesen Release durchgeführt haben, müssen Sie das Formular konfigurieren und dieses Feld hinzufügen.
8. Klicken Sie auf **Transformationszuordnung für Anwenderbereitstellung**, um die vom System automatisch erstellte Zuordnung anzuzeigen.
9. Nehmen Sie bei Bedarf Änderungen an der Zuordnung vor.

Ergebnisse

Wenn die ersten unbekannten Benutzer versuchen, sich anzumelden, erstellt das System die Felder in der Importsatztabelle aus der Datei metadata.xml.

Hinweis: Sie können die Felder erst aus der IdP-Tabelle zuordnen, wenn sich der erste Anwender anmeldet.

SAML 2.0-Problembehandlung

Bevor Sie sich an den Support wenden, versuchen Sie es mit den Problembehandlungslösungen, die in der Knowledge Base unter Hi verfügbar sind.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Die Instanz unterstützt keine Lösungen, die von externen Sites bereitgestellt werden.

Lesen Sie den folgenden Knowledge Base-Artikel: KB0540617 „„SAML-Fehlermatrix“ .

Andere häufige Probleme

Fehler oder Symptom	Lösung
Fehlermeldung: „ist keine Funktion.“ Dieses Problem kann in einer Umgebung mit mehreren Knoten auftreten. Wenn das Plugin nicht auf allen Knoten aktiviert wird, wird ein Fehler wie der folgende angezeigt: org.mozilla.javascript.EcmaFehler: *`[JavaPackage org.opensaml.saml2.core.impl.AuthnRequestBuilder]`* ist keine Funktion.	Dieser Fehler tritt auf, da das Plugin nicht aktiv war und die JAR-Datei nicht geladen wurde. Daher scheint der Code zu fehlen. Wenden Sie sich an den technischen Support, um Knoten neu zu starten, auf denen das Plugin fehlt.
SAML authentifiziert keine Benutzer, die auf CMS-Seiten zugreifen.	Standardmäßig sind CMS-Seiten öffentlich und erfordern daher keine Authentifizierung. Wenn Sie möchten, dass SAML CMS-Seiten authentifiziert, ändern Sie die öffentliche Seite *view_content.do* von *active=true* in *active=false*.
Ein Anwender kann nach der SAML-Authentifizierung nicht zurück zu einer CMS-Seite umgeleitet werden.	Standardmäßig verwendet die SSO-Integration einen URL-Parameter namens *URI*, um zu steuern, wohin der Benutzer nach der Authentifizierung beim IdP geleitet wird. SSO ignoriert relative URLs. Beispielsweise kann SSO Benutzer nicht zu einer relativen */ess-* URL umleiten. Stattdessen muss der Benutzer zu einer URL wie */nav_to.do?uri=/ess navigieren*, die Deep Linking-Syntax verwendet. Dadurch wird jedoch das MSS-Portal in den IFrame des Hauptnavigationsinhalts eingefügt. Mit anderen Worten: Die Site nimmt nicht die gesamte Seite ein, sondern wird als Seite in Ihrer Instanz geladen. Weitere Informationen finden Sie unter CMS-Sites und Single Sign-on.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Andere häufige Probleme (Fortsetzung)

Fehler oder Symptom	Lösung
	Wenn Sie die CMS-Einstiegsseite so ändern, dass sie privat ist, indem *Sie view_content.do* auf *active=false*festlegen, erfordert das Deep-Linking-Verhalten eine Anpassung des Anmeldeskripts für den Installationsausgang. Erstellen Sie ein Skript, das nach dem *URI* -Teil der URL sucht und einen *RelayState*-URL-Parameter erstellt, der den relativen URL-Pfad enthält, um Anwender nach der Authentifizierung beim IdP umzuleiten.
SAML leitet Benutzer nach der Authentifizierung nicht auf die entsprechende Seite weiter.	Bestimmt, ob der Relaisstatus an den IdP übergeben und dann während der Authentifizierung zurückgegeben wird. Sie können dies mit einem Browser tun, der HTTP-Anforderungsheader und POST-Informationen speichern kann, z. B. Chrome mit seinen integrierten Entwicklertools oder Firefox mit dem Add-on HTTPfox. Verwenden Sie für Internet Explorer eine Drittparteianwendung wie z. B. „Fledger“. Das Ziel besteht darin, zu beobachten, wie die Anforderungen vom Client (Browser) an die Instanz und vom Client an den IdP übergeben werden.

Überwachen Sie die Ereigniswarteschlange auf Anmeldeaktivitäten

Jede Single Sign-on-Integration erstellt Ereignisse für Anmeldeaktivitäten.

Sie können diese Ereignisse verwenden, um auf Anmeldefehler zu überwachen und festzustellen, ob Sicherheitsbedenken bestehen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überwachen der Ereigniswarteschlange auf Anmeldefehler

Ereignisname	Beschreibung	Datensatz	Parameter 1	Parameter 2
external.authentication.succeeded	Die externe Authentifizierung war erfolgreich, und der Anwender hat auf die Instanz-URL zugegriffen.	Sitzungs-ID	Anwender-ID des Anwenders, der sich erfolgreich angemeldet hat	Die URL, auf die der An zugegriffen hat (kann e Link sein)
external.authentication.failed	Die Single Sign-on-Anforderungen sind nicht vorhanden oder fehlen.		Sitzungs-ID	Die fehlenden Authentifizierungsanfor
external.authentication.failed	Der Benutzer ist in der Benutzertabelle `[sys_user]` nicht vorhanden		Anwender-ID	Die Zeichenfolge „Benu nicht vorhanden“
external.authentication.failed	Der Anwender ist ausgesperrt.		Anwender-ID	Die Zeichenfolge „Anw ausgesperrt.

Anmeldeereignisse in Ereigniswarteschlangen

Die SAML 2.0-Integration erstellt Ereignisse für Anmeldeaktivitäten.

Sie können diese Ereignisse verwenden, um auf Anmeldefehler zu überwachen und festzustellen, ob Sicherheitsbedenken bestehen.

Anmeldeaktivitäts-Ereignisse

Ereignisname	Beschreibung	Mit dem Ereignis verwendete ID	Ereigniszeichenfolge
saml2.logout.validierung.fehlgeschlagen	Die Abmeldeantwort vom IdP konnte anhand Ihrer Abmeldeanforderung nicht validiert werden. Das Ereignis validiert die<inResponseTo> Element gegen die Sitzungs-ID (ID-Attribut des<saml2p:LogoutRequest> Element). Beispiel: Workflow für Abmeldeanforderung ausgegeben.	Sitzungs-ID	Die Zeichenfolge „Va der SAML2 LogoutRes fehlgeschlagen.“
extern.Authentifizierung.erfolgreich	Externe Authentifizierung erfolgreich.		Die Zeichenfolge „Authentifizierung erf

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anmeldeaktivitäts-Ereignisse (Fortsetzung)

Ereignisname	Beschreibung	Mit dem Ereignis verwendete ID	Ereigniszeichenfolge
extern.Authentifizierung.erfolgreich	Die externe Authentifizierung war erfolgreich, und der Anwender hat auf die Instanz-URL zugegriffen.	Sitzungs-ID und Anwender-ID des Anwenders, der sich erfolgreich angemeldet hat	Die URL, auf die der A zugegriffen hat (kann Link sein)
extern.Authentifizierung.fehlgeschlagen	Die Single Sign-on-Anforderungen sind nicht vorhanden oder fehlen.	Sitzungs-ID	Die fehlenden Authentifizierungsanf
extern.Authentifizierung.fehlgeschlagen	Der Benutzer ist in der Benutzertabelle [sys_user] nicht vorhanden.	Anwender-ID	Die Zeichenfolge „Be nicht vorhanden“
extern.Authentifizierung.fehlgeschlagen	Der Anwender ist ausgesperrt.	Anwender-ID	Die Zeichenfolge „An ausgesperrt“

Eingehende und ausgehende OAuth-Authentifizierung

Die OAuth-basierte Authentifizierung validiert die Identität des Clients, der versucht, mithilfe eines Authentifizierungsprotokolls eine Vertrauensstellung im System herzustellen.

OAuth 2.0 (Offene Autorisierung) ist das Branchenstandardprotokoll für die Autorisierung, das die Client-Entwicklerfreundlichkeit berücksichtigt und gleichzeitig spezifische Autorisierungs-Flows für Webanwendungen, Desktopanwendungen und Mobilgeräte bereitstellt.

Es handelt sich um einen Standard, mit dem eine Website oder Anwendung im Namen eines Benutzers auf Ressourcen zugreifen kann, die von anderen Web-Apps gehostet werden.

Anstatt die Anmeldeinformationen des Ressourcenbenutzers für den Zugriff auf geschützte Ressourcen zu verwenden, erhält der Client ein Zugriffstoken. Zugriffstoken werden mit Genehmigung des Benutzers an Drittpartei-Clients ausgegeben. Der Client verwendet dann das Zugriffstoken, um auf die geschützten Ressourcen zuzugreifen.

Eingang

Erstellen Sie einen Endpunkt für externe Clients, die auf Ihre Instanz zugreifen möchten. Dadurch werden ein OAuth-Client-Anwendungsdatensatz sowie eine Client-ID und ein Clientgeheimnis generiert, die der Client für den Zugriff auf die eingeschränkten Ressourcen in der Instanz benötigt. Weitere Informationen finden Sie unter OAuth Eingehend.

Ausgehend

Verwenden Sie einen OAuth-Drittpartei-Anbieter, der die Autorisierung für den Zugriff auf Ihre Instanz bereitstellt. Geben Sie ein OAuth-Profil und einen OAuth-Bereich an, wenn Sie eine Verbindung zu einem anderen OAuth-Anbieter herstellen. Weitere Informationen finden Sie unter OAuth ausgehend.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OAuth 2.0

Mit OAuth 2.0 können Anwender über externe Clients auf Instanzressourcen zugreifen, indem sie ein Token abrufen, anstatt bei jeder Ressourcenanforderung Anmeldeinformationen einzugeben.

Sie müssen über die Rolle security_admin verfügen, um die OAuth-Integration zu verwalten. Konfigurieren Sie OAuth 2.0 für die folgenden Szenarien:

- **Szenario mit externem OAuth-Client** (eingehend): Ihre Instanz von bietet einen Endpunkt für Drittanbieter-Clients, um Daten aus der Instanz abzurufen.
- **OAuth-Provider-Szenario** (ausgehend): Ihre -Instanz ruft Daten von einem Drittanbieter ab.

Hinweis: Sie müssen sich zum ersten Mal als Anwender authentifizieren, um den Token-Post abzurufen. Sie müssen sich nicht vor Ablauf des Tokens mit einem Anwenderaccount authentifizieren.

Sowohl einfache Sicherheits-Frameworks als auch Hochsicherheits-Frameworks unterstützen OAuth 2.0. Hochsicherheit wird empfohlen. Unter finden Sie Informationen dazu, für welche Versionen bereits hohe Sicherheit aktiviert ist und wie Sie die hohe Sicherheit aktivieren.

Schlüsselkonzepte der OAuth 2.0-Implementierung

Konzept	Beschreibung
Ressourcenbesitzer	Eine Entität, die Zugriff auf eine geschützte Ressource gewähren kann. Ein Ressourcenbesitzer, der eine Person ist, wird als Endanwenderbezeichnet. Der Besitzer der Ressource ist immer ein Benutzeraccount.
Client	Eine Anwendung, die mit der Autorisierung des Ressourcenbesitzers im Namen des Ressourcenbesitzers Anforderungen für geschützte Ressourcen stellt.
Ressourcenserver	Der Server, der die geschützten Ressourcen hostet und Anforderungen für geschützte Ressourcen annehmen und beantworten kann.
Autorisierungsserver	Der Server, der Zugriffstoken an den Client ausgibt, nachdem der Ressourcenbesitzer erfolgreich authentifiziert und die Autorisierung erhalten wurde.
Autorisierungsanforderung	Die Berechtigung, die ein Client für den Zugriff auf eine geschützte Ressource benötigt. Die Autorisierungsanforderung ist immer eine HTTP POST-Nachricht, die die ID des Clients enthält, der im Namen des Ressourcenbesitzers handelt, und Anmeldeinformationen, die die Anforderung autorisieren.
Autorisierungserteilung	Anmeldeinformationen, die die Autorisierung des Ressourcenbesitzers zum Zugriff auf eine Ressource darstellen. Bei der Autorisierungsgewährung handelt es sich entweder um Anmeldeinformationen oder um ein Aktualisierungstoken.
Zugriffs-Token	Eine sichere Zeichenfolge, die ein Client für den Zugriff auf geschützte Ressourcen verwendet. Eine Instanz gibt Zugriffstoken an Clients aus, die über eine gültige Autorisierung verfügen. Jedes Zugriffstoken hat einen bestimmten Umfang, eine bestimmte Lebensdauer und andere Attribute.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konzept	Beschreibung
	Standardmäßig gibt eine Instanz Zugriffstoken mit einer Lebensdauer von 30 Minuten aus, wenn die Instanz der OAuth-Anbieter ist. Für Drittpartei-Token 30 Tage.
Token neu laden	Anmeldeinformationen, mit denen ein Client neue Zugriffstoken erhält, ohne dass eine zusätzliche Benutzerautorisierung erforderlich ist. Eine Instanz gibt ein Aktualisierungstoken an einen Client aus, wenn sie zum ersten Mal autorisiert wird, über ein Zugriffstoken zu verfügen. Standardmäßig gibt eine Instanz Aktualisierungstoken mit einer Lebensdauer von 100 Tagen aus, wenn die Instanz der OAuth-Anbieter ist. Für Drittpartei-Token: 365 Tage.
Selbstsignierte Zertifikate	Now Platform unterstützt keine selbstsignierten Zertifikate. Der OAuth-Client verwendet nicht den Zertifikat-Trust-Store und lässt auch keine Verbindung mit OAuth-Endpunkten zu, die ein selbstsigniertes Zertifikat enthalten.
Anwenderagent	Der Benutzer, der Zugriffsrechte an eine Client-Anwendung delegiert, häufig eine Website. Die Zugriffsrechte ermöglichen der Client-Anwendung oder der Website den Zugriff auf Daten in der Instanz, für die der Benutzer über Zugriffsrechte verfügt. Der Benutzeragent wird im Szenario verwendet.

OAuth-Gewährungstypen

Mit einem Gewährungstyp erhält der Client das Zugriffstoken. Die folgenden Förderungstypen werden unterstützt:

- **Autorisierungscode**: Der Verbraucher erhält zuerst einen Autorisierungscode und verwendet ihn dann, um ein Zugriffstoken zu erhalten. Sie können ein OAuth-Profil angeben und diesen Gewährungstyp angeben. Der Prozess, der den Autorisierungscode verwendet, wird auch als Autorisierungscode- Flow oder Autorisierungscode-Flow bezeichnet.
- **Passwort-Anmeldeinformationen**des Ressourcenbesitzers: Der Verbraucher der Ressource verfügt bereits über die Anmeldeinformationen, um das Zugriffstoken zu erhalten. Dieser Prozess wird auch als Passwort-Flowbezeichnet.
- **Client-Anmeldeinformationen**: Der Verbraucher der Ressource verwendet die Client-ID und den geheimen Clientschlüssel, die bereits in der Anwendungsregistrierung konfiguriert sind.

Speicherung von Anmeldeinformationen für die Authentifizierung

Der OAuth-Clientschlüssel wird als Feld vom Typ *password2* gespeichert, das mit KMF verschlüsselt ist. Anwenderpasswörter, die zur Überprüfung eingehender Endpunktanforderungen verwendet werden, werden als Hash-Wert in der Tabelle „Anwender“ im Typfeld *password* (SHA 256) gespeichert. Weitere Informationen zu dieser Verschlüsselung finden Sie unter Password2-Verschlüsselung mit KMF

Richten Sie OAuth ein

Richten Sie OAuth ein, und aktivieren Sie es, aktivieren Sie die Systemeigenschaft OAuth, erstellen Sie einen OAuth-Anwendungsendpunkt, damit externe Client-Anwendungen auf die Instanz zugreifen können, und legen Sie OAuth-Parameter fest.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Stellen Sie sicher, dass das OAuth-Plugin aktiv ist und die OAuth-Aktivierungseigenschaft auf „wahr“ festgelegt ist.
2. Erstellen Sie mit einer der folgenden Methoden eine OAuth-Anwendungsregistrierung:
   - Erstellen Sie einen Endpunkt für externe Clients, die auf Ihre Instanz zugreifen möchten. Dadurch werden ein **OAuth-Client-Anwendungsdatensatz** sowie eine Client-ID und ein Clientgeheimnis generiert, die der Client für den Zugriff auf die eingeschränkten Ressourcen in der Instanz benötigt.
   - Verwenden Sie einen OAuth-Drittpartei-Anbieter , der die Autorisierung für den Zugriff auf Ihre Instanz bereitstellt.

     Geben Sie ein OAuth-Profil und einen OAuth-Bereich an, wenn Sie eine Verbindung zu einem anderen OAuth-Provider herstellen.
3. Konfigurieren Sie Ihre Client-Anwendungen so, dass ein HTTP POST erstellt wird, der ein OAuth-Token anfordert.
   Die Anwendung muss auch in der Lage sein, die JSON-Antwort zu analysieren, um das zurückgegebene Zugriffs- und Aktualisierungstoken zu verwenden.

Aktivieren Sie OAuth

Standardmäßig ist das Plugin **„OAuth 2.0“ (com.snc.platform.security.oauth)** bei neuen und aktualisierten Instanzen aktiv. Wenn das Plugin in Ihrer Instanz nicht aktiv ist, können Sie es aktivieren.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie das Plugin über die Filterkriterien und die Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: `Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.`

   Nach Abschluss der Installation wird eine Meldung angezeigt.

Legen Sie die OAuth-Eigenschaft fest

Zum Generieren von OAuth 2.0-Token für registrierte Anwendungen muss die Eigenschaft `com.snc.platform.security.oauth.is.active` für die Instanz aktiv sein.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Um OAuth 2.0 zu verwenden, geben Sie im **Filternavigator** des Arbeitsbereichs sys_properties.list ein, und klicken Sie auf **Neu**.
2. Füllen Sie das Formular mit den folgenden Einstellungen aus:

   - **Name**: com.snc.platform.security.oauth.is.active
   - **Typ**: true | false
   - **Wert**: true

Ändern Sie den OAuth-Passwortparameter

Verwenden Sie diese Eigenschaft, um sicherzustellen, dass nur POST-Textparameter als Eingabe für alle unterstützten Gewährungstypen akzeptiert werden.

Das Senden vertraulicher Informationen über URI-Abfrageparameter kann dazu führen, dass Clients, der Server oder andere Hosts zwischen den Anforderungen vertrauliche Informationen offenlegen. Ab dem Madrid-Release stellt diese neue Eigenschaft sicher, dass nur die POST-Textparameter als Eingabe für alle unterstützten Gewährungstypen akzeptiert werden. Folgende Gewährungstypen werden unterstützt:

- Autorisierungscode
- Kennwort
- Client-Anmeldeinformationen
- Aktualisieren Sie das Token

OAuth-Passwortparametereigenschaft

Eigenschaft	Beschreibung
`glide.oauth.allow.parameters.in.post.body.only`	Diese Eigenschaft ist nur für zBoots als Teil des OAuth 2.0-Plugins auf „true“ festgelegt. Wenn Sie diese Einstellung für Ihre Instanz benötigen, erstellen Sie die Eigenschaft und legen Sie sie auf „true“ fest.

OAuth Eingehend

OAuth inbound stellt einen Endpunkt für Drittanbieter-Clients bereit, um Daten aus der Instanz abzurufen.

Sie müssen über die Rolle `security_admin` verfügen, um die OAuth-Integration zu verwalten.

Sie können die Integration des **externen OAuth-Client-Szenarios** (Eingehend) konfigurieren, wenn Ihre Instanz einen Endpunkt für Drittanbieter-Clients bereitstellen soll, um Daten aus der Instanz abzurufen.

Hinweis: Sie müssen sich zum ersten Mal als Anwender authentifizieren, um den Token-Post abzurufen. Sie müssen sich nicht vor Ablauf des Tokens mit einem Anwenderaccount authentifizieren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können die eingehende OAuth-Konfiguration abhängig vom folgenden Gewährungstyp durchführen:

- **Autorisierungscode-Gewährungs-Flow**: Für einen vom Anwender initiierten Gewährungs-Flow, bei dem der Anwender ohne Eingabe eines Anwendernamens oder Passworts, jedoch über das Zugriffstoken eine autorisierte URL für die Authentifizierung konfigurieren kann. Weitere Informationen finden Sie unter Flow zur Gewährung des OAuth-Autorisierungscodes.
- Flow zur**Passwortgewährung**: Für einen vom Anwender initiierten Gewährungs-Flow, bei dem eine Anwenderinteraktion zur Authentifizierung erforderlich ist. Weitere Informationen hierzu finden Sie unter Flow-Konfiguration für die Passwortgewährung.

  Hinweis: Für den Autorisierungscode-Flow muss der Anwender die Authentifizierung durch lokale Anmeldung, SSO oder MFA abschließen und dann seine Einwilligung erteilen.

- **JWT-Bearer-Gewährungs-Flow**: Für eine System-zu-System-Integration, bei der kein Benutzereingriff erforderlich ist. Weitere Informationen finden Sie unter Flow-Konfiguration für JWT-Bearer-Gewährung.
- **ID-Token-Flow**: Für die Verwendung eines ID-Tokens, das von OIDC-Drittanbietern wie Okta oder Azure ausgestellt wurde. Weitere Informationen hierzu finden Sie unter ID-Token-Flow für Authentifizierung.
- **Implizite OAuth-Gewährungen**: Um zuzulassen, dass das Zugriffstoken direkt über den Benutzeragenten an die Client-Anwendung übergeben wird, normalerweise einen Webbrowser oder ein Mobilgerät. Weitere Informationen finden Sie unter Implizite OAuth-Gewährungen.
- **Client-Anmeldeinformationen**: Für die Verwendung des Gewährungstyps für OAuth-Client-Anmeldeinformationen für eingehende Integrationen von einem OAuth-Client einer Drittpartei zur Plattform ServiceNow®. Weitere Informationen finden Sie unter Client-Anmeldeinformationen.

OAuth-Bereiche

Sie können den Umfang der Unterstützung des OAuth-Authentifizierungsbereichs für die REST API festlegen. Der OAuth-Bereich bietet nur Zugriff auf die jeweiligen REST APIs. Weitere Informationen finden Sie unter REST-API-Authentifizierungsbereich.

Flow zur Gewährung des OAuth-Autorisierungscodes

Der Autorisierungscode-Gewährungs-Flow ermöglicht es einem Anwender, auf eine Ressource zuzugreifen, indem er sich direkt bei einem OAuth-Server authentifiziert, der der Ressource vertraut, anstatt sich mit Anwendernamen/Passwort-Anmeldeinformationen zu authentifizieren.

Diese Implementierung des OAuth-Autorisierungscode-Flows ermöglicht den Zugriff auf eine Ressource über REST. Das Autorisierungscode-Framework ruft das Zugriffstoken über die autorisierte URL ab, die der Anwender konfiguriert, anstatt dass der Anwender einen Anwendernamen/ein Passwort eingeben muss. Anwendername/Passwort werden niemals für den Client verfügbar gemacht, der Zugriff auf die Ressource anfordert.

Eine Instanz ServiceNow als Autorisierungsserver

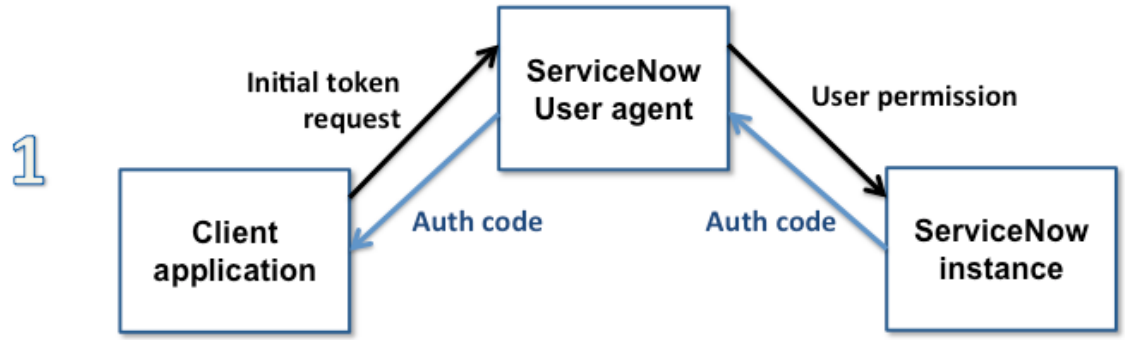
Der OAuth-Server ist normalerweise ein Autorisierungsserver einer Drittpartei. Sie können auch eine Instanz ServiceNow als Autorisierungsserver angeben, der die Token für den Autorisierungscode-Flow ausstellt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Benutzer, der die eingeschränkte Ressource besitzt, muss den Zugriff autorisieren. Der Benutzer kann das ausgestellte Zugriffstoken auch jederzeit widerrufen, um den Zugriff zu beenden.

Flow-Prozess zur Erteilung des Autorisierungscodes

Der Flow-Prozess zur Erteilung des Autorisierungscodes besteht aus den folgenden drei Schritten:



Im ersten Schritt initiiert die Client-Anwendung oder Website in einem REST-API-Aufruf über den -Benutzeragenten eine GET-Anforderung an die Instanz. Normalerweise wird der REST-Aufruf initiiert, wenn der Endanwender auf eine Schaltfläche oder einen Link in der Client-Anwendung oder auf der Website klickt, um ein Zugriffstoken anzufordern. In der Clientanwendung muss der Endanwender auch die Autorisierungs-URL, Token-URL, Client-ID und den geheimen Clientschlüssel angeben. Eine Erklärung dieser Elemente finden Sie in den Feldbeschreibungen in diesem Thema: OAuth-Drittpartei-Anbieter verwenden . Wenn der Client nach einem Erteilungstyp fragt, muss der Endanwender **Autorisierungscode**auswählen.

Beispiel für eine GET-Anforderung von der Client-Anwendung an die Instanz:

```
https://myinstance.service-now.com/oauth_auth.do?response_type=code&redir
ect_uri={the_redirect_url}&client_id={the_client_identifier}
```

Hinweis: Zur Verwendung des standardmäßigen OAuth-Flows zur **Codegewährung** muss für „ressource_type“ „ **Code** “ angegeben werden.

Der Endanwender muss manuell Zugriff auf die eingeschränkte Ressource in der Instanz gewähren. Bei der Implementierung von ServiceNow muss der Endanwender bei der -Instanz angemeldet sein. Die Instanz fordert den Endanwender mit einer UI-Seite auf, die über die Schaltflächen **Zulassen** und **Ablehnen** verfügt.

Das Element, von dem die Client-Anwendung das Token tatsächlich anfordert, ist der von Ihnen erstellte OAuth-Anbieter-Anwendungsregistrierungsdatensatz. Dieser wird auch als Autorisierungsendpunkt bezeichnet (siehe OAuth-Drittpartei verwenden). Der Autorisierungscode wird vom Autorisierungsendpunkt an den Client gesendet. Sie wird nicht direkt an den Client weitergeleitet, sondern an die **Umleitungs-URL**, die Sie im Formular „Autorisierungsendpunkt“ angeben. Diese URL wird auch als Rückruf-URL bezeichnet. Sie können diese URL von der Client-Anwendung oder von der Website von abrufen.

Beispielantwort von der -Instanz an die Client-Anwendung, die einen Autorisierungscode bereitstellt:

```
https/http://{callbackURL}?code={the actual auth code}
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Nachdem die Client-Anwendung nun über den Autorisierungscode verfügt, fordert der Client mit dem Code das Zugriffstoken an. Der Autorisierungscode bestätigt, dass der Anwender in Schritt 1 zugestimmt hat.

Beispiel für eine POST-Anforderung von der Client-Anwendung an die Instanz ServiceNow, die den Authentifizierungscode bereitstellt und das Zugriffstoken anfordert:

```
https://myinstance.service-now.com/oauth_token.do?grant_type=authorizatio
n_code&code={the auth
 code}&redirect_uri={the_same_redirect_url}&client_id={the_same_client_id
entifier}&client_secret={client_secret_value}
```

Der Endpunkt in der Instanz gibt ein Zugriffstoken und ein Aktualisierungstoken zurück. Mit dem Aktualisierungstoken können zusätzliche Zugriffstoken angefordert werden.

Sie können die Token in der Instanz verwalten und auch das Token widerrufen. Siehe OAuth-Token verwalten.



Die Client-Anwendung authentifiziert sich mit dem Zugriffstoken bei der REST-API. Nach dem Authentifizieren der Client-Anwendung gibt die REST API die angeforderten Daten in einer JSON-Nutzlast zurück.

Beispiel für eine GET-Anforderung für die JSON-Nutzlast von Daten für die Incident-Tabelle [incident]:

```
https://myinstance.service-now.com/api/now/table/incident?access_token={t
he_token}
```

Hinweis: Das System unterstützt auch implizite OAuth-Erteilungen , auch bekannt als impliziter Gewährungscode-Flow.

Integrationsunterstützung

Der Autorisierungscode-Flow unterstützt die folgenden Integrationen in der Instanz:

- Multi-SSO
- SAML 2.0 Update 1
- Multifaktor-Authentifizierung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die mobile Schnittstelle wird ebenfalls unterstützt.

Autorisieren Sie den Zugriff auf einen OAuth-Endpunkt mit dem Authentifizierungscode-Flow

Endanwender, die eine geschützte Ressource in der Instanz ServiceNow besitzen, müssen den Zugriff auf die Ressource autorisieren, bevor die Instanz das Zugriffstoken bereitstellen kann.

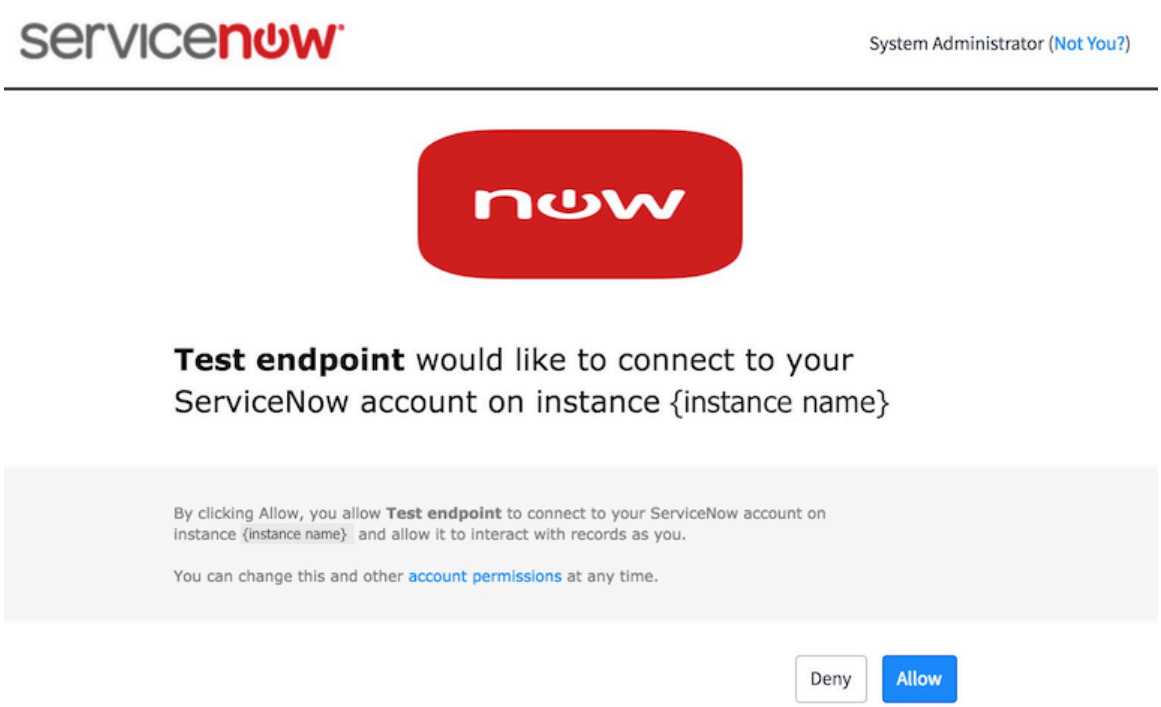
Vorbereitungen

Erforderliche Rolle: keine Sie müssen bereits bei der Instanz angemeldet sein, die die geschützte Ressource enthält. Alternativ können Sie sich mit der Authentifizierungsmethode (z. B. Multifaktor-Authentifizierung oder SAML) anmelden, die Ihr ServiceNow -Administrator bereits eingerichtet hat.

Prozedur

1. Klicken Sie auf den Link oder die Schaltfläche in der Client-Anwendung, in der Sie den Zugriff auf die geschützte Ressource in der -Instanz anfordern.
   Dadurch wird die Tokenanforderung gestartet. Wenn Sie einen REST-Aufruf von einer Instanz zu einer anderen tätigen, finden Sie hier den Link **OAuth-Token** abrufen im Formular „REST-Nachricht“.
2. Wenn Sie nicht angemeldet sind, melden Sie sich jetzt an.
   Wenn Sie nicht mit dem in der oberen rechten Ecke angegebenen Benutzer identisch sind, klicken Sie auf **Nicht Sie?** und melden Sie sich an.
3. Klicken Sie auf Accountberechtigungen, um die Liste der Zugriffstoken zu öffnen, die Sie bereits ausgegeben haben.
   Dieses entspricht dem **Self-Service** > **Meine verbunden** Liste der Apps-Token.
4. Klicken **Sie** auf Zulassen, um den Zugriff zuzulassen und den Autorisierungscode (bei Verwendung des Authentifizierungscode-Flows) oder das Zugriffstoken (bei Verwendung des impliziten Gewährungstyps) von der Instanz ausgeben zu lassen.

   Wenn Sie auf **Ablehnen klicken**, wird die Autorisierung nicht zugelassen, Sie werden jedoch nicht von der Instanz abgemeldet.



Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Es sollte eine Meldung angezeigt werden, die den Zugriff bestätigt. Wenn Sie den Zugriff über das REST-Nachrichtenformular in einer Instanz anfordern, wird die folgende Meldung oben im Formular angezeigt: OAuth-Aktualisierungstoken ist verfügbar und läuft am {Datum} ab.

Flow-Statusparameteranforderung für Autorisierungscode

Mit der Systemeigenschaft „glide.oauth.state.parameter.required“ kann der Parameter „State“ in einer OAuth-Anforderung für den Autorisierungscode-Flow erforderlich sein.

Statusparameter

Erforderliche Rolle: keine

Ab dem Madrid-Release fügt die Systemeigenschaft *glide.oauth.state.parameter.required* einen State-Parameter für eine OAuth-Anforderung hinzu. Für zbooted-Instanzen ist die Eigenschaft wahr. Bei aktualisierten Instanzen ist die Eigenschaft nicht vorhanden, daher ist der Parameter „Status“ nicht aktiviert. Der State-Parameter ist ein Zeichenfolgenwert und darf keine Sonderzeichen enthalten. Der Statusparameter darf nicht leer oder „ “ sein.

Statusparameter wird validiert

Erstellen Sie einen Endpunkt, damit Clients auf die Instanz zugreifen können. Initiieren Sie einen Autorisierungscode-Flow für eine oauth_auth.do. Beispiel:

```
http://myinstance.service-now.com/oauth_auth.do?grant_type=authorization_
code&client_id=e9dba45b380d1300e676ccc91cef468f&response_type=code
```

Wenn Sie den Statusparameter in der Anforderung nicht angeben, erhalten Sie einen Fehler, und der Autorisierungscode wird nicht zurückgegeben.`Fehlender Statusparameter in Anforderung.`

Hinzufügen des State-Parameters zur Anforderung:

```
http://myinstance.service-now.com/oauth_auth.do?grant_type=authorization_
code&client_id=e9dba45b380d1300e676ccc91cef468f&response_type=code&state=
123
```

Durch Hinzufügen des Parameters State werden Sie zum Anmeldebildschirm weitergeleitet, und der reguläre Autorisierungscode-Flow gibt den Autorisierungscode zurück.

Hinweis: Die Antwort-URL enthält den in der Anforderung übergebenen Statusparameter. Im Beispiel lautet der hinzugefügte Parameter `state=123`.

Wenn der Autorisierungscode-Flow von oauth_initiator.do ausgeht:

```
http://myinstance.service-now.com/oauth_initiator.do?oauth_requestor_cont
ext=sys_rest_message&oauth_requestor=eab8341fec0d1300964f214a2c2fcf67&oau
th_provider_profile=dfa8f01fec0d1300964f214a2c2fcf51&response_type=code
```

Der Parameter State wird bei der Umleitung durch oauth_auth.do automatisch hinzugefügt.

```
http://myinstance.service-now.com/oauth_auth.do?response_type=code&state=
-790938844&redirect_uri=http://10.11.95.5:16001/oauth_redirect.do&client_
id=e9dba45b380d1300e676ccc91cef468f
```

Beispiel für den Autorisierungscode-Flow: Instanz ServiceNow als Autorisierungsserver

Sie können eine -Instanz als Autorisierungsserver verwenden, um einem Client mithilfe des Autorisierungscode-Flows Token auszustellen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: keine

In diesem Beispiel werden zwei Instanzen verwendet: eine als Autorisierungsserver und eine andere als Client. Eine Instanz verwendet einen REST-Aufruf, um Token von einer anderen Instanz anzufordern.

Sie müssen in beiden Instanzen Aktivieren Sie OAuth sein.

Prozedur

1. Navigieren Sie auf der Instanz des Autorisierungsservers (mit Istanbul-Release oder höher) zu **System-OAuth** > **Applikationsregistrierung** und klicken Sie dann auf **Neu**.
2. Klicken **Sie auf OAuth-API-Endpunkt für externe Clients erstellen**.
3. Füllen Sie die Formularfelder für den OAuth-Anwendungsdatensatz wie in Erstellen Sie einen Endpunkt, damit Clients auf die Instanz zugreifen könnenbeschrieben aus.
   Durch das Ausführen dieser Schritte wird ein Autorisierungsserver eingerichtet. Führen Sie die nächsten Schritte aus, um den Client-Server einzurichten.
4. Navigieren Sie auf der Client-Instanz zu **System-OAuth** > **Applikationsregistrierung** und klicken Sie dann auf **Neu**.
5. Klicken Sie **auf Mit einem OAuth-Drittpartei-Provider verbinden**.
6. Füllen Sie die Formularfelder für den OAuth-Anwendungsdatensatz wie in beschrieben aus. Beachten Sie die folgenden Feldwerte:
   - **Name**: Ein eindeutiger Name, der die Anwendung identifiziert, für die Sie OAuth-Zugriff benötigen.
   - **Client-ID**: Client-ID des Anwendungsregistrierungsdatensatzes, den Sie für den Autorisierungsserver erstellt haben.
   - **Geheimer Clientschlüssel**: [Schreibgeschützt] Die automatisch generierte eindeutige ID der Anwendung. Die Instanz verwendet die Client-ID, wenn ein Zugriffstoken angefordert wird.
   - **Standard-Gewährungstyp**: Wählen Sie **den Autorisierungscode aus**.
   - **Autorisierungs-URL**: URL der Instanz, die der Autorisierungsserver ist. Denken Sie daran, `„oauth_auth.do“` am Ende der URL anzuhängen.
   - **Logo-URL**: Die URL, die ein Bild enthält, das als Anwendungslogo verwendet werden soll. Das Logo wird auf der Genehmigungsseite angezeigt, wenn der Benutzer eine Anforderung erhält, einer Client-Anwendung Zugriff auf eine eingeschränkte Ressource in der Instanz zu gewähren.
   - **Token-URL**: URL der Instanz, die der Autorisierungsserver ist. Denken Sie daran, `„oauth_token.do“` am Ende der URL anzuhängen.
   - **Umleitungs-URL**: URL der Instanz: die Client-Server-Instanz. Denken Sie daran, `„oauth_redirect.do“` am Ende der URL anzuhängen.
7. Erstellen Sie ein Profil für den Datensatz mit dem Erteilungstyp „ **Autorisierungscode** “.
   Der Client-Server ist eingerichtet. Sie können jetzt eine ausgehende REST-Nachricht erstellen und ein OAuth-Token abrufen.

Erstellen Sie einen Endpunkt, damit Clients auf die Instanz zugreifen können

Erstellen Sie einen OAuth-Anwendungsendpunkt, damit externe Client-Anwendungen auf die Instanz ServiceNow zugreifen können.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **System-OAuth** > **Applikationsregistrierung** und klicken Sie dann auf **Neu**.
2. Klicken Sie auf der Interceptor-Seite auf **OAuth-API-Endpunkt für externe Clients erstellen**, und füllen Sie das Formular aus.

Feld	Beschreibung
Name	Ein eindeutiger Name, der die Anwendung identifiziert, für die Sie OAuth-Zugriff benötigen.
Client-ID	[Schreibgeschützt] Die automatisch generierte eindeutige ID der Anwendung. Die Instanz verwendet die Client-ID, wenn ein Zugriffstoken angefordert wird.
Geheimer Clientschlüssel	[Pflichtfeld] Die gemeinsame geheime Zeichenfolge, die sowohl die Instanz als auch die Clientanwendung oder die Website verwenden, um die Kommunikation miteinander zu autorisieren. Die Instanz verwendet den geheimen Clientschlüssel, wenn sie ein Zugriffstoken anfordert. Lassen Sie dieses Feld leer, damit die Instanz automatisch einen geheimen Clientschlüssel generiert. Um vorhandene geheime Clientschlüssel anzuzeigen, klicken Sie auf das Sperrsymbol.
Umleitungs-URL	Die Rückruf-URL, an die der Autorisierungsserver umleitet. Geben Sie die vollständigen URLs der Clients ein, die Zugriff auf die Ressource anfordern, und `fügen Sie /oauth_redirect.do`an. Beispiel: `http://token_consumer:port/oauth_redirect.do`. Geben Sie so viele URLs wie erforderlich für alle möglichen Token-Verbraucher ein. Die Instanz gleicht die URL der eingehenden Anforderung mit einer der Umleitungs-URLs ab. Wenn keine Übereinstimmung vorliegt, verwendet die Instanz die erste Umleitungs-URL.
Logo-URL	Die URL, die ein Bild enthält, das als Anwendungslogo verwendet werden soll. Das Logo wird auf der Genehmigungsseite angezeigt, wenn der Benutzer eine Anforderung erhält, einer Client-Anwendung Zugriff auf eine eingeschränkte Ressource in der Instanz zu gewähren.
Aktiv	Aktivieren Sie das Kontrollkästchen, um die Anwendungsregistrierung zu aktivieren.
Lebensdauer von Aktualisierungstoken	Die Anzahl an Sekunden, die ein Aktualisierungstoken gültig ist. Die Instanz verwendet den Lebensdauerwert, wenn sie ein Aktualisierungstoken anfordert. Standardmäßig laufen Aktualisierungstoken in 100 Tagen (8640000 Sekunden) ab.
Tokenbeschränkungen erzwingen	Wählen Sie diese Option aus, um nur die Verwendung von Token mit APIs zuzulassen, die das Authentifizierungsprofil zulassen. Sie können den Gewährungszugriff mithilfe einer API-Zugriffsrichtlinie festlegen. Weitere Informationen finden Sie unter REST-API-Zugriffsrichtlinie erstellen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Standard: Nicht ausgewählt.
Mobile-Client	Stellt die Entität für die mobile App oder das Web dar. Diese Informationen werden verwendet, um die Anmeldeinformationen mit Mobile oder Web zu analysieren.
Lebensdauer von Zugriffstoken	Die Anzahl an Sekunden, die ein Zugriffstoken gültig ist. Die Instanz verwendet den Lebensdauerwert, wenn sie ein Zugriffstoken anfordert. Standardmäßig laufen Zugriffstoken in 30 Minuten (1800 Sekunden) ab.
Kommentare	Die der Anwendung zuzuordnenden Informationen.
Clienttyp	Wählen Sie den Clienttyp basierend auf dem Typ Ihres Clients aus. Optionen: ◦ **iFrame – eingebettet** ◦ **Integration als Anwender** ◦ **Integration als Service** Weitere Informationen finden Sie unter Konfigurieren Sie den Clienttyp für OAuth- und SSO-Datensätze.

3. Klicken Sie auf **Absenden**.

Ergebnisse

Das System erstellt in der Tabelle „Anwendungsregistrierungen“ [oauth_entity] einen Datensatz vom Typ „OAuth-Client“. Wenn die Instanz tatsächlich Token und Autorisierungscodes ausgibt, werden diese in der Tabelle gespeichert. Weitere Informationen finden Sie unter OAuth-Token verwalten.

OAuth-API-Antwortparameter

Die OAuth 2.0-API erzeugt eine JSON-Antwort, die die folgenden Parameter als Name:Wert-Paare enthält.

Antwortparameter für Zugriffstoken

Antwortparameter	Beschreibung
scope	Vom Zugriffstoken gewährter Zugriff. Der Bereich ist immer **useraccount**, was bedeutet, dass das Zugriffstoken dieselben Rechte hat wie das Benutzerkonto, das das Token autorisiert hat. Wenn Abel Tuter beispielsweise eine Anwendung durch die Bereitstellung von Anmeldeinformationen autorisiert, gewährt das resultierende Zugriffstoken dem Tokenträger dieselben Zugriffsrechte wie Abel Tuter.
token_type	Typ des von der Anforderung ausgegebenen Tokens gemäß Definition in OAuth-RFC. Der Tokentyp ist immer **Bearer**, was bedeutet, dass jeder, der im Besitz des Zugriffstokens ist, auf eine geschützte Ressource zugreifen kann, ohne einen kryptografischen Schlüssel anzugeben. Unter RFC 6750 finden Sie weitere Informationen darüber, wie OAuth 2.0 Bearer-Token verwendet.
läuft ab_in	Lebensdauer des Zugriffstokens in Sekunden.
Aktualisierung_Token	Zeichenfolgenwert des Aktualisierungstokens.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortparameter für Zugriffstoken (Fortsetzung)

Antwortparameter	Beschreibung
access_token	Zeichenfolgenwert des Zugriffstokens. Zugriffsanforderungen, die innerhalb der Ablaufzeit des Zugriffstokens gestellt werden, geben immer das aktuelle Zugriffstoken zurück.
format	[Optional] Ausgabeformat der Antwort. Dieser Wert ist immer JSON.

Hinweis: Wenn ein OAuth-Anbieter den Antworttext als „Inhaltstyp“ anstelle von „Inhaltstyp“ sendet, analysiert der OAuth-HTTP-Client die Antwort möglicherweise nicht richtig. Um dieses Problem zu beheben, erstellen Sie eine Systemeigenschaft mit diesen Parametern.

Feld	Wert
Name	glide.oauth.inhouse.httpclient.enabled
Typ	Wahr | Falsch
Wert	falsch

Weitere Informationen zum Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen

Das folgende Beispiel veranschaulicht die JSON-Zeichenfolge, die von der Anforderung eines Zugriffstokens zurückgegeben wird. (Leerzeichen wurden hinzugefügt, um die Lesbarkeit zu verbessern).

```
{"scope":"useraccount","token_type":"Bearer","expires_in":1800,
"refresh_token":"w599voG89897rGVDmdp12WA681r9E5948c1CJTPi8g4HGc4NWaz62k6k
1K0FMxHW40H8yOO3Hoe",
"access_token":"F0jh9korTyzd9kaZqZ0SzjKZuS3ut0i4P46Lc52m2JYHiLIcqzFAumpyx
shU9mMQ13gJHtxD2fy"}
```

OAuth-API-Anforderungsparameter

Erfahren Sie mehr über die OAuth-API-Anforderungsparameter, die von Zugriffstoken-Anforderungen verwendet werden.

Hinweis: Der Inhaltstyp der OAuth-API muss „ *`application/x-www-form-urlencoded`" sein*. Der Inhaltstyp „ *`application/json`* “ führt zu einem nicht angegebenen Fehler.

Anforderungsparameter für Zugriffstoken

Anforderungsparameter	Beschreibung
„grant_type“	[Pflichtfeld] Der Typ der Anmeldeinformationen, die die Anforderung eines Zugriffstokens autorisieren. Dieser Parameter muss einen der folgenden Werte aufweisen:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anforderungsparameter für Zugriffstoken (Fortsetzung)

Anforderungsparameter	Beschreibung
	• **Passwort**: Ein Satz von Anwenderanmeldeinformationen zum Autorisieren der Anforderung eines Zugriffstokens. Geben Sie die Anmeldeinformationen des Anwenders in den Parametern Anwendername und Passwort an. • **refresh_token**: Ein vorhandenes Aktualisierungstoken autorisiert die Zugriffstokenanforderung. Geben Sie das Aktualisierungstoken im Parameter „refresh_token“ an.
client_id	[Erforderlich] Automatisch generierte eindeutige ID der Client-Anwendung, die das Zugriffstoken anfordert.
client_secret	[Erforderlich] Gemeinsame geheime Zeichenfolge, die die Instanz und die OAuth-Anwendung verwenden, um die Kommunikation miteinander zu autorisieren.
username	Name des Anwenderaccounts, der die Anforderung des Zugriffstokens autorisiert. Dieser Parameter ist für Zugriffs-Token-Anforderungen mit einem **commit_type-Wert** vom Typ **password**erforderlich.
Kennwort	Passwort für den Anwenderaccount, der die Anforderung des Zugriffstokens autorisiert. Dieser Parameter ist für Zugriffs-Token-Anforderungen mit einem **commit_type-Wert** vom Typ **password**erforderlich.
Aktualisierung_Token	Vorhandenes Aktualisierungstoken, das die Anforderung des Zugriffstokens autorisiert. Dieser Parameter ist für Zugriffs-Token-Anforderungen mit **einemgrant_type** von **refresh_token erforderlich**.

Anforderungen, die Anwenderanmeldeinformationen verwenden

Die Instanz erfordert, dass Clients Anmeldeinformationen bereitstellen, wenn Sie den Client zum ersten Mal autorisieren oder wenn Sie die Erstellung eines neuen Aktualisierungstokens autorisieren. Diese Art von Anforderung gibt immer zwei Token zurück:

- Ein Zugriffstoken
- Ein Aktualisierungstoken

Die Instanz verifiziert, dass der Benutzer aktiv und derzeit nicht ausgesperrt ist und über eine interaktive Sitzung verfügt. Wenn eine dieser Bedingungen „false“ ist, erzeugt die Instanz kein Zugriffstoken. Zugriffsanforderungen, die innerhalb der Ablaufzeit des Zugriffstokens gestellt werden, geben immer das aktuelle Zugriffstoken zurück.

Hinweis: Diese Art der Autorisierungsgewährung basiert auf TLS-Verschlüsselung, um die Anmeldeinformationen der Benutzer während der Übertragung zu schützen.

Das folgende Beispiel veranschaulicht das Anfordern eines Zugriffstokens mit einem Satz von Anwenderanmeldeinformationen (Bereiche wurden hinzugefügt, um die Lesbarkeit zu verbessern).

```
$ curl -d"grant_type=password&client_id=be3aeb583ace210011c15b24a43e25d8
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
&client_secret=client_password
&username=admin&password=admin"
https://instancename.service-now.com/oauth_token.do
```

Anforderungen mit Aktualisierungstoken

Die Instanz kann ein vorhandenes Aktualisierungstoken verwenden, um ein neues Zugriffstoken zu erstellen. Diese Art von Anforderung gibt nur ein Zugriffstoken zurück. Die Instanz bestätigt, dass das Aktualisierungstoken nicht abgelaufen ist, bevor ein neues Zugriffstoken generiert wird. Zugriffsanforderungen, die innerhalb der Ablaufzeit des Aktualisierungstokens gestellt werden, geben immer das aktuelle Aktualisierungstoken zurück. Die Übertragung von Aktualisierungstoken ist im Allgemeinen sicherer als die Übertragung von Benutzeranmeldeinformationen. Das folgende Beispiel veranschaulicht das Anfordern eines Zugriffstokens mit einem vorhandenen Aktualisierungstoken (Leerzeichen wurden hinzugefügt, um die Lesbarkeit zu verbessern).

```
$ curl
 -d"grant_type=refresh_token&client_id=be3aeb583ace210011c15b24a43e25d8
&client_secret=client_password
&refresh_token=w599voG89897rGVDmdp12WA681r9E5948c1CJTPi8g4HGc4NWaz62k6k1K
0FMxHW40H8yOO3Hoe"
https://instancename.service-now.com/oauth_token.do
```

Einen OAuth-JWT-API-Endpunkt für externe Clients erstellen (Maschine-zu-Maschine-Integration)

Mit dem OAuth-JWT-Bearer-Token können sich die Client-Webanwendungen nahtlos bei Ihrer Instanz mithilfe des eingehenden JWT-Gewährungstyps authentifizieren, anstatt dass sich der Endanwender manuell anmelden oder das Passwort teilen muss.

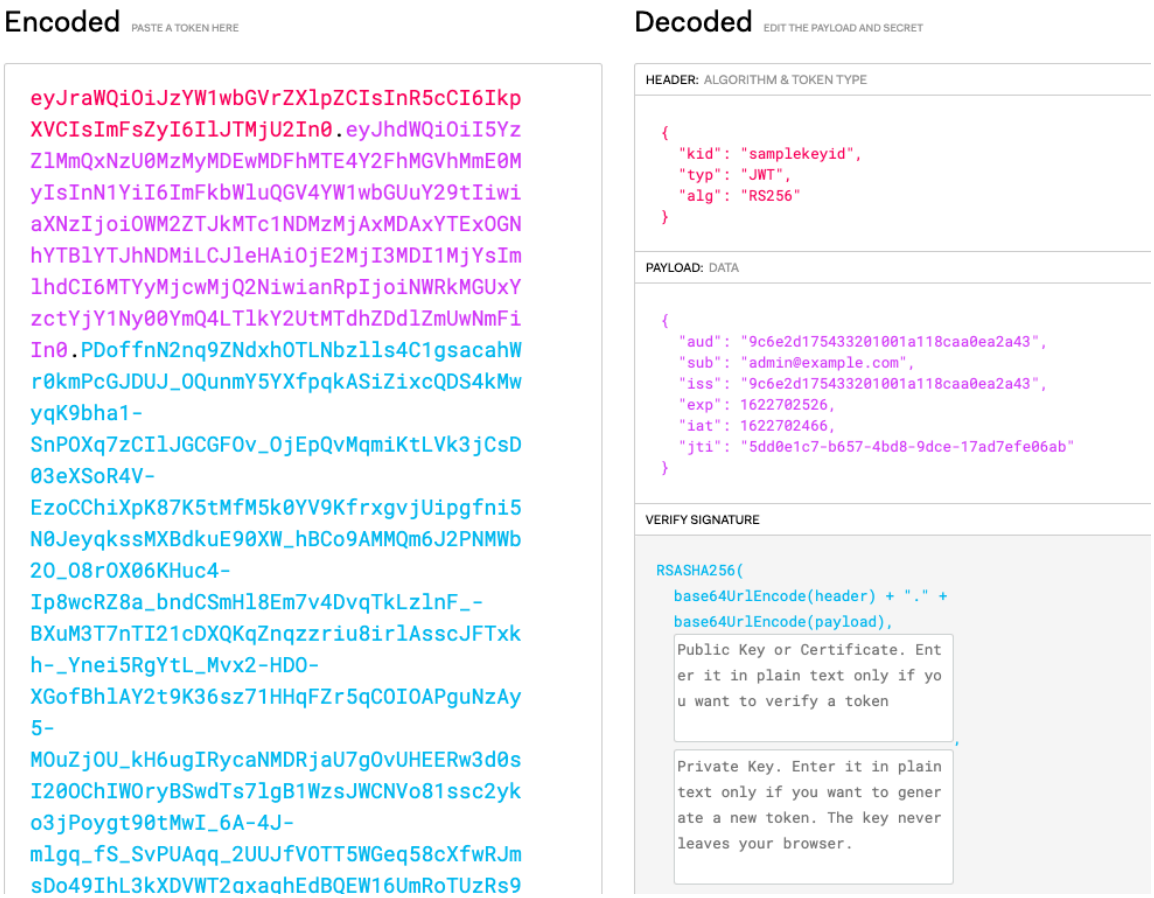
Bevor Sie beginnen

Generieren Sie ein JSON-Web-Token (JWT) mit den folgenden Ansprüchen auf Client-Seite:

- `aud`: Muss mit dem Wert der Client-ID übereinstimmen.
- `sub`: Muss ein Anwenderbezeichner sein, z. B. die E-Mail-Adresse des Anwenders, dem Sie das Token zuordnen möchten.
- `iss`: Empfohlene Übereinstimmung mit dem Wert der Client-ID. Wenn `aud` und `iss` nicht übereinstimmen, fügen Sie den Wert `iss` in der Anspruchsvalidierung hinzu.
- `exp`: Beliebiger Ablauf.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für das decodierte JSON-Web-Token



Konfiguration in ServiceNow

Warum und wann dieser Vorgang ausgeführt wird

Da bei Verwendung des Erteilungstyps JWT das Passwort nicht in der Anforderung enthalten ist, erhöht dies die Sicherheit zwischen Webservices. Sie können beispielsweise eine externe Anwendung entwickeln und Token verwenden, um eingehende Anforderungen an Ihre Instanz ServiceNow zu authentifizieren.

Erforderliche Rolle: admin

Weitere Informationen zu JSON-Web-Token finden Sie unter https://jwt.io/ .

Prozedur

1. Fügen Sie den öffentlichen Schlüssel der Client-App der Tabelle **„sys_certificate“ hinzu**.
2. Richten Sie die -Konfiguration in Ihrer -Instanz ServiceNow ein, um das eingehende JWT zu überprüfen.

   a. Navigieren zu **System-OAuth** > **Applikationsregistrierung**an.

   b. Wählen **Sie Einen OAuth-JWT-API-Endpunkt für externe Clients erstellen aus**.

   c. Füllen Sie das Formular mit Informationen zu Ihrem Token aus.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OAuth-JWT-Tabelle

Feld	Beschreibung
Name	Ein eindeutiger Name, der die Anwendung identifiziert, für die Sie JWT-OAuth-Zugriff benötigen.
Client-ID	Die automatisch generierte eindeutige ID der Anwendung. Das System verwendet den Wert dieses Felds, um den öffentlichen oder freigegebenen Schlüssel abzurufen und das JWT zu validieren. Der Wert dieses Felds muss mit dem Wert der Ansprüche des Ausstellers und der Zielgruppe in JWT übereinstimmen.
Geheimer Clientschlüssel	Die gemeinsame geheime Zeichenfolge, die sowohl die Instanz als auch die Clientanwendung oder Website verwenden, um die Kommunikation miteinander zu autorisieren. Lassen Sie dieses Feld leer, damit die Instanz automatisch einen geheimen Clientschlüssel generiert. Um vorhandene geheime Clientschlüssel anzuzeigen, wählen Sie das Sperrsymbol. **Hinweis:** Wenn „ **Öffentlicher Client** “ ausgewählt ist, können Sie den **geheimen**Clientschlüssel auslassen.
Anwenderfeld	Feld in der Benutzertabelle (sys_user), das vom System verwendet wird, um den Wert des betreffenden Anspruchs in JWT abzugleichen. Wenn Sie beispielsweise ein Token mit dem Betreff-Anspruchwert user.name@example.com hinzufügen, legen Sie das **Benutzerfeld** auf E- **Mail**fest. Dieses Feld weist das System an, das E-Mail-Feld nach dem Wert user.name@example.com zu durchsuchen und den übereinstimmenden Anwenderdatensatz in der eingehenden Anforderung zu verwenden.
JTI-Verifizierung aktivieren	Wählen Sie diese Option aus, um bei jedem Tokenaustausch ein neues Token zu erfordern. Standard: Ausgewählt.
Anwendung	Schreibgeschützter Anwendungsbereich. Dieses Feld wird automatisch gefüllt.
Zugänglich von	Bereichsübergreifende Zugriffsrichtlinie. Weitere Informationen finden Sie unter Einstellungen für den Anwendungszugriff .
Lebensdauer von Zugriffstoken	Gültigkeitsdauer des Tokens. Einheit: Sekunden
Taktversatz	Zulässige Zeitdifferenz zwischen Server- und Client-Uhren beim Validieren der Ansprüche „ `exp` “ und „`nbf`“ in JWT. Einheit: Sekunden Standard: 300
Tokenbeschränkungen erzwingen	Wählen Sie diese Option aus, um nur Token für die Verwendung mit APIs zu aktivieren, die zum Aktivieren des Authentifizierungsprofils festgelegt sind. Sie können den Gewährungszugriff mithilfe einer API-Zugriffsrichtlinie festlegen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Weitere Informationen finden Sie unter REST-API-Zugriffsrichtlinie erstellen. Standard: Nicht ausgewählt.
Kommentare	Die der Anwendung zuzuordnenden Informationen.
Öffentlicher Client	Fügen Sie dieses Feld dem Formular hinzu, wenn der JWT-Client öffentlich ist. Wenn diese Option ausgewählt ist, müssen Sie keinen **Clientschlüssel angeben**. Standard: Nicht ausgewählt.
Clienttyp	Wählen Sie den Clienttyp basierend auf dem Typ Ihres Clients aus. Optionen: ▪ **iframe Eingebettet** ▪ **Integration als Anwender** ▪ **Integration als Service** Weitere Informationen finden Sie unter Konfigurieren Sie den Clienttyp für OAuth- und SSO-Datensätze.

d. Speichern Sie das Formular.

e. Fügen Sie der zugehörigen Liste „JWT-Verifiziererzuordnungen“ Datensätze hinzu, um die JWT-Signatur zu überprüfen.

Tabelle „JWT-Verifizierungszuordnungen“.

Feld	Beschreibung
Name	Name des JWT-Mapping-Datensatzes.
Kind	Schlüssel-ID aus dem JWT.
Freigegebener Schlüssel	Der freigegebene Schlüssel für die angegebene Schlüssel-ID.
Anwendung	Schreibgeschützter Anwendungsbereich.
Sys-Zertifikat	Zertifikatdatensatz in der Tabelle „X.509-Zertifikate“ (sys_certificate). Das Zertifikat, das in Schritt 1 hochgeladen wurde.

f. Fügen Sie der zugehörigen Liste „OAuth-JWT-Anspruchvalidierungen“ alle anwenderdefinierten Ansprüche hinzu, die Ihrem JWT zugeordnet sind.

Für die folgenden erforderlichen Ansprüche müssen Sie keine Datensätze hinzufügen:

- iss
- aud
- sub
- abgel

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Wenn `aud` und `iss` nicht übereinstimmen, fügen Sie den Wert `iss` in der Anspruchsvalidierung hinzu.
- Für Zertifikate können Sie mehrere Verifiziererzuordnungen hinzufügen, die mehreren Schlüsseln zugeordnet sind.

OAuth-JWT-Anspruchvalidierungstabelle

Feld	Beschreibung
Mein externer Client	Automatisch mit dem OAuth-JWT-Datensatz ausgefüllt.
Anspruchwerttyp	Datentyp des Anspruchswerts.
Anspruchname	Name des Anspruchs, den Sie hinzufügen möchten.
Anspruchwert	Wert des Anspruchs.
Anwendung	Schreibgeschützter Anwendungsbereich.

3. Senden Sie eine cURL-Anforderung, die das JWT-Token enthält, um ein Zugriffstoken von Ihrer -Instanz zu erhalten.

Example

Im Folgenden finden Sie ein Beispiel für einen cURL-Befehl zum Anfordern eines Zugriffstokens:

```
$ curl -d"grant_type= urn:ietf:params:oauth:grant-type:jwt-bearer
&client_id=be3aeb583ace210011c15b24a43e25d8
&client_secret=client_password
&assertion=
 eyJraWQiOiJzYW1wbGVrZXlpZCIsInR5cCI6IkpXVCIsImFsZyI6IlJTMjU2In0.eyJhdW
QiOiI5YzZlMmQxNzU0MzMyMDEwMDFhMTE4Y2FhMGVhMmE0MyIsInN1YiI6ImFkbWluQGV4Y
W1wbGUuY29tIiwiaXNzIjoiOWM2ZTJkMTc1NDMzMjAxMDAxYTExOGNhYTBlYTJhNDMiLCJl
eHAiOjE2MjI3MDI1MjYsImlhdCI6MTYyMjcwMjQ2NiwianRpIjoiNWRkMGUxYzctYjY1Ny0
0YmQ4LTlkY2UtMTdhZDdlZmUwNmFiIn0.PDoffnN2nq9ZNdxhOTLNbzlls4C1gsacahWr0k
mPcGJDUJ_OQunmY5YXfpqkASiZixcQDS4kMwyqK9bha1-SnPOXq7zCIlJGCGFOv_OjEpQvM
qmiKtLVk3jCsD03eXSoR4V-EzoCChiXpK87K5tMfM5k0YV9KfrxgvjUipgfni5N0Jeyqkss
MXBdkuE90XW_hBCo9AMMQm6J2PNMWb2O_O8rOX06KHuc4-Ip8wcRZ8a_bndCSmHl8Em7v4D
vqTkLzlnF_-BXuM3T7nTI21cDXQKqZnqzzriu8irlAsscJFTxkh-_Ynei5RgYtL_Mvx2-H
DO-XGofBhlAY2t9K36sz71HHqFZr5qCOIOAPguNzAy5-MOuZjOU_kH6ugIRycaNMDRjaU7g
OvUHEERw3d0sI20OChIWOryBSwdTs7lgB1WzsJWCNVo81ssc2yko3jPoygt90tMwI_6A-
4J-mlgq_fS_SvPUAqq_2UUJfVOTT5WGeq58cXfwRJmsDo49IhL3kXDVWT2gxaqhEdBQEW16
UmRoTUzRs9A9sOm18y3skmOVtnEOm-MlJMFQZ754UMzbiH0ZsMmk1ivCGIjex5J0_lDjKEl
WF5RHGz3YShCoa4JKDZsqYMvIk1SvzyQXjuFqPdS2vzg2m1eKGUwr3m6uNs_HflcDystwVd
MZ7nLlBG4"
https://instancename.service-now.com/oauth_token.do
```

Wenn der JWT-Client ein öffentlicher Client ist, wie z. B. das Mobile SDK, können Sie die Parameter „client_id“ und „client_secret“ in der Anforderung weglassen. Im Folgenden finden Sie ein Beispiel für einen cURL-Befehl zum Anfordern eines Zugriffstokens, bei dem client_id und client_secret fehlen:

```
$ curl -d"grant_type= urn:ietf:params:oauth:grant-type:jwt-bearer
&assertion=
 eyJraWQiOiJzYW1wbGVrZXlpZCIsInR5cCI6IkpXVCIsImFsZyI6IlJTMjU2In0.eyJhdW
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
QiOiI5YzZlMmQxNzU0MzMyMDEwMDFhMTE4Y2FhMGVhMmE0MyIsInN1YiI6ImFkbWluQGV4Y
W1wbGUuY29tIiwiaXNzIjoiOWM2ZTJkMTc1NDMzMjAxMDAxYTExOGNhYTBlYTJhNDMiLCJl
eHAiOjE2MjI3MDI1MjYsImlhdCI6MTYyMjcwMjQ2NiwianRpIjoiNWRkMGUxYzctYjY1Ny0
0YmQ4LTlkY2UtMTdhZDdlZmUwNmFiIn0.PDoffnN2nq9ZNdxhOTLNbzlls4C1gsacahWr0k
mPcGJDUJ_OQunmY5YXfpqkASiZixcQDS4kMwyqK9bha1-SnPOXq7zCIlJGCGFOv_OjEpQvM
qmiKtLVk3jCsD03eXSoR4V-EzoCChiXpK87K5tMfM5k0YV9KfrxgvjUipgfni5N0Jeyqkss
MXBdkuE90XW_hBCo9AMMQm6J2PNMWb2O_O8rOX06KHuc4-Ip8wcRZ8a_bndCSmHl8Em7v4D
vqTkLzlnF_-BXuM3T7nTI21cDXQKqZnqzzriu8irlAsscJFTxkh-_Ynei5RgYtL_Mvx2-H
DO-XGofBhlAY2t9K36sz71HHqFZr5qCOIOAPguNzAy5-MOuZjOU_kH6ugIRycaNMDRjaU7g
OvUHEERw3d0sI20OChIWOryBSwdTs7lgB1WzsJWCNVo81ssc2yko3jPoygt90tMwI_6A-
4J-mlgq_fS_SvPUAqq_2UUJfVOTT5WGeq58cXfwRJmsDo49IhL3kXDVWT2gxaqhEdBQEW16
UmRoTUzRs9A9sOm18y3skmOVtnEOm-MlJMFQZ754UMzbiH0ZsMmk1ivCGIjex5J0_lDjKEl
WF5RHGz3YShCoa4JKDZsqYMvIk1SvzyQXjuFqPdS2vzg2m1eKGUwr3m6uNs_HflcDystwVd
MZ7nLlBG4"
https://instancename.service-now.com/oauth_token.do
```

Die Instanz gibt das Zugriffstoken in ihrer Antwort zurück:

```
{
    "access_token":
 "KynMY2H0uwWkRc8g8YLXjnQxWbH5_wbnSiLsnaOoKw61GZkkV0ytZP74uF7hJyjfsWfaa
FijqQzq2kcABNJxNA",
    "scope": "useraccount",
    "token_type": "Bearer",
    "expires_in": 1799
}
```

Hinweis: Der eingehende JWT-Gewährungstyp enthält keine Aktualisierungstoken.

4. Führen Sie einen REST-API-Aufruf durch, um mit dem Zugriffstoken auf eine Ressource zuzugreifen.

   Example

   Im Folgenden finden Sie einen cURL-Befehl für den Zugriff auf die Incident-Tabelle mit dem Token.

```
$ curl -H "Authorization: Bearer
 KynMY2H0uwWkRc8g8YLXjnQxWbH5_wbnSiLsnaOoKw61GZkkV0ytZP74uF7hJyjfsWfaaF
ijqQzq2kcABNJxN"
https://instancename.service-now.com/api/now/v1/table/incident
```

Ergebnisse
Das System ruft im REST-Aufruf das Zugriffstoken ab und ermöglicht den Zugriff auf die angeforderte Ressource.

Konfigurieren Sie einen OAuth-OIDC-Provider für die Annahme von Drittanbieter-Token

Sie können einen OAuth-OIDC-Anbieter so konfigurieren, dass er Identitätstoken akzeptiert, die von einem OIDC-Drittanbieter mithilfe eingehender API-Aufrufe mit der Option Single Sign-on (Mehrere Anbieter-SSO) generiert wurden.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Now Platform unterstützt neben eingehenden API-Aufrufen auch OIDC durch unsere externe Implementierung von Single Sign-On (SSO). Ein Beispiel für eine OIDC-Anbieterkonfiguration

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

finden Sie unter Azure AD einrichten. Ein SSO-spezifisches Beispiel für eine OIDC-Providerkonfiguration finden Sie unter OpenID Connect-Konfiguration (OIDC) für Single Sign-on (SSO) erstellen.

Prozedur

1. Navigieren zu **Alle** > **System-OAuth** > **Applikationsregistrierung**an.
   - Wählen Sie **Neu**, wählen Sie **Konfigurieren Sie einen OIDC-Anbieter, um ID-Token zu verifizieren**, und füllen Sie dann das Formular aus.
   - Wählen Sie eine vorhandene Vorlage für einen OIDC-Anbieter (ADFS, Auth0, Azure AD, Google, Okta) aus, und füllen Sie das Formular aus.

     Hinweis: OIDC-Provider-Vorlagen sind nach dem Laden von Demodaten mit dem Plugin OAuth 2.0 verfügbar.

Feld	Beschreibung
Name	Ein eindeutiger Name, der die OAuth-OIDC-Entität identifiziert
Client-ID	Die Client-ID der Anwendung, die beim OAuth-OIDC-Server des Drittanbieters registriert ist. Dieser Wert muss mit dem Wert der `aud-Anforderung` im JWT-Token übereinstimmen.
OAuth-API-Skript	Ein Skript, mit dem Sie Anforderungen und Antworten an einen externen OAuth-Provider anpassen können.
OAuth-OIDC-Providerkonfiguration	Die OIDC-Anbieter (ADFS, Auth0, Azure AD, Google, Okta) können zur Validierung des JWT-Tokens verwendet werden. Wählen Sie den Datensatz Ihrer **OIDC** -Anbieterkonfiguration aus, um zu überprüfen, ob der **Anwenderanspruch** und das Anwenderfeld entsprechend eingestellt sind. Füllen Sie außerdem folgende Felder aus: ◦ **JTI-Anspruchzertifizierung aktivieren**: Wenn diese Option aktiviert ist,validiert die Validierung des JWT-Tokens ServiceNow auch das vom Anbieter gesendete JTI. ◦ **OIDC-Metadaten-URL**: Details der bekannten Konfiguration des OIDC-Anbieters. **Hinweis:** Wenn die Validierung nicht aktiviert ist, kann das `JTI` nicht validiert werden, unabhängig davon, ob es im JWT-Token vorhanden ist. Der Anspruchsname im Token muss `jti lauten`.
Taktversatz	Die Anzahl in Sekunden, nach der die Einschränkung als gültig betrachtet werden soll. Der Standardwert ist 300.
Tokenbeschränkungen erzwingen	Wählen Sie diese Option aus, um nur Token für die Verwendung mit APIs zu aktivieren, die zum Aktivieren des Authentifizierungsprofils festgelegt sind. Sie können den Gewährungszugriff mithilfe einer API-Zugriffsrichtlinie festlegen. Weitere Informationen finden Sie unter REST-API-Zugriffsrichtlinie erstellen. Standard: Nicht ausgewählt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Aktiv	Aktivieren Sie das Kontrollkästchen, um die OAuth-Anwendung zu aktivieren.
Clienttyp	Wählen Sie den Clienttyp basierend auf dem Typ Ihres Clients aus. Optionen: ◦ **iFrame – eingebettet** ◦ **Integration als Anwender** ◦ **Integration als Service** Weitere Informationen finden Sie unter Konfigurieren Sie den Clienttyp für OAuth- und SSO-Datensätze.

2. Wählen Sie **Absenden**.
   Der Datensatz wird in der Tabelle der Anwendungs-Registrys [oauth_entity] gespeichert. Wenn Ihre -Instanz Token und Autorisierungscodes ausgibt, erstellt sie in der Tabelle „Anwendungsregistrierungen“ [oauth_entity] einen Datensatz vom Typ **Externer OIDC-Anbieter**. Weitere Informationen finden Sie unter .
3. Wahlweise: Wechseln Sie zur zugehörigen Liste im Datensatz „OAuth-Entitätsprofile“, um ein vom System generiertes Standardprofil für den neuen OAuth-Provider ohne Bereich zu validieren.
   Sie können ein OAuth-Provider-Profil ändern oder hinzufügen, einschließlich Name, Erteilungstyp und OAuth-Bereich.
4. Wahlweise: Wechseln Sie zur zugehörigen Liste im Datensatz „OAuth-Entitätsbereiche“, um alle verfügbaren OAuth-Bereiche für diesen OAuth-Provider zu definieren.
   Die definierten Umfänge können beim Erstellen oder Aktualisieren eines Profils ausgewählt werden. Jeder definierte OAuth-Bereich enthält einen Namen und einen Bereich, die Sie der Anbieterspezifikation entnehmen müssen, z. B. einen Lesebereich oder einen Schreibbereich. Jeder Bereich muss separat definiert werden.
5. Wahlweise: Wechseln Sie zur zugehörigen Liste im Datensatz Anwenderbereitstellung, um die automatische Anwenderbereitstellung zu aktivieren.

Option	Bezeichnung
Anwender automatisch bereitstellen	Option zum Erzwingen der Authentifizierung für Anwender.
Bereitstellungsdatenquelle	Die Datenquelle, die zum Transformieren eines OIDC-Tokens in einen ServiceNow -Benutzer verwendet werden soll. Verwenden Sie die **Liste Nachschlagen**, um die vordefinierte Datenquellenvorlage auszuwählen, und öffnen Sie dann den Datensatz, um die Zuordnung der transformierten Tabelle zu konfigurieren. Bei der Konfiguration der Transformationszuordnung stammen die Quellfelder aus der Tabelle *JWT token*, die Zielfelder aus der Tabelle *sys_user*.
Auf bereitgestellte Anwender angewendete Anwenderrollen	Die Anwenderrollen, die auf die neu bereitgestellten ServiceNow -Anwender angewendet werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Example: Im Folgenden finden Sie ein Beispiel für eine cURL-Anforderung zum Aufrufen eines REST-API-Aufrufs

Rufen Sie einen REST-API-Aufruf auf.

Führen Sie die nachfolgenden Schritte durch:

- Registrieren Sie die App beim OpenID Connect-Anbieter.
- Konfigurieren Sie die OAuth-OIDC-Entität.
- Konfigurieren Sie den OIDC-Provider:

OIDC-Provider

OIDC-Provider	Name des OIDC-Anbieters.
OIDC-Metadaten-URL	Geben Sie die OIDC-Metadaten-URL an (bekannte Konfigurations-URL). Diese Informationen werden verwendet, um die öffentlichen Schlüssel zum Validieren des Tokens über den `JWKS-` Endpunkt abzurufen.
Anwenderanspruch	Der Anspruch, der anhand der Anwendertabelle validiert wird.
Anwenderfeld	Anwenderanspruch, der den Anwenderdatensatz identifiziert.
JTI-Anspruchzertifizierung aktivieren	Wenn diese Option aktiviert ist, validiert die Validierung des ServiceNow JWT-Tokens auch die vom Anbieter gesendete JTI. **Hinweis:** Wenn die Validierung nicht aktiviert ist, kann das `JTI` nicht validiert werden, unabhängig davon, ob es im JWT-Token vorhanden ist. Der Anspruchsname im Token muss `jti lauten`. Diese Informationen werden verwendet, um Replay-Angriffe zu verhindern.

- Rufen Sie ein JWT-Token ab.
- Rufen Sie einen REST-API-Aufruf auf.
  - Das ID-Token im Autorisierungsheader für den Zugriff auf die Tabellen-API oder den Scripted Web Service.

```
curl -X GET --header "Accept:application/json"
 https://<instance_name>.service-now.com/api/now/table/incident/897b04
f2dbd4a300a135364e9d961952 -k
--header "Authorization: Bearer
 eyJraWQiOiJjNTZtZTlXU0xPVnY3UFMwcTg4Qzl1b0lzNjFQYTdmUG4yZFVFOW9RNUg4I
iwiYWxnIjoiUlMyNTYifQ.eyJzdWIiOiIwMHVnZDg1OD
VkczI1WXpUSjBoNyIsIm5hbWUiOiJpbXJhbiBhbGkiLCJsb2NhbGUiOiJlbi1VUyIsImVt
YWlsIjoiaW1yb241NDNAZ21haWwuY29tIiwidmVyIjoxLCJpc3MiOiJodHRwczovL2Rldi
05MzQ
```

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
xMjEub2t0YXByZXZpZXcuY29tIiwiYXVkIjoiMG9hZ2Q4bzk3a2lCT3dwd0IwaDciLCJpY
XQiOjE1Mzc5MzMzMjYsImV4cCI6MTUzNzkzNjkyNiwianRpIjoiSUQueThVdXpWNUg2bm1
6SzRs
OTI1RFVrQnJoR1o1MmJzVVpGVHRVTEphQjg3ayIsImFtciI6WyJwd2QiXSwiaWRwIjoiMD
BvZ2Q4NTgycEFqZDZTemcwaDciLCJub25jZSI6InNub3ciLCJwcmVmZXJyZWRfdXNlcm5h
bWUiO
iJpbXJvbjU0M0BnbWFpbC5jb20iLCJnaXZlbl9uYW1lIjoiaW1yYW4iLCJmYW1pbHlfbmF
tZSI6ImFsaSIsInpvbmVpbmZvIjoiQW1lcmljYS9Mb3NfQW5nZWxlcyIsInVwZGF0ZWRfY
XQiOj
E1Mzc5MzAxOTcsImVtYWlsX3ZlcmlmaWVkIjp0cnVlLCJhdXRoX3RpbWUiOjE1Mzc5Mjk2
NjF9.OG87SYxWFgHGlhBYby2H79diRm9rlYZTeEkIINRUatwg-p4739htB8xEY-5_t6yU_
6k5w1
0pdgtt5M5QFZRPXVbQZNoGtY-Bxn0BjaimcFgoWfhY_0ldnGTkzN2RYyIHvrf9-yhxg347
zvczmLrgMMa_VwG4rxrtE6rUXaIpIeIK5b-Deq8ADz8UTUTKpF_5RWk4X-oh5xK6BLniFH
k4ShO
Zq2v_mjproXwKk5euJKrVrar2lQ4adZCOSTRuTf3ThMO5WDh0sel-82LngXtLzRJJ51Iqx
AsXns0kJHLLqLtH1hXNRKfwT1ScQoE_OfWm4t0KryI2j4wSMEanFtLXIw"
```

◦ Wenn der Anwender authentifiziert ist, wird eine gültige Anwendungs-/JSON-Antwort zurückgegeben. Andernfalls wird eine Fehlermeldung für nicht authentifizierten Anwender zurückgegeben.

```
User Not Authenticated
{"error":{"message":"User Not Authenticated","detail":"Required to
 provide Auth information"},"status":"failure"}
```

Konfigurieren Sie den Clienttyp für OAuth- und SSO-Datensätze

Konfigurieren Sie das Feld Clienttyp für **OAuth-** und SSO-Datensatz-bezogene Konfigurationen.

Beim Einrichten von Sitzungen für verschiedene Anmeldetypen wie Web-UI (interaktive Anmeldung), Eingebetteter IFrame, Eingebettet oder Integration, können Sie den Clienttyp für die OIDC- (OAuth-Entität), SAML- und Digest-Datensätze konfigurieren, die für verschiedene Anmeldungen verwendet werden.

Die Auswahlmöglichkeiten für Clienttypen lauten wie folgt:

- **IFrame Eingebettet**: Kann für die interaktive Instanz ServiceNow verwendet werden, die sich in einem IFrame auf den Websites von Drittanbietern befindet. Wenn beispielsweise eine vertrauliche Tabelle vorhanden ist (Tabelle „sys_user“ – Telefonnummer des Anwenders), können Sie als Administrator die ACL so konfigurieren, dass das Sicherheitsattribut (Iframe Eingebettet) auf „falsch“ festgelegt ist, um zu verhindern, dass der Anwender auf die Daten (Tabelleninformationen) zugreift. in der eingebetteten Iframe-Sitzung in der Drittpartei.
- **Integration als Anwender**: Kann für Virtual Agent-Chat-Bots verwendet werden, die in Desktop-Apps wie Slack, Teams usw. installiert sind.
- **Integration als Service**: Kann für die Machine-to-Machine-Integration (Kommunikation zwischen Services) verwendet werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Für OIDC (OAuth-Entität): Alle Auswahlmöglichkeiten sind verfügbar.
- Für SAML und Digest: Nur Iframe eingebettet. Sie müssen das Formular bearbeiten, dem Datensatz das Feld „Clienttyp“ hinzufügen und den Clienttyp „ **IFrame – Eingebettet** “ auswählen.
- Wenn „Keiner“ als **Clienttyp** ausgewählt ist, gibt es keine Klassifizierung der Sitzung.

Es wird empfohlen, das Feld „Clienttyp“ für alle Datensätze zu verwenden, die für OIDC (OAuth-Entität), SAML und Digest erstellt wurden. Dies ermöglicht Ihnen eine bessere Kontrolle über alle Anmeldemethoden, die dieselben Konfigurationen aufweisen, sich jedoch je nach Clienttyp unterscheiden.

Wenn sich nach der Konfiguration des Felds ein Anwender über die entsprechende Konfiguration (OAuth oder SSO) anmeldet, wird die Sitzung bei erfolgreicher Authentifizierung auf Grundlage des konfigurierten Clienttyps betrachtet und entsprechend die Zeitüberschreitung der Sitzung genutzt.

Für die aktuelle Sitzung sind die entsprechenden Sicherheitsattribute enthalten oder können genutzt werden, um zu verhindern, dass Benutzer innerhalb des ausgewählten Clienttyps auf tabellenspezifische Informationen zugreifen. Weitere Informationen finden Sie unter OOB (vordefinierte) Sicherheitsattribute.

Sitzungstimeout für die Clienttypen

Im Folgenden werden die Systemeigenschaften im Zusammenhang mit der Sitzungsüberschreitung für die verschiedenen Clienttypen aufgeführt:

- `glide.session_timeout.iframe_embedded`
- `glide.session_timeout.integration_as_a_user`
- `glide.session_timeout.integration_as_a_service`

Implizite OAuth-Gewährungen

ServiceNow -Instanzen unterstützen die implizite Gewährung eines Zugriffstokens.

Der implizite Gewährungstyp, auch bekannt als *`implicit grant code flow`*, ermöglicht die direkte Gewährung des Zugriffstokens an die Client-Anwendung über den Benutzeragenten, in der Regel ein Webbrowser oder ein Mobilgerät. Es werden keine Aktualisierungstoken gewährt. Der Endanwender muss weiterhin Zugriff auf die geschützte Ressource in der -Instanz gewähren, genau wie beim Standard-.

Flow-Prozess für implizite OAuth-Gewährung

Wie beim Standard-Autorisierungscode-Flow fordert die Clientanwendung die Verwendung der eingeschränkten Ressource in der Instanz an, und der Endanwender genehmigt sie. Die Anforderung wird in Form einer URL an die -Instanz gesendet. Die URL muss die folgenden Parameter enthalten:

- `client_id=`<the necessary client ID> . Dies ist obligatorisch, um zu identifizieren, auf welche geschützte Ressource die Client-Anwendung zugreifen möchte.
- `response_type=token`. Dies ist erforderlich, um das Zugriffstoken direkt anzufordern (anstatt nach einem Autorisierungscode zu fragen). Der Wert muss für implizite Gewährungen ein `Token` sein. Im Beispiel für den Standard-Autorisierungscode-Flow lautet der Antworttyp „ `code`“.
- `redirect_uri=<a URL>`Der Ort, an den das Token gesendet wird.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Autorisierungsserver sendet das Zugriffstoken anstelle eines Autorisierungscodes über den -Benutzeragenten an die Client-Anwendung.

Hier sehen Sie ein Beispiel für eine GET-Anforderung zum Empfangen der JSON-Nutzlast der Daten für die Incident-Tabelle [Incident]:

```
https://myinstance.servicenow.com/oauth_auth.do?response_type=token&redir
ect_uri={the_redirect_url}&client_id={the_client_identifier}
```

Wenn der Benutzer Zugriff gewährt, wird das Token in die Umleitungs-URL (Rückruf-URL) aufgenommen:

```
https/http://{callbackURL}?access_token={the_token}
```

Verwalten Sie OAuth-Token

Öffnen Sie OAuth-Token, um Zugriff auf eingeschränkte Ressourcen zu gewähren.

Vorbereitungen
Erforderliche Rolle: beliebiger Anwender oder Administrator

Warum und wann dieser Vorgang ausgeführt wird
Von der -Instanz und einem OAuth-Drittanbieter ausgegebene OAuth-Token werden in der Tabelle „oauth_credential“ gespeichert.

Einige der wichtigen Spalten in dieser Tabelle:

- Token: Wert des von der Instanz ServiceNow ausgegebenen Tokens.
- Typ: Bestimmt, ob das Token ein Zugriffstoken oder ein Aktualisierungstoken ist.
- Läuft ab: Datum/Uhrzeit, zu der das Zugriffs- oder Aktualisierungstoken abläuft.
- Token erhalten: Wert des Tokens, der von einem OAuth-Drittpartei-Provider ausgegeben wurde. Dieser Wert liegt im verschlüsselten Format vor.

Tokenablauf und Gültigkeit lauten wie folgt:

- Zugriffstoken: Standardmäßig gibt eine -Instanz Zugriffstoken mit einer Lebensdauer von 30 Minuten aus, wenn die Instanz der OAuth-Anbieter ist.
- Aktualisierungstoken: Standardmäßig gibt eine Instanz Aktualisierungstoken mit einer Lebensdauer von 100 Tagen aus, wenn die Instanz der OAuth-Anbieter ist.

Prozedur

1. Navigieren Sie zu einer der folgenden Menüoptionen:
   - **Self-Service** > **Meine verbundenen Apps** um die Token anzuzeigen, die erstellt wurden, als Sie in der Instanz Zugriff auf eine Ressource gewährt haben.
   - **System-OAuth** > **Tokens verwalten** , um alle Token anzuzeigen. Nur Administratoren können auf dieses Modul zugreifen.
2. Klicken Sie auf den **Namen**, um das Token zu öffnen.
3. Klicken Sie auf **Zugriff widerrufen**, um den Zugriff auf die eingeschränkte Ressource zu verhindern.

   Sie können auch andere Informationen zum Token anzeigen, einschließlich des Bereichs, auf den der Zugriff ermöglicht wird, und des Ablaufdatums.

   Sie können den Datensatz „Abgelaufene **OAuth-Anmeldeinformationen** bereinigen“ auf der Seite „Zeitplan“ (`sys.trigger.list`) auswählen und Folgendes konfigurieren:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **com.snc.platform.security.oauth.is.active**: Standardmäßig ist der Wert auf 0 (wahr) festgelegt.
- **com.snc.platform.security.oauth.hours.expired.credential.is.kept**: Legen Sie den Wert basierend auf Ihren Anforderungen fest, um die Anzahl der Stunden zu bestimmen, für die die abgelaufenen `OAuth-` Anmeldeinformationen im System aufbewahrt werden sollen.
- **com.snc.platform.security.oauth.day.old.credential.is.kept**: Legen Sie den Wert basierend auf Ihren Anforderungen fest, um die Anzahl der Tage zu bestimmen, für die die abgelaufenen `oatuh-` Anmeldeinformationen im System aufbewahrt werden sollen.

Widerruft ein OAuth-Token

Aus Sicherheitsgründen möchten Sie möglicherweise einen OAuth-Zugriff oder ein Aktualisierungstoken widerrufen.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Das Widerrufen des Tokens bezieht sich auf eine Situation, in der Ihre -Instanz als OAuth-Ressourcenserver fungiert. Sie können das Token über eine URL oder per widerrufen.

Prozedur

Greifen Sie mit `oauth_revoke_token.do` auf Ihre Instanz zu, und hängen Sie das Zugriffs- oder Aktualisierungstoken an.

Beispiel: `https://[Ihre_ServiceNow_Instanz]:[Port]/oauth_revoke_token.do?token=[Zugriffs- oder Aktualisierungstoken]` ohne die Klammern `[ ]`.

Ergebnisse
Für diesen Endpunktzugriff ist keine Authentifizierung erforderlich. Das Token in dieser Anforderung ist als abgelaufen markiert.

Client-Anmeldeinformationen

Verwenden Sie den Gewährungstyp für OAuth-Client-Anmeldeinformationen für eingehende Integrationen von einem OAuth-Client einer Drittpartei in die Plattform ServiceNow®.

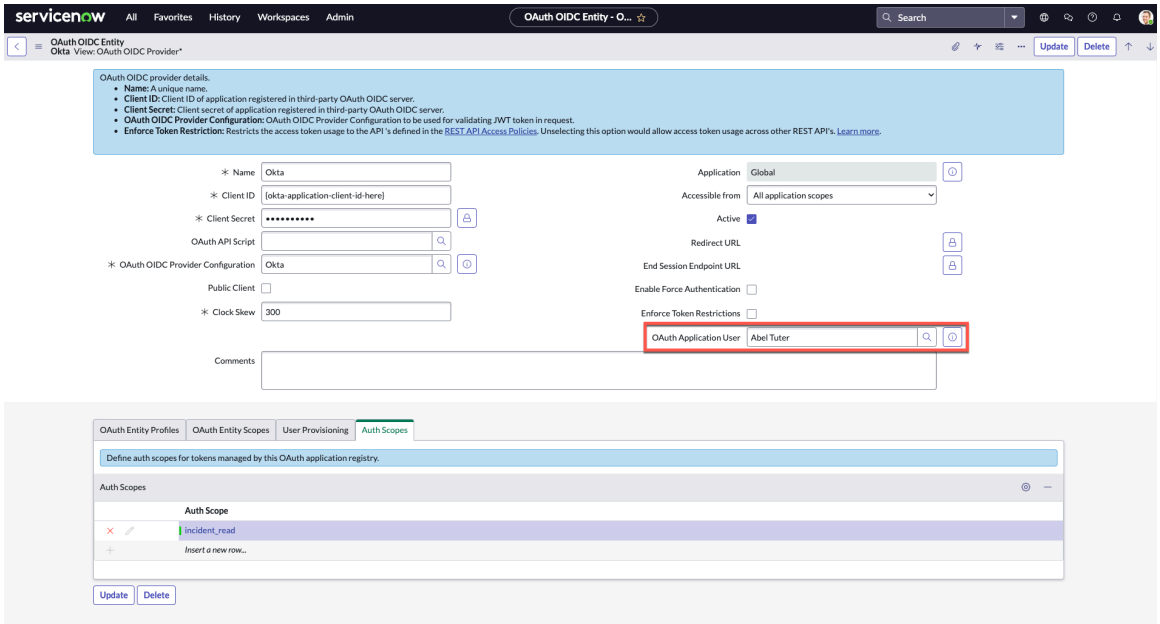
Administratoren können den Gewährungstyp Client-Anmeldeinformationen (CC) verwenden, um die Integration von einem OAuth-Client einer Drittpartei in die Plattform ServiceNow zu ermöglichen.

Der Gewährungstyp für eingehende Client-Anmeldeinformationen ist eine Fähigkeit, die über eine Systemeigenschaft gesteuert werden kann. Standardmäßig ist die Systemeigenschaft auf „false“ festgelegt.

Um den Gewährungstyp für Client-Anmeldeinformationen zu verwenden, müssen Sie die folgenden Schritte ausführen:

- Erstellen Sie die Systemeigenschaft „ `glide.oauth.inbound.client.credential.grant_type.enabled` “.
- Fügen Sie dem Formular „OAuth-Entität“ das Feld „ **OAuth-Anwendungsbenutzer** “ hinzu.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Erstellen Sie die Systemeigenschaft Client-Anmeldeinformationen

Erstellen Sie die Systemeigenschaft „`glide.oauth.inbound.client.credential.grant_type.enabled`“, um den Gewährungstyp „Client-Anmeldeinformationen“ für eingehende OAuth-Integrationen zu verwenden.

Vorbereitungen

Erforderliche Rolle: admin

Erforderliches Plugin: OAuth 2.0.

Prozedur

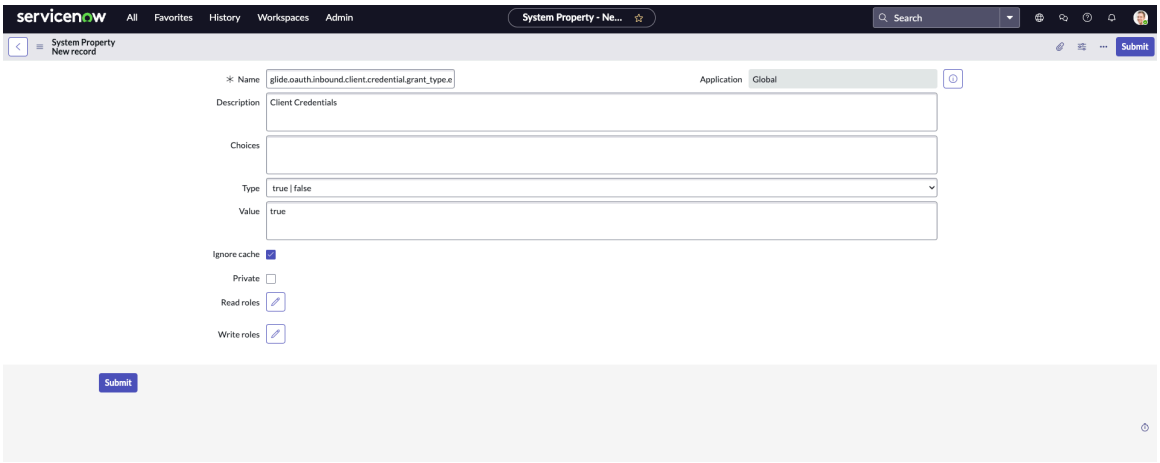
1. Geben Sie im Navigationsfilter `sys_properties.list` ein.
   Die gesamte Liste der Eigenschaften in der Tabelle „Systemeigenschaften“ [sys_properties] wird angezeigt.
2. Wählen Sie **Neu**.
3. Füllen Sie die folgenden Felder im Formular aus.

Feld	Beschreibung
Name	Name der Eigenschaft, die Sie erstellen. In diesem Fall `glide.oauth.inbound.client.credential.grant_type`
Beschreibung	Geben Sie einen kurzen, beschreibenden Ausdruck ein, der die Funktion der Eigenschaft beschreibt.
Typ	Wählen Sie den entsprechenden Datentyp aus der Liste aus. In diesem Fall `true|false`.
Wert	Legen Sie den gewünschten Wert für die Eigenschaft fest. In diesem Fall „`true`“, um den Gewährungstyp für Client-

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Anmeldeinformationen für eingehende OAuth-Integrationen zu aktivieren.



Hinweis: Andere Felder im Formular wie Auswahlmöglichkeiten, Cache ignorieren, Privat, Leserollen und Schreibrollen können entsprechend Ihren Anforderungen konfiguriert werdens.

4. Wählen Sie **Absenden**.

Hinweis: Wenn die **Checkbox Cache ignorieren aktiviert** ist, leert das System den Servercache, wenn der Parameter geändert wird.

Als Nächstes müssen Sie einen OAuth-Client (OAuth-API-Endpunkt für externen Client) erstellen und dem OAuth-Client-Datensatz das Feld „OAuth-Anwendungsbenutzer“ hinzufügen.

Fügen Sie den OAuth-Anwendungsbenutzer hinzu

Fügen Sie dem Formular „OAuth-Entität“ das Feld „OAuth-Anwendungsbenutzer“ hinzu, um für eingehende OAuth-Integrationen den Gewährungstyp „Client-Anmeldeinformationen“ zu verwenden.

Vorbereitungen

Erforderliche Rolle: admin

Erforderliches Plugin: OAuth 2.0.

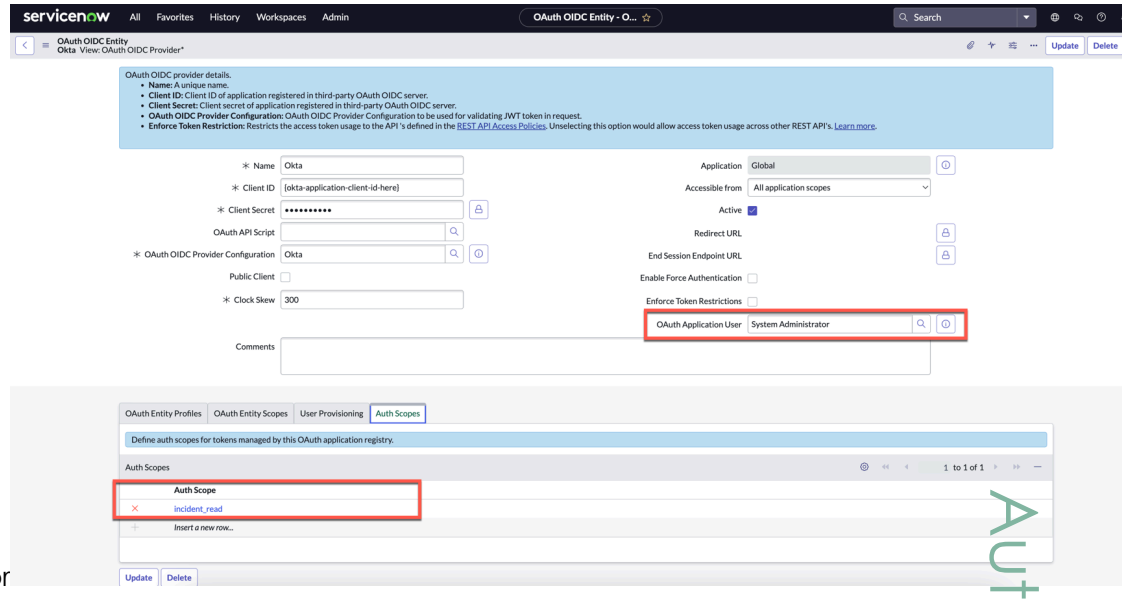
Sie müssen einen OAuth-Client erstellen. Weitere Informationen finden Sie unter Erstellen Sie einen Endpunkt, damit Clients auf die Instanz zugreifen können.

Prozedur

1. Öffnen Sie den erstellten OAuth-Client-Datensatz.
2. Symbol „Weitere Optionen auswählen“ im Seitenheader.
3. Auswahlvorgang **Konfigurieren** > **Formulardesign**an.
4. Fügen Sie auf der Seite „Formulardesign“ in der Liste der Felder **OAuth-Anwendungsbenutzer** hinzu.
5. Speichern oder aktualisieren Sie das Formular.
6. Wählen Sie den Anwender für den **OAuth-Anwendungsbenutzer**aus.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel:



Systemadministrator

Hinweis: Sie müssen den REST-API-Authentifizierungsbereich mit dem Gewährungstyp für Client-Anmeldeinformationen verwenden, um den Zugriff auf den Drittanbieter-Client zu steuern.

7. Speichern oder aktualisieren Sie das Formular.

   Jede Autorisierungsanforderung mit dem **ErteilungstypClient-Anmeldeinformationen**, **Client-IDund Geheimnis** wird für den zugeordneten OAuth-Anwendungsbenutzer in ServiceNow® übergeben.

   Hinweis: Wenn der OAuth-Anwendungsbenutzer im OAuth-Client-Datensatz nicht ausgewählt ist oder die Eigenschaft Client-Anmeldeinformationen auf `false`festgelegt ist, wird die Autorisierungsanforderung nicht übergeben.

OAuth ausgehend

Mit OAuth outbound können Sie Daten von einem Drittanbieter in Ihre -Instanz abrufen.

Sie müssen über die Rolle security_admin verfügen, um die OAuth-Integration zu verwalten.

Sie können ausgehendes OAuth 2.0 für die folgenden Gewährungstypen konfigurieren:

- **Verbindung mit Drittanbieter herstellen: Verwenden Sie die Client-ID und das Geheimnis, um sie an den OAuth-**Anbieter zu senden. Weitere Informationen finden Sie unter Stellen Sie eine Verbindung zu einem OAuth-Drittpartei-Anbieter her.
- **JWT Bearer**: Ein Autorisierungsserver validiert ein JWT-Token, das die Weitergabe von Identitäts- und Sicherheitsinformationen zwischen Sicherheitsdomänen ermöglicht. Weitere Informationen finden Sie unter Richten Sie den OAuth-Provider mit dem Gewährungstyp „JWT Bearer“ ein.
- **SAML2-Bearer**: Generiert die SAML2-Assertion und tauscht die Assertion dann für die Zugriffstoken mit dem Anbieter aus.

  Hinweis: Verwenden Sie für die ausgehende Anforderung an SuccessFactors den **SAML2-Bearer** als standardmäßigen Gewährungstyp. Weitere Informationen zur Konfiguration **des SAML2-Bearers**finden Sie im Beispiel unter Richten Sie v4.xx ein .

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Autorisierungscode**: Der Code, der dem Client gewährt wird, um ein Zugriffstoken zu erhalten, das dann verwendet wird, um Zugriff auf die Ressource zu erhalten. Wenn Sie diese Option auswählen, benötigen Sie eine Autorisierungs-URL (die URL des Autorisierungsservers).
- **Anmeldeinformationen des Ressourcenbesitzers**: Der Benutzername und das Passwort des Benutzers, der versucht, auf die Ressource zuzugreifen.
- **Client-Anmeldeinformationen**: Die Client-ID und der Client-Secret, die beide zum Abrufen des Zugriffstokens verwendet werden. Bei dieser Methode werden keine Aktualisierungstoken bereitgestellt.

Sie können das **OAuth-Anbieterszenario** (Ausgehend) konfigurieren: Ihre -Instanz ruft Daten von einem Drittanbieter ab.

Hinweis: Sie müssen sich zum ersten Mal als Anwender authentifizieren, um den Token-Post abzurufen. Sie müssen sich nicht vor Ablauf des Tokens mit einem Anwenderaccount authentifizieren.

Stellen Sie eine Verbindung zu einem OAuth-Drittpartei-Anbieter her

Konfigurieren Sie, wie die Client-ID und das Geheimnis an Ihren OAuth-Anbieter gesendet werden.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **System-OAuth** > **Applikationsregistrierung** und klicken Sie dann auf **Neu**.
2. Klicken Sie auf der Interceptor-Seite **auf Verbindung mit einem OAuth-Drittpartei-Anbieter herstellen**, und füllen Sie das Formular aus.

Feld	Beschreibung
Name	Eindeutiger Name für die OAuth-Drittpartei-Verbindung.
Client-ID	Die Client-ID der Anwendung, die beim OAuth-Server des Drittanbieters registriert ist.
Geheimer Clientschlüssel	Der geheime Clientschlüssel der beim OAuth-Server des Drittanbieters registrierten Anwendung.
OAuth-API-Skript	Das Skript, das zum Anpassen der Anforderung und Antwort an den externen OAuth-Anbieter verwendet wird.
Logo-URL	Die Logo-URL der OAuth-Anwendung.
Standardgewährungstyp	Der Standardgewährungstyp, der zum Erstellen des Tokens verwendet wird. Zur Auswahl stehen: ◦ **Autorisierungscode**: Der Code, der dem Client gewährt wird, um ein Zugriffstoken zu erhalten, das dann verwendet wird, um Zugriff auf die Ressource zu erhalten. Wenn Sie diese Option auswählen, benötigen Sie eine Autorisierungs-URL (die URL des Autorisierungsservers).

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	◦ **Anmeldeinformationen des Ressourcenbesitzers**: Der Benutzername und das Passwort des Benutzers, der versucht, auf die Ressource zuzugreifen. ◦ **Client-Anmeldeinformationen**: Die Client-ID und der Client-Secret, die beide zum Abrufen des Zugriffstokens verwendet werden. Bei dieser Methode werden keine Aktualisierungstoken bereitgestellt. ◦ **JWT Bearer**: Ein Autorisierungsserver validiert ein JWT-Token, das die Weitergabe von Identitäts- und Sicherheitsinformationen zwischen Sicherheitsdomänen ermöglicht. ◦ **SAML2-Bearer**: Generiert die SAML2-Assertion und tauscht die Assertion dann für die Zugriffstoken mit dem Anbieter aus. **Hinweis:** Verwenden Sie für die ausgehende Anforderung an SuccessFactors den **SAML2-Bearer** als standardmäßigen Gewährungstyp.
Lebensdauer von Aktualisierungstoken	Zeit in Sekunden, die das Aktualisierungstoken gültig ist. Die Standardzeit beträgt 8.640.000 Sekunden.
Öffentlicher Client	Ermöglicht öffentlichen Clients, PKCE für eine Autorisierung anzufordern. **Hinweis:** Sie können nur Autorisierungscode als *Default Grant type* verwenden, wenn PKCE aktiviert ist.
Abfragecodemethode	Die im OAuth-PCKE-Workflow verwendete Codeabfragemethode. Zur Auswahl stehen: ◦ S256 [Standard] ◦ Einfach ◦ Keine
Kommentare	Fügen Sie Kommentare zur OAuth-App hinzu.
Anwendung	Anwendung und Umfang, die diesen Datensatz enthalten.
Zugänglich von	Machen Sie diese App aus allen Anwendungsbereichen oder nur aus diesem Bereich zugänglich.
Aktiv	Aktivieren Sie das Kontrollkästchen, um die App zu aktivieren.
Autorisierungs-URL	Der OAuth-Autorisierungscode-Endpunkt.
Token-URL	Der OAuth-Servertoken-Endpunkt.
Token-Sperr-URL	Der OAuth-Servertoken-Rücknahme-Endpunkt.
Umleitungs-URL	Der OAuth-Callback-Endpunkt. Wenn leer, generiert die Instanz automatisch einen Eintrag.
Gegenseitige Authentifizierung aktivieren	Aktivieren Sie das Kontrollkästchen, um die gegenseitige Authentifizierung für die Tokenanforderung und den Widerruf zu verwenden. Für diese Funktion muss ein Profil für die gegenseitige Authentifizierung angegeben werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Anmeldeinformationen senden	Der OAuth-Client füllt die Client-Anmeldeinformationen in der Anforderung aus: ◦ In Anforderungstext (URL-codiertes Formular) ◦ Header „Basisautorisierung“. ◦ Als Private Key JWT
Clienttyp	Wählen Sie den Clienttyp basierend auf dem Typ Ihres Clients aus. Optionen: ◦ **iFrame – eingebettet** ◦ **Integration als Anwender** ◦ **Integration als Service** Weitere Informationen finden Sie unter Konfigurieren Sie den Clienttyp für OAuth- und SSO-Datensätze.

Das System erstellt in der Tabelle „Anwendungsregistrierungen“ [oauth_entity] einen Datensatz vom Typ „OAuth-Provider“.

3. Wahlweise: Wechseln Sie zur zugehörigen Liste im Datensatz „OAuth-Entitätsprofile“, um ein vom System generiertes Standardprofil für den neuen OAuth-Provider ohne Bereich zu validieren.
   Sie können ein OAuth-Provider-Profil ändern oder hinzufügen, einschließlich Name, Erteilungstyp und OAuth-Bereich.
4. Wahlweise: Wechseln Sie zur zugehörigen Liste im Datensatz „OAuth-Entitätsbereiche“, um alle verfügbaren OAuth-Bereiche für diesen OAuth-Provider zu definieren.
   Sie können die Bereiche auswählen, wenn Sie ein Profil erstellen oder aktualisieren. Jeder OAuth-Bereich enthält einen Namen und einen Bereich, die Sie der Spezifikation des Anbieters entnehmen müssen, z. B. einen Lese- oder Schreibbereich. Jeder Bereich muss separat definiert werden.

JWT Bearer

JSON-Web-Token (JWT) ermöglichen die Konfiguration von Server-zu-Server-API-Interaktionen zwischen ServiceNow und externen API-Anbietern, ohne dass ein Benutzereingriff erforderlich ist.

Die JSON-Web-Token(JWT)-Bearer-Gewährung ist eine JSON-Zeichenfolge, die Anspruchswerte enthält, die von den JWT-Grant-Handlern auf der Seite des Autorisierungsservers ausgewertet und validiert werden, bevor ein Zugriffstoken ausgestellt wird.

Mit dem Gewährungstyp „JWT-Bearer“ können Sie den OAuth 2.0-JWT-Bearer-Gewährungs-Flow für ausgehende REST-Nachrichten konfigurieren.

Richten Sie den OAuth-Provider mit dem Gewährungstyp „JWT Bearer“ ein

JSON-Web-Token (JWT) ermöglichen die Konfiguration von Server-zu-Server-API-Interaktionen zwischen ServiceNow und externen API-Anbietern, ohne dass ein Benutzereingriff erforderlich ist. Diese Unterstützung ermöglicht IntegrationHub oder anderen automatisierten Aufgaben mithilfe von JWT die Konfiguration von API- und Serviceintegrationen mit verschiedenen Anbietern.

Vorbereitungen

Erforderliche Rolle: admin

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Die folgenden Aufgaben zeigen, wie ServiceNow für die Verwendung von JWTs für die OAuth 2.0-Client-Authentifizierung und Autorisierungserteilungen eingerichtet werden kann. ServiceNow ist der OAuth-Client, und Sie können einen OAuth-Anbieter wie Box oder DocuSign konfigurieren.

Prozedur

1. Laden Sie das Java-Schlüsselspeicher-Zertifikat hoch
   Fügen Sie Ihrer -Instanz ein JKS-Zertifikat hinzu, um die JWT-Clientauthentifizierung zu aktivieren.
2. Konfigurieren Sie einen JWT-Signaturschlüssel
   Erstellen Sie einen JWT-Signaturschlüssel, der Ihrem Java KeyStore-Zertifikat (JKS) zugewiesen werden soll.
3. Erstellt einen JWT-Provider mit einem JWT-Signaturschlüssel
   Fügen Sie Ihrer Instanz ServiceNow einen JWT-Provider hinzu.
4. Stellen Sie eine Verbindung zu einem OAuth-Drittpartei-Anbieter her
   Erstellen Sie einen OAuth-Drittpartei-Anbieter mit einem JWT-Bearer als standardmäßigem Gewährungstyp in der ServiceNow Anwendungsregistrierung.
5. OAuth-Profile angeben
   Öffnen Sie das OAuth-Entitätsprofil des OAuth-Providers, und weisen Sie einen JWT-Provider zu.

Laden Sie das Java-Schlüsselspeicher-Zertifikat hoch

Sie können Ihrer -Instanz ein Java KeyStore-Zertifikat (JKS) anhängen, um die JWT-Client-Authentifizierung zu aktivieren.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **x509-Zertifikat**an.
2. Füllen Sie das Formular nach Bedarf aus.

Option	Bezeichnung
Name	Ein eindeutiger Name für Ihr Zertifikat.
Benachrichtigung bei Ablauf	Legen Sie fest, wer benachrichtigt werden soll, wenn das Zertifikat abläuft.
Tage vor Ablauf benachrichtigen	Senden Sie eine E-Mail-Benachrichtigung an Ihren Zertifikatmanager, bevor Ihr Zertifikat abläuft.
Aktiv	Aktiviert die Verwendung des Zertifikats für Tokenanforderungen.
Typ	Der Typ des Zertifikats, das Sie hochladen.
Läuft in Tagen ab	Anzahl der Tage, bis das Zertifikat abläuft.
Schlüsselspeicher-Passwort	Das dem Zertifikat zugeordnete Passwort.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
Kurzbeschreibung	

3. Klicken Sie auf **Absenden**.

Konfigurieren Sie einen JWT-Signaturschlüssel

Erstellen Sie einen JSON-Web-Token-Signaturschlüssel (JWT), um ihn Ihrem Java KeyStore-Zertifikat (JKS) zuzuweisen.

Vorbereitungen

Erforderliche Rolle: admin

Hinweis: Wenn Sie dem Header als Teil des JWT-Schlüssels „SHA-1-Fingerabdruck des X.509-Zertifikats int (**x5t**)“ hinzufügen möchten, müssen Sie das Formular konfigurieren und das Feld **„SHA-1-Fingerabdruck des X.509-Zertifikats int (x5t)“ hinzufügen**.

Prozedur

1. Navigieren zu **Alle** > **System-OAuth** > **JWT-Schlüssel**an.
2. Füllen Sie das Formular nach Bedarf aus.

Option	Bezeichnung
Name	Ein eindeutiger Name für Ihre JWT-Schlüssel-signaturkonfiguration.
Signatur-Schlüsselspeicher	Der beim Signieren des JWT angegebene Schlüsselspeicher.
Schlüssel-ID	Die Schlüssel-ID (untergeordnetes Element) hilft zu identifizieren, welcher Schlüssel verwendet wird, wenn mehrere Schlüssel zum Signieren von Token verwendet werden. **Hinweis:** Wenn Sie dieses Feld konfigurieren, wird die Schlüssel-ID-Anforderung in das JWT aufgenommen. Wenn Sie dieses Feld nicht konfigurieren, hat Ihr JWT keinen Schlüssel-ID-Anspruch.
Signaturalgorithmus	Der zum Signieren mit dem JWT-Schlüssel zu verwendende Algorithmus. RSA 256 ist der einzige verfügbare Algorithmus.
Signaturschlüssel-Passwort	Das dem Signaturschlüssel zugeordnete Passwort.
Aktiv	Geben Sie an, dass der JWT-Schlüsselalias aktiv von einem JWT-Anbieter referenziert wird.

3. Klicken Sie auf **Absenden**.

Erstellt einen JWT-Provider mit einem JWT-Signaturschlüssel

Fügen Sie Ihrer -Instanz ServiceNow einen JSON-Web-Token-Provider (JWT) hinzu.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur
1. Navigieren zu **Alle** > **System-OAuth** > **JWT-Anbieter**an.
2. Füllen Sie das Formular aus, und klicken Sie auf **Absenden**.

Option	Bezeichnung
Name	Ein eindeutiger Name für Ihre JWT-Provider-Konfiguration.
Ablaufintervall (Sek.)	Die Lebensdauer der vom JWT-Anbieter generierten Token in Sekunden.
Signierkonfiguration	Die anzuwendende JWT-Signaturschlüsselkonfiguration ServiceNow.

JSON-Web-Token (JWT) generieren
Erstellen Sie ein JSON-Web-Token (JWT) für die sichere Darstellung von Ansprüchen zwischen zwei Parteien in Now Platform.

Die GlideJWT-API ist eine bereichsbezogene, skriptfähige API, die ein JWTgeneriert. Vor dem Generieren des JWT sind drei Argumente erforderlich:

- Sys_id des JWT-Providers
- Serialisierter JSON-Header
- Serialisierte JSON-Nutzlast

Es gibt zwei JWT-API-Skripts, JWTTokenInternal und JWTTokenRestricted, die Sie beim Konfigurieren eines JWT-Providers verwenden können. Mit dem Skript JWTTokenRestricted können Administratoren konfigurieren, wer ein JWT generieren kann. Das JWTTokenInternal-Skript ist schreibgeschützt und ermöglicht nur angemeldeten Benutzern das Generieren eines JWT.

So generieren Sie ein JWT:

- JWT-Schlüssel mit einem gemeinsam genutzten Schlüssel (HMAC) oder einem Signaturschlüsselspeicher (RSA) erstellen
- Ordnen Sie der Signaturkonfiguration einen JWT-Provider zu, der auf einen JWT-Schlüssel verweist

Sie können die -API verwenden, um Ihr Token zu erstellen.

Sie können standardmäßige und anwenderdefinierte Ansprüche verwenden, wenn Sie einen JWT-Anbieter konfigurieren. Sie können dynamische Header- und Nutzlastansprüche als Teil dergenerateJWT-API-Signatur übergeben.

Beispielskript zum Testen der API:

```
var jwtAPI = new sn_auth.GlideJWTAPI();
var headerJSON = {  "kid": "a1234"  };
var header = JSON.stringify(headerJSON);

var payloadJSON = { "jti": "testjti", "iss": "testiss", "sub":
 "testsub" };
var payload = JSON.stringify(payloadJSON);
```

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
var jwtProviderSysId = "7a40dde2d5303300964fb7c8f3c14ab5";
var jwt = jwtAPI.generateJWT(jwtProviderSysId, header, payload);

gs.info("JWT:" + jwt);
```

OAuth-Client-APIs

Die OAuth-Client-API bietet Methoden zum Anfordern und Widerrufen von OAuth-Token.

Der OAuth-Client stellt die folgenden Klassen bereit:

- GlideOAuthClient : Methoden zum Anfordern und Widerrufen der Aktualisierungs- und Zugriffstoken.
- GlideOAuthClientRequest : Methoden zur Verarbeitung von Client-Anforderungen.
- GlideOAuthClientResponse : Methoden zur Verarbeitung von Client-Antworten.
- GlideOAuthToken : Methoden zum Abrufen des Zugriffstokens und Informationen zum Zugriffstoken.

Sie können auch die OAuthUtil-Skripteinbindung anpassen, um die Anforderungsparameter abzufangen und die Antworten von externen OAuth-Anbietern zu analysieren.

Wenn Sie OAuth-Klassen in einem bereichsbezogenen Skript verwenden, verwenden Sie den Namespace-Bezeichner `sn_auth`.

OAuth-Parameter für die Unterstützung von Standardprofilen

Für das Standardprofil-Feature ist ein Parametersatz erforderlich, den Sie mit dem API *`setParameter()`* zur Angabe des OAuth-Anforderers, eines Kontexts für die Anforderung und des Anbieterprofils verwenden können.

Im OAuth-Provider-Szenario müssen drei Parameter festgelegt werden, die dem OAuth-Provider mitteilen, welches OAuth-Profil standardmäßig verwendet werden soll. Wenn diese drei Parameter festgelegt sind, wird das Zugriffs-Token in der Instanzdatenbank gespeichert. Verwenden Sie die Parameter mit *`GlideOAuthClientRequest`*.

OAuth-Parameter für die Unterstützung von Standardprofilen

Parameter	Beschreibung
`oauth_requestor`	Die sys_id des Objekts. Dies kann ein Benutzerdatensatz oder ein E-Mail-Account sein.
`oauth_requestor_context`	Deskriptor, der den Kontext für den OAuth-Anforderer bereitstellt. Verwenden Sie als bewährte Methode den Namen der Tabelle, in der das Objekt `oauth_requestor` gespeichert wird.
`oauth_provider_profile`	Die sys_id des OAuth-Profildatensatzes, der der Standard ist (siehe OAuth-Profil angeben).

Sie müssen keine Parameter zum Festlegen von Grant-Typ und Gültigkeitsbereich verwenden, da die Werte im OAuth-Profildatensatz konfiguriert sind. Wenn Sie die Parameter nicht verwenden, können Sie die GlideOAuthClientRequest-API-Methoden *`setScope`* und *`setGrantType`* verwenden. Weitere Informationen finden Sie unter setScope und setGrantType .

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

JWT-Unterstützung für den privaten Schlüssel für OAuth 2.0-Clientauthentifizierung

Support für JWT-Unterstützung für OAuth 2.0-Clientauthentifizierung.

Die JWT-Client-Authentifizierung für den privaten Schlüssel ist eine Authentifizierungsmethode, die von Clients zur Authentifizierung beim Autorisierungsserver verwendet werden kann, wenn sie den Tokenendpunkt verwenden.

Bei diesem Authentifizierungsmechanismus können sich nur Clients authentifizieren, die einen öffentlichen Schlüssel registriert und ein JWT mit diesem Schlüssel signiert haben.

Das JWT muss ERFORDERLICHE Anspruchswerte enthalten und kann OPTIONALE Anspruchswerte enthalten. Weitere Informationen zu den Anspruchswerten, die für das JWT für die `Private_key_jwt-` Authentifizierung erforderlich sind, finden Sie im Abschnitt „Client-Authentifizierung“ in der OpenID Connect-Core- Dokumentation.

Hinweis: Das Authentifizierungstoken muss als Wert des Parameters „client_assertion“ gesendet werden. Der Wert des Parameters „ **client_assertion_type“** muss `urn:ietf:params:oauth:client-assertion-type:jwt-bearer lauten`.

Plugins, die für die OAuth 2.0-Client-Authentifizierung mit JWT-Token erforderlich sind:

- **OAuth 2.0 (com.snc.platform.security.oauth)**: Dieses Plugin ist auf neuen und aktualisierten Instanzen aktiv. Wenn das Plugin in Ihrer Instanz nicht aktiv ist, können Sie es aktivieren.
- **Integration – Single Sign-on-Installationsprogramm für mehrere Anbieter (com.snc.integration.sso.multi.installer)**: Für OIDC-basierten Single Sign-on-Anwendungsfall.

Sie können die OAuth 2.0-Clientauthentifizierung mit Private Key JWT für Folgendes verwenden:

- OIDC-basiertes Single Sign-on
- Ausgehende OAuth-Integrationen

Konfigurieren Sie Private Key JWT für OIDC-basiertes SSO

Konfigurieren Sie Private Key JWT für OIDC-basierte SSO-Integrationen.

Vorbereitungen

Erforderliche Rolle: admin

Sie müssen die folgenden Aufgaben ausführen, bevor Sie Private Key JWT für OIDC-basiertes SSO auswählen.

- Laden Sie das Java-Schlüsselspeicher-Zertifikat hoch: Fügen Sie Ihrer Instanz ein JKS-Zertifikat hinzu, um die JWT-Client-Authentifizierung zu aktivieren.
- Konfigurieren Sie einen JWT-Signaturschlüssel: Erstellen Sie einen JWT-Signaturschlüssel, der Ihrem Java KeyStore-Zertifikat (JKS) zugewiesen werden soll.

  Hinweis: Wenn Sie dem Header als Teil des JWT-Schlüssels „SHA-1-Fingerabdruck des X.509-Zertifikats int (**x5t**)“ hinzufügen möchten, müssen Sie das Formular konfigurieren und das Feld **„SHA-1-Fingerabdruck des X.509-Zertifikats int (x5t)“ hinzufügen**.

- Erstellt einen JWT-Provider mit einem JWT-Signaturschlüssel: Fügen Sie Ihrer Instanz ServiceNow] einen JWT-Anbieter hinzu.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um einen JWT-Schlüssel für den OIDC-basierten Identitätsanbieter einzubeziehen, müssen Sie:

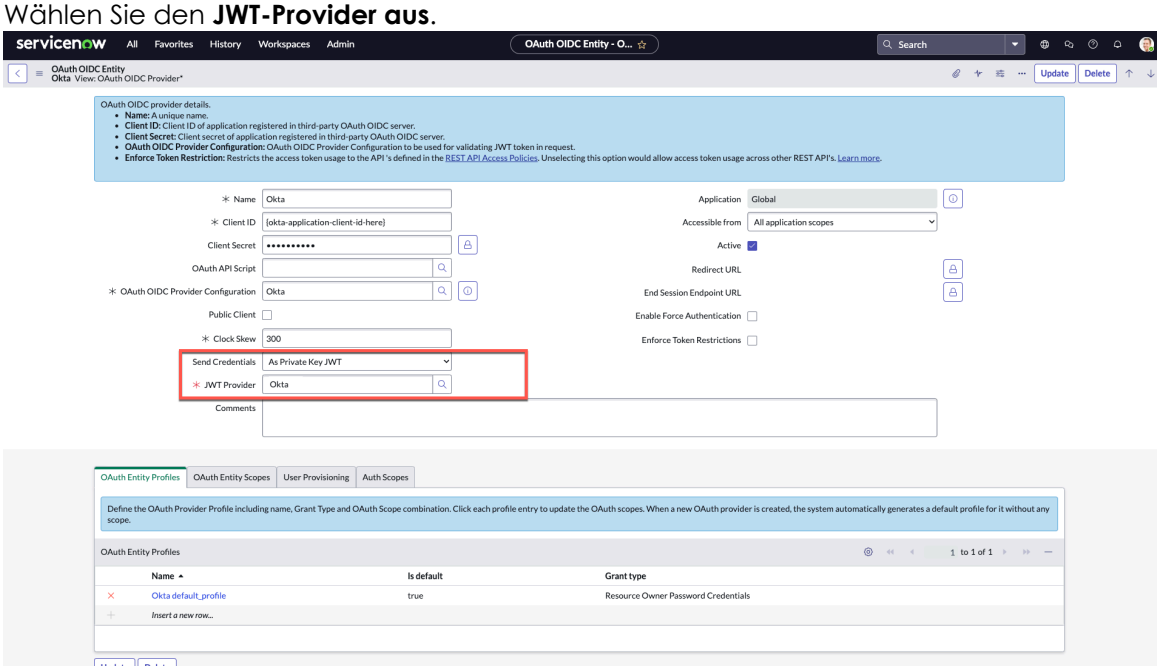
- Installieren Sie das Plugin **Integration – Single Sign-on-Installationsprogramm für mehrere Anbieter** (`com.snc.integration.sso.multi.installer`).
- Aktivieren Sie die Eigenschaften für **SSO-Eigenschaften für mehrere Anbieter**. Weitere Informationen finden Sie unter Eigenschaften, Tabellen und Skripts für Mehrfachanbieter-SSO.
- Erstellen Sie einen OIDC-Identitätsanbieter. Weitere Informationen finden Sie unter Eine OpenID Connect-Konfiguration (OIDC) für Single Sign-on (SSO) erstellen.

Prozedur

1. Navigieren zu **Alle** > **System-OAuth** > **Applikationsregistrierung**an.
2. Wählen Sie den von Ihnen erstellten OIDC-Identitätsanbieter aus.
3. Wählen Sie oben im Formular aus **Konfigurieren** > **Formulardesign**an.

   Hinweis: Sie müssen dem Formular die Felder „ **Anmeldeinformationen senden**“ und „ **JWT-Provider** “ hinzufügen, um das Private Key JWT für OIDC-basierte Identitätsanbieter-Authentifizierungsanforderungen zu verwenden.

4. Wählen Sie **Als privater Schlüssel JWT** für Anmeldeinformationen senden aus.
5. Wählen Sie den **JWT-Provider aus**.



Wenn sich der Anwender authentifiziert, bietet die Authentifizierungsseite Optionen für die Anmeldung über Okta.

Konfigurieren Sie das JWT mit dem privaten Schlüssel für Outbound OAuth

Konfigurieren Sie Private Key JWT für ausgehende OAuth-Integrationen.

Vorbereitungen

Erforderliche Rolle: admin

Bevor Sie Private Key JWT für ausgehende OAuth-Integrationen konfigurieren, müssen Sie die folgenden Aufgaben ausführen:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Laden Sie das Java-Schlüsselspeicher-Zertifikat hoch: Fügen Sie Ihrer Instanz ein JKS-Zertifikat hinzu, um die JWT-Client-Authentifizierung zu aktivieren.
- Konfigurieren Sie einen JWT-Signaturschlüssel: Erstellen Sie einen JWT-Signaturschlüssel, der Ihrem Java KeyStore-Zertifikat (JKS) zugewiesen werden soll.

  Hinweis: Wenn Sie dem Header als Teil des JWT-Schlüssels „SHA-1-Fingerabdruck des X.509-Zertifikats int (**x5t**)“ hinzufügen möchten, müssen Sie das Formular konfigurieren und das Feld **„SHA-1-Fingerabdruck des X.509-Zertifikats int (x5t)“ hinzufügen**.

- Erstellt einen JWT-Provider mit einem JWT-Signaturschlüssel: Fügen Sie Ihrer Instanz ServiceNow] einen JWT-Anbieter hinzu.

Prozedur

1. Navigieren zu **Alle** > **System-OAuth** > **Applikationsregistrierung** und klicken Sie dann auf **Neu**.
2. Klicken Sie auf der Interceptor-Seite **auf Verbindung mit einem OAuth-Drittpartei-Anbieter herstellen**, und füllen Sie das Formular aus.

   Hinweis: Sie müssen dem Formular die Felder **Anmeldeinformationen senden** und **JWT-Provider** hinzufügen, um für ausgehende OAuth-Authentifizierungsanforderungen das Private Key JWT zu verwenden.

Feld	Beschreibung
Name	Eindeutiger Name für die OAuth-Drittpartei-Verbindung.
Client-ID	Die Client-ID der Anwendung, die beim OAuth-Server des Drittanbieters registriert ist.
Geheimer Clientschlüssel	Der geheime Clientschlüssel der beim OAuth-Server des Drittanbieters registrierten Anwendung.
OAuth-API-Skript	Das Skript, das zum Anpassen von Anforderungen und Antworten an den externen OAuth-Provider verwendet wird.
Logo-URL	Die Logo-URL der OAuth-Anwendung.
Standardgewährungstyp	Wählen Sie: **Client-Anmeldeinformationen**: Die Client-ID und der geheime Clientschlüssel, die beide zum Abrufen des Zugriffstokens verwendet werden. Bei dieser Methode werden keine Aktualisierungstoken bereitgestellt.
Lebensdauer von Aktualisierungstoken	Zeit in Sekunden, die das Aktualisierungstoken gültig ist. Die Standardzeit beträgt 8.640.000 Sekunden.
Öffentlicher Client	Ermöglicht öffentlichen Clients, PKCE für eine Autorisierung anzufordern. **Hinweis:** Sie können nur Autorisierungscode als *Default Grant type* verwenden, wenn PKCE aktiviert ist.
Kommentare	Fügen Sie Kommentare zur OAuth-App hinzu.
Anwendung	Anwendung und Umfang, die diesen Datensatz enthalten.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zugänglich von	Machen Sie diese App aus allen Anwendungsbereichen oder nur aus diesem Bereich zugänglich.
Aktiv	Aktivieren Sie das Kontrollkästchen, um die App zu aktivieren.
Autorisierungs-URL	Der OAuth-Autorisierungscode-Endpunkt.
Token-URL	Der OAuth-Servertoken-Endpunkt.
Token-Sperr-URL	Der OAuth-Servertoken-Rücknahme-Endpunkt.
Umleitungs-URL	Der OAuth-Callback-Endpunkt. Wenn leer, generiert die Instanz automatisch einen Eintrag.
Gegenseitige Authentifizierung aktivieren	Aktivieren Sie das Kontrollkästchen, um die gegenseitige Authentifizierung für die Tokenanforderung und den Widerruf zu verwenden. Für diese Funktion muss ein Profil für die gegenseitige Authentifizierung angegeben werden.
Anmeldeinformationen senden	Wählen Sie: **Als Private Key JWT**
JWT-Anbieter	Details zum JWT-Provider. Sie können die Suche verwenden, um den JWT-Anbieter auszuwählen.

Das System erstellt in der Tabelle „Anwendungsregistrierungen“ [oauth_entity] einen Datensatz mit dem Typ „OAuth-Provider“, der für die Authentifizierung des privaten JWT-Schlüssels verwendet werden kann.

Erstellen Sie eine ausgehende REST-Nachricht

Erstellen Sie eine ausgehende REST-Nachricht, um die Instanz als Autorisierungsserver zu autorisieren.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **System-Webservices** > **Ausgehend** > **REST-Nachricht** und klicken Sie dann auf **Neu**.
2. Füllen Sie die Formularfelder für den OAuth-Anwendungsdatensatz wie in beschrieben aus. Beachten Sie die folgenden Feldwerte:
   - **Endpunkt**: URL der Instanz, die der Autorisierungsserver ist.
   - **Authentifizierungstyp**: **OAuth 2.0**.
   - **OAuth-Profil**: OAuth-Profil, das Sie für den Clientserver erstellt haben.
3. Klicken Sie im REST-Nachrichtendatensatz auf **OAuth-Token abrufen**.
4. Authentifizieren Sie sich mit der Instanz, die das Token bereitstellt. Die Methode hängt von der Single Sign-on-Integration ab.
   Mögliche Verwendung:
   - Benutzername und Passwort, mit denen Sie sich bei der Instanz authentifizieren.
   - Anwendername und Passwort für den IdP, falls aktiviert. Klicken Sie auf **Externe Anmeldung verwenden**, um auf den IdP-Anmeldebildschirm zuzugreifen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Um automatisch zur IdP-Anmeldeseite umgeleitet zu werden, müssen Sie die Systemeigenschaft „glide.authenticate.external“ festlegen.

- Ihr Code, wenn MFA aktiviert ist.

5. Klicken Sie auf **Zulassen** oder **Ablehnen**, um die Autorisierung abzuschließen und die Token auszustellen.
   Der folgende Prozess ist in Flow zur Gewährung des OAuth-Autorisierungscodesbeschrieben.

Selbstregistrierung bei Instanz ServiceNow .

Verwenden Sie die Selbstregistrierung externer Anwender, um das Onboarding einer großen Anzahl externer Anwender für Ihre Instanz durchzuführen. Diese Funktion verbessert die Identitätsverifizierung, um die Kunden-Experience zu verbessern, und unterstützt häufig verwendete Registrierungs-Flows.

Untersuchen



Lernen Sie die Funktionen und den Geschäftsnutzen der Selbstregistrierung kennen.

Aktivieren



Erfahren Sie, wie Sie die externe Selbstregistrierung aktivieren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren



Konfigurieren Sie die Selbstregistrierung.

Aktivieren



Machen Sie sich mit den Eigenschaften der Selbstregistrierung vertraut.

Selbstregistrierung erkunden

Verwenden Sie die Selbstregistrierung externer Anwender, um das Onboarding einer großen Anzahl externer Anwender für Ihre Instanz durchzuführen. Diese Funktion verbessert die Identitätsverifizierung, um die Kunden-Experience zu verbessern, und unterstützt häufig verwendete Registrierungs-Flows.

Die Selbstregistrierung externer Anwender ermöglicht es einer großen Gruppe von Anwendern, sich ohne Hilfe eines Administrators bei einer App ServiceNow zu registrieren. Zum Beispiel könnte sich eine Universität mit einer großen Gruppe von Studenten, die einen Parkplatz auf dem Campus benötigen, bei der Campus-Park-App registrieren. Jeder Kursteilnehmer erhält eine begrenzte Anzahl spezifischer Berechtigungen für das Parken und absolviert einen automatisierten Registrierungsprozess. Dieses System könnte eine Parkplatznummer generieren, die für jeden Studenten eindeutig ist, und sicherstellen, dass er/sie einen Parkplatz hat.

Ein Selbstregistrierungs-Flow besteht aus einer anwenderdefinierten App ServiceNow, in diesem Fall einer Campus-Park-App. Nach der Konfiguration einer App mit den erforderlichen Tabellen konfiguriert ein Administrator die Registrierung, einschließlich eines Vorregistrierungs-Flows, einer Feldzuordnung, einer Zuordnung nach der Registrierung, eines Captcha-Elements, einer Rollenzuordnung und eines Flows nach der Registrierung.

Die Selbstregistrierung für externe Anwender wirdaktiviert

Wenn Sie die Administratorrolle innehaben, können Sie das Plugin „External User Self-Registration“ (com.snc.external_user_self_registration) aktivieren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie das Plugin über die Filterkriterien und die Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.

3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: `Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.`

   Nach Abschluss der Installation wird eine Meldung angezeigt.

Externe Rollen in der Selbstregistrierung

Um zu verhindern, dass externen Anwendern versehentlich Zugriff gewährt wird, können Sie allen externen Anwendern die Rolle snc_external zuweisen.

Externen Anwendern, die sich selbst registrieren, muss die Rolle „snc_external“ mit den geringsten Berechtigungen zugewiesen werden. Die Rolle snc_external gibt an, dass es sich um einen für Ihre Organisation externen Benutzer handelt, der keinen Zugriff auf Ressourcen hat, solange der Rolle snc_external oder anderen Rollen, die die Rolle snc_external übernehmen, keine expliziten Zugriffsrechte über ACLs erteilt wurden.

Standardmäßig haben Benutzer mit der Rolle snc_external keinen Zugriff auf:

- Scripted REST API-Ressourcen, die nicht als extern markiert sind
- Tabellen ohne die Rolle, die die Rolle snc_external oder public erbt
- Ressourcen, die keine Datensatztypen sind, z. B. Prozessoren und UI-Seiten ohne die Rolle snc_external oder eine Rolle, die die Rolle snc_external erbt
- Platform Analytics-Dashboards.

Ab dem Paris-Release müssen Sie eine Ausschlusslisteigenschaft aktivieren, um die explizite Zuweisung von snc_external-Rollen zu erzwingen. Informationen zum Aktivieren der Eigenschaft finden Sie unter Zuweisungen zukünftiger interner Rollen für externe Benutzer verhindern .

Konfiguration einer Benutzerregistrierungskonfiguration für externe Benutzer

Erstellen Sie einen Konfigurationsdatensatz für die Anwenderregistrierung, um den Onboarding-Prozess externer Anwender für anwenderdefinierte ServiceNow -Anwendungen zu beschleunigen. Dieses Formular leitet externe Anwender durch den Prozess der Selbstregistrierung.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Erforderliche Rolle: admin
- Die Selbstregistrierung für externe Anwender wirdaktiviert

Prozedur

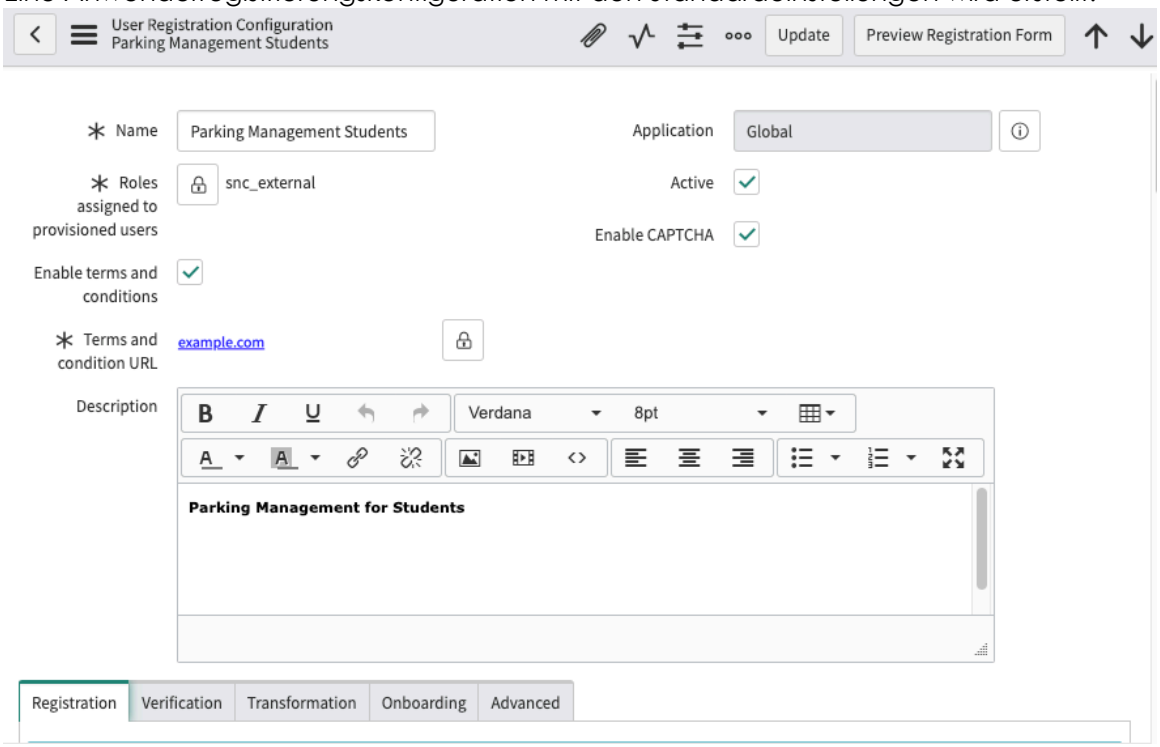
1. Navigieren zu **Alle** > **Selbstregistrierung für externe Anwender** > **Konfigurationen der Anwenderregistrierung** und klicken Sie auf **Neu**.
2. Füllen Sie die Felder des Formulars aus.

Konfigurationsformular für die Anwenderregistrierung

Feld	Beschreibung
Name	Name des Registrierungsformulars. Eine Studentenparkplatzregistrierung könnte z. B. Parkplatzmanagement-Studenten sein.
Bereitgestellten Anwendern zugewiesene Rollen	Rollen, die den bereitgestellten Anwendern zugewiesen sind. Die angegebenen Rollen müssen die Rolle „`snc_external`“ erweitern oder enthalten. Die angegebene Rolle kann auch die Rolle „ `snc_external`“ sein. Bei externen Benutzern muss für jede Rolle ein `snc_external vorhanden` sein, um einen externen Benutzer zu notieren. Wenn Sie über vorkonfigurierte Rollen verfügen, sollten die Rollen zugänglich sein, wenn Sie die Rollen entsperren und nach Benutzern suchen.
Nutzungsbedingungen aktivieren	Option zum Hinzufügen einer URL mit Nutzungsbedingungen zur Registrierungsseite.
URL der Nutzungsbedingungen	Die öffentlich zugängliche URL, die die Nutzungsbedingungen des Registrierungsformulars enthält. Dieses Feld wird nur angezeigt, wenn **Nutzungsbedingungen aktivieren** ausgewählt ist.
Beschreibung	Die Beschreibung des Registrierungsformulars. Dieses Feld wird nur angezeigt, wenn Sie die Konfiguration speichern oder absenden. In diesem Feld können Sie weitere Informationen zum Registrierungsformular hinzufügen. **Hinweis:** Sie können nur eine Beschreibung hinzufügen, nachdem Sie eine Anwenderregistrierungskonfiguration gespeichert oder aktualisiert haben.
Anwendung	Anwendung, die diesen Datensatz enthält. Die Anwendung wird automatisch auf `Global`festgelegt.
Aktiv	Option, die die Konfiguration der Anwenderregistrierung aktiviert. Diese Option ist standardmäßig ausgewählt.
CAPTCHA aktivieren	Option zum Hinzufügen eines CAPTCHA zum Registrierungsformular. Der Standard-CAPTCHA-Anbieter ist Google reCAPTCHA. **Hinweis:** Führen Sie zum Aktivieren von CAPTCHA für die Anwenderregistrierung die Schritte in Konfigurieren Sie Google reCAPTCHA für die Selbstregistrierung externer Anwenderaus.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf **Absenden**.
   Eine Anwenderregistrierungskonfiguration mit den Standardeinstellungen wird erstellt.



4. Wahlweise: Konfigurieren Sie die Registerkarte **Registrierung**, um Felder und deren Reihenfolge anzuzeigen:

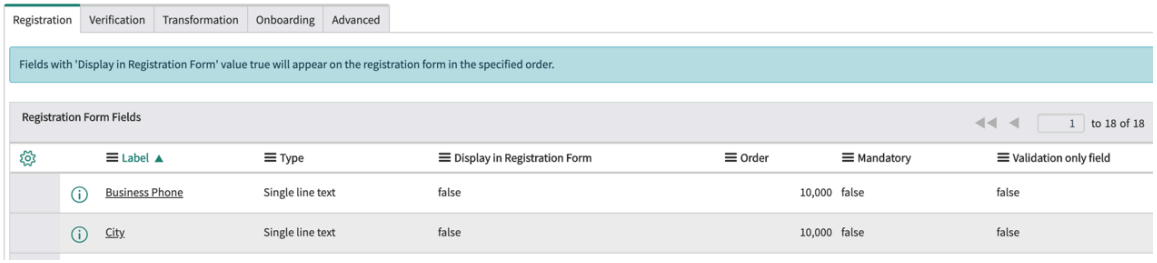
Registrierungsformularfelder

Spalte	Beschreibung
Im Registrierungsformular anzeigen	Legen Sie für jedes Feld, das Sie anzeigen möchten, den Wert `true fest`.
Bestellung	Legen Sie eine Ordnungszahl für die Anzeige von Feldern in Ihrem Formular fest.
Obligatorisch	Legen Sie für jedes Feld, das Sie als Pflichtfeld festlegen möchten, den Wert `True fest`.
Nur Validierungsfeld	Legen Sie ein beliebiges Feld fest, das Sie nur zur Validierung verwenden möchten. Beispiel: Registrierungscode.

Sie können die Standardformularfelder anzeigen oder dem Registrierungsformular anwenderdefinierte Formularfelder hinzufügen. Weitere Informationen finden Sie unter Standardfelder des Registrierungsformulars.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Registrierung“.



Sie können auch anwenderdefinierte Registrierungsformularfelder hinzufügen. Weitere Informationen finden Sie unter Fügen Sie ein anwenderdefiniertes Registrierungsformularfeld hinzu.

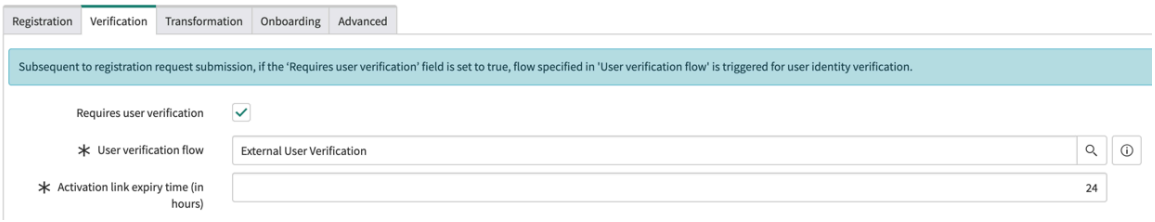
5. Wahlweise: Konfigurieren Sie die Registerkarte **Verifizierung**, um die Identität der registrierten Benutzer zu überprüfen. Wenn der Flow zur Benutzerverifizierung ausgelöst wird, wird ein Aktivierungslink an die registrierte E-Mail-Adresse des Benutzers gesendet.

Felder der Registerkarte „Verifizierung“.

Feld	Beschreibung
Anwenderverifizierung erforderlich	Option zum Auslösen eines Subflows zur Anwenderverifizierung, der nach der Anwenderregistrierung ausgeführt wird. Der Subflow dient der Verifizierung der Anwenderidentität.
Flow der Anwenderverifizierung	Der zum Überprüfen der Identität des Benutzers verwendete Subflow. Der Subflow wird nur ausgelöst, wenn Sie die Benutzerüberprüfung aktivieren. (Optional) Der Subflow „ **Verifizierung durch externe Anwender** “ ist standardmäßig verfügbar. Sie können eine Kopie des Standard-Subflows in Flow Designer erstellen und entsprechend Ihren Anforderungen ändern. Weitere Informationen finden Sie unterFlow Designer . **Hinweis:** Um eine Vorschau des Subflows „ **Verifizierung externer Anwender** “ auf einer neuen Registerkarte anzuzeigen, verwenden Sie die folgenden Verknüpfungen: ◦ Macintosh: Befehlstaste + Klicken ◦ Windows: Strg + Klicken
Ablaufzeit des Aktivierungslinks (in Stunden)	Die Anzahl der Stunden, nach der ein Aktivierungslink abläuft. Der Standardwert ist 24.

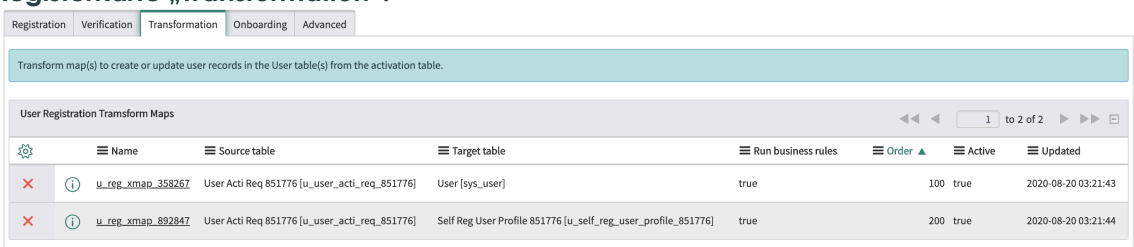
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Verifizierung“.



6. Wahlweise: Konfigurieren Sie die Registerkarte **Transformation** für die Zuordnung von selbstregistrierten Benutzern und aktivierten Benutzern.
   Es gibt zwei Transformationszuordnungen (u_reg_xmap_[number]), die die registrierten Benutzer automatisch aus der Tabelle „User Acti Req [number]“ der Tabelle „Selbstregistrierte Anwender [number]“ zuordnen. Sie können eine Kopie dieser Standardtransformationszuordnungen erstellen und die Zuordnung entsprechend Ihren Anforderungen ändern. Weitere Informationen finden Sie unter Transformationszuordnungen .

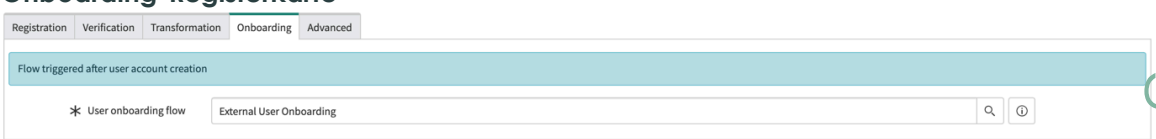
Registerkarte „Transformation“.



7. Konfigurieren Sie die Registerkarte Onboarding, um **Subflows** für das Onboarding aktivierter Benutzer auszulösen.
   Der Standard **-Subflow für das Onboarding externer Anwender** sendet eine E-Mail an den Anwender, die einen Link zum Zurücksetzen des Passworts enthält. Sie können eine Kopie des Standard-Subflows erstellen und entsprechend Ihren Anforderungen ändern.

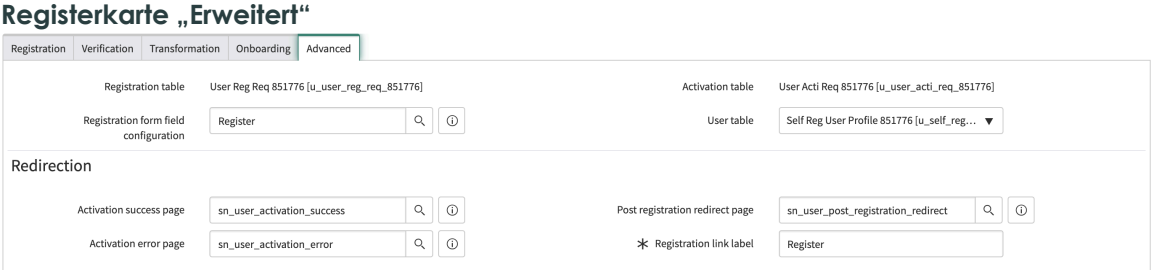
   Hinweis: Wenn der **Subflow** „Onboarding externer Anwender“ ausgelöst wird, sendet der Subflow eine E-Mail an den Benutzer, die einen Link zum Zurücksetzen des Passworts enthält.

Onboarding-Registerkarte



8. Wahlweise: Konfigurieren Sie die Registerkarte **Erweitert**, um Benutzertabellen und Umleitungsseiten des Registrierungsformulars zuzuordnen.

Registerkarte „Erweitert“



Automatische Übersetzung

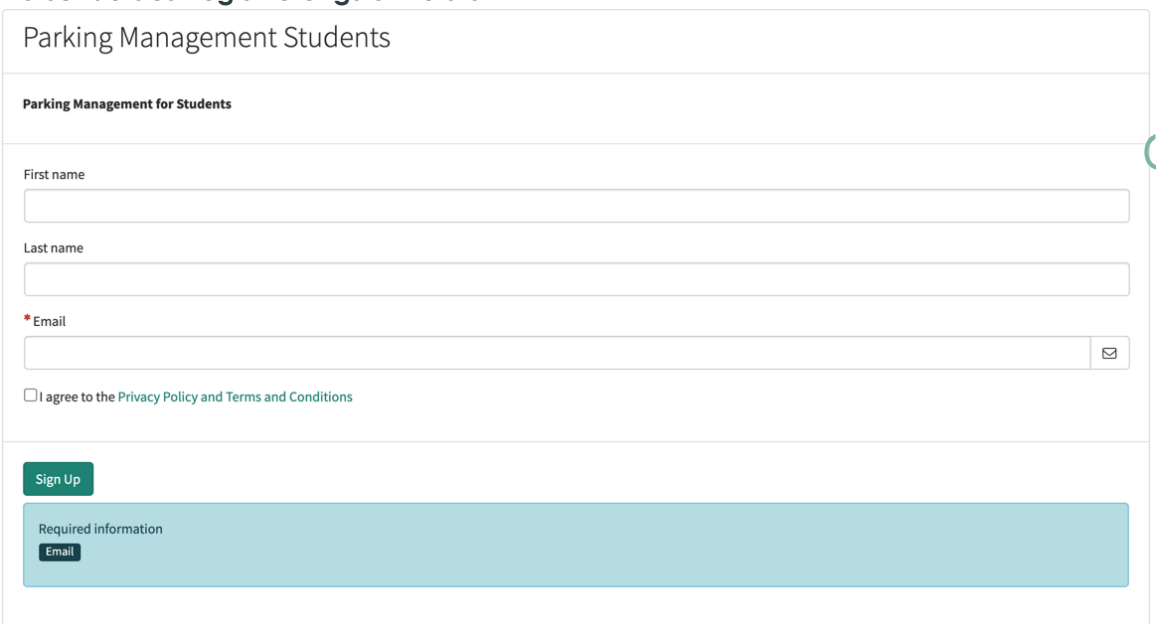
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Erweitert“

Feld	Beschreibung
Registrierungstabelle	Name der Tabelle, in der die Informationen zum Registrierungsformular gespeichert werden.
Konfiguration des Registrierungsformularfelds	Der Datensatz, der dem Registrierungsformular im Datensatzersteller zugeordnet ist
Aktivierungstabelle	Bezeichnung und Name der Tabelle, die für die Anwenderaktivierung verwendet wird. Die Aktivierungstabelle enthält Datensätze der Benutzer, die die Verifizierung abgeschlossen haben.
Anwendertabelle	Bezeichnung und Name der Anwenderprofiltabelle.
Aktivierungserfolgsseite	Die Seite, auf die ein Anwender nach erfolgreicher Aktivierung umgeleitet wird.
Aktivierungsfehlerseite	Die Seite, auf die ein Benutzer umgeleitet wird, wenn die Aktivierung fehlschlägt.
Weiterleitungsseite nach Registrierung	Die Seite, auf die der Anwender nach der Registrierung weitergeleitet wird.
Registrierungslinkbezeichnung	Der Schaltflächenname, der für die Registrierung im Serviceportal verwendet wird. Der Standardwert ist Register.

Während Sie Änderungen vornehmen oder nachdem Sie alle Änderungen in der Konfiguration der Anwenderregistrierung vorgenommen haben, können Sie über die Schaltfläche Vorschau des **Registrierungsformulars** eine Vorschau der Änderungen im Registrierungsformular anzeigen.

Vorschau des Registrierungsformulars



© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie Google reCAPTCHA für die Selbstregistrierung externer Anwender

Um den Service Google reCAPTCHA zu verwenden, müssen Sie ein API-Schlüsselpaar von Google anfordern und dann die zugehörigen Systemeigenschaften konfigurieren.

Vorbereitungen

- Fordern Sie ein API-Schlüsselpaar (einen Site-Schlüssel und ein Geheimnis) von Google unter https://www.google.com/recaptcha an.
- Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**an.
2. Suchen Sie nach den folgenden Eigenschaften, und legen Sie die Werte fest:

Eigenschaft	Wert
glide.user.registration.google.recaptcha.secret	Das Geheimnis autorisiert die Kommunikation zwischen der -Anwendung und dem reCAPTCHA-Server. Typ: password2
glide.user.registration.google.recaptcha.site_key	Der Websiteschlüssel, der zum Aufrufen des reCAPTCHA-Service auf Ihrer Registrierungsseite verwendet wird. Typ: Zeichenfolge
glide.user.registration.captcha.widget	Die Sys_ID des Captcha-Widgets. Typ: Zeichenfolge

Standardfelder des Registrierungsformulars

Sie können die Standardfelder des Registrierungsformulars verwenden oder anwenderdefinierte Registrierungsformularfelder erstellen.

Felder des Registrierungsformulars

Die folgenden Formularfelder werden standardmäßig im Registrierungsformular hinzugefügt.

Feldbezeichnung	Typ
Geschäftstelefon	Einzeiliger Text
Stadt	Einzeiliger Text
Land	Auswahlfeld
EDU-Status	Auswahlfeld

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feldbezeichnung	Typ
Wird verwendet, um Mitarbeiter, Studenten und Besucher zu unterscheiden. **Hinweis:** Dieses Feld ist nützlich, wenn das Registrierungsformular für eine Bildungseinrichtung gilt.	
E-Mail	E-Mail
Vorname	Einzeiliger Text
Geschlecht	Einzeiliger Text
Telefon (privat)	Einzeiliger Text
Sprache	Auswahlfeld
Nachname	Einzeiliger Text
Zweiter Vorname	Einzeiliger Text
Mobiltelefon	Einzeiliger Text
Name	Einzeiliger Text
Präfix Titel des Anwenders. Zum Beispiel: Mr. , Dr. usw.	Auswahlfeld
Bundesland/Region	Einzeiliger Text
Straße	Breite einzeilige Textzeile
Titel: Stellenbezeichnung	Auswahlfeld
Postleitzahl	Einzeiliger Text

Hinweis: Sie können die Standardfelder des Registrierungsformulars nicht löschen.

Fügen Sie ein anwenderdefiniertes Registrierungsformularfeld hinzu

Im Formular zur Selbstregistrierung von Benutzern können Sie anwenderdefinierte Felder hinzufügen.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Selbstregistrierung für externe Anwender** > **Konfigurationen der Anwenderregistrierung**an.
2. Öffnen Sie den Datensatz für die erforderliche Anwenderregistrierungskonfiguration.
3. Navigieren Sie zum Ende des Abschnitts „Registrierungsformularfelder“, und klicken Sie auf **Neue Zeile einfügen...**.
4. Geben Sie den Feldnamen unter der **Spalte** Bezeichnung ein, und klicken Sie auf das Häkchen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine neue Zeile mit den Standardwerten wird hinzugefügt. Sie können das anwenderdefinierte Registrierungsformularfeld entsprechend Ihren Anforderungen konfigurieren.

Feldspalten des Registrierungsformulars

Spalte	Beschreibung
Bezeichnung	Der Feldname, der im Registrierungsformular angezeigt wird.
Typ	Der Typ des Anwenderoberflächenelements. Nachstehend die unterstützten Typen: ◦ Einzeiliger Text ◦ E-Mail ◦ Datum ◦ Datum/Uhrzeit ◦ Ja/Nein ◦ Breite einzeilige Textzeile ◦ Multiple-Choice ◦ Auswahlfeld
Im Registrierungsformular anzeigen	Option zum Anzeigen des Felds im Registrierungsformular.
Bestellung	Die Reihenfolge, in der die Formularfelder auf dem Registrierungsformular angezeigt werden. Das Feld mit dem niedrigsten Wert für die Reihenfolge wird zuerst angezeigt und das Feld mit dem Wert für die höchste Reihenfolge wird zuletzt angezeigt. Der Standardwert ist 10.000.
Obligatorisch	Option, ein Feld auf dem Registrierungsformular obligatorisch zu machen.
Nur Validierungsfeld	Option, ein Feld nur zu Validierungszwecken zu verwenden. Beispiel: Registrierungscode. Bei Festlegung auf „wahr“ wird dieses Feld nicht in der Benutzertabelle (sys_user) gespeichert.

5. Speichern oder aktualisieren Sie die Änderungen.

Aktivieren der Selbstregistrierung von externen Anwendern für Serviceportal

Ermöglichen Sie externen Benutzern die Registrierung für ServiceNow-Apps über Serviceportal.

Vorbereitungen

Erforderliche Rolle: admin

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Service Portal** > **Portale**an.
2. Öffnen Sie einen Portaldatensatz.
3. Füllen Sie im Formular das **Konfigurationsfeld für die Registrierung externer Anwender** aus.

   Wählen Sie eine Anwenderregistrierungskonfiguration aus.
4. Klicken Sie auf **Aktualisieren**.

Ergebnisse

Das Anmelde-Widget enthält einen Link zum Registrierungsformular, das Sie zuvor konfiguriert haben.

Verifiziert die Anforderungen zur Selbstregistrierung von Anwendern

Nachdem sich ein Benutzer über Serviceportal registriert hat, wird dem Modul Registrierungsanforderungen ein Benutzerdatensatz hinzugefügt. Sie können die Liste der registrierten Benutzer anzeigen, die sich erfolgreich bei Serviceportal registriert haben.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Selbstregistrierung für externe Anwender** > **Anforderungen zur Registrierung**an.
   Die Liste der Benutzerdatensätze wird angezeigt.
2. (Optional) RÜberprüfen Sie die einzelnen Benutzerdatensätze, und ändern Sie sie entsprechend Ihren Anforderungen. Sie können beispielsweise den Status eines Benutzerdatensatzformulars **Ausstehend** in **Verarbeitet**ändern.

Tokenbasierte Authentifizierung (Anwenderanmeldungen)

Verbessern Sie den Sicherheitsmechanismus für Benutzer, um mithilfe der tokenbasierten Authentifizierung auf ein Netzwerk zuzugreifen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeitlich begrenzte Authentifizierung



Die tokenbasierte Authentifizierung ist ein Protokoll, mit dem Anwender ihre Identität überprüfen und im Gegenzug ein eindeutiges Zugriffstoken erhalten.

Es hilft, den Sicherheitsmechanismus für den Zugriff von Benutzern auf ein Netzwerk zu verbessern.



der Digest-Token-Authentifizierung

Die Digest-Token-Authentifizierung übergibt Benutzeranmeldeinformationen und ein Digest-Token in einem unverschlüsselten HTTP-Header.

Zeitlich begrenzte Authentifizierung

Unterstützen Sie die zeitlich begrenzte Authentifizierung für Ihre Instanz ServiceNow.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Untersuchen



Lernen Sie die Funktionen und den Geschäftsnutzen der zeitlich begrenzten Authentifizierung kennen.

Aktivieren



Erfahren Sie, wie Sie die zeitlich begrenzte Authentifizierung aktivieren.

Lernprogramm: Zeitlich begrenzte Authentifizierung



© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeitbegrenzte Authentifizierung erkunden

Unterstützen Sie die zeitlich begrenzte Authentifizierung für Ihre Instanz ServiceNow.

Hinweis: Die zeitlich begrenzte Authentifizierung ist sehr spezifisch für die Instanz ServiceNow, die anwenderdefinierten Links für Anwender können nur innerhalb von ServiceNowerstellt werden.

Administratoren können die linkbasierte Authentifizierung in der Instanz ServiceNow konfigurieren. Der konfigurierte Link kann per E-Mail oder SMS für den Benutzer freigegeben werden, und der Benutzer kann sich mit diesen Links bei der Instanz anmelden.

Die Anmeldung bei Instanz mit diesem Authentifizierungsschema wird über Richtlinien der adaptiven Authentifizierung gesteuert, die in der Instanz ServiceNow konfiguriert sind.

Mit der zeitbasierten Authentifizierung können Sie:

- Administratoren können die linkbasierte Authentifizierung so konfigurieren, dass sie innerhalb einer Ablaufzeit verwendet wird.
- Das Anwendungsteam kann Nonce abrufen, die mit dem Link für das spezifische Konfigurationselement verwendet werden soll, indem eine verfügbar gemachte skriptfähige API verwendet wird. Die Linkgenerierung wird vom Anwendungsteam übernommen.
- Das Anwendungsteam kann den Link generieren und über einen vorhandenen Kanal an den Benutzer senden.
- Benutzer mit dem Link können sich einmalig und innerhalb der in der Konfiguration angegebenen Ablaufzeit bei der Instanz anmelden.
- Administratoren können Rollen mit geringen Berechtigungen für das Authentifizierungsschema konfigurieren.
- Administratoren können MFA für das Authentifizierungsschema als zweiten Faktor für die Authentifizierung mit dem TLA-Link erzwingen.

Aktivieren Sie die zeitlich begrenzte Authentifizierung

Die zeitlich begrenzte Authentifizierung wird über das Plugin „Integration – Single Sign-on-Installationsprogramm für mehrere Anbieter“ aktiviert.

Vorbereitungen

Erforderliche Rolle: admin

Hinweis: Die zeitlich begrenzte Authentifizierung ist sehr spezifisch für die Instanz ServiceNow, die anwenderdefinierten Links für Anwender können nur innerhalb von ServiceNowerstellt werden.

Prozedur

1. Navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie das Plugin „Zeitlich begrenzte Authentifizierung“ (*com.snc.authenticate.time_limited_authentication*) mithilfe der Filterkriterien und der Suchleiste.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.

3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: `Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.`

   Nach Abschluss der Installation wird eine Meldung angezeigt.

Zeitlich begrenzte Authentifizierung mit SMS – Twilio Lernprogramm

Richten Sie eine zeitlich begrenzte Authentifizierung mit MFA-Faktoren wie SMS mithilfe von Twilioein.

Vorbereitungen

Erforderliche Rolle: admin

Erforderliche Plugins:

- *com.snc.authenticate.time_limited_authentication* (Zeitlich begrenzte Authentifizierung)
- *com.snc.authentication.sms_mfa* (Mehrstufige Authentifizierung mit SMS)

Hinweis: Die zeitlich begrenzte Authentifizierung (Time begrenzte Authentifizierung, TLA) ist sehr spezifisch für die Instanz ServiceNow, die anwenderdefinierten Links für Anwender können nur innerhalb von ServiceNowerstellt werden.

Die bereitgestellten Tutorial-Anweisungen ermöglichen es dem Administrator, eine linkbasierte Anmeldung mit SMS als zweiten Faktor (MFA) für Benutzer mit einer bestimmten Rolle bereitzustellen.

Nach einer erfolgreichen Konfiguration generiert das System einen Link und gibt den Link dann über den Benachrichtigungskanal (E-Mail/SMS) für den Benutzer frei. Durch Klicken auf den Link wird der Anwender aufgefordert, das OTP anzugeben, das an den Faktor „E-Mail“ oder „SMS“ gesendet wird, basierend auf der Anwenderrolle (Konfiguration).

Hinweis:

- Auf TLA muss immer MFA folgen, und MFA muss vom Administrator mithilfe der adaptiven Authentifizierung für die TLA-Anmeldung aktiviert werden. Weitere Informationen zum Konfigurieren von MFA mit adaptiver Authentifizierung finden Sie unter MFA-Kontext (Multifaktor-Authentifizierung)..
- TLA sollte für Anwender mit eingeschränkten Berechtigungen verwendet werden.

Prozedur

1. Eine Twilio -Konfiguration wird erstellt.
   a. Erstellen Sie einen Twilio -Test-Account. Weitere Informationen finden Sie unter Twilio an.
   b. Navigieren zu **Alle** > **Benachrichtigen** > **Administration** > **Twilio Direct-Konfiguration**an.
   c. Geben Sie die **Account-SID** und das **Auth-Token** (erstellt aus Twilio) an, und speichern Sie den Datensatz.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Sie können Ihre eigene Anbieterkonfiguration erstellen und diese für TLA verwenden. In diesem Beispiel ist dies Twilio. Weitere Informationen zum Erstellen einer MFA-Anbieterkonfiguration finden Sie unter Konfigurieren Sie den MFA-Anbieter.

2. Zeitbegrenzte Authentifizierung (TLA) wird konfiguriert und aktiviert.

   a. Navigieren zu **Alle** > **Konfigurationsdatensätze für zeitlich begrenzte Authentifizierung** und klicken Sie auf **Neu**.

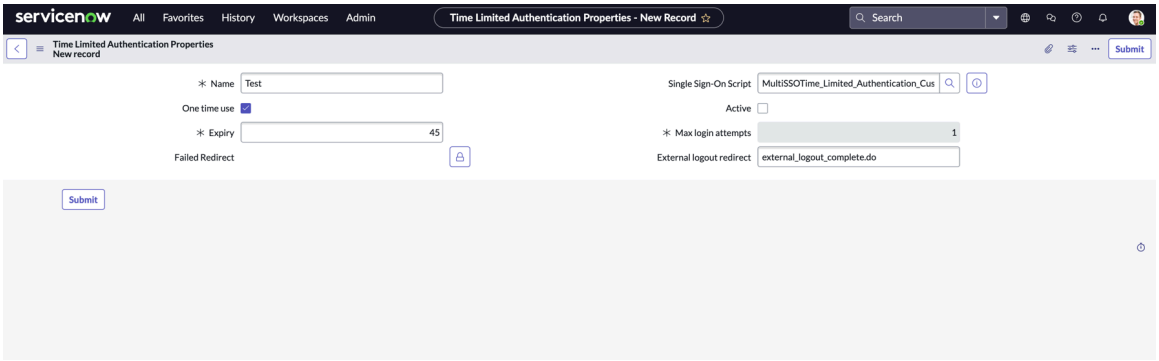
   b. Füllen Sie die Felder im Formular aus.

Eigenschaften der zeitlich begrenzten Authentifizierung

Feld	Beschreibung
Name	Name des Datensatzes.
Einmalige Nutzung	Aktivieren Sie diese Option, um den TLA-Link einmal zu verwenden.
Ablauf	Geben Sie die Sekunden für den Linkablauf an. Der Standardwert ist 45 Minuten.
Fehlerhafte Umleitung	Geben Sie die URL ein, um Anwender nach einer fehlgeschlagenen Authentifizierung umzuleiten.
Single Sign-on-Skript	Details des SSO-Skripts, das Sie verwenden möchten.
Aktiv	Option zum Aktivieren der Konfiguration.
Max. Anmeldeversuche	Geben Sie die Anzahl der Versuche an, die mit dem generierten TLA-Link für die Anmeldung zulässig sind. Deaktivieren Sie das Kontrollkästchen **Einmalige Verwendung**, um die maximale Anzahl von Versuchen anzugeben.
Weiterleitung für externe Abmeldung	Geben Sie die URL ein, um Anwender nach der Abmeldung umzuleiten.

   c. Klicken Sie auf **Absenden**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



d. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Administration** > **Eigenschaften** und aktivieren Sie die Eigenschaft **SSO mit mehreren Providern** aktivieren und anschließend **Speichern**.

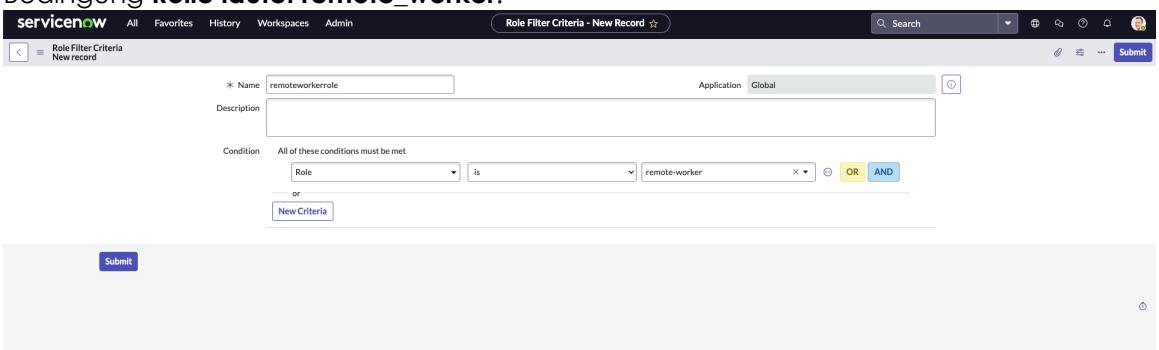
3. Mithilfe der Kontextrichtlinie der Nachauthentifizierung wird TLA nur für eine bestimmte Benutzerpersona zugelassen.

a. Navigieren Sie zu **Rollen** und erstellen Sie eine Rolle. Beispiel: remote_worker.

b. Erstellen Sie einen Anwender mit einer gültigen E-Mail-ID und Mobiltelefonnummer. Informationen zum Erstellen eines Benutzers finden Sie unter Benutzer erstellen .

c. Weisen Sie dem Anwender die Rolle zu. Informationen zum Zuweisen der Rolle an den Benutzer finden Sie unter Einem Benutzer eine Rolle zuweisen .

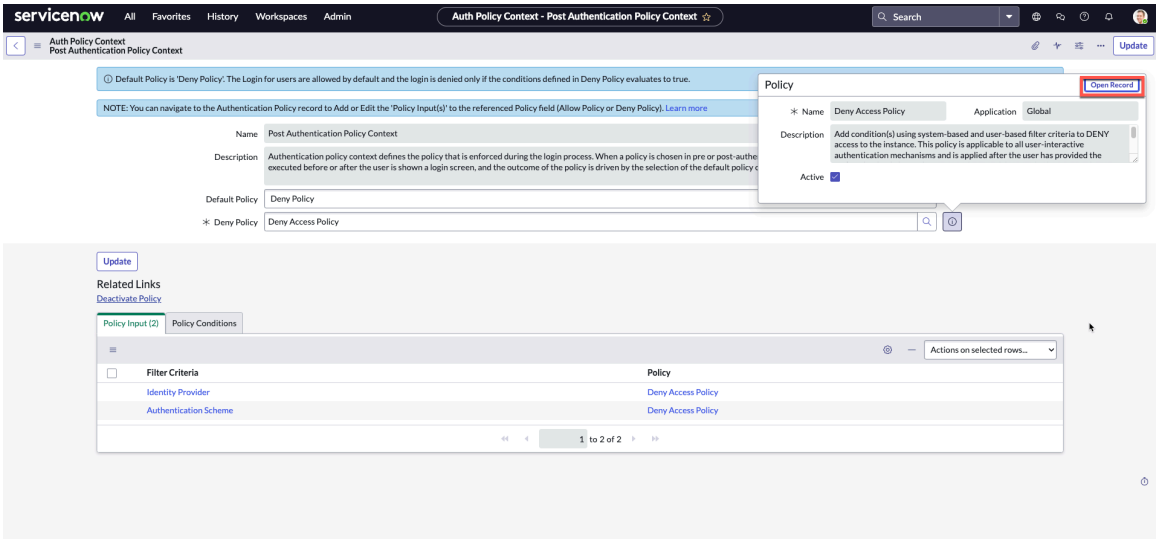
d. Um ein Rollenfilterkriterium zu erstellen, navigieren Sie zu **Alle** > **Adaptive Authentifizierung** > **Rollen-Filterkriterien**, erstellen Sie einen neuen Filter **remoteworkerrole** und die Bedingung **Rolle lautet remote_worker**.



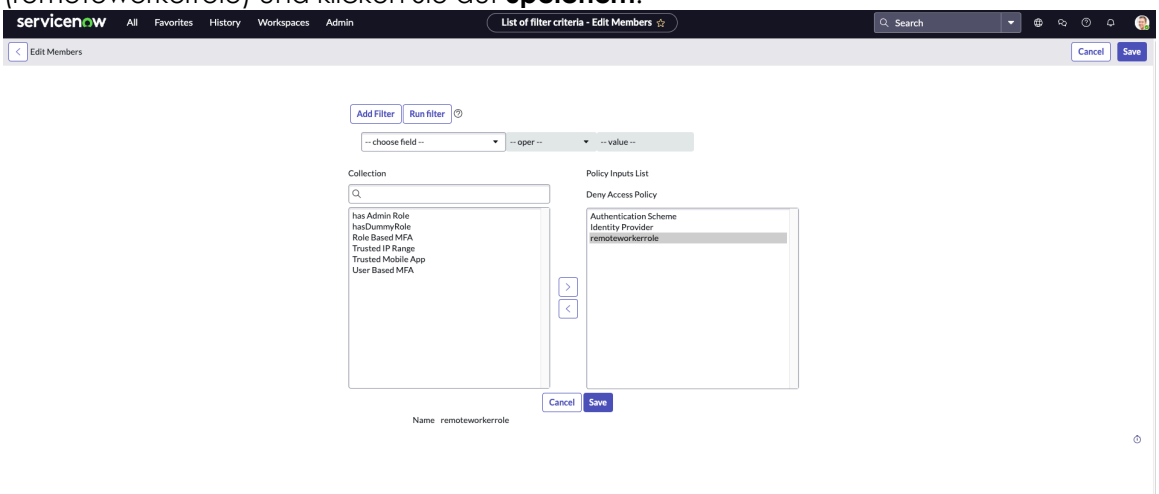
e. Um eine Richtlinienbedingung basierend auf dem Ablehnungsrichtlinienkontext basierend auf den IdP- und Rollenfilterkriterien hinzuzufügen, navigieren Sie zu **Alle** > **Adaptive Authentifizierung** > **Kontext nach der Authentifizierung**an.

f. Klicken Sie auf das Informationssymbol, und **öffnen Sie den Datensatz**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



g. Klicken Sie in der Richtlinieneingabe auf **Bearbeiten**, fügen Sie die Rolle hinzu (remoteworkerrole) und klicken Sie auf **Speichern**.



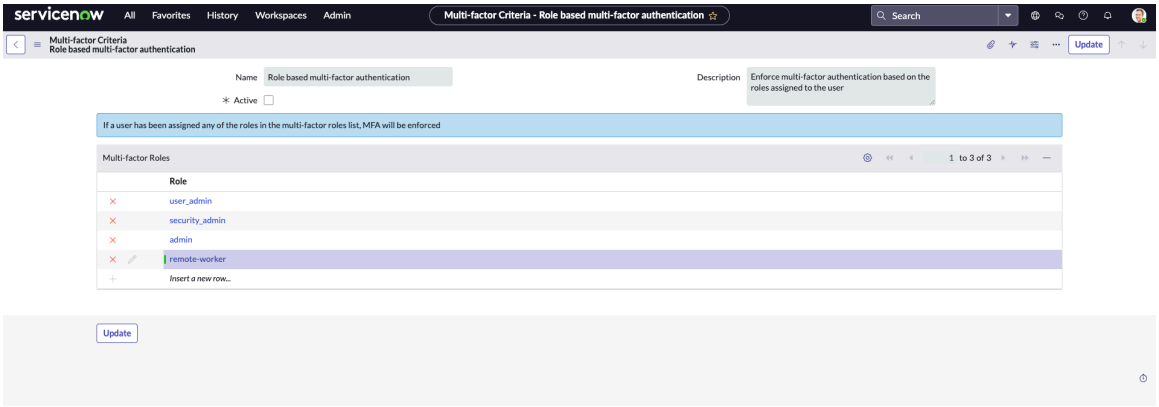
h. Fügen Sie in Richtlinienbedingung die Bedingung für die Richtlinieneingabe hinzu, und **übermitteln** Sie den Datensatz.

4. Konfigurieren der Richtlinie für die Step-Up-Authentifizierung – MFA-Kontext.

a. Navigieren zu **Alle** > **Multifaktor-Kriterien**an.

b. Wählen Sie die **Rollenbasierte Multifaktor-Authentifizierung aus**, und fügen Sie die Rolle im Abschnitt Multifaktor-Rollen und unter **Aktualisieren**hinzu. In diesem Beispiel: **remote_worker**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

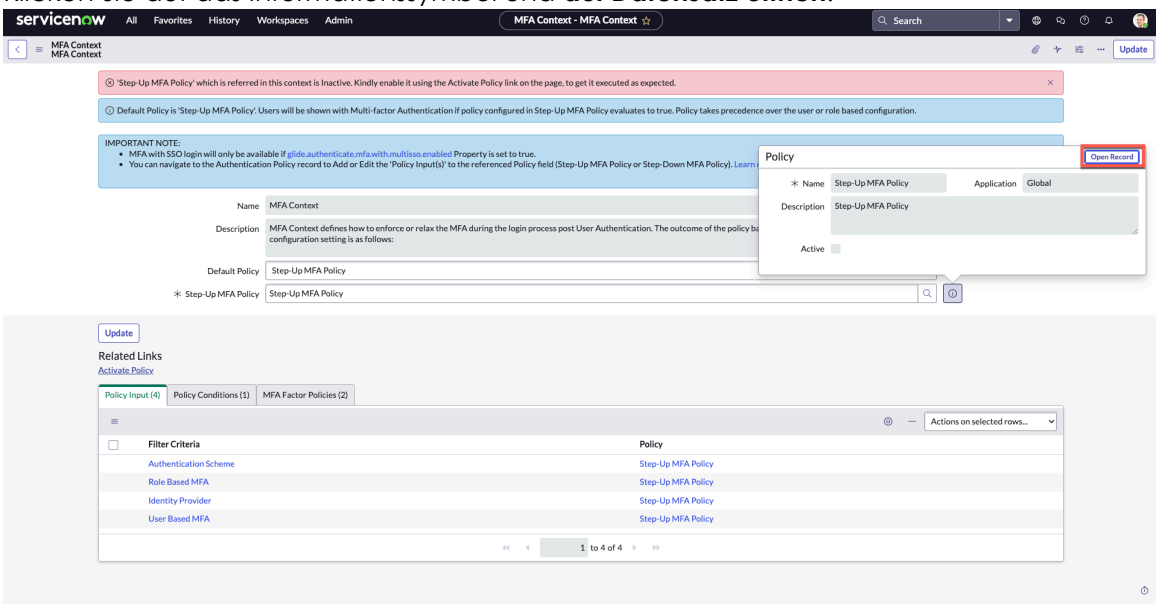


c. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **MFA-Kontext**an.

d. Stellen Sie Folgendes sicher:

- Das Feld „Standardrichtlinie“ ist **Step-up-MFA-Richtlinie**
- Die Step-Up-MFA-Richtlinie ist die **Step-Up-MFA-Richtlinie**

e. Klicken Sie auf das Informationssymbol und **auf Datensatz öffnen**.



f. Klicken Sie im Formular „Step-Up-MFA-Richtlinie“ unter Richtlinieneingaben auf **Bearbeiten**.

g. Fügen Sie der Liste die **rollenbasierte Multifaktor-Authentifizierung** hinzu, und **speichern Sie**. In diesem Beispiel die **Rolle remoteworker**.

h. Klicken Sie in der **Richtlinienbedingung auf MFA erzwingen, wenn rollenbasierte oder anwenderbasierte MFA-Einstellungen auf true festgelegt sind**.

i. Stellen Sie auf der Seite MFA erzwingen, wenn rollenbasierte oder anwenderbasierte MFA-Einstellungen „wahr“ sind, stellen Sie sicher, dass **rollenbasierte** MFA auf „ **wahr**“ festgelegt ist.

5. MFA wird erzwungen, um SMS als MFA-Faktorrichtlinie zu verwenden.

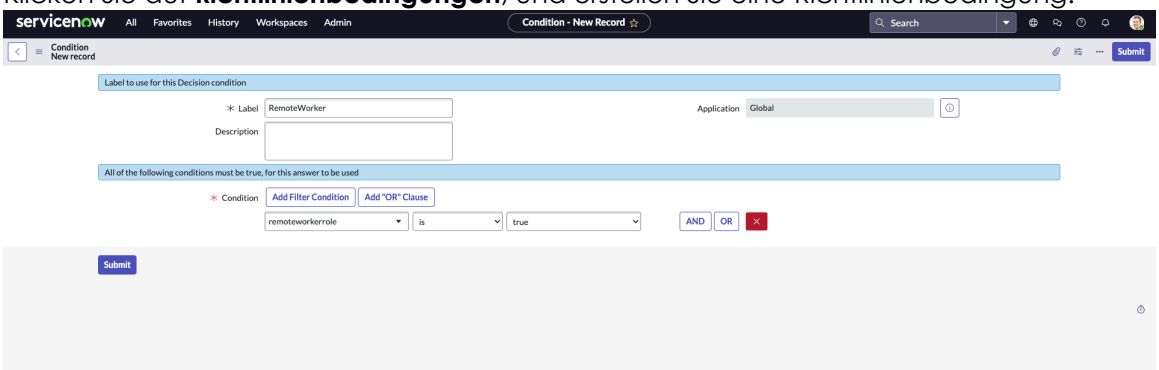
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **MFA-Kontext**an.

b. Klicken Sie auf der Seite „MFA-Kontext“ auf **MFA-Faktorrichtlinien** und anschließend auf die Richtlinie **SMS OTP als MFA-Faktorrichtlinie anzeigen**.

c. Klicken Sie auf **Bearbeiten**, und fügen Sie in den **Richtlinieneingaben** die **Rolle remoteworker**hinzu.

d. Klicken Sie auf **Richtlinienbedingungen**, und erstellen Sie eine Richtlinienbedingung.



e. Klicken Sie auf **Absenden**.

Der TLA-Link, der generiert und für die Anwender freigegeben wird, denen die Rolle **remoteworker** zugewiesen ist, wird so heraufgestuft, dass er den SMS-Code als zweiten Faktor für die Anmeldung bei der Instanz verwendet.

6. Die anderen erforderlichen Eigenschaften werden aktiviert.

a. Navigieren zu **Alle** > **Multi-Faktor-Authentifizierung** > **Eigenschaften**an.

b. Aktivieren Sie die folgenden Kontrollkästchen.

- **Multi-Faktor-Authentifizierung aktivieren**
- **Aktivieren Sie die Multifaktor-Authentifizierung mit SSO**

c. Speichern Sie den Datensatz.

d. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Authentifizierungsrichtlinien** > **Eigenschaften**an.

e. Aktivieren Sie das Kontrollkästchen **Authentifizierungsrichtlinie** aktivieren.

f. Speichern Sie den Datensatz.

7. Generieren eines TLA-Links – Beispiel.

a. Navigieren zu **Alle** > **Systemdefinition** > **Skripts: Hintergrund**an.

b. Verwenden Sie die folgende API, indem Sie die Anwender-Sys-ID und die Konfigurations-ID angeben.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
var tla = neu global.TimeLimitedAuthentication();
gs.info(tla.generateNonce("user_sysid", "config1_sys_id","IAR2"));
```

Hinweis: Die Quelle (IAR2) ist kein obligatorischer Parameter.

c. Der Abfrageparameter wird wie folgt zurückgegeben:
`Nonce=VCeinfboDt0M&glide_sso_id=b3277f1b44351110f8779b5a2d9909f3&user=3b0277d3443511`

d. Erstellen Sie eine URL im folgenden Format:
`https://<instance-url> /login_with_sso.do?uri=<encoded url> &`
`Nonce=2olIQSxdgkjs&glide_sso_id=0c15bf09c3711110c5ec4e483c40dd7a&user=62826bf0371020`

8. Klicken Sie auf die URL. Der folgende MFA-Bildschirm wird zur Anmeldung angezeigt.

Digest-Token-Authentifizierung

Die Digest-Token-Authentifizierung übergibt Benutzeranmeldeinformationen und ein Digest-Token in einem unverschlüsselten HTTP-Header.

Automatische Übersetzung

Untersuchen



Lernen Sie die Funktionen und den Geschäftsnutzen der Digest-Token-Authentifizierung kennen.

Konfigurieren



Erfahren Sie, wie Sie die Digest-Token-Authentifizierung konfigurieren.

Digest-Token-Authentifizierung erkunden

Die Instanz liest den HTTP-Headerwert und vergleicht den berechneten Hash-Wert des Digest-Tokens. Wenn der berechnete Hash-Wert mit dem Digest-Token-Wert übereinstimmt, sucht die Instanz nach einem übereinstimmenden Wert in der Benutzertabelle. Wenn in der Benutzertabelle ein übereinstimmender Wert vorhanden ist, betrachtet die Instanz den Benutzer als vorauthentifiziert und meldet ihn an.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Digest-Token-Authentifizierung ist sicherer als einfache unverschlüsselte HTTP-Header, da jede versehentliche oder beabsichtigte Änderung des unverschlüsselten HTTP-Headers einen anderen Hash-Wert erzeugt. Wenn der Hash-Wert nicht übereinstimmt, verweigert die Instanz dem Benutzer den Zugriff auf die angeforderte Instanz. Dadurch wird verhindert, dass Benutzer versuchen, sich mit den Anmeldeinformationen eines anderen Benutzers anzumelden.

Weitere Informationen zum Ablauf von Digest-Links finden Sie in diesem KB-Artikel .

Hinweis: Verwenden Sie die zeitlich begrenzte Authentifizierung (TLA), um zeitbasierte Ablauflinks zu konfigurieren. Weitere Informationen finden Sie unter Zeitlich begrenzte Authentifizierung.

Integrationsanforderungen

Eine Integration mit der Digest-Token-Authentifizierung erfordert:

- Ein Webserver
- SiteMinder oder eine andere Single Sign-on-Anwendung zur Vorauthentifizierung des Benutzers im lokalen Netzwerk
- Eine Webseite oder ein Portal, die bzw. das Anmeldeinformationen in einem dieser Formate an die Zielinstanz übergibt
  - HTTP-Header
  - URL-Parameter
  - Cookie
- Eine Webseite oder ein Portal, die bzw. das ein Digest-Token erstellt und mithilfe einer dieser Codierungstechniken an die Zielinstanz übergibt
  - SHA1
  - MD5
  - SHA 256 (empfohlen)

Digest-Eigenschaften für Single Sign-on (SSO) für mehrere Provider konfigurieren

Nachdem Sie ein vorhandenes Skript für eine Digest-Installation aktiviert haben, konfigurieren Sie Eigenschaften für SSO mit mehreren Anbietern.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn Sie kein Single Sign-on für mehrere Anbieter verwenden, konfigurieren Sie die Standard-Single Sign-on-Eigenschaften.

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identity Provider**an.
2. Füllen Sie die Felder des Formulars Digest-Eigenschaften aus.

Option	Bezeichnung
Name	Geben Sie den Namen des Digest-Tokens ein.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
Benutzer	Geben Sie das Feld sys_user ein, das die übereinstimmenden Daten für den eingehenden Header enthält.
HTTP-Digest-Headername	Geben Sie den von Ihnen generierten HTTP-Header ein. Beispiel: `DE_USER`.
HTTP-Headername	Geben Sie den HTTP-Header ein, den Sie für Ihr erstelltes Digest-Token generiert haben. Beispiel: `SM_USER`.
Geheime Passphrase	Geben Sie den geheimen Schlüssel ein, der zum Codieren von Digest-Schlüsseln verwendet werden soll. Zum Beispiel `32 oder mehr Zeichen`.
Feld „SSO-Umleitung fehlgeschlagen“	Geben Sie die URL ein, um Anwender nach einer fehlgeschlagenen Authentifizierung umzuleiten.
Weiterleitung für externe Abmeldung	Geben Sie die URL ein, um Anwender nach einer Abmeldung umzuleiten.
Single Sign-on-Skript	Wählen **Sie MultiSSO_DigestToken aus**.
Clienttyp	Wählen Sie den Clienttyp basierend auf dem Typ Ihres Clients aus. Optionen:**IFrame Eingebettet**. **Hinweis:** Wenn das Feld „Clienttyp“ für Ihre Konfiguration erforderlich ist, können Sie das Formular bearbeiten und das Feld hinzufügen. Weitere Informationen finden Sie unter Konfigurieren Sie den Clienttyp für OAuth- und SSO-Datensätze.

3. Klicken Sie auf **Aktualisieren**.
4. Legen Sie den Standardwert für Ihr verarbeitetes Token auf „wahr“ fest.
   Wenn Sie den Standardwert auf „true“ festlegen, wird der dem SSO zugeordnete Systemstandard-Digest-Token-Datensatz überschrieben. Sobald der erste mit Mehrfachanbieter-SSO verbundene IdP-Datensatz aktiviert ist, werden nur Datensätze verwendet, die Mehrfachanbieter-SSO zugeordnet sind.

   Digest-Token-Datensätze, die in der Digest-Eigenschaftentabelle vorhanden sind, können einzeln aufgerufen werden, indem die Sys_ID des IdP angehängt wird. Zum Beispiel ein Digest-Token-Datensatz in der folgenden Authentifizierungs-URL: `https://`<instance_name> .service-now.com/login_with_sso.do? glide_sso_id=<sys_id_of_Digest_token_record> &SM_USER=<user_name> &DE_USER=<digested_token>

Beispiel für Implementierungen des Digest-Tokens

Im Folgenden finden Sie einige Beispiele für die Erstellung eines Digest-Tokens.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für Implementierungen der Digest-Authentifizierung

Digest erstellt mit	Wert des geheimen Schlüssels	Hash-Methode	Beispiel
Java	32 und mehr Zeichen	SHA256	Beispiel für einen Java-Digest-Algorithmus für die Verschlüsselung
C	Wert des Parameters „sharedKey“.	Wert des Parameters „strEncryptionMethod“ (SHA256 oder MD5)	Beispiel C

Beispiel für einen Java-Digest-Algorithmus für die Verschlüsselung

Dieser Java-Algorithmus veranschaulicht das Erstellen eines Digest-Tokens aus einem HTTP-Header.

Dieses Beispiel setzt Folgendes voraus:

- Der Webserver unterstützt Java
- Die Hash-Berechnungsmethode ist SHA1
- Der Wert des geheimen Schlüssels ist abc123
- Der unverschlüsselte HTTP-Headername lautet „user_name“.

Ändern Sie den Java-Code so, dass ein anderer Mechanismus für die Hash-Berechnung verwendet wird (z. B. MD5), und ändern Sie den Wert des geheimen Schlüssels oder den Namen des HTTP-Headers.

```
public class DigestTest
{
    private static final String MAC_ALG = "HmacSHA256";
       fKey  = {32 or more characters};
    public byte[] getDigest(String acct) {
        try {
            byte[] bkey = fKey.getBytes();
            byte[] data = acct.getBytes();
            Mac mac = null;
            try {
                mac = Mac.getInstance(MAC_ALG);
                mac.init(new SecretKeySpec(bkey, MAC_ALG));
            } catch (Exception e) {
                e.printStackTrace();
            }
            byte[] sig = mac.doFinal(data);
            String signature = new String(sig);
            System.out.println("value:" + acct);
            System.out.println("digested value:  " + signature);
            return sig;
        } catch (IllegalStateException e) {
            e.printStackTrace();
        }
        return null;
    }
    public static void main(String[] args) {
        BASE64Encoder encoder = new BASE64Encoder();
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
        DigestTest test = new DigestTest();
        String userName = "user_name";
        System.out.println("base 64 digest username: " +
encoder.encode(test.getDigest(userName)));
    }
}
```

Beispiel C

Diese C-Klasse veranschaulicht das Erstellen eines Digest-Tokens aus drei Eingabeparametern.

- strengEncryptionMethod – listet die Hash-Berechnungsmethode auf (SHA1, SHA256 oder MD5)
- Nachricht: Listet den Wert auf, der in ein Digest-Token konvertiert werden soll
- SharedKey: Listet den geheimen Schlüssel auf

Hinweis: Verwenden Sie einen stärkeren sicheren Hash-Algorithmus wie SHA256 für die Generierung von Digest-Token.

Dieses Beispiel setzt Folgendes voraus:

- Der Webserver unterstützt C
- Anderer Code ruft diese Klasse auf und übergibt die erwarteten Parameter

Beispielcode

```
 private stringdigestData(string strEncryptionMethod , string message ,
string sharedKey ) {
           UnicodeEncoding myUnicodeEncoding  = new UnicodeEncoding
( ) ;

           byte [ ] messageBytes  = System. Text. Encoding. ASCII.
GetBytes (message ) ;
           byte [ ] sharedKeyBytes  = System. Text. Encoding. ASCII.
GetBytes (sharedKey ) ;
           byte [ ] hashedMessage ;

           string b64SHA1Message ;

            if (this. DEBUG ) {
               TextBoxMessage. Text = message ;
               TextBoxSecret. Text = sharedKey ; }

            switch ( (strEncryptionMethod ) )

            { case "SHA1" :

                  HMACSHA1 hmacsha1  = new HMACSHA1 ( ) ;
                  hmacsha1. Key = sharedKeyBytes ;
                  hashedMessage  = hmacsha1. ComputeHash
(messageBytes ) ;
                  b64SHA1Message  = Convert. ToBase64String
(hashedMessage ) ; if (this. DEBUG ) TextBoxDigest. Text = Convert.
ToString (hashedMessage ) ; break ;
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
                case "MD5" :

                   HMACMD5 hmacmd5  = new HMACMD5 (sharedKeyBytes ) ;
                   hashedMessage  = hmacmd5. ComputeHash
(messageBytes ) ;
                   b64SHA1Message  = Convert. ToBase64String
(hashedMessage ) ; if (this. DEBUG ) TextBoxDigest. Text = Convert.
ToString (hashedMessage ) ; break ;

                default :

                   b64SHA1Message  = "Unknown Encryption Method" ;
break ;

             }


           TextBoxBase64. Text = b64SHA1Message ; return
b64SHA1Message ;

         }
```

Webservice – Sicherheit

Erzwingen Sie Sicherheit mit Standardauthentifizierung, gegenseitiger Authentifizierung oder WS-Security.

Machen Sie sich mit der Websicherheit vertraut



Lernen Sie die Funktionen und Geschäftsnutzen der Webservicesicherheit kennen.

Konfigurieren Sie die gegenseitige Authentifizierung



Verwenden Sie die gegenseitige Authentifizierung, um Vertrauen durch den Austausch von SSL-Zertifikaten (Secure Sockets Layer) herzustellen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Webservice-Sicherheit erkunden

Erzwingen Sie Sicherheit mit Standardauthentifizierung, gegenseitiger Authentifizierung oder WS-Security.

Standardauthentifizierung

Um die Standardauthentifizierung bei jeder Anforderung für ein WSDL-Dokument oder beim Veröffentlichen von SOAP-Nachrichten zu erzwingen, können Sie die Eigenschaft *glide.basicauth.required* auf `true` festlegen. In diesem Fall muss jede WSDL- oder SOAP-Anforderung den Header „Autorisierung“ enthalten, wie im Standardauthentifizierungsprotokoll angegeben. Da die Anforderung nicht interaktiv ist, ist der **Autorisierungs** -Header während einer Anforderung immer erforderlich.

Die Bereitstellung von Informationen für die Standardauthentifizierung hat unabhängig davon, ob sie erforderlich sind oder nicht, den Vorteil, dass die Daten, die infolge des Aufrufs des Webservice erstellt oder aktualisiert werden, im Namen des Benutzers erstellt werden, der in den Anmeldeinformationen für die Standardauthentifizierung angegeben ist. Beispiel: Beim Erstellen eines Incident-Datensatzes enthalten die Journalfelder die Anwender-ID des standardmäßigen authentifizierten Anwenders anstelle des standardmäßigen **Gastanwenders**.

Damit der Autorisierungsheader die Kapitalisierungsregeln ignoriert, verwenden Sie die Eigenschaft *glide.security.script.include.name.case.insensitive.list*. Sie können diese Eigenschaft in der Tabelle „Systemeigenschaften“ [sys_properties] ändern und die Skripteinbindungen hinzufügen, die für die Verarbeitung der Authentifizierung erforderlich sind. Standardmäßig weist diese Eigenschaft die folgenden Werte auf:

- BasicAuth
- CustomAuth

Fügen Sie nach Bedarf weitere Skripteinbindungen hinzu.

Um die Basic Authentication bei Verwendung von Perl und der SOAP::Lite-Bibliotheken bereitzustellen, können Sie die folgende Funktion implementieren:

```
sub SOAP :: Transport :: HTTP :: Client :: get_basic_credentials { return
 'user_name' => 'password' ; }
```

- Wenn Sie C# .NET VS 2005 oder älter verwenden, können Sie das Anmeldeinformationsobjekt nutzen, z. B.:

```
System.Net . ICredentials cred  = new System.Net . NetworkCredential
 ( "user_name",  "password" ) ;

service . ServiceNow proxy  = new service . ServiceNow ( ) ;
service . get getService  = newservice . get ( ) ;
service . getResponse getServiceResponse  = new service . getResponse
 ( ) ;

 try {
  proxy . Credentials = cred ;
  getService . sys_id = "bf522c350a0a140701972dbf876f1610" ;
  getServiceResponse  = proxy . get (getService ) ; catch (Exception
 ex ) { }
```

- Wenn Sie C# .NET VS 2008 verwenden, können Sie das ClientCredentials-Objekt nutzen, z. B.:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
Demo_Incident. ServiceNowSoapClient client  = new Test08WebService .
 Demo_Incident . ServiceNowSoapClient ( ) ;
client . ClientCredentials . UserName . UserName = "admin" ;
client . ClientCredentials . UserName . Password = "admin" ;
```

Suchen Sie dann in Ihrer Datei app.config nach Folgendem, und ändern Sie `None` in `Basic`:

```
<transport clientCredentialType= "None" proxyCredentialType= "None"
 realm= "" />
```

- Bei der Verwendung von VB .NET würde das Objekt „Anmeldeinformationen“ folgendermaßen aussehen:

```
Sub Main()
         Dim cred  As New System.Net.NetworkCredential( "user_name",
 "password")

         Dim proxy  As New VB_Democm.incident.ServiceNow
         Dim getIncident  As New VB_Democm.incident. get Dim
 getResponse  As New VB_Democm.incident.getResponse

        proxy.Credentials = cred

        getIncident.sys_id =  "[your sysID here]"

        getResponse = proxy. get(getIncident)

     End Sub
```

Die resultierende Antwort, wenn die Basic Authentication aktiviert ist und keine Anmeldeinformationen angegeben werden, sieht folgendermaßen aus:

```
<html> <head > <title >Apache Tomcat/5.0.28
 - Error report </ title > <style > <!--H1
 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525
D76;font-size:22px;}    H2
 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525
D76;font-size:16px;}    H3
 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525
D76;font-size:14px;}    BODY
 {font-family:Tahoma,Arial,sans-serif;color:black;background-color:whit
e;}    B
 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525
D76;}    P
 {font-family:Tahoma,Arial,sans-serif;background:white;color:black;fo
nt-size:12px;}   A {color : black;}   A.name {color : black;}
   HR {color : #525D76;}--> </ style > </ head > <body > <h1 >HTTP
 Status 401 -\ </ h1 > <HR size = "1" noshade = "noshade" > <p >< b
 >type </ b > Status report </ p > <p >< b >message </ b > <u >< / u
 >< / p > <p >< b >description </ b > <u >This request requires HTTP
 authentication (). </ u >< / p > <HR size = "1" noshade = "noshade" >
 <h3 >Apache Tomcat/5.0.28 </ h3 > </ body > </ html >
```

Konfigurieren der gegenseitigen Authentifizierung

Die gegenseitige Authentifizierung stellt Vertrauen durch den Austausch von SSL-Zertifikaten (Secure Sockets Layer) her.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Während des SSL-Handshake stellt der Server dem Client sein Zertifikat vor. Anschließend kann der Server je nach Konfiguration ein Zertifikat vom Client anfordern. Sowohl der Server als auch der Client führen Zertifikatvalidierungsverfahren durch, um die Authentizität und Integrität der vorgelegten Zertifikate sicherzustellen.

Nach einer erfolgreichen Validierung werden vor dem Initiieren der HTTPS-Verbindung Bestätigungen ausgetauscht.

Administratoren führen die vorbereitenden Arbeiten durch, um den Clientschlüsselspeicher einzurichten und Zertifikate zu generieren, bevor Zertifizierungsanforderungen erfüllt werden.

Warnung: Diese Funktion ermöglicht nur die gegenseitige Authentifizierung bei ausgehenden HTTPS-Verbindungen.

Erstellen des Schlüsselspeichers

Die Instanz unterstützt derzeit das Hochladen einer Java Key Store-Datei, die einen privaten Schlüssel und ein öffentliches Zertifikatpaar enthält. Das öffentliche Zertifikat enthält die vollständige Kette einschließlich des Stammzertifikats.

So richten Sie Ihren Clientschlüsselspeicher ein:

- Sie benötigen ein Zertifikat, das von einer vertrauenswürdigen Zertifizierungsstelle signiert wurde.
- Ihr API-Endpunktanbieter kann Sie beim Generieren des Schlüsselspeichers unterstützen.

Wenn Sie den Schlüsselspeicher generieren müssen, umfasst der Prozess mehrere Schritte unter Verwendung von Befehlen der Befehlszeilenschnittstelle, um eine neue Schlüsselspeicherdatei zu generieren, eine Zertifikatsignaturanforderung (Certificate Signing Request, CSR) zu erstellen und signierte Zertifikate zu importieren. Bevor Sie das primäre Zertifikat Ihrer Domäne importieren, sollten alle Stamm- oder Zwischenzertifikate zuerst importiert werden. Hier ist eine Schritt-für-Schritt-Anleitung:

1. Generieren Sie einen Java-Schlüsselspeicher und ein Schlüsselpaar.

```
keytool -genkey -alias mydomain -keyalg RSA -keystore my.keystore
```

2. Generieren Sie eine CSR für einen vorhandenen Java-Schlüsselspeicher.

```
keytool -certreq -alias mydomain -keystore my.keystore -file
 mydomain.csr
```

3. Senden Sie die CSR an Ihre CA-Signaturstelle, um die Zertifikatdateien zu signieren und zurückzugeben, einschließlich Zwischen- und Stammzertifikaten sowie dem signierten Zertifikat.
4. Importieren Sie ein CA-Zertifikat einer Stamm- oder Zwischenzertifizierungsstelle in einen vorhandenen Java-Schlüsselspeicher.

```
keytool -import -trustcacerts -alias root -file Thawte.crt -keystore
 my.keystore
```

Hinweis: Sie können alle Zertifikate in einer Datei bündeln und importieren. Dies ist die bevorzugte Option. Auf diese Weise können Sie 5 überspringen

```
keytool -import -alias mydomain -file merged.crt -keystore
 my.keystore
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Importieren Sie ein signiertes primäres Zertifikat in einen vorhandenen Java-Schlüsselspeicher.

```
keytool -import -trustcacerts -alias mydomain -file mydomain.crt
 -keystore my.keystore
```

Einrichtung des Schlüsselspeichers

Nachdem der Schlüsselspeicher erstellt wurde, kann er in die Tabelle „Zertifikate“ hochgeladen werden. Auf der **Systemdefinition** > **Zertifikate** Klicken Sie auf **Neu**, und legen Sie die folgenden Felder fest:

- Geben Sie einen **Zertifikatnamen**ein.
- Speichern Sie den Schlüsselspeicher als **Aktiv**.
- Legen Sie den **Typ = Java-Schlüsselspeicher fest**.
- Geben Sie ein **Schlüsselspeicher-Passwort an**. Dies ist das Passwort, das zum Erstellen des Schlüsselspeichers verwendet wurde.

Klicken Sie auf **Absenden**, um den Java Key Store-Eintrag zu erstellen.

Schlüsselspeicher

X.509 Certificate | = Required field — Update | Delete

Attachments: my.keystore [view]

Name:	Key store	Type:	Java Key Store
Active:	☑	Key store password:	••••••••••••••••••••••
Short description:	key store used for mutual authentication		

Angeben eines vertrauenswürdigen Serverzertifikats

Während einer ausgehenden SSL-Verbindung, bei der es sich um einen HTTPS-Webservice-Aufruf handelt, kann ein vom Service Provider bereitgestelltes Zertifikat angegeben werden, das die Gültigkeit des Service Providers während der SSL-Verbindung sicherstellt. Beispiel: Ein Browser, der versucht, eine Verbindung zu einem sicheren Service herzustellen, der sich durch ein Zertifikat identifiziert.

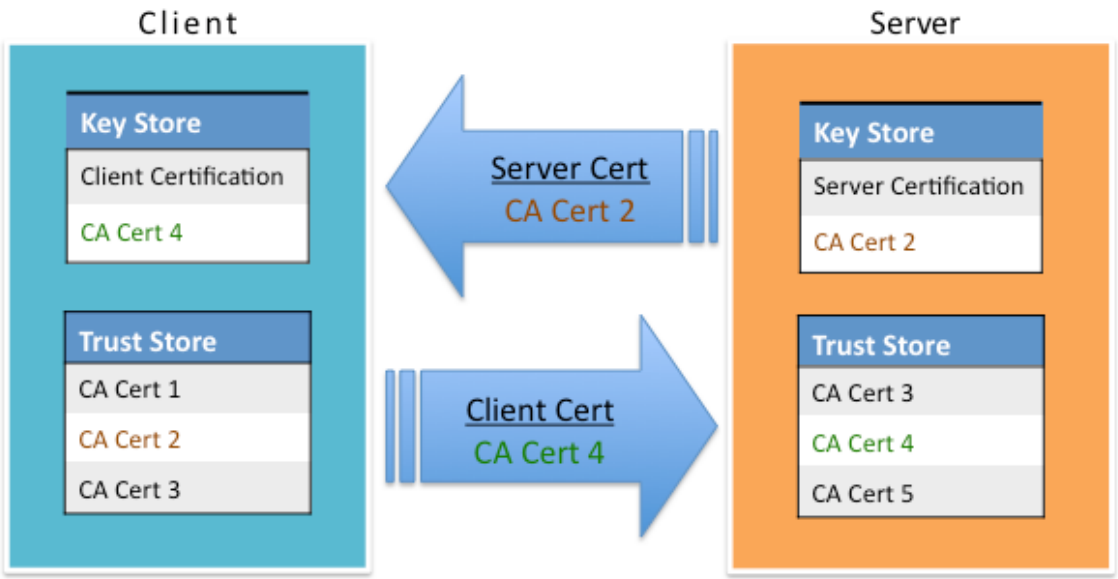
Durch das Hochladen des vertrauenswürdigen Serverzertifikats stellt ServiceNow sicher, dass der Service, mit dem eine Verbindung hergestellt wird, gültig und sicher ist.

Erstellen Sie einen neuen Zertifikateintrag mit dem Typ „Trust Store-Zertifikat“, und hängen Sie ein DER-formatiertes Zertifikat an, oder kopieren Sie das PEM-Format und fügen Sie es in das Feld „ **PEM-Zertifikat** “ ein.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Protokollprofil

Zertifikataustausch



- Wenn ein Client das Serverzertifikat zur Authentifizierung anfordert, wird eine Zertifikatsignaturanforderung (Certificate Signing Request, CSR) generiert.
- Um auf eine CSR zu antworten, generiert der Server zwei eindeutige kryptografische Schlüssel: einen öffentlichen Schlüssel, der zum Verschlüsseln von Nachrichten an den Server verwendet wird, und einen privaten Schlüssel, der zum Entschlüsseln von Nachrichten verwendet wird. Beide Schlüssel werden im Schlüsselspeicher aufbewahrt.
- Schlüssel werden verwendet, um die sicheren Nachrichten des Clients zu entschlüsseln, damit sie vom Server gelesen werden können. Jede ausgehende Verbindung, die über HTTPS hergestellt wird, überprüft die Zertifizierung, indem sie den Schlüsselspeicher überprüft, seine öffentliche Zertifizierung anbietet und die Truststore-Zertifikate verwendet, um das gegenseitige Vertrauen zu überprüfen.
- Um die sichere Verbindung zwischen Client und Server herzustellen, gleicht der Server das Zertifikat mit dem entsprechenden privaten Schlüssel ab. Da nur der Server Zugriff auf den privaten Schlüssel hat, kann der Server die Daten des Clients entschlüsseln.

Hier sehen Sie ein Beispiel für einen Befehl, der MYHTTPS bei der Socket-Werkseinstellung `com.glide.certificates.DBKeyStoreSocketFactory` an Port 443 registriert. Die Datenbank-Schlüsselspeicher-Factory wird während des SSL-Austauschprozesses verwendet, um ein Client-Zertifikat für die gegenseitige Authentifizierung bereitzustellen.

```
glide.httpclient.protocol.myhttps.class =
 "com.glide.certificates.DBKeyStoreSocketFactory"
glide.httpclient.protocol.myhttps.port = "443"
```

Die obige Konfiguration wirkt sich auf alle ausgehenden `myhttps://host.domain.com/target-URLs` aus, um die anwenderdefinierte Socket-Fabrik zu verwenden und Zertifikate während SSL auszutauschen.

Hinweis: Das Überschreiben der Standard-HTTPS-Protokoll-Socket-Factory wirkt sich auf alle ausgehenden HTTPS-Verbindungen aus. Dies ist normalerweise unerwünscht.

Der Server antwortet mit dem Senden eines -Zertifikats. Ist dies ein Zertifikat, das der Client akzeptiert? Falls ja, wird eine Nachricht an den Server gesendet, der das Zertifikat akzeptiert,

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

und ein sicherer Kanal wird initiiert. Wenn das Zertifikat nicht akzeptiert wird, kann dies bedeuten, dass die Stammzertifizierung für die Zertifizierung erforderlich ist.

Regeln für Zugriffssteuerungsliste

Regeln für Zugriffssteuerungslisten (ACLs) schränken den Zugriff auf Daten ein, indem sie von Anwendern die Erfüllung einer Reihe von Anforderungen verlangen, bevor sie mit der Interaktion beginnen können.

Untersuchen	Konfigurieren
	
Erfahren Sie mehr über die ACL.	Konfigurieren Sie die ACL.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Referenz



Rufen Sie Details zum Kontextsicherheits-Manager ab.

Erweitert



Erfahren Sie mehr über erweiterte ACL.

Zugriffssteuerungslisten erkunden

Erkunden Sie Zugriffssteuerungslisten (ACLs).

Alle Regeln für Zugriffssteuerungslisten legen Folgendes fest:

- Der Entscheidungstyp, der Regeltyp und der Vorgang, die die ACL definieren
- Das Objekt, das gesichert wird
- Die für den Zugriff auf das Objekt erforderlichen Bedingungen

Komponenten der ACL

Der Entscheidungstyp definiert, ob Benutzer auf das Objekt zugreifen dürfen, wenn die Bedingungen erfüllt sind, oder ob der Zugriff auf das Objekt verweigert wird, wenn die Bedingungen nicht erfüllt sind.

Entscheidungstyp	Beschreibung
Verweigern-Unless	Beschränken Sie den Zugriff auf die Ressource, indem Sie den Zugriff explizit verweigern, sofern keine Bedingungen übergeben werden. Weitere Informationen finden Sie unter #unique_1366_Connect_42_section_qnd_snl_zbc.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Entscheidungstyp	Beschreibung
Zulassen-Wenn	Zugriff auf Ressource zulassen, wenn Bedingungen übergeben werden.

Das Objekt ist das Ziel, auf das der Zugriff gesteuert werden muss. Jedes Objekt besteht aus einem Typ und einem Namen, der eine bestimmte Tabelle, ein bestimmtes Feld oder einen bestimmten Datensatz eindeutig identifiziert. Mit dem Feld Gilt für haben Benutzer eine granulare Kontrolle darüber, für welche spezifischen Datensätze diese ACL gilt.

Alle diese Einträge geben beispielsweise ein Objekt an:

Typ	Name	Objekt gesichert
record	[Incident].[--Keine--]	Die Incident-Tabelle.
record	[Incident].[Aktiv]	Feld „Aktiv“ in der Incident-Tabelle
record	[incident] Betrifft: Priorität = P1	Nur Incidents mit Priorität 1 in der Incident-Tabelle
REST_Endpoint	user_role_inheritance	Der Datensatz für die geskriptete REST API „user_role_inheritance“.

Jeder Vorgang beschreibt eine gültige Aktion, die das System für das angegebene Objekt ausführen kann. Einige Objekte, z. B. Datensätze, unterstützen mehrere Vorgänge, während andere Objekte, z. B. ein REST-Endpunkt, nur einen Vorgang unterstützen.

Alle diese Einträge geben beispielsweise einen Vorgang an:

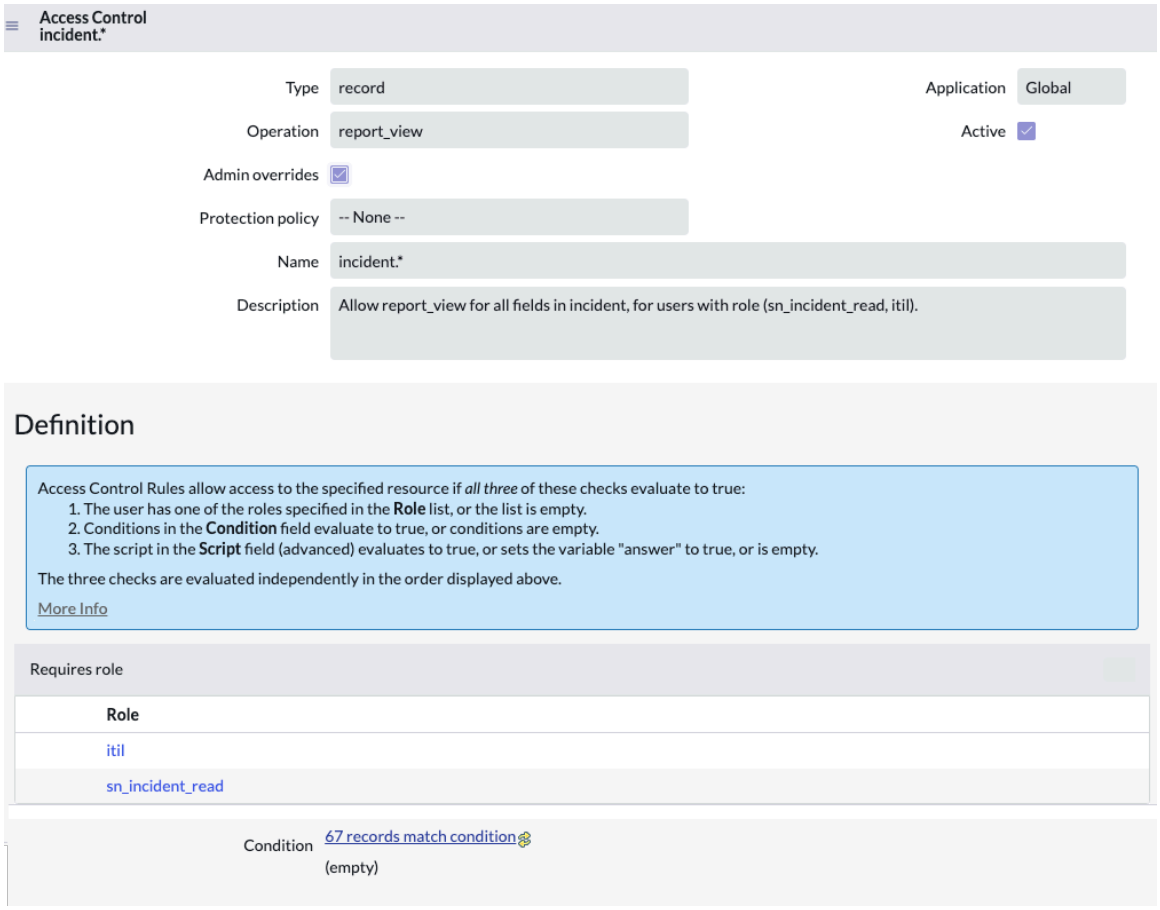
Typ	Name	Vorgang	Vorgang gesichert
record	[Incident].[--Keine--]	Erstellen	Datensätze in der Incident-Tabelle erstellen.
record	[Incident].[Aktiv]	write	Das Feld „Aktiv“ in der Incident-Tabelle wird aktualisiert.
REST_Endpoint	user_role_inheritance	ausführen	Ausführen der geskripteten REST API „user_role_inheritance“.

Die Bedingungen geben an, wann ein Benutzer auf das benannte Objekt und den benannten Vorgang zugreifen kann. Sicherheitsadministratoren können Bedingungsanforderungen angeben, indem sie Folgendes hinzufügen:

- Mindestens eine Anwenderrolle für die Liste **„Erfordert Rolle“**.
- Mindestens ein Sicherheitsattribut muss als „wahr“ ausgewertet werden.
- Mindestens eine Datenbedingung
- Ein Skript, das „wahr“ oder „falsch“ ergibt oder das die `Antwortvariable` auf „wahr“ oder „falsch“ setzt.

Um Zugriff auf ein Objekt und einen Vorgang zu erhalten, muss ein Benutzer alle in einer Zugriffssteuerung aufgeführten Bedingungen erfüllen. Diese Zugriffssteuerung schränkt beispielsweise den Zugriff auf das Anzeigen von Vorgängen in der Incident-Tabelle ein.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Um einen Datensatz in der Incident-Tabelle zu aktualisieren, muss ein Benutzer über die aufgeführten Rollen verfügen, und der Datensatz muss die Bedingung erfüllen.

Bedingungstyp	Anforderung	Beschreibung
Erfordert Rolle	**Erfordert die Rolle**itil	Erlauben Sie nur Benutzern mit der Rolle „itil“, Incidents zu aktualisieren.
Sicherheitsattribute	UserIsAuthenticated	Nur authentifizierte Anwender dürfen Incidents aktualisieren.
Datenbedingung	[Incident-Status] [ist nicht] [Geschlossen]	Lassen Sie nur Aktualisierungen für aktive Incident-Datensätze zu.

Standardmäßig ablehnen

Standardmäßig verweigert die ACL-Engine den Zugriff vollständig, wenn eine ACL leer oder ungültig ist. Leere ACLs werden als ACLs ohne eine oder mehrere der folgenden Komponenten definiert:

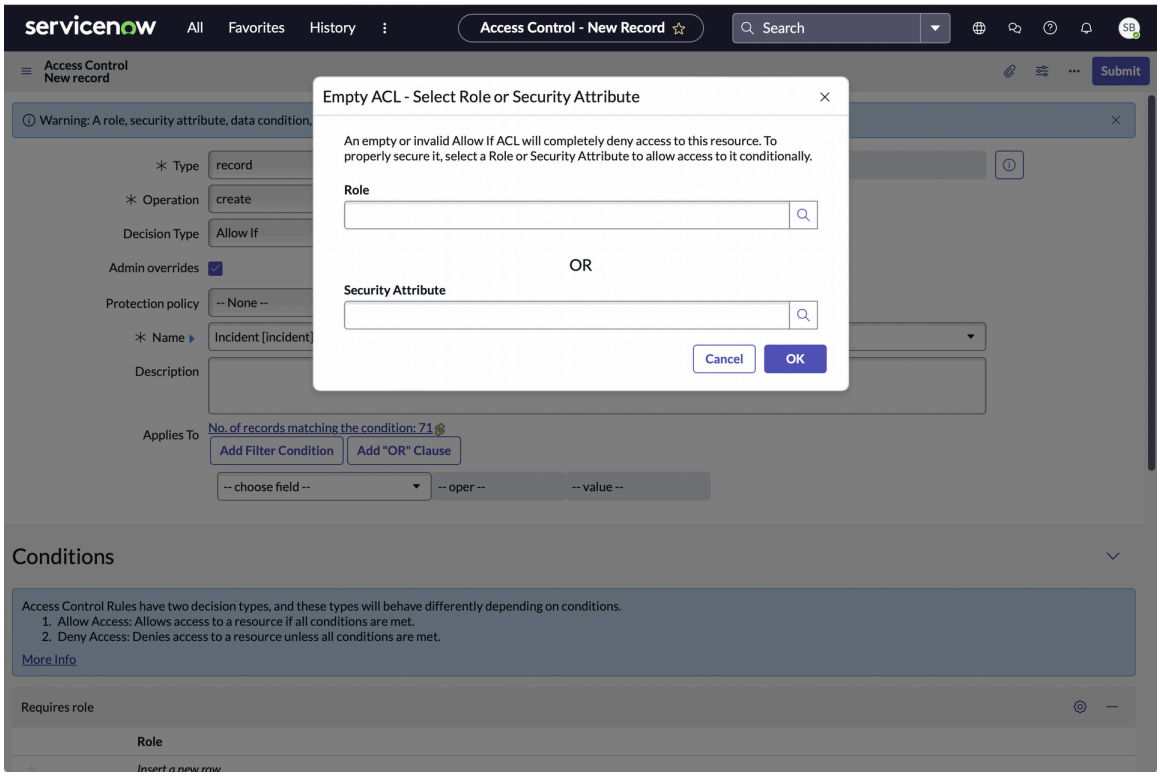
- Definierte Rolle
- Sicherheitsattribut
- Datenbedingung
- Skript

Ungültige ACLs sind definiert als:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- ACLs mit Rollen, die nicht vorhanden sind (haben z. B. keine Zeile in der Datenbank)
- ACLs mit Sicherheitsattributen, die nicht vorhanden sind (haben z. B. keine Zeile in der Datenbank)
- ACLs mit einem Skript, das „answer=true“ oder „wahr“ enthält

Wenn das System erkennt, dass der Anwender eine ACL erstellt, fordert es den Anwender auf, eine Rolle oder ein vorhandenes Sicherheitsattribut auszuwählen.



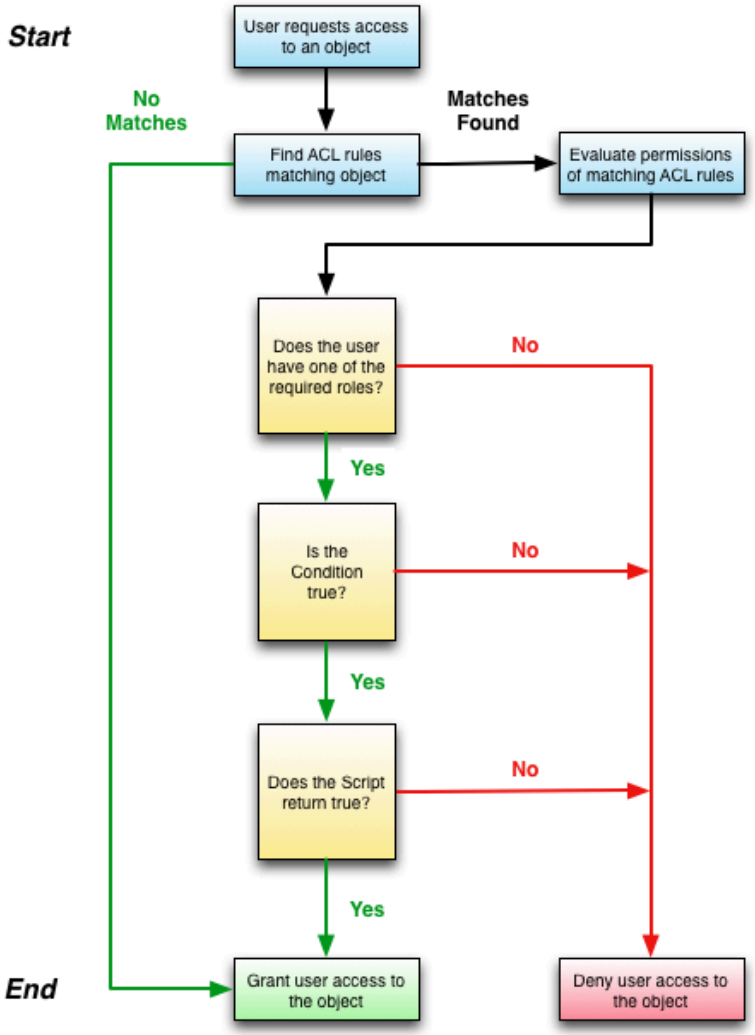
ACL-Bewertungsprozess

Eine ACL-Regel gewährt einem Benutzer nur dann Zugriff auf ein Objekt, wenn der Benutzer alle Bedingungen erfüllt, die für die entsprechende ACL-Regel erforderlich sind.

- Die Bedingung muss als *true*ausgewertet werden.
- Das Skript muss als *true* ausgewertet werden oder eine Antwortvariable mit dem Wert *true*zurückgeben.
- Der Benutzer muss eine der Rollen in der Liste der erforderlichen Rollen aufweisen. Wenn die Liste leer ist, wird diese Bedingung als *true*ausgewertet.
- [Nur Datensatz-ACL-Regeln] Die übereinstimmenden ACL-Regeln auf Tabellenebene und Feldebene müssen als *true*ausgewertet werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ACL-Bewertungsbedingungen



Immer wenn eine Sitzung Daten anfordert, sucht das System nach Zugriffssteuerungsregeln, die dem angeforderten Objekt und Vorgang entsprechen. Wenn eine übereinstimmende Zugriffssteuerungsregel vorhanden ist, wertet das System aus, ob der Benutzer über die erforderlichen Bedingungen für den Zugriff auf das Objekt und den Vorgang verfügt. Wenn eine Zugriffssteuerungsregel mehr als eine Bedingung angibt, muss der Benutzer alle Bedingungen erfüllen, um Zugriff auf das Objekt und den Vorgang zu erhalten. Wenn eine Bedingungsprüfung fehlschlägt, kann der Anwender nicht auf das entsprechende Objekt und den entsprechenden Vorgang zugreifen.

Wenn ein Benutzer die Bedingungen der ersten Übereinstimmungsregel nicht erfüllt, wertet das System die Bedingungen der nächsten übereinstimmenden Zugriffssteuerungsregel gemäß der Verarbeitungsreihenfolge der Zugriffssteuerung aus. Wenn ein Benutzer die Bedingungen einer übereinstimmenden Zugriffssteuerungsregel nicht erfüllt, verweigert das System den Zugriff auf das angeforderte Objekt und den angeforderten Vorgang.

Hinweis: Wenn für das angeforderte Objekt und den angeforderten Vorgang keine übereinstimmenden Zugriffssteuerungsregeln vorhanden sind, gewährt das System dem Benutzer Zugriff darauf. In der Praxis kommt es selten vor, dass das System keine übereinstimmenden Regeln findet, da das System über eine Reihe von standardmäßigen Zugriffssteuerungsregeln verfügt, die alle Datensatzvorgänge schützen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Auswirkungen der Verweigerung des Zugriffs auf ein Objekt hängen von der ACL-Regel ab, die der Benutzer fehlgeschlagen hat. Wenn beispielsweise eine ACL-Regel für einen Lesevorgang fehlschlägt, kann der Benutzer das Objekt nicht sehen. Je nach gesichertem Objekt blendet die ACL-Regel ein Feld in einem Formular aus, blendet Zeilen aus einer Liste aus oder verhindert, dass ein Benutzer auf eine UI-Seite zugreift. Die folgende Tabelle enthält eine vollständige Liste der Ergebnisse des Fehlschlagens einer ACL-Regel für einen bestimmten Vorgang und Objekttyp.

ACL-Prüfungen vor und nach der Abfrage

Ihre Instanz von prüft ACL-Regeln sowohl vor als auch nach dem Stellen einer Abfrage durch einen Anwender. Da vor und nach einer Abfrage unterschiedliche Informationen verfügbar sind, können die Ergebnisse unterschiedlich sein.

ACL-Prüfung vor der Abfrage

Bevor Ihre Instanz eine Datenbankabfrage ausführt, prüft sie die ACL-Regeln für jedes Feld in der abgefragten Tabelle, um zu bestimmen, auf welche Felder ein Benutzer zugreifen darf. Diese Prüfung berücksichtigt nur die Rollen des Anwenders und prüft, ob diese Rollen Zugriff auf Felder gewähren. Da diese Prüfung vor der Abfrage ausgeführt wird, hat die ACL keinen Zugriff auf die Datensätze in der Tabelle und kann diese Daten daher nicht berücksichtigen. Skripts und Bedingungen, die auf der Kenntnis des Inhalts eines Datensatzes beruhen, werden nicht ausgewertet.

Wenn der Benutzer zu diesem Zeitpunkt keinen Lesezugriff hat, wird ihm der Wert für das Feld nicht angezeigt.

ACL-Prüfung nach der Abfrage

Nach der Abfrage prüft Ihre -Instanz jeden von der Abfrage zurückgegebenen Datensatz. Während dieser Prüfung ist Kontext für die ACL vorhanden, sodass die Rollen-, Bedingungs- und Skriptteile der ACL ausgewertet werden. Wenn der Anwender zu diesem Zeitpunkt keinen Lesezugriff hat, wird ihm der Wert für das Feld nicht angezeigt. Der Anwender sieht jedoch die Feldbezeichnung, wenn seine Rollen Zugriff auf das Feld zulassen.

Vorgang	Ergebnisse des Fehlschlagens einer ACL-Regel für ein Objekt
ausführen	Anwender können keine Skripts für einen Datensatz oder eine UI-Seite ausführen.
Erstellen	Anwender können die UI-Aktion „ **Neu** “ in Formularen nicht sehen. Der Benutzer kann auch keine Datensätze mithilfe von API-Protokollen wie Webdiensten in eine Tabelle einfügen. Eine ACL mit einer Bedingung **erstellen**, die erfordert, dass ein Feld, das einen bestimmten Wert enthält, immer als „falsch“ ausgewertet wird. Felder in neuen Datensätzen gelten als leer, bis der Datensatz gespeichert wird.
gelesen	Der Anwender kann das Objekt nicht in Formularen oder Listen anzeigen. Der Benutzer kann auch keine Datensätze mit API-Protokollen wie Webdiensten abrufen.
write	Dem Anwender wird in Formularen und Listen ein schreibgeschütztes Feld angezeigt, und er kann Datensätze nicht mit API-Protokollen wie Webdiensten aktualisieren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorgang	Ergebnisse des Fehlschlagens einer ACL-Regel für ein Objekt
delete	Der Anwender kann die UI-Aktion **„Löschen** “ in Formularen nicht sehen. Der Benutzer kann auch keine Datensätze mithilfe von API-Protokollen wie Webdiensten aus einer Tabelle entfernen.
edit_task_relations	Anwender kann keine Beziehungen zwischen Aufgabentabellen definieren.
edit_ci_beziehungen	Der Benutzer kann keine Beziehungen zwischen Tabellen für Konfigurationselemente [cmdb_ci] definieren.
save_as_template	Wird verwendet, um die Felder zu steuern, die gespeichert werden sollen, wenn eine Vorlage erstellt wird.
add_to_list	Anwender können bestimmte Spalten in der Listenmechanik nicht anzeigen oder personalisieren.
list_edit	Anwender kann keine Datensätze (Zeilen) aus einer Liste aktualisieren.
report_on	Anwender kann keinen Bericht in der ACL-Tabelle erstellen. Weitere Informationen finden Sie unter Berichterstellung mit einer ACL-Regel einschränken .
report_view	Der Anwender kann den Inhalt eines Berichts in der ACL-Tabelle oder im ACL-Feld nicht anzeigen. Weitere Informationen finden Sie unter Reporting .
personalize_choices	Der Benutzer kann nicht mit der rechten Maustaste auf ein Listenfeld klicken und Auswahlmöglichkeiten **konfigurieren**auswählen.

ACL, die den Anforderungen für Objekte entspricht

Objekttyp	Übereinstimmende ACL-Regeln für Zugriffsobjekt erforderlich	Vorhandene Platzhalter-ACL-Regeln
Vom Client aufrufbare Skripteinbindungen Prozessoren	Benutzer müssen die Bedingungen von zwei ACL-Regeln erfüllen: **1.** Alle ACL-Regeln mit Platzhaltern für das Objekt (sofern für den Vorgang eine ACL-Regel vorhanden ist). **2.** Die erste ACL-Regel, die dem Namen des Objekts entspricht (sofern für den Vorgang eine ACL-Regel vorhanden ist).	Standardmäßig sind für diese Objekttypen keine Platzhalterregeln (*) vorhanden. Wenn Sie eine Platzhalter-ACL-Regel für eines dieser Objekte erstellen, gilt die ACL-Regel für alle Objekte dieses Typs.
UI-Seiten Datensatz	Benutzer müssen die Bedingungen von zwei ACL-Regeln erfüllen: **1.** Die erste ACL-Regel, die dem Feld des Datensatzes entspricht (sofern für den	Standardmäßig gibt es Platzhalter-Tabellenregeln (*) für die Vorgänge zum Erstellen, Lesen, Schreiben und Löschen sowie Platzhalter-Feldregeln (*.*) für die Vorgänge

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Objekttyp	Übereinstimmende ACL-Regeln für Zugriffsobjekt erforderlich	Vorhandene Platzhalter-ACL-Regeln
	Vorgang eine ACL-Regel vorhanden ist). 2. Die erste ACL-Regel, die der Tabelle des Datensatzes entspricht (sofern für den Vorgang eine ACL-Regel vorhanden ist).	„personalize_choices“, „create“ und „save_as_template“. Wenn Sie eine Tabelle erstellen, erstellen Sie ACL-Regeln für die Tabelle, es sei denn, Sie möchten die bereitgestellten ACL-Regeln für Platzhalter verwenden.

Hinweis: Die Eigenschaft Security Manager-Standardverhalten (*glide.sm.default_mode*) bestimmt, ob Benutzer auf Objekte zugreifen können, die nur mit ACL-Regeln der Platzhaltertabelle übereinstimmen. Wenn diese Eigenschaft auf *Zugriff verweigern*festgelegt ist, können nur Administratoren auf Objekte zugreifen, die den ACL-Regeln der Platzhaltertabelle entsprechen.

Hinweis: Die ACL-Regel für das Platzhalterfeld (*.*) für den Erstellungsvorgang verwendet dieselben Bedingungen wie der Schreibvorgang. Dies bedeutet, dass die Erstellungsbedingungen mit den Schreibbedingungen übereinstimmen, es sei denn, Sie definieren eine explizite ACL-Regel für den Erstellungsvorgang.

Mehrere ACL-Regeln am selben Punkt in der Verarbeitungsreihenfolge

Wenn zwei oder mehr Regeln am selben Punkt in der Verarbeitungsreihenfolge übereinstimmen, muss der Benutzer eine beliebige ACL-Regelbedingung übergeben, um auf das Objekt zuzugreifen. Wenn Sie beispielsweise zwei Feld-ACL-Regeln für *incident.number*erstellen, hat ein Benutzer, der eine Regel übergibt, Zugriff auf das Zahlenfeld, unabhängig davon, ob der Benutzer eine andere Feld-ACL-Regel am selben Punkt in der Verarbeitungsreihenfolge verfehlt hat.

Erforderliche Rolle

Normale Administratorbenutzer können Zugriffssteuerungsregeln anzeigen und debuggen. Um jedoch vorhandene Zugriffssteuerungsregeln zu erstellen oder zu aktualisieren, müssen Administratoren Berechtigungen für die Rolle security_admin erhöhen. Siehe Auf eine privilegierte Rolle hochstufen für Anweisungen.

ACL-Regeln in bereichsbezogenen Anwendungen

Sie können ACL-Regeln für Objekte im gleichen Umfang wie die ACL-Regel erstellen. Sie können ACL-Regeln auch für Tabellen mit mindestens einem Feld erstellen, das sich im gleichen Umfang wie die ACL-Regel befindet.

Für Tabellen, die sich in einem anderen Bereich als der ACL-Regeldatensatz befinden, sind die Regeltypen eingeschränkt.

- Sie können eine ACL-Regel für jede Tabelle, UI-Seite oder ein anderes Objekt erstellen, das sich im selben Bereich wie die ACL-Regel befindet.
- Sie können eine ACL für ein Feld erstellen, das sich im gleichen Umfang wie die ACL-Regel befindet.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

  - Wenn sich die Tabelle im gleichen Bereich befindet, können Sie ein Skript verwenden, um Bedingungen auszuwerten.
  - Wenn sich die Tabelle in einem anderen Bereich befindet, können Sie kein Skript zum Auswerten von Bedingungen verwenden.
- Sie können keine ACL-Regeln für Objekte erstellen oder ändern, die sich in einem anderen Bereich als die in der Anwendungsauswahl ausgewählte Anwendung befinden, einschließlich durch Hinzufügen einer Rolle zu einer ACL in einem anderen Bereich.
- Sie können Platzhalter-Tabellenregeln (*) nur im globalen Bereich erstellen.
- Sie können Platzhalter-Feldregeln (*) nur für Tabellen erstellen, die sich im gleichen Umfang wie die ACL-Regel befinden.

ACL_Regeltypen

Erstellen Sie ACL-Regeln für verschiedene Komponenten des Systems.

Datensatz-ACL-Regeln

Datensatz-ACL-Regeln bestehen aus Tabellen- und Feldnamen.

- Der Tabellenname ist die Tabelle, die Sie sichern möchten. Wenn andere Tabellen von dieser Tabelle ausgehend erweitert werden, wird die Tabelle als übergeordnete Tabelle betrachtet. ACL-Regeln für übergeordnete Tabellen gelten für jede Tabelle, die die übergeordnete Tabelle erweitert.
- Der Feldname ist das Feld, das Sie sichern möchten. Einige Felder sind aufgrund der Tabellenerweiterung Teil mehrerer Tabellen. ACL-Regeln für Felder in einer übergeordneten Tabelle gelten für jede Tabelle, die die übergeordnete Tabelle erweitert.

ACL-Regeln können die folgenden Datensatzvorgänge sichern:

Vorgang	Beschreibung
Erstellen	Ermöglicht Anwendern das Einfügen neuer Datensätze (Zeilen) in eine Tabelle.
gelesen	Ermöglicht Anwendern das Anzeigen von Datensätzen aus einer Tabelle.
write	Ermöglicht Anwendern das Aktualisieren von Datensätzen in einer Tabelle.
delete	Ermöglicht Benutzern das Entfernen von Datensätzen aus einer Tabelle oder das Löschen einer Tabelle.
edit_task_relations	Ermöglicht Benutzern das Erweitern der Aufgabentabelle [task]
edit_ci_beziehungen	Ermöglicht Benutzern das Erweitern der Tabelle „Configuration Item“ [cmdb_ci].
save_as_template	Ermöglicht Benutzern das Speichern eines Datensatzes als Vorlage.
add_to_list	Verhindert, dass Anwender bestimmte Spalten in der Listenmechanik anzeigen oder personalisieren. **Hinweis:** Bedingungen und Skripts werden nicht unterstützt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorgang	Beschreibung
list_edit	Ermöglicht Anwendern das Aktualisieren von Datensätzen (Zeilen) aus einer Liste.
report_on	Ermöglicht Benutzern das Erstellen von Berichten über Tabellen.
report_view	Ermöglicht Anwendern das Erstellen von Berichten zu Feld-ACLs.
personalize_choices	Ermöglicht Benutzern das Konfigurieren der Tabelle oder des Felds.
query_exact	Ermöglicht Anwendern das Senden von Übereinstimmungsabfragen („ist“, „ist nicht“, „ist leer“ usw.).
query_range	Ermöglicht Anwendern das Senden von Bereichsabfragen („beginnt mit“, „endet mit“, „enthält“ usw.) und die Sortierung ist unbeschränkt.

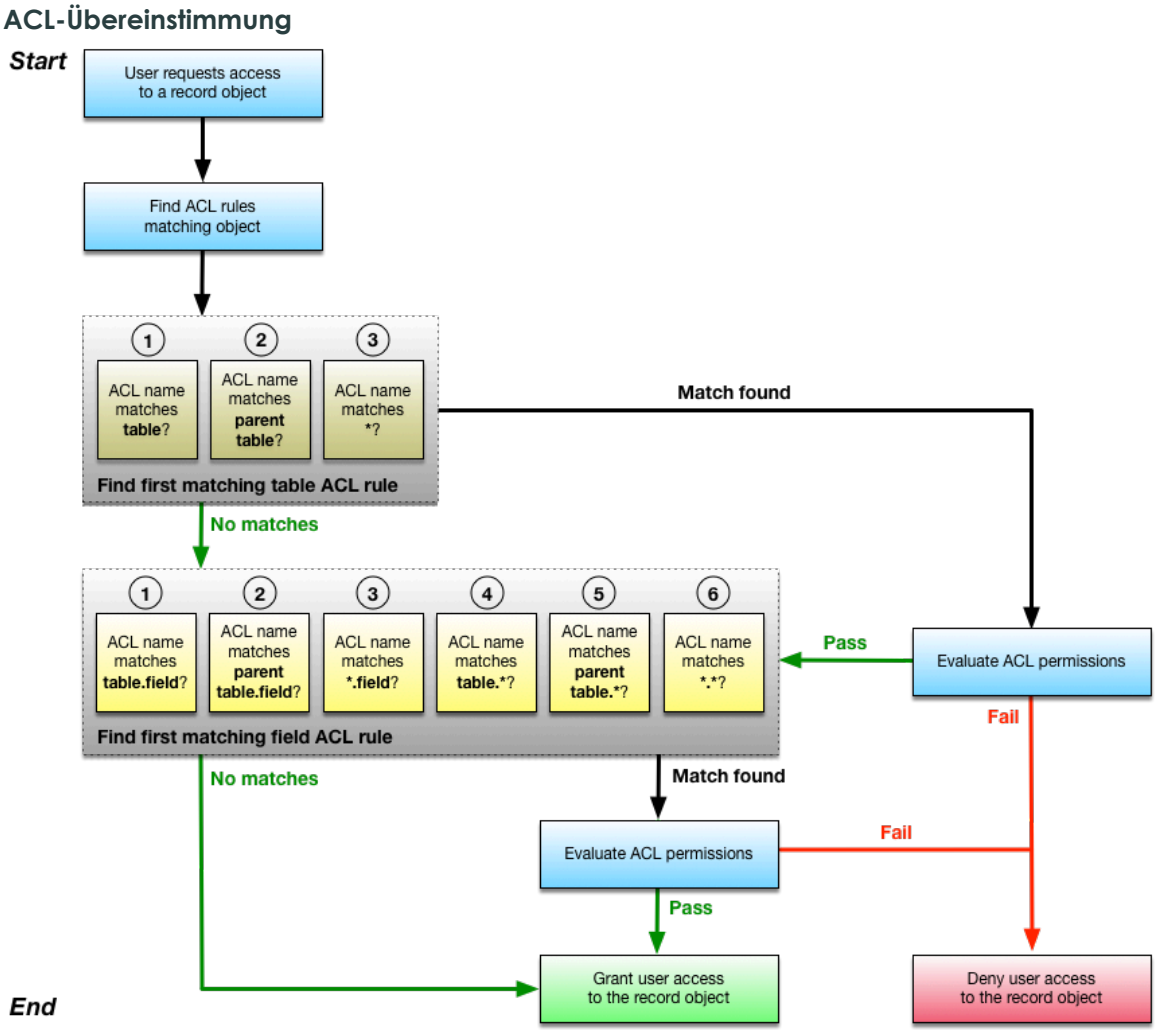
Datensatz-ACL-Regeln werden in der folgenden Reihenfolge verarbeitet:

- Ordnen Sie das Objekt den ACL-Regeln der Tabelle zu.
- Objekt mit Feld-ACL-Regeln abgleichen.

Diese Verarbeitungsreihenfolge stellt sicher, dass Anwender Zugriff auf spezifischere Objekte erhalten, bevor sie Zugriff auf allgemeinere Objekte erhalten. Ein Benutzer muss ACL-Regeln für Tabellen und Felder übergeben, um auf ein Datensatzobjekt zugreifen zu können.

- Wenn ein Benutzer eine Tabellen-ACL-Regel nicht erfüllt, wird ihm der Zugriff auf alle Felder in der Tabelle verweigert, auch wenn er eine Feld-ACL-Regel übergibt.
- Wenn ein Benutzer eine Tabellen-ACL-Regel übergibt, eine Feld-ACL-Regel jedoch fehlschlägt, kann er nicht auf das durch die Feld-ACL-Regel beschriebene Feld zugreifen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



ACL-Regeln für Prozessor

Prozessor-ACL-Regeln geben den Prozessor an, den Sie sichern möchten. Eine Liste der verfügbaren Prozessoren finden Sie, wenn Sie zu navigieren **Systemdefinition** > **Prozessoren**an.

Standardmäßig ist eine ACL-Regel für den EmailClientProcessor enthalten, um den E-Mail-Client auf Benutzer mit der Rolle itil zu beschränken.

ACL-Regeln für Prozessoren berücksichtigen die STERNE (*)-Regel, wenn sie keine spezifischere ACL für diese Ressourcen finden können.

ACL-Regeln für Tabelle

Der Benutzer muss zuerst die ACL-Regel der Tabelle übergeben. Da das Basissystem START-Tabellen-ACL-Regeln (*) enthält, die mit jeder Tabelle übereinstimmen, muss der Benutzer immer mindestens eine Tabellen-ACL-Regel übergeben. Das Basissystem bietet zusätzliche ACL-Regeln für Tabellen, um den Zugriff auf bestimmte Tabellen zu steuern.

Tabellen-ACL-Regeln werden in der folgenden Reihenfolge verarbeitet:

1. Passen Sie den Tabellennamen an. Beispiel: Incident.
2. Passen Sie den Namen der übergeordneten Tabelle an. Beispiel: Aufgabe.
3. Beliebigen Tabellennamen abgleichen (*). Beispiel: *.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn ein Benutzer alle ACL-Regeln der Tabelle fehlschlägt, kann er auf keine Felder in der Tabelle zugreifen. Wenn ein Benutzer eine Tabellen-ACL-Regel übergibt, wertet das System das Feld ACL-Regeln aus.

Feld-ACL-Regeln

Nachdem ein Benutzer eine Tabellen-ACL-Regel übergeben hat, werden die Feld-ACL-Regeln in der folgenden Reihenfolge verarbeitet:

1. Passen Sie die Tabelle und den Feldnamen an. Beispiel: incident.number.
2. Übereinstimmen Sie die übergeordnete Tabelle und den Feldnamen. Beispiel: task.number.
3. Beliebige Tabelle (*) und Feldname abgleichen. Beispiel: *.number.
4. Die Tabelle und ein beliebiges Feld (*) abgleichen. Beispiel: incident.*.
5. Übereinstimmen Sie die übergeordnete Tabelle und ein beliebiges Feld (*). Beispiel: Aufgabe.*.
6. Jede Tabelle (*) und jedes Feld (*) abgleichen. Beispiel: *.*.

Ein Benutzer muss die ACL-Regel der Tabelle übergeben, um Zugriff auf die Felder der Tabelle zu erhalten. Beispielsweise muss der Benutzer zuerst die Tabellen-ACL-Regel für die Incident-Tabelle übergeben, um auf das Feld **Nummer** in der Incident-Tabelle zugreifen zu können.

Die erste erfolgreiche Feld-ACL-Auswertung stoppt die ACL-Regelverarbeitung auf Feldebene. Wenn ein Benutzer eine Feld-ACL-Regel übergibt, beendet das System die Suche nach anderen übereinstimmenden Feld-ACL-Regeln. Wenn ein Benutzer beispielsweise das Feld ACL-Regel für incident.number übergibt, beendet das System die Suche nach anderen ACL-Regeln, die das Feld **Nummer** in der Incident-Tabelle sichern.

Der Zugriff auf die Abfrage von Informationen abgeleiteter Daten ist für geschützte Felder eingeschränkt, wodurch die Rückgabe prädiktiver Informationen verhindert wird.

ACL-Regeln für UI-Seiten

ACL-Regeln für UI-Seiten geben die zu sichernde UI-Seite an. Eine Liste der verfügbaren UI-Seiten finden Sie, wenn Sie zu navigieren **System-UI** > **UI-Seiten**an. Verwenden Sie beim Definieren einer ACL-Regel für eine UI-Seite den vollständigen Seitennamen. Beispiel: **x_myapp_mypage**.

Hinweis: Sie können das Zeichen STERN (*) im Feld **Name** in ACLs vom Typ **„ui_page** “ verwenden, um beliebige UI-Seiten abzugleichen.

ACL-Regeln für UI-Seiten berücksichtigen die STERNE (*)-Regel, wenn sie keine spezifischere ACL für diese Ressourcen finden können. Wenn Sie beispielsweise eine UI-Seite mit dem Namen `mysecretpage` haben, für diese UI-Seite jedoch keine ACL definieren, wird für die Zugriffsprüfung die Regel Star (*) für den UI-Seitenprozessor verwendet.

ACL-Regeln können den folgenden UI-Seitenvorgang sichern:

Vorgang	Beschreibung
gelesen	Ermöglicht Anwendern das Anzeigen der UI-Seite.

Vom Client aufrufbare Skripteinbindungs-ACL-Regeln

Skripteinbindungs-ACL-Regeln geben die vom Client aufrufbare Skripteinbindung an, die gesichert werden soll. Eine Liste der verfügbaren Skripteinbindungen finden Sie durch

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Navigieren zu **Systemdefinition** > **Skripteinbindungen**an. Sie können die Liste personalisieren, um die Spalte *Vom Client aufrufbar* anzuzeigen.

Das Basissystem enthält keine ACL-Regeln für vom Client aufrufbare Skripteinbindungen.

ACL-Regeln für vom Client aufrufbare Skripteinbindungen berücksichtigen die START-Regel (*), wenn für diese Ressourcen keine spezifischere ACL gefunden werden kann.

ACL-Steuerung von Funktionsfeldern

Bei der Auswertung des Zugriffs auf ein Funktionsfeld prüft das System nicht nur den Zugriff auf das Funktionsfeld selbst, sondern auch auf die beitragenden Felder der Funktion. Beitragende Felder sind diejenigen, die als Argumente in einer bestimmten Funktionsdefinition verwendet werden.

Weitere Informationen zu Funktionsfeldern finden Sie unter Funktionsfeld .

In Rome und früheren Versionen prüft das System einfach den Zugriff auf das Funktionsfeld selbst (wie bei jedem anderen Feld auch). Wenn die ACLs für dieses Feld den Zugriff zulassen, erhält der Benutzer den resultierenden Wert, unabhängig davon, ob er Zugriff auf die beitragenden Felder hat.

In Xanadu und höher benötigt das System außerdem Zugriff auf alle beitragenden Felder, um den Zugriff auf das Funktionsfeld zu ermöglichen. Wenn eine oder mehrere der beitragenden Feld-ACLs den Zugriff verweigern, verweigert auch das Funktionsfeld den Zugriff.

Die einzigen von der neuen Anforderung betroffenen Vorgänge sind „read“ und „report_view“. „report_view“ hat eigene zusätzliche Anforderungen.

Vorgang	Beschreibung
Lesevorgang	Ein Benutzer hat nur dann Lesezugriff auf ein Funktionsfeld, wenn beide der folgenden Bedingungen erfüllt sind: • Der Benutzer hat Lesezugriff auf das Funktionsfeld. • Der Benutzer hat Lesezugriff auf alle beitragenden Felder, die in der Funktion verwendet werden.
report_view-Vorgang	Ein Benutzer hat nur dann report_view-Zugriff auf ein Funktionsfeld, wenn alle der folgenden Bedingungen erfüllt sind: • Der Benutzer hat Zugriff vom Typ report_view auf das Funktionsfeld. • Der Anwender hat Zugriff vom Typ „report_view“ auf alle beitragenden Felder. • Es gibt eine Lese-ACL nur für Rollen ohne Bedingungen und ohne Skript, und der Benutzer hat diese Rolle. • Der Benutzer hat nur über die Rolle Lesezugriff auf die beitragenden Felder, sodass dies nur ACLs ohne Bedingung oder Skript zulassen.

Beispiele

Gegeben:

- Tabelle: Gehalt
- Spalten: Base, Bonus, Total (in diesem Beispiel sind alle Ganzzahlen)

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Funktionsfeld: Die Gesamtsummenspalte ist als Funktionsfeld markiert, mit der Funktionsdefinition `„glidefunction:add(base, Bonus)“`.
- Beitragende Felder: Basis und Bonus, da sie in der Funktionsdefinition verwendet werden
- Rollen: Gehalt_Administrator, Bonus_Administrator

Beispiel 1: Alle Felder erlauben Zugriff

ACLs	Ergebnis
„total“, „base“, „bonus: read“ und „report_view“ für die Rolle „gehalt_admin“ ohne Bedingungen oder Skripts	Einem Benutzer mit der Rolle „gehalt_admin“ wird der Lese- und Bericht_Ansichtszugriff auf „total“ gewährt, da er über die erforderliche Rolle verfügt.

Beispiel 2: Beitragendes Feld verweigert Lesezugriff

ACLs	Ergebnis
• „total“, „base: read“ und „report_view“ für die Rolle „gehalt_admin“ ohne Bedingungen oder Skripts • „bonus“: „report_view“ für die Rolle „salary_admin“ , ohne Bedingungen oder Skripts • Bonus: gelesen für Rolle „bonus_admin“, ohne Bedingungen oder Skripts	Einem Anwender mit der Rolle „salary_admin“ wird der Lese- und report_view-Zugriff auf „total“ verweigert, da der Bonus den Lesezugriff für seine Rolle verweigert.

Beispiel 3: Beitragende Feld-ACL hat Skript

ACLs	Ergebnis
• „total“, „base: read“ und „report_view“ für die Rolle „gehalt_admin“ ohne Bedingungen oder Skripts • Bonus: report_view für die Rolle „bonus_admin“ ohne Bedingungen oder Skripts • Bonus: gelesen für Rolle Gehalt_Administrator, mit einem Skript (beachten Sie, dass es keine Rolle spielt, was im Skript enthalten ist, nur, dass es vorhanden ist)	Einem Benutzer mit der Rolle „gehalt_admin“ wird Lesezugriff auf „total“ gewährt, da er über die erforderliche Rolle für alle Felder verfügt. Dem gleichen Anwender mit „gehalt_admin“ wird jedoch der Zugriff auf „report_view“ verweigert, da die Lese-ACL mit dem Skript den Zugriff für diesen Fall standardmäßig verweigert, obwohl er über die erforderliche Rolle verfügt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitshilfe: Plugin „ACL-Regeln“.

Das Sicherheits-Jump-Start-Plugin „Access Control Level (ACL Rules)“ wird automatisch auf allen neuen Instanzen installiert. Verwenden Sie dieses Plugin, um schnell mehrere Systemtabellen zu sichern und den Produktionsstart für Ihre Organisation zu beschleunigen.

Dieses Plugin ist nicht für vorhandene Instanzen vorgesehen, da es den Sicherheitszugriff auf Tabellen ändern kann, die bereits in einer Produktionsumgebung verwendet werden. Wenn ein Administrator dieses Plugin unbedingt auf einer vorhandenen Instanz installieren möchte, sollte es zuerst in einer Testinstanz gründlich getestet werden. Auf diese Weise können Sie die Kompatibilität mit der aktuellen -Implementierung des Unternehmens überprüfen.

Wenn ein Administrator an den neuen ACL-Regeln interessiert ist, die von diesem Plugin bereitgestellt werden, kann er manuell eine oder mehrere Regeln in einer vorhandenen Instanz erstellen und dabei die Liste der ACLs als Leitfaden verwenden.

Die folgenden ACLs sind in diesem Plugin enthalten. Wählen Sie das Symbol in einer Headerzeile aus, um diese Spalte in aufsteigender oder absteigender Reihenfolge zu sortieren. Der Vorgangsschlüssel lautet wie folgt:

- R=lesen
- W=write
- D=löschen
- C=erstellen

Name	Vorgang	Beschreibung
`cmdb_ci`	WCD	Asset- oder ITIL-Rolle zum Schreiben/Erstellen/Löschen von Konfigurationselement-Datensätzen erforderlich
`cmn_department`	WD	Zum Schreiben/Löschen von Abteilungsdatensätzen ist die Rolle „user_admin“ erforderlich
`cmn_location`	WC	Rolle „user_admin“ zum Schreiben/Erstellen von Standortdatensätzen erforderlich
`core_company`	WD	Die Rolle „user_admin“ ist zum Schreiben/Löschen von Unternehmensdatensätzen erforderlich
`kb_knowledge`	Erstellen	Zum Erstellen von Knowledge-Datensätzen ist eine Knowledge-Rolle erforderlich
`ldap_u_config`	RWCD	Die Rolle „user_admin“ ist zum Lesen/Schreiben/Erstellen/Löschen von LDAP-OU-Definitionsdatensätzen erforderlich
`ldap_server_config`	RWCD	Die Rolle „user_admin“ ist zum Lesen/Schreiben/Erstellen/Löschen von LDAP-Server-Datensätzen erforderlich
`process_guide`	WCD	Administratorrolle zum Schreiben/Erstellen/Löschen von Prozessleitfaden-Datensätzen erforderlich

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Vorgang	Beschreibung
process_step	WCD	Administratorrolle zum Schreiben/Erstellen/Löschen von Prozessschritt-Datensätzen erforderlich
sc_category	Erstellen	Rolle „catalog_admin“ zum Erstellen von Datensätzen für Servicekatalogkategorien erforderlich
sc_category	delete	Die Rolle „catalog_admin“ ist zum Löschen von Servicekatalog-Kategoriedatensätzen erforderlich
sc_category	write	Rolle „catalog_admin“ ist zum Schreiben in Datensätze der Servicekatalog-Kategorie erforderlich
Katalogelement	write	Rolle „catalog_admin“ zum Schreiben in Katalogelementdatensätze erforderlich
Katalogelement	delete	Die Rolle „catalog_admin“ ist zum Löschen von Katalogelementdatensätzen erforderlich
Katalogelement	Erstellen	Rolle „catalog_admin“ ist zum Erstellen von Katalogelementdatensätzen erforderlich
sysevent_email_action	gelesen	Alle Benutzer können E-Mail-Benachrichtigungsdatensätze lesen (für Abonnementzwecke).
sysevent_register	RWCD	Administratorrolle zum Lesen/Schreiben/Erstellen/Löschen von Ereignisregistrierungsdatensätzen erforderlich
sysevent_script_action	RWCD	Administratorrolle zum Lesen/Schreiben/Erstellen/Löschen von Skriptaktionsdatensätzen erforderlich
syslog	RWCD	Zum Lesen/Schreiben/Erstellen/Löschen von Protokolleintragsdatensätzen ist ein Administrator erforderlich
sysrule	RWCD	Administrator zum Lesen/Schreiben/Erstellen/Löschen von Regeldatensätzen (E-Mail-Benachrichtigungen, Aktionen für eingehende E-Mails, Genehmigungsregeln usw.) erforderlich
sysrule	gelesen	Alle Benutzer können E-Mail-Benachrichtigungsdatensätze für (Abonnementbasierte Benachrichtigungen) lesen.
sys_app_application	WCD	Zum Schreiben/Erstellen/Löschen von Anwendungsdatensätzen ist ein Administrator erforderlich
sys_app_category	WCD	Administratorrolle zum Schreiben/Erstellen/Löschen von Anwendungskategorie-Datensätzen erforderlich

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Vorgang	Beschreibung
sys_app_module	WCD	Zum Schreiben/Erstellen/Löschen von Moduldatensätzen ist ein Administrator erforderlich
sys_audit	RWCD	Administrator zum Lesen/Schreiben/Erstellen/ Löschen von Audit-Datensätzen erforderlich
sys_dictionary	RWC	Rolle „personalize_dictionary“ zum Lesen/Schreiben/Erstellen von Wörterbuchdatensätzen erforderlich
sys_dictionary.*	gelesen	Die Rolle „personalize_dictionary“ kann Wörterbuchfelder lesen
sys_documentation	delete	Rolle „personalize_dictionary“ erforderlich, um Feldbezeichnungsdatensätze zu löschen
sys_documentation	Erstellen	Rolle „personalize_dictionary“ erforderlich, um Feldbezeichnungsdatensätze zu erstellen
sys_documentation	write	Rolle „personalize_dictionary“ erforderlich, um in Feldbezeichnungsdatensätzen zu schreiben
sys_gage	RWCD	Administratorrolle zum Lesen/Schreiben/ Erstellen/Löschen von Anzeigedatensätzen erforderlich
sys_anzeige_count	RWCD	Administratorrolle zum Lesen/Schreiben/ Erstellen/Löschen von Datensätzen für Anzeigezähler erforderlich
sys_group_has_role	gelesen	Rolle itil zum Anzeigen von Gruppenrollendatensätzen erforderlich
sys_home	WCD	Die Rolle „itil_admin“ ist zum Schreiben/ Erstellen/Löschen von Datensätzen für den Willkommensseitenabschnitt erforderlich
sys_installation_exit	WCD	Administratorrolle zum Schreiben/Erstellen/Löschen von Installationsbeendigungsdatensätzen erforderlich
sys_job	WCD	Administratorrolle zum Schreiben/Erstellen/ Löschen von Sys-Job-Datensätzen erforderlich
sys_nav_link	WCD	Administratorrolle zum Schreiben/Erstellen/ Löschen von Navigationslink-Datensätzen erforderlich
sys_perperspektive	WCD	Administratorrolle zum Schreiben/Erstellen/ Löschen von Menülisten-Datensätzen erforderlich
sys_portal	RWCD	Administratorrolle zum Lesen/Schreiben/ Erstellen/Löschen von Portaldatensätzen erforderlich
sys_portal_page	RWCD	Administratorrolle zum Lesen/Schreiben/ Erstellen/Löschen von Homepage-Datensätzen erforderlich

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Vorgang	Beschreibung
sys_portal_preferences	RWCD	Administratorrolle zum Lesen/ Schreiben/Erstellen/Löschen von Portaleinstellungsdatensätzen erforderlich
sys_processor	WC	Administratorrolle zum Schreiben/Erstellen von Prozessordatensätzen erforderlich
sys_properties	WC	Administratorrolle zum Schreiben/Erstellen von Systemeigenschaften-Datensätzen erforderlich
sys_properties_category	WCD	Administratorrolle zum Schreiben/Erstellen/ Löschen von Eigenschaftskategorie-Datensätzen erforderlich
sys_report	delete	Rollen, die Berichtsdatensätze löschen können (schränkt das Löschen über die Berichts-UI nicht ein)
sys_report	write	Rollen, die in Berichtsdatensätze schreiben können (schränkt die Bearbeitung über die Berichts-UI nicht ein)
sys_report	gelesen	Anwender können ihre eigenen Berichtsdatensätze, die ihrer Gruppe sowie GLOBALE Datensätze lesen (hat keine Auswirkung auf die Anzeige über die Berichts-UI).
sys_report	gelesen	Rollen, die Berichtsdatensätze lesen können (Schränkt die Anzeige über die Berichts-UI nicht ein)
sys_reportroles	gelesen	Administratorrolle zum Lesen von Berichtsrollendatensätzen erforderlich
sys_script	WCD	Administratorrolle zum Schreiben/Erstellen/ Löschen von Business-Regel-Datensätzen erforderlich
sys_script_ajax	WCD	Administratorrolle zum Schreiben/Erstellen/ Löschen von AJAX-Skriptdatensätzen erforderlich
sys_script_client	WCD	Administratorrolle zum Schreiben/Erstellen/ Löschen von Clientskript-Datensätzen erforderlich
sys_script_include	WCD	Administratorrolle zum Schreiben/Erstellen/ Löschen von Skripteinbindungsdatensätzen erforderlich
sys_security_acl	write	Administratorrolle ist zum Schreiben in Zugriffssteuerungsdatensätze erforderlich
sys_security_acl_role	Erstellen	Administratorrolle zum Erstellen von Zugriffsrollendatensätzen erforderlich
sys_security_acl_role	delete	Administratorrolle zum Löschen von Zugriffsrollendatensätzen erforderlich
sys_security_acl_role	write	Administratorrolle zum Schreiben in Datensätze für Zugriffsrollen erforderlich

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Vorgang	Beschreibung
sys_security_operation	delete	-Administratorrolle zum Löschen von Security Operation-Datensätzen erforderlich
sys_security_operation	Erstellen	-Administratorrolle zum Erstellen von Security Operation-Datensätzen erforderlich
sys_security_operation	write	Administratorrolle zum Schreiben in Datensätze von Security Operations erforderlich
sys_security_operation	query_range	
sys_security_operation		
sys_security_type	write	Administratorrolle zum Schreiben in Sicherheitstypdatensätze erforderlich
sys_security_type	Erstellen	-Administratorrolle zum Erstellen von Sicherheitstypdatensätzen erforderlich
sys_security_type	delete	Administratorrolle zum Löschen von Sicherheitstypdatensätzen erforderlich
sys_status	Erstellen	-Administratorrolle zum Erstellen von Systemstatusdatensätzen erforderlich
sys_status	delete	Administratorrolle zum Löschen von Systemstatusdatensätzen erforderlich
sys_status	write	Administratorrolle zum Schreiben in Systemstatus-Datensätze erforderlich
sys_template	write	Die Rolle „template_editor“ ist zum Schreiben in Vorlagendatensätze erforderlich
sys_template	Erstellen	Rolle „emplate_editor“ zum Erstellen von Vorlagendatensätzen erforderlich
sys_template	delete	Die Rolle „template_editor“ ist zum Löschen von Vorlagendatensätzen erforderlich
sys_template	gelesen	Rolle „template_editor“ zum Lesen von Vorlagenrollendatensätzen erforderlich
sys_ui_action	Erstellen	-Administratorrolle zum Erstellen von UI-Aktionsdatensätzen erforderlich
sys_ui_action	delete	Administratorrolle zum Löschen von UI-Aktionsdatensätzen erforderlich
sys_ui_action	write	Administratorrolle zum Schreiben in UI-Aktionsdatensätze erforderlich
sys_ui_action_view	write	Administratorrolle zum Schreiben in Datensätze von UI-Ansichtsaktionen erforderlich
sys_ui_action_view	Erstellen	-Administratorrolle zum Erstellen von Datensätzen für UI-Ansichtsaktionen erforderlich
sys_ui_action_view	delete	Administratorrolle zum Löschen von UI-Ansichtsaktionsdatensätzen erforderlich
sys_ui_policy	Erstellen	-Administratorrolle zum Erstellen von UI-Richtliniendatensätzen erforderlich

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Vorgang	Beschreibung
sys_ui_policy	delete	-Administratorrolle zum Löschen von UI-Richtliniendatensätzen erforderlich
sys_ui_policy	write	Administratorrolle zum Schreiben in UI-Richtliniendatensätze erforderlich
sys_ui_policy_action	Erstellen	Administratorrolle zum Erstellen von Datensätzen für UI-Richtlinienaktionen erforderlich
sys_ui_policy_action	delete	Administratorrolle zum Löschen von UI-Richtlinien-Aktionsdatensätzen erforderlich
sys_ui_policy_action	write	Administratorrolle zum Schreiben in Datensätze von UI-Richtlinienaktionen erforderlich
sys_ui_script	write	Administratorrolle zum Schreiben in UI-Skriptdatensätze erforderlich
sys_ui_script	delete	Administratorrolle zum Löschen von UI-Skriptdatensätzen erforderlich
sys_ui_script	Erstellen	Administratorrolle zum Erstellen von UI-Skriptdatensätzen erforderlich
sys_user	write	Anwender ohne Rolle können nur ihren eigenen Datensatz aktualisieren
sys_user_grmember	delete	Die Rolle „user_admin“ ist zum Löschen von Gruppenmitgliedsdatensätzen erforderlich
sys_user_grmember	write	Die Rolle „user_admin“ ist zum Schreiben in Gruppenmitgliedsdatensätze erforderlich
sys_user_group	Erstellen	Nur itil und höhere Versionen können Gruppendatensätze erstellen
sys_user_group	write	Nur itil und höhere Versionen können in Gruppendatensätzen schreiben
sys_user_has_role	gelesen	Rolle itil zum Anzeigen von Benutzerrollendatensätzen erforderlich
sys_user_role	Erstellen	Administratorrolle zum Erstellen von Rollendatensätzen erforderlich
sys_user_role	delete	Administratorrolle zum Löschen von Rollendatensätzen erforderlich
sys_user_role	write	Administratorrolle zum Schreiben in Rollendatensätze erforderlich
sys_user_role_contains	gelesen	Rolle „itil“ erforderlich, um enthaltene Rollendatensätze anzuzeigen
sys_user_role_contains	write	Administratorrolle zum Schreiben in Datensätze für enthaltene Rollen erforderlich
sys_user_token	RWCD	Administratorrolle zum Lesen/Schreiben/ Erstellen/Löschen von Anwender-Token-Datensätzen erforderlich

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Weitere Informationen zu diesem Plugin finden Sie unter Sicherheits-Jump-Start (ACL-Regeln) (Härtung der Instanzsicherheit) in Einstellungen für die Härtung der Instanzsicherheit.

Konfigurieren einer ACL-Regel

Konfigurieren Sie eine anwenderdefinierte ACL-Regel, um den Zugriff auf neue Objekte zu sichern oder das Standardsicherheitsverhalten zu ändern.

Vorbereitungen

Erforderliche Rolle: security_admin

Warum und wann dieser Vorgang ausgeführt wird

Zum Erstellen von ACL-Regeln müssen Sie Berechtigungen für die Rolle security_admin erhöhen.

Für Tabellen, die sich in einem anderen Bereich als der ACL-Regeldatensatz befinden, sind die Regeltypen beschränkt. Damit Bereichsmastertabellen den Bereich ableiten und bereichsbezogene ACLs ausführen, legen Sie die Eigenschaft *glide.enforce_security_scope.<scope_name>* auf **true**fest. Dadurch wird sichergestellt, dass ACLs im globalen Bereich nicht übereinstimmen, wenn in der relevanten Tabelle bereichsspezifische ACLs erstellt werden. Beispiele sind das Sichern von Daten in gemeinsam genutzten Anwendungstabellen im globalen Bereich, z. B. in den Tabellen „sys_attachment“ oder „question_answer“.

Prozedur

1. Berechtigungsrollen auf die Rolle „security_admin“ erhöht.
2. Navigieren zu **Systemsicherheit** > **Zugriffssteuerung (ACL)**an.
3. **Tipp:** Beim Erstellen einer neuen ACL ist es hilfreich, Deny-Unless-ACLzu überprüfen.

   Klicken Sie auf **Neu**.
4. Füllen Sie das Formular aus.

Zugriffssteuerungsfelder

Feld	Beschreibung
Typ	Wählen Sie aus, welche Art von Objekt diese ACL-Regel sichert. Der Objekttyp bestimmt, wie das Objekt benannt wird und welche Vorgänge verfügbar sind. Dieses Feld wird schreibgeschützt, nachdem die ACL-Regel erstellt wurde. Wenn Sie den Typ ändern möchten, müssen Sie die ACL löschen und eine neue mit dem richtigen Typ erstellen.
Vorgang	Wählen Sie den Vorgang aus, den diese ACL-Regel sichert. Jeder Objekttyp verfügt über eine eigene Liste von Vorgängen. Eine ACL-Regel kann nur einen Vorgang sichern. Um mehrere Vorgänge zu sichern, erstellen Sie für jeden eine separate ACL-Regel.
Admin-Aufhebungen	Aktivieren Sie dieses Kontrollkästchen, damit Anwender mit der Administratorrolle automatisch die Berechtigungsprüfung für diese ACL-Regel bestehen. Administratorbenutzer bestehen unabhängig davon, welche Skript- oder Rollenbeschränkungen gelten. Die Rolle **niemand**, die nur von ServiceNow -Mitarbeitern zugewiesen werden kann, hat jedoch Vorrang vor der Option zum Überschreiben des Administrators. Wenn

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	einer ACL die Rolle **niemand** zugewiesen ist, können Administratoren nicht auf die Ressource zugreifen, auch wenn **Administratorüberschreibungen** ausgewählt sind. Siehe Basissystemrollen . Deaktivieren Sie dieses Kontrollkästchen, wenn Administratoren die in dieser ACL-Regel definierten Berechtigungen erfüllen müssen, um Zugriff auf das gesicherte Objekt zu erhalten. Da Administratoren Rollenprüfungen immer übergeben (siehe Beschreibung des Felds **Erfordert Rolle**), verwenden Sie den Bedingungsgenerator oder das Feld **Skript**, um eine Berechtigungsprüfung zu erstellen, die Administratoren übergeben müssen.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um diese ACL-Regel zu erzwingen.
Erweitert	Aktivieren Sie dieses Kontrollkästchen, um das Feld **Skript** anzuzeigen. **Wichtig:** Ob im Feld Skript ein **Skript** vorhanden ist. Dieses Skript wird ausgeführt, auch wenn das Feld nicht im Formular angezeigt wird.
Name	Geben Sie den Namen des gesicherten Objekts ein, entweder den Datensatznamen oder die Tabellen- und Feldnamen. Je spezifischer der Name, desto spezifischer die ACL-Regel. Sie können das Platzhalterzeichen Sternchen (*) anstelle eines Datensatzes, einer Tabelle oder eines Feldnamens verwenden, um alle Objekte auszuwählen, die einem Datensatztyp, allen Tabellen oder allen Feldern entsprechen. Sie können ein Platzhalterzeichen und eine Textsuche nicht kombinieren. Beispiel: Incident* ist kein gültiger ACL-Regelname, Incident.* und *.number sind jedoch gültige ACL-Regelnamen. **Hinweis:** Klicken Sie auf das blaue Dreieck, um den Datensatznamen oder die Tabellen- und Feldnamen des gesicherten Objekts manuell einzugeben. Verwenden Sie diese Option, um ein Objekt zu sichern, das nicht in der Dropdownliste angezeigt wird.
Beschreibung	Geben Sie eine Beschreibung des Objekts oder der Berechtigungen ein, die diese ACL-Regel sichert.
Erfordert Rolle	Verwenden Sie diese Liste, um die Rollen anzugeben, die ein Anwender für den Zugriff auf das Objekt haben muss. Wenn Sie mehrere Rollen auflisten, kann ein Benutzer mit einer der aufgeführten Rollen auf das Objekt zugreifen. Die Liste „ *Erfordert Rolle* “ wird als zugehörige Liste angezeigt. **Hinweis:** Benutzer mit der Administratorrolle bestehen diese Berechtigungsprüfung immer, da die Administratorrolle Benutzern automatisch alle anderen Rollen gewährt.
Bedingung	Verwenden Sie diesen Bedingungsgenerator , um die Felder und Werte auszuwählen, die „wahr“ sein müssen, damit Anwender auf das Objekt zugreifen können.
Skript	Geben Sie ein anwenderdefiniertes Skript ein, das die für den Zugriff auf das Objekt erforderlichen Berechtigungen beschreibt. Das Skript kann die Werte der *aktuellen* und *vorherigen* globalen Variablen in

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Geschäftsregeln sowie Systemeigenschaften verwenden. Das Skript muss auf eine von zwei Arten eine Wahr- oder Falsch-Antwort generieren: ◦ geben Sie eine *Antwortvariable* zurück, die auf den Wert „true“ oder „false“ festgelegt ist ◦ als „true“ oder „false“ auswerten In beiden Fällen erhalten Benutzer nur dann Zugriff auf das Objekt, wenn das Skript als „true“ ausgewertet wird und der Benutzer die Bedingungen der ACL-Regel erfüllt. Sowohl die Bedingungen als auch das Skript müssen zu „true“ ausgewertet werden, damit ein Benutzer auf das Objekt zugreifen kann. **Hinweis:** Wenn sich das ausgewertete Element in einer zugehörigen Liste befindet, verweist **current** auf das Element, auf dem sich die zugehörige Liste befindet, und nicht auf das aktuelle Element, für das die ACL gilt. Wenn sich das Element jedoch, für das Sie die ACL auswerten, nicht in einer zugehörigen Liste befindet, verweist **current** auf das tatsächliche Element.

5. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.

Deny-Unless-ACL

Erfahren Sie mehr über Deny-Unless-ACLs.

Deny-Unless-ACLs werden mit einem „deny-unless“-Ansatz ausgewertet. Die ACL definiert die Anwender, die NICHT abgelehnt werden. Anders ausgedrückt: Dem Benutzer wird der Zugriff verweigert, **wenn** die Rollen-, Bedingungs- und Skriptanforderungen nicht erfüllt sind.

Wichtig: „Deny-Unless“-ACLs haben in der ACL-Auswertung Priorität gegenüber „Allow-If“-ACLs, da sie zuerst ausgewertet werden.

Eine Deny-Unless-ACL erzeugt 2 Ergebnisse

Auswertungsergebnis	Ergebnis
Bestanden	Die definierten Rollen, Datenbedingungen, Sicherheitsattribute und Skriptanforderungen werden erfüllt. Die ACL fährt mit einer weiteren Auswertung fort **Wichtig:** Zulassen, wenn ACLs dem Betreff noch Zugriff auf die Ressource gewähren müssen.
Fehlgeschlagen	Die Deny-Unless-ACL wird als fehlgeschlagen markiert, und der Zugriff wird verweigert.

Im Folgenden finden Sie ein erläutertes Beispiel für eine Deny-Unless-ACL:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- ACL hat die Rollen `sn_hr_core.manager` und `itil`
- Bedingung hat aktiv = `wahr`
- Skript hat Antwort = `gs.isLoggedIn();`

Dem Anwender wird der Zugriff verweigert, es sei denn, alle 3 Anforderungen für diese ACL sind erfüllt. Damit diese Deny-Unless-ACL übergeben werden kann, muss ein Anwender entweder über die Rolle „ `sn_hr_core.manager`" oder „`itil` " verfügen, auf einen Datensatz mit dem Feld „aktiv" = `true`zugreifen und angemeldet sein. Die Deny-Unless-ACL schlägt fehl, wenn eine der drei Anforderungen nicht erfüllt ist.

Abfrage-ACLs

Mit Abfrage-ACLs können Sie eine präzisere Zugriffssteuerung definieren, indem Sie explizit festlegen, wer die Daten abfragen kann.

Was ist eine Abfrage-ACL?

Bei Abfrage-ACLs wird der Vorgang entweder auf `„query_range"` oder `„query_match"` festgelegt. Abfrage-ACLs ermöglichen eine spezifischere Kontrolle von Anwenderabfragen und schränken oder ermöglichen den Zugriff basierend auf ihrem Setup. Abfrage-ACLs sind leistungsstarke Tools gegen Blind-Query-Angriffe, , bei denen ein Angreifer die Daten blind abfragt, um Informationen aus den Ergebnissen zu extrahieren, auch wenn er die Werte nicht sehen kann.

Wann eine Abfrage-ACL verwendet werden soll

Immer wenn eine Spalte vertrauliche Werte enthält und teilweisen/bedingten Zugriff auf Daten ermöglicht, sollte eine Abfrage-ACL berücksichtigt und nach Bedarf basierend auf der Vertraulichkeit der Daten implementiert werden. Überall dort, wo ein teilweiser/bedingter Zugriff auf Zeilen und ihre Spalten in Tabellen besteht, insbesondere wenn dieser Zugriff nicht durch Datenfilter erzwungen wird, sollten Abfrage-ACLs nach Bedarf basierend auf der Vertraulichkeit der Daten implementiert werden.

Hinweis: Berücksichtigen Sie Abfrage-ACLs, wenn einige Anwender Zugriff auf einige Zeilen oder Spalten haben und andere nicht.

Example: Abfragesteuerelement für die Gehaltsabrechnung

Ich kann eine Zeile in der Gehaltsabrechnungstabelle mit meinem Gehalt sehen, aber es gibt keinen Grund für mich, Bereichsabfragen zu stellen, um Benutzer mit einem Gehalt innerhalb von 2 Grenzen abzufragen. Eine `„query_range"-ACL` für das Gehalt würde verhindern, dass ich diese Abfrage stellen kann.

Example: Steuerelement für HR-Abfragen

Ich kann alle hr_profiles sehen, aber nur die Sozialversicherungsnummer für mich. Ich habe keine geschäftlichen Abfragen der Sozialversicherungsnummer, und Abfrage-ACLs sollten verhindern, dass ich Abfragen der Sozialversicherungsnummer anderer HR-Profile ausführen kann, um zu versuchen, Sozialversicherungszuordnungen zu extrahieren.

ACL-Verhalten abfragen

Abfrage-ACLs verwenden die Vorgänge „ `query_match"` und `„query_range"`, um ein sicheres und granulares Tabellenabfrageverhalten zu gewährleisten. Ihr Verhalten wird im Folgenden beschrieben:

`Abfrage_Übereinstimmung`

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Woraus besteht „`query_match` “: EQUALS, NOT_EQUALS, IN, NOT_IN, SAMEAS, NSAMEAS, ANYTHING, ISAMPTYSTRING, ISAMPTY, ISNOTEMPTY, ISNULL, ISNOTNULL „ `query_match` “ besteht aus den „sicheren Operatoren“ in dem Sinne, dass sie zum Abrufen bestimmter Datensätze erstellt werden und nicht zur Rückgabe anderer Datensätze ausgenutzt werden können.

Auswertungsergebnis	Ergebnis
Bestanden	Der Benutzer kann Übereinstimmungsabfragen übermitteln
Fehlgeschlagen	Anwender kann keine Übereinstimmungsabfragen übermitteln: • GLEICH • NOT_GLEICH • IN • NOT_IN • SAMEAS • NSAMEAS • ALLES • ISTLEERSTRING • IST leer • ISNOTEMPTY • ISNULL • ISNOTNULL

`query_range`

„`query_range`“ besteht aus allen anderen (STARTS_WITH, CONTAINS, >=, <= usw.), die gefährlicher sind, da sie es Benutzern ermöglichen, durch Anpassen der Grenzwerte weitere Datensätze abzufragen.

Auswertungsergebnis	Ergebnis
Bestanden	Anwender können Bereichsabfragen übermitteln, und die Sortierung ist unbeschränkt
Fehlgeschlagen	Der Anwender kann keine Bereichsabfragen mit (STARTS_WITH, CONTAINS, >=, <= usw.) übermitteln. Das Sortieren nach Spalte ist eingeschränkt

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:

Abfrage-ACLs (query_match und query_range) sind standardmäßig auf eine Star-Stern-ACL festgelegt, die den Lesezugriff delegiert. Dies bedeutet, dass, wenn ACLs für Abfragen erzwungen werden, der Lesezugriff auf die Spalte ausgewertet wird, wenn keine Abfrage-ACL erstellt wurde. Wenn Abfrage-ACLs definiert sind, überschreiben sie das Standardverhalten.

Sichern Sie Datensätze in einer eingebetteten Liste

Um Sicherheit auf die Datensätze in eingebetteten Listen anzuwenden, beschränken Sie das Bearbeiten und Löschen von Datensätzen in eingebetteten Listen auf bestimmte Rollen.

Vorbereitungen
Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Zugriffssteuerung (ACL)**an.
2. Öffnen Sie den Datensatz **Schreiben** oder **Löschen** für die entsprechende Tabelle.
3. Fügen Sie im Abschnitt „Erfordert Rolle“ des Formulars die Rollen hinzu, die über Schreib- oder Löschberechtigungen für diese Tabelle verfügen.
4. Speichern Sie die Änderungen.
   Wenn Datensätze aus der zugehörigen Tabelle in einer eingebetteten Liste angezeigt werden, sind die Optionen zum Bearbeiten und Löschen nur für Benutzer mit den angegebenen Rollen verfügbar.

Contextual Security Manager

Der Kontextsicherheitsmanager schützt Ihre Daten, indem er die Autorisierung zum Lesen, Schreiben, Erstellen und Löschen steuert.

Hauptvorteile

Der Kontextsicherheitsmanager kennt die Systemtabellenhierarchie, sodass Sie spezifische Sicherheitsregeln für ein Feld basierend darauf erstellen können, wo es in der Hierarchie angezeigt wird. Der Kontextsicherheitsmanager bietet folgende Vorteile:

- **Kontextbezogene Sicherheit**: Sichern Sie einen Datensatz basierend auf dem Inhalt des Datensatzes.
- **Hierarchische Sicherheit**: Wenden Sie Sicherheitsregeln auf jede Ebene in der Objekthierarchie an.

Felder und Tabellen werden gesichert

Mit dem Legacy Simple Security Manager können Sie Felder und Tabellen sichern, indem Sie dem entsprechenden Wörterbucheintrag Rollen hinzufügen. Mit dem Kontextsicherheitsmanager werden diese Wörterbuchrollen nicht mehr getestet. Stattdessen sucht das System in Feldern und Tabellen nach ACL-Regeln.

Warnung: Nachdem Sie den Kontextsicherheitsmanager installiert haben, müssen Sie Felder und Tabellen über ACL-Regeln sichern. Selbst wenn Sie das Formularlayout des Wörterbuchformulars konfigurieren und einem Wörterbucheintrag Rollen hinzufügen, werden die Rechte nicht geändert.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kontextbezogene Sicherheit und Rollen

Sie können Benutzern oder Gruppen Rollen zuweisen. Nach der Installation des Kontextsicherheitsmanagers wird jedoch das Feld „ **Rollen** “ im Benutzerdatensatz nicht mehr aktiviert und wird in Ihren Benutzer- und Gruppenformularen nicht mehr angezeigt. Stattdessen müssen Sie Rollen zur zugehörigen Liste „Rollen“ und nicht zum Benutzer- oder Gruppendatensatz hinzufügen.

Anwendungen und Module enthalten Listen der Rollen, die zum Anzeigen dieser Anwendungen erforderlich sind. Um beispielsweise die Systemdefinitionsanwendung anzuzeigen, ist die Administratorrolle erforderlich. Sicherheitsrechte für Anwendungen und Module werden weiterhin über Rollen-Arrays definiert.

Sowohl Katalogelemente als auch Katalogvariablen enthalten Listen der Rollen, die zum Anzeigen erforderlich sind. Sicherheitsrechte für Katalogelemente und Katalogvariablen werden weiterhin über diese Rollen-Arrays definiert.

Unter dem Kontextsicherheits-Manager erbt eine Gruppe weiterhin automatisch jede Rolle, die der Gruppe gewährt wird, wenn die Kennzeichnung „herbs“ für die Rolle auf *true*festgelegt ist.

Der Manager für Kontextsicherheit wird aktiviert

Der Kontextsicherheitsmanager ist im Basissystem aktiv. Wenn in der Tabelle „Anwenderrollen“ viele doppelte Einträge vorhanden sind, müssen Sie möglicherweise ein Upgrade auf Kontextsicherheit: Rollenverwaltung V2 durchführen, um doppelte Rollen zu entfernen. Plugins umfassen:

Kontextbezogene Sicherheit: Rollenverwaltung [com.glide.role_management]

Bietet kontextbezogene Sicherheitsfunktionen. Dieses Plugin wird automatisch installiert.

Contextual Security: Role Management V2 [com.glide.role_management.inh_count]

Verhindert doppelte Einträge durch geerbte Rollen in der Tabelle „Anwenderrollen“ [sys_user_has_role]. Dieses Plugin wird automatisch auf neuen Instanzen installiert und kann für Upgrades aktiviert werden. Das Plugin „Kontextsicherheit: Erweiterungen der Rollenverwaltung“ ist eine frühere Version dieses Plugins. Das Plugin „Extensions Role Management“ enthält das Skript RoleManagementVerify() nicht. Dieses Skript gibt eine Liste der Änderungen zurück, die bei einem Upgrade durchgeführt werden, sodass Sie die vom Plugin vorgenommenen Änderungen überwachen können.

Hinweis: Nach der Aktivierung von Role Management V2 müssen Sie die Systemeigenschaft „glide.role_management.v2.audit_roles“ festlegen, damit die Tabelle „Audit-Rollen“ Audit-Datensätze im Zusammenhang mit Anwenderrollen erstellen kann. Weitere Informationen zum Festlegen dieser Eigenschaft und zur Tabelle mit den Audit-Rollen finden Sie unter:

- Aktivieren Sie das Rollenauditing mit Kontextsicherheit: Rollenmanagement V2.
- Kontextsicherheit: Plugin für Rollenmanagement in den Härtungseinstellungen für die Instanzsicherheit.
- Audit-Anwenderrollen

Verhindern Sie doppelte Einträge mit Kontextsicherheit: Rollenverwaltung V2

Von anderen Rollen geerbte Rollen werden als einzelne Einträge in der Tabelle „Anwenderrollen“ [sys_user_has_role] hinzugefügt, was möglicherweise dazu führt, dass eine

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rolle doppelte Einträge aufweist. Kontextbezogene Sicherheit: Das Rollenmanagement V2 entfernt diese doppelten Einträge und verhindert zukünftige Duplikate.

Doppelte Einträge durch Vererbungsanzahl eliminieren

Kontextbezogene Sicherheit: Das Rollenmanagement V2 verwendet die Spalte „Anzahl der Übernahmen“ (inh_count), um nachzuverfolgen, wie oft eine Rolle von einer anderen Rolle oder Gruppe geerbt wird. In der Tabelle „Benutzerrollen“ [sys_user_has_role] kann ein Benutzer eine bestimmte Rolle nur einmal erben, wodurch doppelte Einträge vermieden werden. Die Spalte „Anzahl der Übernahmen“ (inh_count) ist schreibgeschützt und berechnet, wie oft der Benutzer eine Rolle erbt.

Aktivierungsänderungen

Kontextbezogene Sicherheit: Das Rollenmanagement V2 wird automatisch auf neuen Instanzen installiert und kann für -Upgrades aktiviert werden. Kontextsicherheit: Rollenverwaltung V2 ersetzt bei Aktivierung sowohl Kontextsicherheit als auch Kontextsicherheit: Rollenverwaltungserweiterungen.

Wenn Kontextsicherheit: Rollenmanagement V2 aktiviert ist, sind die folgenden Spalten veraltet, verbleiben jedoch aus Gründen der Abwärtskompatibilität in der Tabelle „Benutzerrollen“:

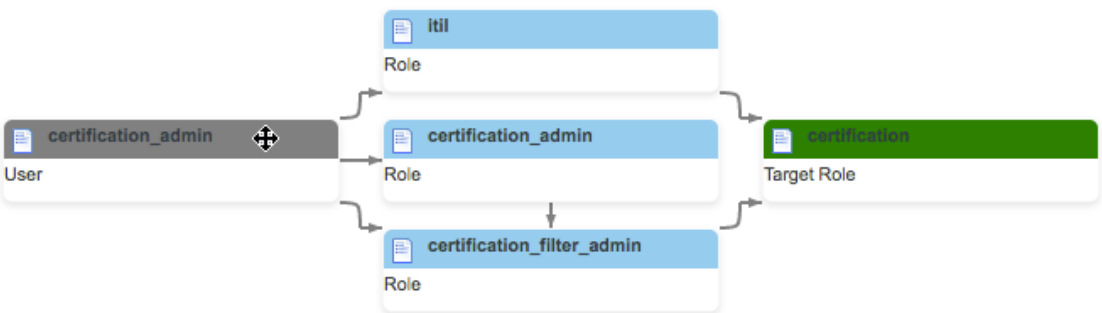
- assigned_by (wird nur von der Rollendelegierung verwendet)
- „included_in_role“
- „included_in_role_instance“

Warnung: Wenn diese Spalten in anwenderdefinierten Skripts in Ihrer Instanz verwendet werden, führen Sie kein Upgrade auf Role Management V2 durch.

Visualisieren Sie die Rollenvererbung über die Rollenvererbungszuordnung

Die Zuordnung der Rollenvererbung zeigt eine visuelle Darstellung der geerbten Rollen. Sie können diese Zuordnung verwenden, um die in der Spalte „Anzahl der Vererbung“ (inh_count) dargestellten Rollen zu verstehen. Um die Rollenvererbungszuordnung anzuzeigen, konfigurieren Sie die Tabelle „Anwenderrollen“ [sys_user_has_role] so, dass die Spalte „Rollenvererbungszuordnung“ angezeigt wird.

Rollenvererbungskarte



© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Upgrade auf Kontextsicherheit: Rollenverwaltung V2

Kontextbezogene Sicherheit: Das Rollenmanagement V2 wird automatisch auf neuen Instanzen installiert. Sie können ein Upgrade von Kontextsicherheit: Rollenmanagement auf Kontextsicherheit: Rollenmanagement V2 durchführen, um doppelte Rollen in der Tabelle „Anwenderrollen“ zu entfernen und zukünftige Duplikate zu verhindern.

Vorbereitungen

Erforderliche Rolle: admin, security_admin
Sie müssen die Administratorrolle und Auf eine privilegierte Rolle hochstufen innehaben, um die effektive Rolle security_admin zu erhalten.

Hinweis: Vor dem Upgrade auf Kontextsicherheit: Rolle: Management V2 müssen Sie die Tabelle „Audit-Rollen“ aktivieren, um Audit-Datensätze zu erstellen, die sich auf Anwenderrollen beziehen. Weitere Informationen zum Festlegen der erforderlichen Systemeigenschaft finden Sie unter Aktivieren Sie das Rollenauditing mit Kontextsicherheit: Rollenmanagement V2.

Warum und wann dieser Vorgang ausgeführt wird

Dieses Verfahren beschreibt, wie Sie Ihre Rolle für die kontextbezogene Sicherheit aktualisieren und wie Sie die zugehörigen Plugins aktivieren, die in der folgenden Tabelle beschrieben werden.

Plugins für Kontextsicherheit: Rollenverwaltung V2

Plugin	Beschreibung
Kontextbezogene Sicherheit: Rollenverwaltung V2 [com.glide.role_management.inh_count]	Verhindert doppelte Einträge in der Tabelle „Benutzerrollen“ [sys_user_has_role]. Zur Aktivierung des Plugins ist die Rolle „security_admin“ oder ein Benutzer mit erweiterten Rechten erforderlich. Sie können auch Kundenservice und Supportkontaktieren.
Kontextbezogene Sicherheit: REST API für Rollenmanagement V2 [com.glide.role_management.inh_count.rest_api]	Aktiviert API-Funktionen für die Rollenverwaltung.

Testen Sie vor dem Upgrade von Kontextsicherheit: Rollenmanagement auf Kontextsicherheit: Rollenmanagement V2 die Ergebnisse eines Upgrades, indem Sie das Skript ausführen. Das Skript gibt eine Liste der Changes zurück, die durch ein Upgrade durchgeführt werden. Wenn die Änderungen akzeptabel sind, installieren Sie das Plugin „Contextual Security: Role Management V2“. Wenn die Änderungen nicht akzeptabel sind, installieren Sie das Plugin „Contextual Security: Role Management V2“ nicht. Alternativ können Sie das Upgrade durchführen und dann die erforderlichen Änderungen manuell vornehmen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Testen Sie die Auswirkungen eines Upgrades vor dem Upgrade, indem Sie das folgende Skript ausführen.

   a. Navigieren zu **Systemdefinition** > **Skripts – Hintergrund**an.

   b. Führen Sie das folgende Skript im globalen Bereich aus.

   ```
   new RoleManagementVerify().verifyInheritedRoles();
   ```

   Bei großen sys_user_has_role-Tabellen kann die Ausführung mehrere Stunden dauern. Bearbeiten oder fügen Sie während dieser Zeit keine Anwenderrollen hinzu. Beispielergebnis basierend auf Testdaten:

   ```
   *** Script: 2016-12-01 19:58:54 Starting checking of inherited roles
    for all users...
   *** Script: User: itam, inherited roles to be ADDED:
    financial_mgmt_user
   *** Script: User: bernard.laboy, inherited roles to be DELETED:
    api_analytics_read,pa_viewer,rest_api_explorer,a123
   *** Script: User: bernard.laboy, inherited roles to be ADDED:
    dependency_views
   *** Script: Number of inherited-role records in sys_user_has role,
    current: 260, after re-calculation: 258
   *** Script: Number of users with discrepancies for inherited roles: 2
   *** Script: 2016-12-01 19:58:55 Finished checking of inherited roles
    for all users!
   ```

   c. Werten Sie die Skriptergebnisse aus, um zu bestimmen, ob die vorgeschlagenen Änderungen akzeptabel sind.

2. Aktivieren Sie das Plugin „Contextual Security: Role Management V2“.

   Wichtig: Zur Aktivierung des Plugins ist die Rolle „security_admin“ oder ein Benutzer mit erweiterten Rechten erforderlich. Sie können auch Kundenservice und Supportkontaktieren.

   a. Navigieren zu **Systemdefinition** > **Plugins**an.

   b. Suchen Sie nach dem Namen des Plugins, und klicken Sie darauf.

   c. Überprüfen Sie im System-Plugin-Formular die Plugin-Details, und klicken Sie dann auf den zugehörigen Link **Aktivieren/Aktualisieren**.

   d. Klicken Sie auf **Aktivieren**.

Ergebnisse

Nach der Aktivierung von Role Management V2 werden die im Skriptergebnis beschriebenen Changes umgesetzt. Die Spalte „Anzahl der Übernahmen“ (inh_count) in der Tabelle „Benutzerrollen“ ist schreibgeschützt und spiegelt automatisch wider, wie oft der Benutzer eine Rolle erbt.

Aktivieren Sie das Rollenauditing mit Kontextsicherheit: Rollenmanagement V2

Legen Sie eine Systemeigenschaft fest, damit die Tabelle mit den Audit-Rollen Audit-Datensätze erstellen kann, die sich auf Anwenderrollen beziehen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn diese Option aktiviert ist, werden in der Tabelle „Audit-Rollen“ [sys_audit_role] Änderungen an Benutzerdatensätzen verwaltet. Weitere Informationen zu Rollen-Audits finden Sie unter Audit-Anwenderrollen . Wenn das Plugin „Contextual Security: Role Management V2“ [com.glide.role_management.inh_count] installiert ist, müssen Sie eine Systemeigenschaft auf „ **true** “ festlegen, um das Rollenauditing zu aktivieren.

Prozedur
1. Navigieren Sie zur Tabelle „Systemeigenschaften“ [sys_properties].
2. Fügen Sie die Systemeigenschaft *glide.role_management.v2.audit_roles* hinzu, und setzen Sie sie auf **true**.

   Wenn das Plugin „Kontextsicherheit: Rollenmanagement V2“ [com.glide.role_management.inh_count] installiert ist und diese Eigenschaft auf „ **wahr** “ festgelegt wird, kann die Tabelle „Audit-Rollen“ [sys_audit_role] Datensätze erstellen, wenn sich die Anwenderrollen ändern.

Überprüfen Sie noch einmal, ob das Formular übermittelt wird

Wenn das System feststellt, dass ein bestimmtes Feld (z. B. task.number) vom aktuellen Benutzer nicht beschrieben werden darf, stellt das System dieses Feld schreibgeschützt dar, weswegen das Nummernfeld bei den meisten Incidents nicht bearbeitet werden kann.

Wenn Sie das System so einstellen, dass die Werte eingehender Felder noch einmal auf die Bearbeitbarkeit überprüft werden, wendet das System dieselben Sicherheitsregeln auf den eingehenden Zweig einer Transaktion an. Wenn Sie beispielsweise einen Incident übermitteln, prüft das System noch einmal, ob das Nummernfeld geschrieben werden kann, bevor Änderungen veröffentlicht werden.

Wenn Sie dem System mitteilen, dass eingehende Transaktionen nicht doppelt überprüft werden sollen, können Sie in ein nominell schreibgeschütztes Feld schreiben, wenn dies die Transaktion ist, die der Client zurücksendet. In vielen Bereitstellungen ist dies tatsächlich ein wünschenswertes Verhalten, wenn Sie beispielsweise Client-Skripts verwenden, um nominell schreibgeschützte Felder als Reaktion auf Benutzerauswahlen in anderen, bearbeitbaren Feldern festzulegen.

Eigenschaft	Standort	Standard
Sicherheit eingehender Transaktionen bei der Formularübermittlung nochmals überprüfen (Rechte werden immer bei der Formularerstellung überprüft)	**Systemeigenschaften** > **Sicherheit**	Deaktiviert (keine doppelte Kontrolle)

Standardmäßige Verweigerungseigenschaft

Die standardmäßige Deny-Eigenschaft (`glide.sm.default_mode`) steuert das Standardverhalten des Sicherheitsmanagers, wenn die einzigen übereinstimmenden ACL-Regeln die ACL-Regeln der Platzhaltertabelle sind.

Eine Reihe von ACL-Regeln für Platzhaltertabellen für die gängigsten datensatzbasierten Vorgänge sind verfügbar: Lesen, Schreiben, Erstellen und Löschen. Eine erhebliche Anzahl von ACLs für den rollenbasierten Zugriff auf Systemtabellen ist ebenfalls verfügbar.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispielsweise gibt es ACLs, die sys_script-Zugriff auf die Rolle „business_rule_admin“ gewähren, da diese Rolle nachweislich Geschäftsregeln verwalten kann.

Verwenden Sie die Eigenschaft `„glide.sm.default_mode“`, um diese Vorgänge für alle Tabellen zu verweigern oder zuzulassen:

- **Zugriff verweigern**: Die ACL-Regeln für Platzhaltertabellen schränken die Lese-, Schreib-, Erstellungs- und Löschvorgänge für alle Tabellen ein, es sei denn, der Benutzer verfügt über die Administratorrolle oder erfüllt die Anforderungen einer anderen ACL-Regel für Tabelle. Andere Vorgänge wie report_on und personalize_choices sind von dieser Einstellung nicht betroffen.
- **Zugriff zulassen**: Die ACL-Regeln für Platzhaltertabellen erlauben Lese-, Schreib-, Erstellungs- und Löschvorgänge für alle Tabellen, es sei denn, es sind bestimmte ACL-Regeln für Tabellen vorhanden, die diese Vorgänge einschränken.

Sie können `„glide.sm.default_mode“` nicht auf „ **Zugriff zulassen** “ zurücksetzen, nachdem die Option Zugriff **verweigern**festgelegt wurde.

Hinweis: Standardmäßig sind die ACL-Regeln der Platzhaltertabelle die einzigen ACL-Regeln, die den Wert der Eigenschaft `glide.sm.default_mode` überprüfen. Wenn Sie andere Vorgänge mit dieser Einstellung steuern möchten, erstellen Sie eigene ACL-Regeln, um nach diesem Eigenschaftswert zu suchen.

Weitere Informationen zu dieser Eigenschaft finden Sie unter Standardmäßig ablehnen in Härtungseinstellungen für Instanzsicherheit.

Erweiterte ACL-Konfiguration

Sie können nicht nur neue ACLs erstellen oder vorhandene ACLs ändern, sondern auch andere Aspekte der ACL-Funktionalität konfigurieren.

ACL-Regeln verweigern

Verweigern-Unless

Abfrage-ACL-Regeln

Aufgabe	Beschreibung
Wenden Sie ACL-Skriptbedingungen auf Referenzfelder an	Aktivieren Sie eine Eigenschaft, damit Skriptbedingungen auf Referenzfelder angewendet werden können, wenn Sie den Zugriff auf die Daten steuern möchten, die ein Referenzfeld in einem Formular oder in einer Liste anzeigt. Wenn Sie diese Option aktivieren, kann dies Auswirkungen auf die Leistung Ihrer Instanz haben.
ACLs auf AJAXGlideRecord (clientseitiger Glide-Datensatz) anwenden	Wenden Sie ACLs auf *`GlideAjax`*-API-Aufrufe an, damit das System nur die Daten abfragt, für die der aktuell verbundene Anwender berechtigt ist, darauf zuzugreifen.
Bewerten Sie die Administratorüberschreibung auf Zugriffsebene	ACL-Auswertung für Administratorüberschreibungen auf Zugriffsebene erzwingen. Standardmäßig übergeben Anwender mit der Administratorrolle automatisch die Berechtigungsprüfung für diese ACL-Regel, wenn im

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Beschreibung
	Formular „ACL-Regeln“ die Option Admin-Überschreibungen ausgewählt ist.
Verwenden Sie Tools für ACL-Debugging und Problembehandlung	Verwenden Sie Tools wie den ACL-Watcher, Debugging auf Feldebene und den Zugriff auf Ausgabenachrichten von ACL-Regeln, um Probleme bei der Problembehandlung und beim Debuggen von ACLs zu beheben.

Externen Benutzern Zugriff auf eine Tabelle bereitstellen

Um Benutzern mit nur der Rolle snc_external den Zugriff auf die Listenansicht einer Tabelle zu ermöglichen, müssen Sie eine Reihe von ACLs erstellen.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Auf eine privilegierte Rolle hochstufen
2. Erstellen Sie eine ACL-Regel mit den folgenden Einstellungen:
   - **Typ**: ui_page
   - **Operation**: Lesen
   - **Name**: {table_name}_list
   - **Erforderliche Rolle**: snc_external
3. Fügen Sie in der standardmäßigen **Lese**-ACL für die Tabelle **snc_external** in die Liste „Erforderliche Rolle“ hinzu.
   Erstellen Sie die ACL, wenn sie nicht bereits vorhanden ist.
4. Verwenden Sie diese Einstellungen, um eine andere ACL zu erstellen:
   - **Typ**: ui_page
   - **Operation**: Lesen
   - **Name**: {table_name}
   - **Erforderliche Rolle**: snc_external
5. Verwenden Sie diese Einstellungen, um eine weitere ACL zu erstellen, um dem Benutzer Schreibzugriff für ein Feld in der Tabelle zu gewähren:
   - **Typ**: Datensatz
   - **Operation**: Erstellen
   - **Name**: {table_name} {column_name}
   - **Erforderliche Rolle**: snc_external

   Wiederholen Sie diesen Schritt für jedes Feld, auf das Sie dem Benutzer Schreibzugriff gewähren möchten. Verwenden Sie ein Sternchen ***** anstelle des Spaltennamens, um Zugriff auf alle Felder gleichzeitig bereitzustellen.

Wenden Sie ACL-Skriptbedingungen auf Referenzfelder an

Verwenden Sie die Systemeigenschaft *glide.sys_reference_row_check*, um geskriptete Bedingungen für Referenzfelder zu aktivieren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Standardverhalten soll die Leistung der Instanz verbessern. Wenn Sie Skriptbedingungen für Referenzfelder aktivieren möchten, fügen Sie die folgende Systemeigenschaft hinzu.

Hinweis: Weitere Informationen zum Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Systemeigenschaft

Eigenschaft	Beschreibung
glide.sys_reference_row_check	Steuert, ob die Skriptbedingungen von Zugriffskontrollregeln für Referenzfelder einer Tabelle gelten. • Typ: Wahr | Falsch • Standardwert: **false** • Speicherort: Fügen Sie der Tabelle „Systemeigenschaften“ [sys_properties] eine Systemeigenschaft hinzu

Hinweis: Wenn die Systemeigenschaft *glide.sys_reference_row_check* nicht vorhanden ist oder auf „false“ festgelegt wurde, werden Skriptbedingungen für Zugriffssteuerungsregeln nicht angewendet. Dies bedeutet, dass eine ACL, die geskriptete Bedingungen enthält, ihre Prüfung besteht, solange die anderen ACL-Kriterien erfüllt sind (z. B. Rollenanforderungen).

ACLs auf AJAXGlideRecord (clientseitiger Glide-Datensatz) anwenden

Verwenden Sie eine Systemeigenschaft, um die Validierung der Zugriffssteuerungsliste (ACL) durchzuführen, wenn auf serverseitige Datensätze (z. B. Tabellen) mithilfe von GlideAjax-APIs in einem Client-Skript zugegriffen wird.

Wenn Sie Zugriffssteuerungslisten (ACL) auf *GlideAjax-* API-Aufrufe anwenden, können Sie nur Daten abfragen, für die der aktuell verbundene Benutzer über Zugriffsrechte verfügt. Wenn der Benutzer beispielsweise als ESS-Benutzer angemeldet ist, der keine Rechte zum Lesen der Tabelle „`cmn_location`“ hat, schlägt jeder *GlideAjax-* API-Aufruf durch den Benutzer fehl.

Wenn Sie das System ohne ACL ausführen, die *GlideAjax-* Aufrufe überprüft, kann die API Informationen zurückgeben, auf die der aktuell angemeldete Benutzer ansonsten nicht über die Anwenderoberfläche zugreifen könnte.

Hinweis: Legen Sie diese Eigenschaft in fest **Systemeigenschaften** > **Sicherheit**an.

Eigenschaft	Standard
Standardsicherheits-ACLs auf *AJAXGlideRecord-* Aufrufe anwenden	ACL-Überprüfung erzwungen

Warnung: `sys_class_name`, `sys_id` und `sys_domain` werden bei ACL-Prüfungen ignoriert.

Weitere Informationen zu dieser Eigenschaft finden Sie unter Aktivieren der AJAXGlideRecord-ACL-Überprüfung in Härtungseinstellungen für Instanzsicherheit.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bewerten Sie die Administratorüberschreibung auf Zugriffsebene

Wenn Sie die ACL-Bewertung für Administratorüberschreibungen auf Zugriffsebene erzwingen möchten, können Sie eine Systemeigenschaft hinzufügen.

Vorbereitungen
Erforderliche Rolle: security_admin

Warum und wann dieser Vorgang ausgeführt wird
ACLs werden kumulativ ausgewertet. Wenn in einem bestimmten Feld eine Anzahl von ACLs vorhanden ist und die Option **Admin** -Überschreibungen für eine davon auf „ **falsch** “ (nicht ausgewählt) festgelegt ist, werden die effektiven Administratorüberschreibungen für alle ACLs als **falsch**betrachtet. Dies führt dazu, dass Administratoren nicht einmal die ACL übergeben können, in der die Überschreibung wirksam sein sollte.

Prozedur

Fügen Sie der Tabelle „Systemeigenschaften“ die folgende Eigenschaft hinzu:

Eigenschaft	Beschreibung
glide.security.admin.override.accessterm	Wertet die Überschreibungsbedingung des Administrators auf Zugriffsebene aus. • Typ: Wahr | Falsch • Standardwert: „ **true** “ für neue Instanzen, „ **false** “ für Upgrades • Speicherort: Der Tabelle „Systemeigenschaften *[sys_properties]* “ hinzufügen **Hinweis:** Wenn die Eigenschaft in der Instanz nicht definiert ist, wird der Wert als „false“ ausgewertet.

ACL-Debugging-Tools

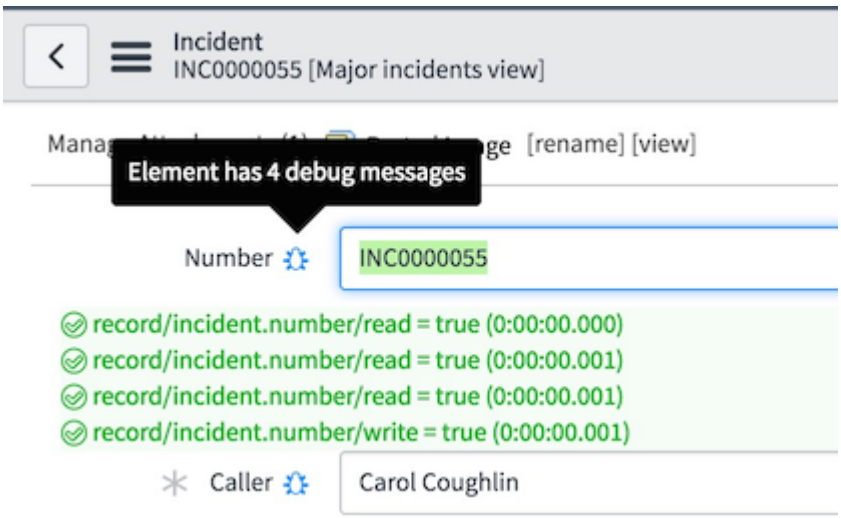
Debugging auf Feldebene und Ausgabenachrichten für Zugriffs-ACL-Regeln sind verfügbar, um Sie bei der Fehlerbehebung und beim Debuggen von ACLs zu unterstützen. Der ACL-Konfigurationsbeobachter zeigt Ihnen an, welche zugehörigen ACLs vorhanden sind, wenn Sie eine ACL ändern.

Debugging auf Feldebene

Wenn das Debugging aktiviert ist, wird neben jedem Feld mit einer ACL-Regel ein kleines Fehlersymbol ( ) angezeigt. Durch Klicken auf das Symbol werden die ACL-Regeln, die für das Feld gelten, und die Auswertungsergebnisse aufgelistet. Aktivieren Sie das Debugging, indem Sie zu navigieren **Systemsicherheit** > **Debugging** > **Sicherheitsregeln debuggen**an.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheit auf Feldebene für einen Incident



Nachdem Sie das ACL-Debugging aktiviert haben, können Sie die Identität eines anderen Anwenders annehmen, um zu sehen, welche ACL-Regeln der Anwender besteht und welche Fehler er aufweist. Wenn Sie die Identität eines Anwenders annehmen, können Sie nur das sehen, was dieser Anwender sehen darf. Sie können beispielsweise einen Datensatz nicht anzeigen, den eine ACL für den Benutzer nicht sichtbar macht. Um das Debuggen zu erleichtern, ist standardmäßig der Lesezugriff auf bestimmte ACL-bezogene Tabellen aktiviert, auch wenn die Identität eines Benutzers angenommen wird, der keinen Lesezugriff auf die Tabellen hat. Um diese Funktionalität zu ändern, legen Sie die folgende Eigenschaft auf **false**fest.

Um das Debuggen von ACL-Regeln zu aktivieren, navigieren Sie zu **Systemsicherheit** > **Sicherheitsregeln debuggen**an.

Systemeigenschaft	Beschreibung	Standardeinstellung
glide.security.access_acl_grant_read	Ermöglicht Lesezugriff auf die folgenden Tabellen, während die Identität eines Anwenders angenommen wird: sys_security_acl, sys_security_operation, sys_security_type und sys_user_role. Daher kann der Benutzer, der die Identität angenommen hat, Daten lesen, die der Benutzer, der die Identität angenommen hat, nicht lesen kann.	wahr **Hinweis:** Wenn die Eigenschaft auf „false“ festgelegt ist, kann der Benutzer, dessen Identität angenommen wurde, möglicherweise keine ACL-bezogenen Daten lesen. In diesem Fall ist möglicherweise eine zweite Sitzung erforderlich, in der Sie als Administrator oder Security_Administrator angemeldet sind, um ACLs zu debuggen.

ACL-Regelausgabenachrichten

Beim ACL-Debugging werden ACL-Regelausgabenachrichten am Ende jeder Liste und jedes Formulars angezeigt. In der Ausgabenachricht wird Folgendes angezeigt:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachrichtenelement	Beschreibung
TIME	Die Gesamtzeit, die für die Verarbeitung dieser ACL-Regel benötigt wird.
PFAD	Informationen, die jede ACL-Regel im Format eindeutig identifizieren:<ACL rule type> /<ACL rule name> /<Operation> .
Kontext	Das Objekt, das von der ACL-Regel ausgewertet wird.
RC	Der Rückgabecode der ACL-Regel. Der Wert „true“ übergibt die ACL-Regel. Bei einem „false“-Wert schlägt die ACL-Regel fehl.
REGEL	Eine kurze Zusammenfassung von Prozessoren und Skripts, gefolgt von ACL-Ergebnissen für die einzelnen ACL-Bewertungen auf Tabellen- und Feldebene. Die meisten ACL-Bewertungen zeigen ein Gesamtergebnis „Bestanden“ oder „Nicht bestanden“, gefolgt von einer Aufgliederung der Ergebnisse für jeden Typ von ACL-Kriterien: • iAccessHandler: Eine interne Systemprüfung mit ausgeblendetem Quellcode auf der Plattform. Dies ist eine Systemsicherheitsprüfung, die Sie nicht ändern können. IAccessHandler kann den Zugriff auf eine Ressource gewähren oder verweigern, ohne ACLs auszuwerten. Wenn IAccessHandler ignoriert wird, werden die ACLs ausgewertet. Sie können die IAccessHandler-Prüfungen in keiner Weise ändern. Beispielsweise wird eine IAccessHandler-Implementierung für Zugriffsprüfungen auf Anwendungsressourcen verwendet, und dies kann nicht geändert werden. Dies ist ab dem Release Istanbul verfügbar. • Rollen: Verifiziert, ob der Benutzer über die richtige Rolle verfügt. • Bedingung: Überprüfung, ob der Anwender die in der ACL-Regel (falls vorhanden) angegebene Bedingung erfüllt hat • Skript: Überprüfung, ob der Benutzer das in der ACL-Regel (falls vorhanden) angegebene Skript übergeben hat

Die angezeigten Symbole zeigen an, wie die ACL ausgewertet wurde:

Symbol	Beschreibung
Ein grünes Häkchen ()	Gibt an, dass die Tabelle oder das Feld die Kriterien erfüllt hat.
Ein rotes x-Symbol ()	Gibt an, dass die Tabelle oder das Feld nicht bestanden hat.
Ein leeres grauer Kreissymbol ()	Gibt an, dass die ACL-Bewertung nicht durchgeführt werden musste.
Ein blaues Häkchen, ein x oder ein leerer Kreis	Gibt an, dass die ACL aus einem zwischengespeicherten Ergebnis einer vorherigen ACL-Prüfung übernommen wurde. Die Symbole haben die gleiche Bedeutung wie die obigen.

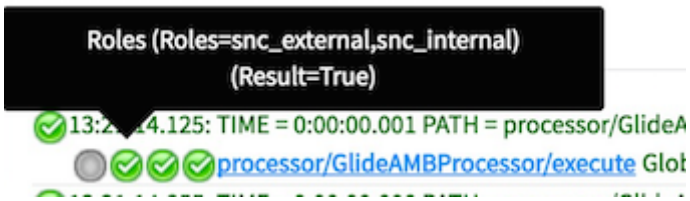
Sie können diese Aktionen für die ACL-Debug-Ausgabe ausführen:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Aktivieren oder deaktivieren Sie diese Kontrollkästchen oben in der Debug-Ausgabe:
  - **Sicherheitsregeln**: Ergebnisse der ACL-Prüfungen anzeigen oder ausblenden.
  - **Andere**: Andere Warnungen oder Nachrichten ein- oder ausblenden.
- Klicken Sie auf den Namen der ACL neben einer der Ausgabenachrichten, um diesen ACL-Datensatz zu öffnen.



- Bewegen Sie den Mauszeiger über eines der Symbole für die vier ACL-Prüfungen, um weitere Informationen anzuzeigen.



ACL-Fehlerbehebungsreferenz

Eine Liste häufiger ACL-Regelfehler und ihrer Lösungen.

Aktivieren Sie das Debugging, um bei der Behebung eines Problems zu helfen.

Problembehandlung

Fehler oder Symptom	Lösung
Sie können nicht auf Datensätze aus einer benutzerdefinierten Tabelle zugreifen.	Erstellen Sie eine Tabellen-ACL-Regel für die anwenderdefinierte Tabelle, die Anwendern Zugriff auf die Tabelle gewährt. Ohne eine explizite Tabellen-ACL-Regel müssen Benutzer die Berechtigungen in der Platzhalter-ACL-Regel für die Tabelle übergeben, die standardmäßig den Zugriff auf Administratoren beschränkt. Aktivieren Sie das Debugging, und bestimmen Sie, welche ACL-Regeln für die benutzerdefinierte Tabelle ausgewertet werden.
Sie erstellen eine anwenderdefinierte ACL-Regel, die nicht ordnungsgemäß funktioniert.	Die wahrscheinlichsten Probleme bestehen darin, dass eine andere Regel in der Verarbeitungsreihenfolge Vorrang vor Ihrer anwenderdefinierten Regel hat oder dass der Benutzer nicht alle Berechtigungsanforderungen für den Objekttyp erfüllt. Aktivieren Sie das Debugging, und verifizieren Sie, dass die ACL-Regel ausgewertet wird.
Die Feld-ACL-Regel funktioniert nicht ordnungsgemäß.	Wahrscheinlich ist eine Tabellen-ACL-Regel vorhanden, die vom Benutzer nicht erfüllt wurde. Aktivieren Sie das Debugging, und bestimmen Sie, welche ACL-Regeln für das Feld ausgewertet werden. Stellen Sie sicher, dass keine in Konflikt stehende Tabellen-ACL-Regel oder doppelte Feld-ACL-Regel vorhanden ist.
Die ACL-Regel für Ihre Tabelle	Entweder ist eine ACL-Regel höher in der Verarbeitungsreihenfolge oder eine doppelte Tabellen-ACL-Regel vorhanden, die die Tabellen-ACL-Regel beeinträchtigt. Aktivieren Sie das Debugging, und

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problembehandlung (Fortsetzung)

Fehler oder Symptom	Lösung
funktioniert nicht ordnungsgemäß.	bestimmen Sie, welche ACL-Regeln für die Tabelle ausgewertet werden.
Ein Feld wird in einer Liste angezeigt, nicht jedoch im Formular.	Es ist möglich, dass die ACL-Regelbedingungen oder das Skript in der Liste ausgelöst werden, aber nicht im Formular. Aktivieren Sie das Debugging, und legen Sie fest, wann die ACL-Regeln als „wahr“ ausgewertet werden. Aktualisieren Sie die Bedingungen oder das Skript so, dass sie in der Liste und im Formular dasselbe Verhalten aufweisen.
Sie erhalten eine Fehlermeldung, wenn Sie versuchen, einen Prozessor oder eine vom Client aufrufbare Skripteinbindung auszuführen.	Es ist eine ACL-Regel für den Prozessor oder die vom Client aufrufbare Skripteinbindung vorhanden, die der Anwender nicht erfüllt hat. Wenn der Benutzer Zugriff auf das Objekt haben soll, aktivieren Sie das Debugging, und bestimmen Sie, welche ACL-Regeln für den Prozessor oder die Skripteinbindung ausgewertet werden. Aktualisieren Sie die ACL-Regel oder die Anwenderrollen nach Bedarf, um auf das Objekt zuzugreifen.

ACL-Konfigurationsbeobachter

Der ACL-Konfigurationsbeobachter informiert Sie darüber, welche zugehörigen ACLs in einer Tabelle vorhanden sind, wenn Sie in derselben Tabelle eine ACL einfügen, aktualisieren oder löschen.

Der ACL-Konfigurationsbeobachter ist ein Interceptor-Fenster, das jedes Mal angezeigt wird, wenn Sie wichtige Änderungen an der Zugriffssteuerungstabelle [sys_security_acl] vornehmen. Zeigt ein Fenster mit der Zusammenfassung der Sicherheitsregeln an, in dem Sie ACLs anzeigen können, die sich auf die beziehen, die Sie ändern. Sie können keine ACLs im Sicherheitsregelfenster ändern. Um Änderungen vorzunehmen, schließen Sie das Beobachter-Fenster, und wechseln Sie zu diesen ACLs.

Der ACL-Konfigurationsbeobachter wird in den folgenden Situationen nicht angezeigt:

- Wenn Sie einen ACL-Datensatz speichern oder aktualisieren, ohne tatsächlich Änderungen vorzunehmen.
- Wenn Sie geringfügigere Änderungen vornehmen (kein Einfügen oder Löschen), z. B. das Aktualisieren von Skripts, Bedingungen und der Option admin-overrides.
- Wenn der ACL-Datensatz nicht aktiv ist.

Fenster „ACL-Sicherheitsregeln“.

Der Konfigurationsbeobachter zeigt den ACL-Ausführungsplan an. Der Ausführungsplan wird im Popup-Fenster für die Sicherheitsregeln angezeigt. Sie können diese Art von Informationen anzeigen:

Elemente des ACL-Konfigurationsfensters

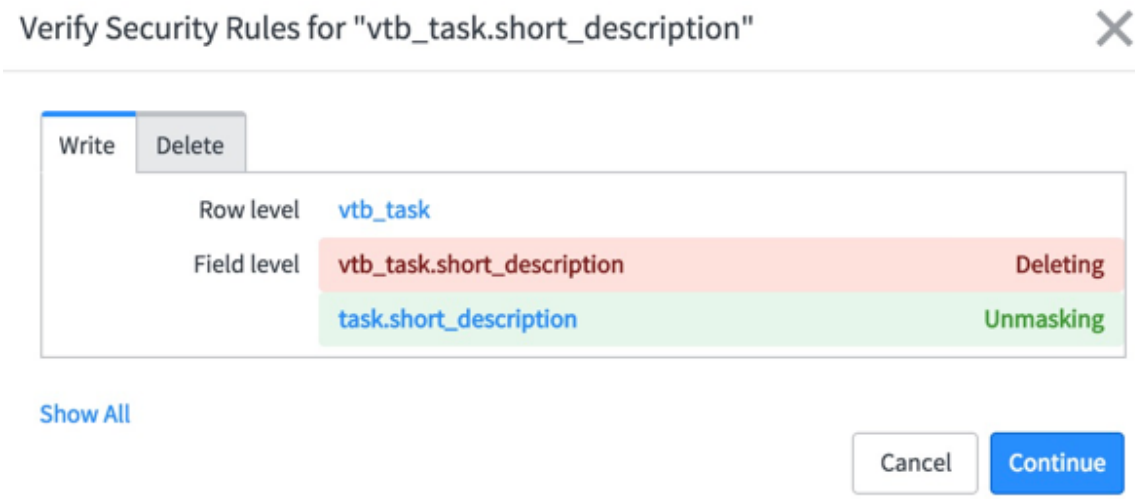
Element	Beschreibung
rot hervorgehoben	Eine ACL, die gelöscht oder deaktiviert ist.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Elemente des ACL-Konfigurationsfensters (Fortsetzung)

Element	Beschreibung
blau hervorgehoben	Eine ACL, die geändert wurde.
grün hervorgehoben	Eine ACL, die hinzugefügt wird oder aktiv wird.
Maskierung	Eine ACL, die gültig war, bis Sie eine Änderung vorgenommen haben.
Demaskiert	Eine ACL, die gerade erst wirksam wurde, als Sie eine Änderung vorgenommen haben.

Beispiel für Configuration Watcher



ACL-Ausführungsplan anzeigen

Administratoren können anzeigen, wie ACLs miteinander in Beziehung stehen, indem sie einen Ausführungsplan für eine beliebige ACL in der Instanz anzeigen.

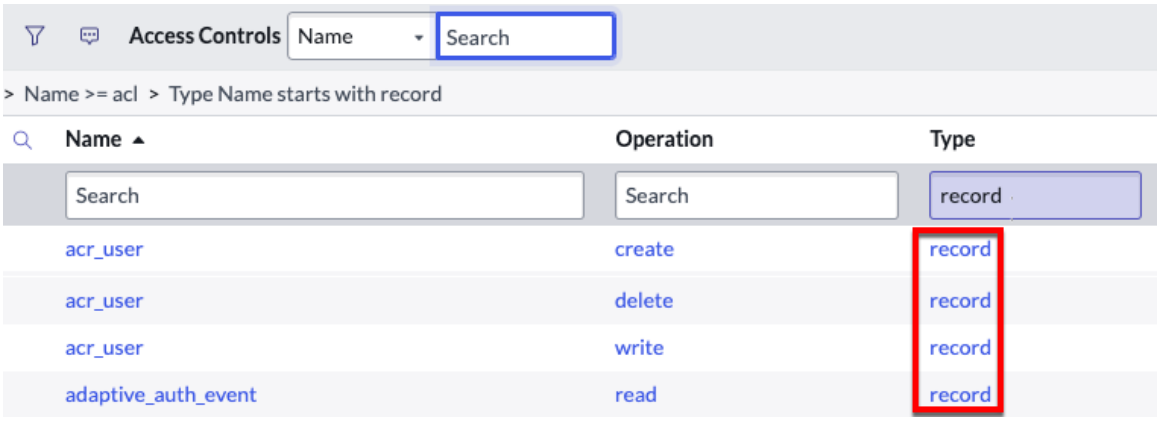
Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

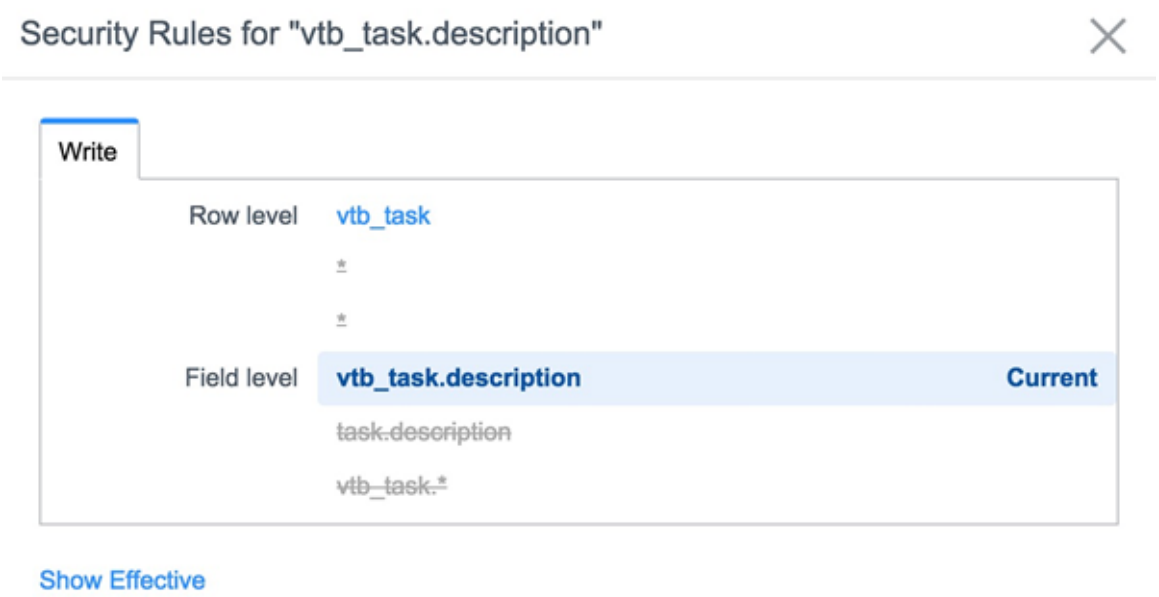
1. Auf eine privilegierte Rolle hochstufen.
2. Navigieren zu **Systemsicherheit** > **Zugriffssteuerung (ACL)**an.
3. Öffnen Sie eine ACL des Typs *record*.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Klicken Sie im Abschnitt „Zugehörige Links“ auf **ACL-Ausführungsplan** anzeigen.

   Das Fenster mit den Sicherheitsregeln für die ACL wird angezeigt. Im Beispiel wird der Ausführungsplan für „vtb_task“ angezeigt.



Fenster für ACL-Ausführungsplan

UI-Element	Beschreibung
Titel	Der Name der ACL.
Registerkartenname	Ob die ACL erstellt, gelesen, geschrieben oder gelöscht wird.
Zeilenebene	ACLs auf Zeilenebene, die für diese Tabelle ausgeführt werden.
Feldebene	ACLs auf Feldebene, die nur für dieses Feld (oder Spalte in der Tabelle) ausgeführt werden.

5. **Klicken** Sie auf Alle anzeigen, um alle zugehörigen ACLs anzuzeigen, einschließlich der überschriebenen ACLs und generischen ACLs, die für alle Datensätze gelten.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bei überschriebenen ACLs ist der Name durchgestrichen, bei generischen ACLs das Platzhalterzeichen Sternchen (*).

6. Zeigen Sie nur die unmittelbaren ACLs im Zusammenhang mit der angezeigten an, und blenden Sie die ACLs in Tabellen aus, aus denen die ACL-Tabelle erweitert wird, sowie die generischen Platzhalter-ACLs (*), indem Sie auf **Effektive**anzeigen klicken.

Verwenden Sie den ACL-Konfigurationsbeobachter

Verwenden Sie den ACL-Konfigurationsbeobachter, nachdem Sie eine Hochstufung zur Rolle security_admin durchgeführt haben.

Vorbereitungen

Erforderliche Rolle: security_admin
Auf eine privilegierte Rolle hochstufen

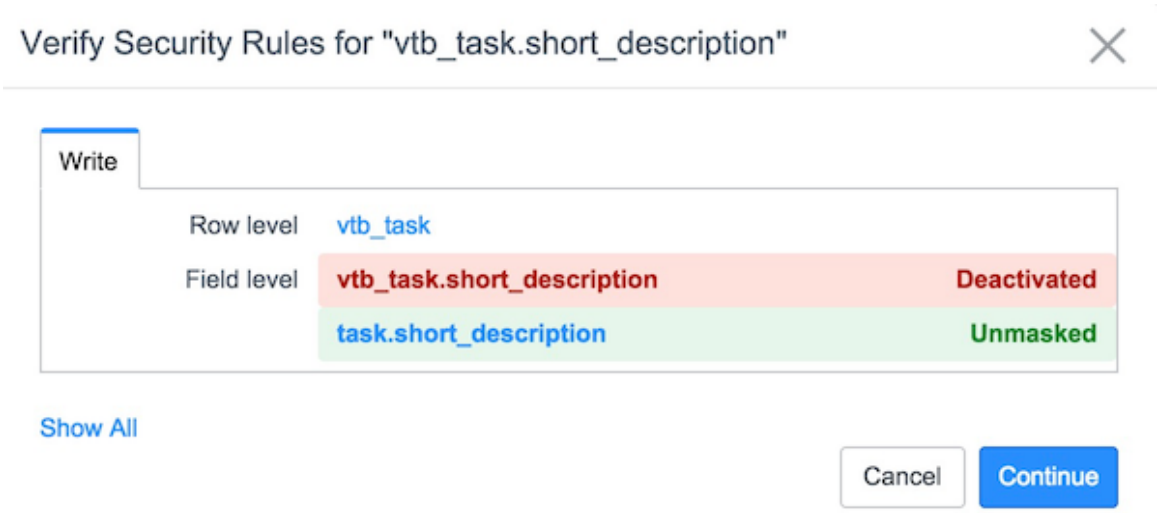
Prozedur

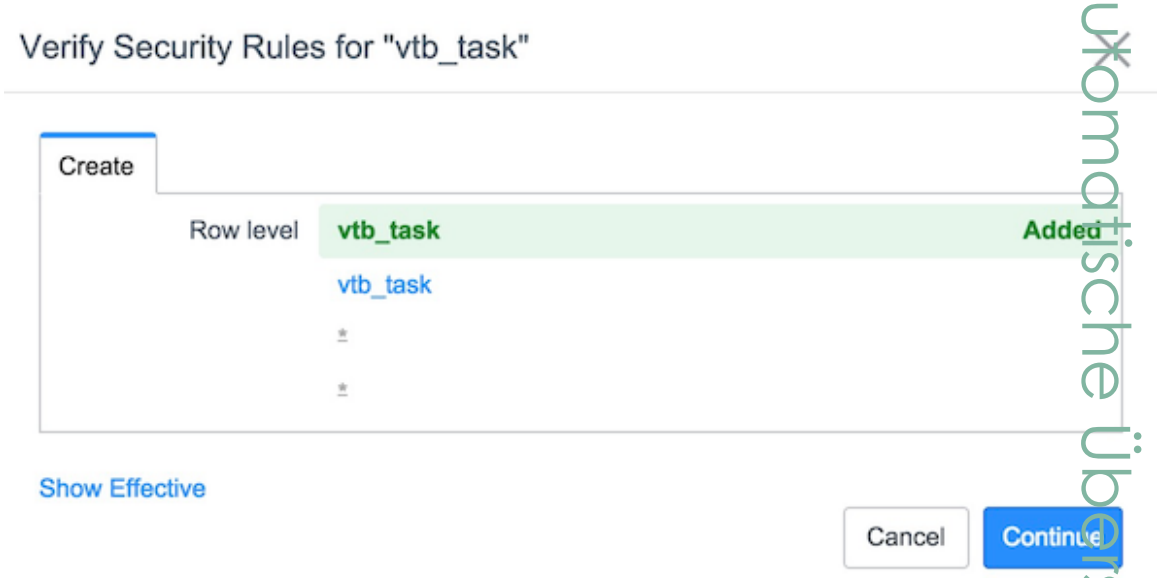
1. Öffnen Sie eine ACL, die eine Datensatztyp-ACL ist.
2. Führen Sie eine Aktion für die ACL aus, z. B. Ändern oder Auswählen einer Option aus dem Kontextmenü wie **Einfügen**.
3. Wenn Sie Werte im Formular „Zugriffssteuerung“ geändert haben, klicken Sie mit der rechten Maustaste auf den Header, und wählen **Sie Speichern**, oder wählen Sie **Aktualisieren** oder **Löschen**aus.

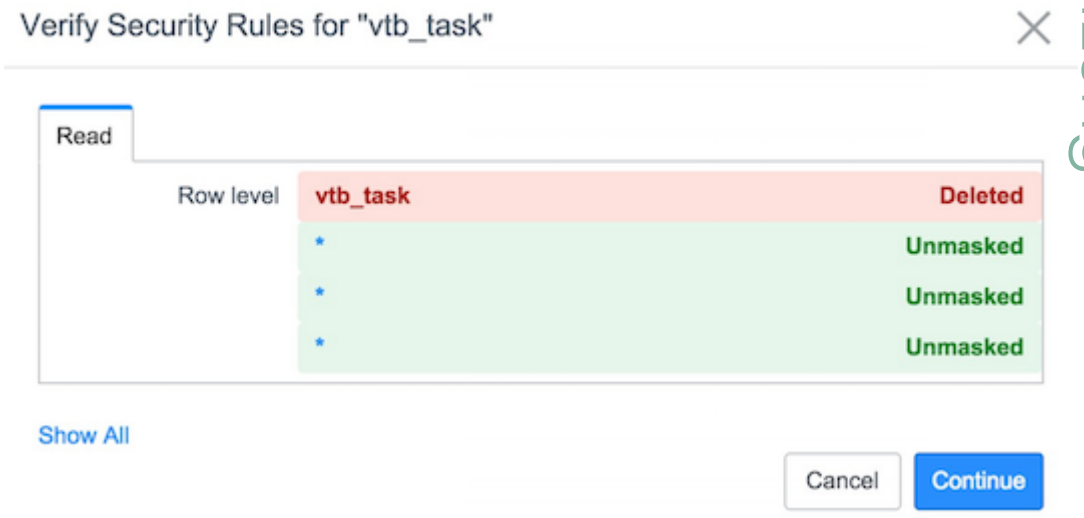
   Das Fenster „Security Rules“ (Sicherheitsregeln) wird angezeigt. Das System hat die Datenbankaktion für die ACL noch nicht ausgeführt, daher wurden die Änderungen noch nicht gespeichert.

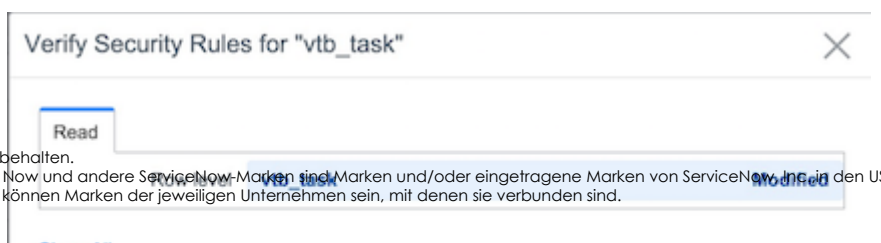
   Dies sind Beispiele für Sicherheitsregeln in der Tabelle für private Aufgaben [vtb_task] der Anwendung „Visuelle Taskboards“. Eine Beschreibung der Elemente in diesem Fenster finden Sie unter ACL-Konfigurationsbeobachter.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.









Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc. in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

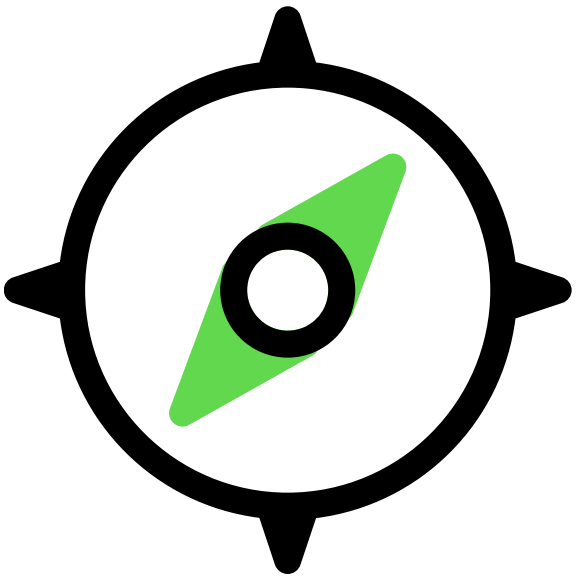
4. Wie beim Ausführungsplankönnen Sie auf Alle anzeigen **klicken**, um alle zugehörigen ACLs anzuzeigen, einschließlich der überschriebenen und generischen ACLs, die für alle Datensätze gelten, oder auf **Effektive** anzeigen klicken, um nur die unmittelbaren ACLs anzuzeigen, die sich auf die gerade angezeigte beziehen.
5. Zeigen Sie mit der Maus auf eine der ACLs, um eine Beschreibung anzuzeigen.

Sicherheitsattribute

Sicherheitsattribute bieten eine flexible Alternative zum Zugriff auf Steuerungslisten.

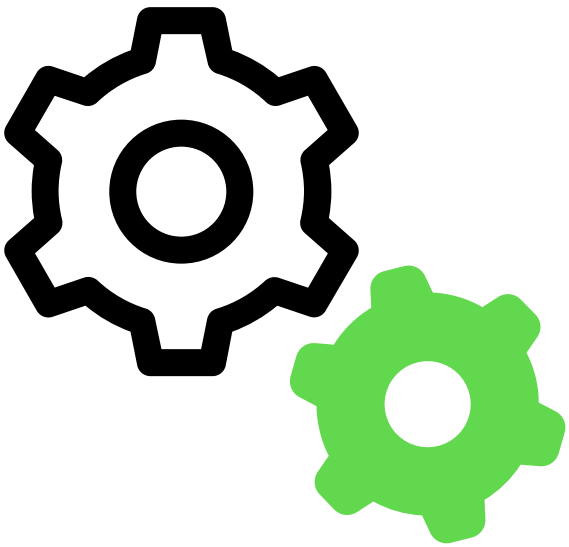
Erste Schritte

Erkunden Sie Sicherheitsattribute



Erlernen Sie die Grundlagen von Sicherheitsattributen

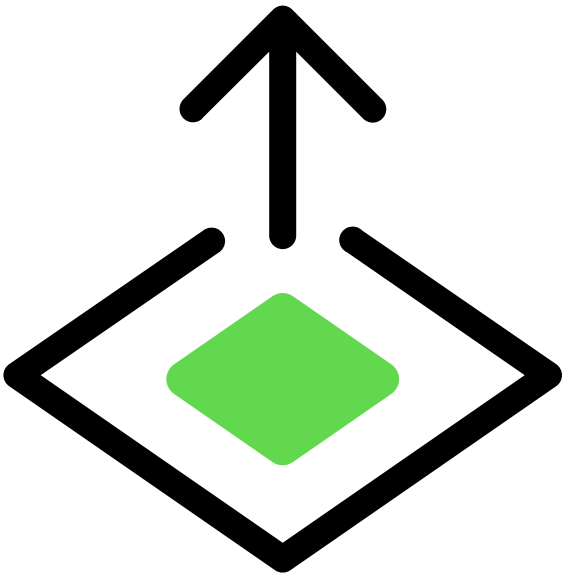
Erstellen Sie Sicherheitsattribute



Erstellen Sie neue Sicherheitsattribute

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OOB (vordefinierte) Sicherheitsattribute



Erklären Sie die OOB-Sicherheitsattribute

Protokollierung von Sicherheitsattributen



Überprüfen Sie die Protokollierung der Sicherheitsattribute

Sicherheitsattribute – Grundlagen

Ein Sicherheitsattribut ist ein hoch konfigurierbares Stück Information über ein Thema oder seine Umgebung. Wenn es in Zugriffssteuerungen verwendet wird, ermöglicht es eine detaillierte Sicherheitskonfiguration auf nicht komplexe Weise.

Übersicht

Sicherheitsattribute bieten eine alternative Methode für die Zugriffssteuerung über Rollendefinitionen zur derzeit angewendeten ACL-Konfiguration (Access Control List, Zugriffssteuerungsliste). Sicherheitsattribute bieten ACL-basierte Konfigurationen mehrere Vorteile:

Mehr Sicherheit

Eine verbesserte Verschleierung der Berechtigungsbewertung stellt sicher, dass Ihre Organisation sicher bleibt.

Für Menschen lesbar

Sicherheitsattribute sollen die Erstellung und Verwendung von Sicherheitsberechtigungen vereinfachen.

Flexible Sicherheit

Erstellen Sie Persona-Definitionen aus sofort einsatzbereiten Konfigurationen in Kombination mit vom Kunden definierten Personas.

Protokollierung und Auditing

Sicherheitsattribute bieten detaillierte Auditing- und Protokollierungsfunktionen, um mehr Einblick in Sicherheitsmaßnahmen und -Theorien zu erhalten.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie Sicherheitsattribute

Erstellen Sie neue Sicherheitsattribute mit einer Schritt-für-Schritt-Anleitung.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **System Sicherheit** > **Sicherheitsattribute**an.
2. Wählen Sie in der Liste der Sicherheitsattribute **Neu**.
3. Füllen Sie die Felder des Felderformulars für Sicherheitsattribute aus.

Sicherheitsattributfelder

Feld	Beschreibung
Bezeichnung	Bezeichnung des Sicherheitsattributs.
Name	Name des Sicherheitsattributs.
Typ	Der Typ des Sicherheitsattributs. ◦ Verbindung **Hinweis:** Weitere Informationen zu zusammengesetzten Sicherheitsattributen finden Sie unter Zusammengesetzte Sicherheitsattribute ◦ integer ◦ Liste ◦ Zeichenfolge ◦ boolean(true | false)
Ist dynamisch	Ob der Sicherheitsattributwert für jeden neu ausgewertet werden muss
Beschreibung	Anwendergenerierte Beschreibung des Sicherheitsattributs
Anwendung	Statisches Feld, Anwendungsbereich.
Suchtabelle	Verweisen Sie zur Auswertung auf eine externe Tabelle.
Tabellenspalte suchen	Verweisen Sie zur Auswertung auf eine Tabellenspalte.
Skript	Leiten Sie einen Wert von einem Skript ab.

OOB (vordefinierte) Sicherheitsattribute

Häufig verwendete, verallgemeinerte Sicherheitsattribute-Rollen sind einsatzbereit.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übersicht

Die vordefinierten Sicherheitsattribute (Out-of-Box) sind eine einfache Möglichkeit, mit der Verwendung und dem Erlernen der Funktionen von Sicherheitsattributen mit einer Reihe von vorkonfigurierten Sicherheitsattributrollen zu beginnen. Die Rollen für das OOB-Sicherheitsattribut sind häufig verwendete Zugriffssteuerungsrollen.

Um ein eigenes Sicherheitsattribut zu erstellen oder die Fähigkeiten eines OOB-Sicherheitsattributs zu erweitern, siehe Zusammengesetzte Sicherheitsattribute

OOB-Sicherheitsattribute

Attribut	Beschreibung
Gruppe	Anwender ist Mitglied einer angegebenen Gruppe
GroupExplicit	Anwender ist ein explizites Mitglied einer bestimmten Gruppe
HatAdminRolle	Der Benutzer hat die Administratorpersona
Verwendung einer anderen Identität	Die Identität des Anwenders wurde angenommen
InteraktiveSitzung	Aktuelle Sitzung interaktiv
Angemeldet	Der Anwender ist angemeldet und authentifiziert
Netzwerkkriterien	Zusätzliche Netzwerkkriterien
Rolle	Der Benutzer hat eine bestimmte Rolle
RoleExplicit	Für den Anwender ist eine bestimmte Rolle explizit definiert

Sicherheitsattribute für Client-Sitzung

Die folgenden Sicherheitsattribute werden für die Clientsitzung hinzugefügt (Plugin: `com.glide.client_session_security_attributes`):

- **IsIframeEmbeddedSession**: Das Attribut wird in eingebetteten IFrames in Drittanbieterportalen verwendet. Zum Beispiel Engagement Messenger, Virtual Agent Web Client, Eingebettete Sitzung usw.
- **IsIntegrationAsAServiceSession**: Das Attribut wird in Messaging-Apps wie Virtual Agent in Teams, Virtual Agent in Slack und Virtual Agent in WhatApp verwendet.
- **IsIntegrationAsAUserSession**: Das Attribut wird im Integrationsaccount-Anwender oder im Webservice-Anwender verwendet.
- **Ist ServiceNow-Websitzung**: Das Attribut wird in interaktiven Mobilsitzungen verwendet.
- **Ist Mobile-App-Sitzung**: Das Attribut wird verwendet, wenn die Eigenschaft **mobile_client** im Datensatz **oauth_entity** auf „wahr“ festgelegt ist.

Nicht explizites und explizites Verhalten erklärt

Sicherheitsattribute behandeln differenzierte Berechtigungsanforderungen mit einer expliziten vs. nicht expliziten (übernommenen) Bewertung von Rollenberechtigungen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusammengesetzte Sicherheitsattribute

Mit zusammengesetzten Sicherheitsattributen können Sie konsistente und wiederverwendbare Sicherheitsattributprofile erstellen, die Ihren Geschäftsanforderungen entsprechen

Übersicht

Zusammengesetzte Sicherheitsattribute werden aus einem oder mehreren bereits vorhandenen Sicherheitsattributen definiert, um eine einzige Referenzkombination von Sicherheitsattributen für die Berechtigungsbewertung zu erstellen.

Erstellen Sie zusammengesetzte Sicherheitsattribute

Erstellen Sie ein zusammengesetztes Sicherheitsattribut zur einfachen Wiederverwendung.

Vorbereitungen
Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Systemsicherheit** > **Sicherheitsattribute**an.
2. Wählen Sie in der Liste der Sicherheitsattribute **Neu**.
3. Wählen Sie `Verbindung` im Feld **Typ** aus.
4. Füllen Sie die Felder des Felderformulars für Sicherheitsattribute aus.

Sicherheitsattributfelder

Feld	Beschreibung
Bezeichnung	Bezeichnung des Sicherheitsattributs.
Name	Name des Sicherheitsattributs.
Beschreibung	Anwendergenerierte Beschreibung des Sicherheitsattributs
Bedingung	Die spezifischen Sicherheitsattributbedingungen, die zum Definieren der Sicherheitsattributbewertung verwendet werden.
Neues Kriterium	Fügen Sie einen zusätzlichen Satz von **Oder** -Bedingungen für die Auswertung hinzu.

Sicherheitsattribut , Umfang

Sicherheitsattribute unterstützen die Umfangsdefinition.

Umfangsdefinition von Sicherheitsattributen

Das bereichsbezogene Verhalten von Sicherheitsattributen stimmt mit dem bereichsbezogenen Verhalten der Plattform überein. Innerhalb eines Bereichs erstellte Sicherheitsattribute sind nur in Zugriffssteuerungen im selben Bereich verfügbar.

Lokale und vorhandene Sicherheitsattribute

Vorhandene und lokale Sicherheitsattribute ermöglichen Kunden die Wiederverwendung von Bedingungssätzen für Sicherheitsattribute.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Lokale und vorhandene Attribute

Mit dem Bedingungsgenerator für ACL-Sicherheitsattribute können Kunden angeben, ob ein Sicherheitsattribut vorhanden oder lokal ist.

Hinweis: Sicherheitsattributbedingungen sind standardmäßig auf „lokal“ festgelegt.

Ein lokal definiertes Sicherheitsattribut wird nur in der ACL gespeichert, in der es erstellt wurde.

Mit der Option „Vorhanden“ können Anwender eine vorhandene Sicherheitsattributbedingung für den Bedingungsgenerator referenzieren.

Feldabfragerollen und -einschränkungen

Mit den Attributen „ **Feldabfragerollen** “ und „ **Feldabfragebeschränkungen**“ können Sie besser steuern, welche Informationen für Benutzer in Tabellen verfügbar sind.

Übersicht

Die Attribute **„Feldabfragerollen“** und **„Feldabfragebeschränkungen“** ermöglichen eine genauere Kontrolle darüber, welche Aktionen Anwender für Tabellen ausführen können.

Feldabfragerollen

Verhindert die Abfrage sensibler Felder basierend auf der Anwenderrolle.

Feldabfragebeschränkungen

Beschränken Sie den Zugriff auf den Datensatz, wenn der Zugriff auf das entsprechende Feld verweigert wird.

Konfigurieren Sie eine Feldabfragerolle

Erfahren Sie, wie Sie ein Attribut für eine Feldabfragerolle aktivieren und konfigurieren.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Tabellen**an.
2. Wählen Sie eine **Tabelle** aus.
3. Wählen Sie eine **Spaltenbezeichnung** aus, um den zugehörigen **Wörterbucheintrag** anzuzeigen.
4. Wählen Sie die Registerkarte **Attribute** aus.
5. **Tipp:** Wenn Sie das **Feld Feldabfragerollen** nicht haben, wählen Sie **Neu**, um eines zu erstellen

   Wählen Sie das Attribut **Feldabfragerollen aus**.
6. Geben Sie die Rollen ein, die zum Anzeigen dieser Tabellenspalte erforderlich sind, im **Feld Wert**
7. Wählen Sie **Aktualisieren aus**

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse
Die Tabellenspalte kann nur von den im Attribut „ **Feldabfragerollen** “ definierten Rollen abgefragt werden. Wenn ein Anwender ohne die definierten Rollen die Tabellenspalte abfragt, wird ihm der Zugriff auf den Vorgang verweigert.

Konfigurieren Sie Einschränkungen für Feldabfragen

Erfahren Sie, wie Sie eine Feldabfragebeschränkung konfigurieren

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Tabellen**an.
2. Wählen Sie eine **Tabelle** aus.
3. Wählen Sie eine **Spaltenbezeichnung** aus, um den zugehörigen **Wörterbucheintrag** anzuzeigen.
4. Wählen Sie die Registerkarte **Attribute** aus.
5. **Tipp:** Wenn Sie das **Feld „Feldabfrage-Datensatzzugriff einschränken** “ nicht haben, wählen Sie **Neu**, um eines zu erstellen

   Wählen Sie das Attribut **Feldabfrage Datensatzzugriff einschränken** aus.
6. Geben Sie `true` im Feld **Wert** ein, um den Datensatzzugriff auf Anwender zu beschränken, die das Feld anzeigen können, andernfalls geben Sie `false`ein.
7. Wählen Sie **Aktualisieren aus**

Ergebnisse
Die Tabellenspalte schränkt die Ergebnisse von Abfragen ein. Eingeschränkte Anwender werden darüber informiert, wie viele Ergebnisse eine Abfrage zurückgegeben hat, aber keine weiteren Informationen.

Datenfilterung

Verwenden Sie die Datenfilterung, um bei Leseabfragen den Zugriff auf Tabellen und Datensätze basierend auf Themenattributen zu steuern.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkunden Sie Datenfilterung



Erfahren Sie mehr über Datenfilterung.

Erstellen Sie Datenfilterungsregeln



Erstellen Sie eigene Datenfilterungsregeln, die Ihren Anforderungen entsprechen.

Daten debuggen



Erfahren Sie, wie Sie Ihre Datenfilterungsergebnisse debuggen.

Datenfilterung erkunden

Verwenden Sie die Datenfilterung, um bei Leseabfragen den Zugriff auf Tabellen und Datensätze basierend auf Themenattributen zu steuern.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Datenfilterung ist eine separate Form der Zugriffssteuerung, die auf die vorhandenen Zugriffssteuerungsregeln (ACLs) in Ihrer Instanz abgestimmt ist. Die Datenfilterung verweigert den Zugriff auf Tabellen und Datensätze, die nicht mit den von einem Administrator definierten Betreffattributen übereinstimmen. Die Datenfilterung soll Auditing, Berichterstellung und Problembehandlung erleichtern.

Dies ist eine optionale Funktion, die Administratoren in ihrer Instanz aktivieren können.

Funktionen zur Datenfilterung

Datenfilter

Verwenden Sie Datenfilter, um Zugriff auf Grundlage von Informationen in einem Datensatz zu gewähren. Datenfilter verwenden Daten in einem Tabellenfeld, um zu bestimmen, ob ein Datensatz für Ihre Benutzer verfügbar ist.

Bedingungsgenerator basierend auf dem Antragstellerattribut

Verwenden Sie Betreffattribute, um Anwenderrolle, Gruppe, Betreffkriterien oder IP-Netzwerkadresse auszuwerten.

Die Datenfilterung verwendet ein auf Verweigern basierendes Modell

Die Datenfilterung verwendet ein auf Verweigern basierendes Modell, um den Zugriff auf Datensätze zu steuern. Bei der Datenfilterung verweigert Ihre -Instanz den Zugriff auf Datensätze, es sei denn, ein Datensatz erfüllt die durch die Datenfilterung definierten Kriterien.

Durchsetzung der Datenfilterung

Datenfilterungsregeln werden nach der Datenbankabfrage für READ-Vorgänge ausgeführt und vor ACLs ausgewertet. Ein Datensatz, der von einer Datenfilterungsregel abgelehnt wird, wird nicht fortgesetzt und von ACL-Regeln ausgewertet.

- Die Erzwingung von Datenfilterungsregeln stimmt mit denen von READ ACLs überein.
- Die Datenfilterung funktioniert ähnlich wie ACLs in Verbindung mit vorhandenen *Report view access control list*-Verhaltensweisen. Weitere Informationen zur Konfiguration dieser Berichtssteuerelemente finden Sie unter Zugriffssteuerung für Berichtansicht .

Debugging von Sitzungen

Die Datenfilterung unterstützt das Debugging von Sitzungen. Verwenden Sie das Sitzungs-Debugging, um zu sehen, welche Datenfilterungsdatensätze für eine bestimmte Abfrage gelten. Administratoren können diese Informationen verwenden, um Probleme mit dem Benutzerzugriff auf Datensätze zu beheben.

Komponenten der Datenfilterung

Die Datenfilterung funktioniert mit den folgenden Datensatztypen:

Datensätze zur Datenfilterung

Erstellen Sie einen Datenfilterungs-Datensatz [sys_df_data_filter], um Tabellenzugriff in Ihrer Instanz zu gewähren. Der Datenfilterungsdatensatz enthält die oben beschriebenen Bedingungen für **Datenfilter** und **Betreffattribut**, um den Umfang der Regel und die betroffenen Anwender einzuschränken.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

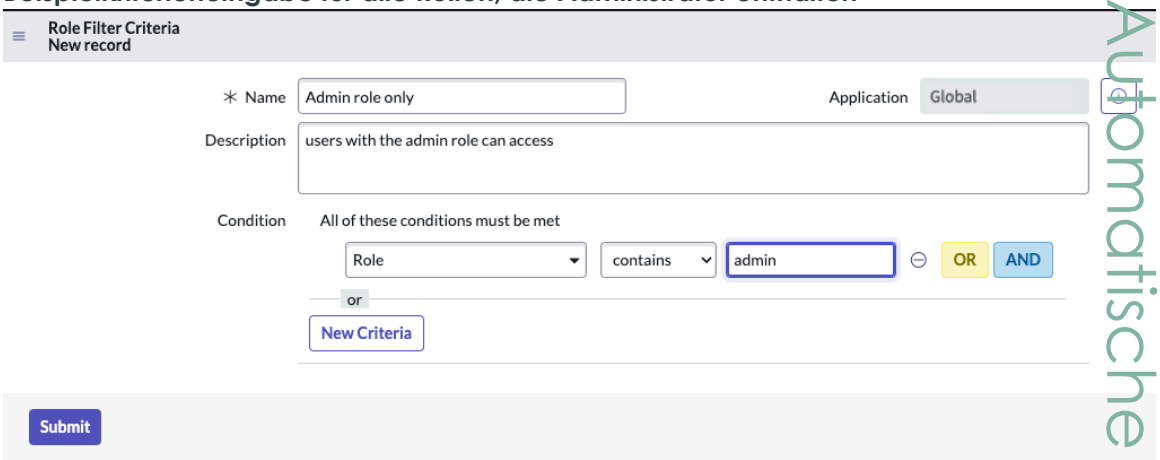
Datensätze mit Betreffkriterien

Datensätze mit Betreffkriterien [sys_df_subject_criteria] stellen bestimmte Anwenderattribute dar, mit denen Sie bestimmen können, ob Zugriff mit einer Datenfilterungsregel gewährt werden soll. Diese Attribute können die Gruppen, Rollen oder IP-Adresse eines Anwenders sein. Um ein Betreffkriterium zu erstellen, müssen Sie den Betreffkriteriendatensatz sowie Datensätze für die Kriterieneingabe und Kriterienbedingungen erstellen. Details zu diesem Vorgang finden Sie unter Betreffkriterien werden erstellt.

Nachdem Sie Datensätze mit Betreffkriterien erstellt haben, können Sie sie auf eine Regel anwenden. Dies geschieht auf der Registerkarte **Betreffbedingung** Ihrer Datenfilterregel.

Beispiele für Datensätze für Kriterieneingabe

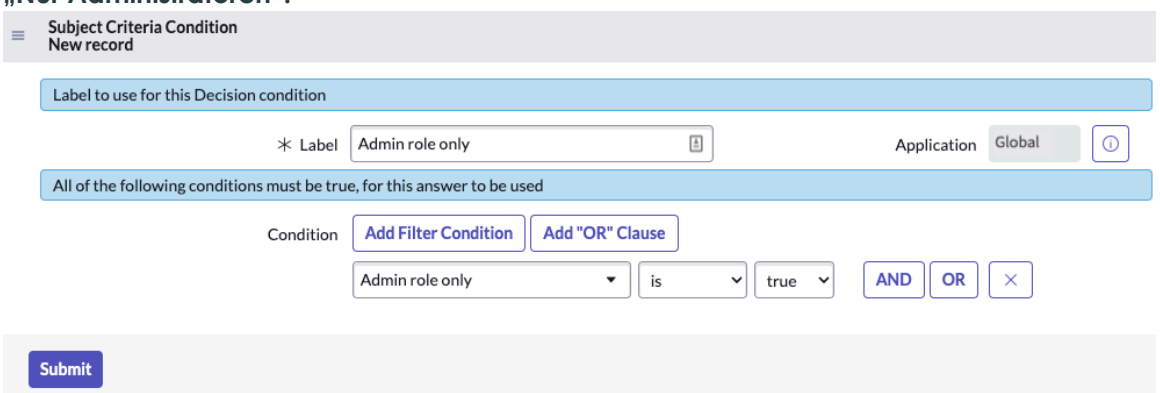
Beispielkriterieneingabe für alle Rollen, die Administrator enthalten



Kriterieneingaben [sys_df_subject_filter_criteria_m2m] sind Datensätze, die Kriterien für den Vergleich mit dem Benutzer enthalten. Dies kann eine Liste von Anwendergruppen oder -rollen, ein IP-Adressbereich oder ein IP-Adresssubnetz sein. Diese Datensätze werden zusammen mit Bedingungsdatensätzen für Betreffkriterien verwendet, um anhand der Gruppen, Rollen oder IP-Adresse eines Anwenders auszuwerten, um den Zugriff auf eine Tabelle oder ihre Datensätze zu bestimmen.

Bedingungsdatensätze für Betreffkriterien

Beispielkriterienbedingung für die Verwendung der Kriterieneingabe „Nur Administratoren“.



Verwenden Sie Datensätze für die Betreffkriterienbedingung [sys_df_subject_criteria_condition], um zu definieren, wie Anwenderattribute

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

mit den in Ihren Kriterieneingaben definierten Rollen, Gruppen oder IP-Adressen verglichen werden. Sie können mehrere Kriterieneingaben in einer einzelnen Betreffkriterienbedingung verwenden, um den Zugriff auf Ihre Datensätze weiter einzugrenzen.

Datenfilterung wird aktiviert

Erfahren Sie, wie Sie die Datenfilterung in Ihrer -Instanz aktivieren.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Plugins**an.
2. Verwenden Sie das Suchfeld, um das Plugin „Data Filter“ (com.glide.data_filterung) zu finden.
3. Klicken Sie auf **Installieren**, und klicken Sie dann im Dialogfeld „Plugin aktivieren“ auf **Aktivieren**.

Erstellen von Datenfilterungsregeln

Erfahren Sie, wie Sie Datenfilterungsregeln erstellen, um Ihren Anwendern Zugriff auf Datensätze und Tabellen zu gewähren.

Vorbereitungen

Erforderliche Rolle: security_admin

Hinweis: Um Datenfilterungsregeln zu erstellen oder zu ändern, müssen Sie auf die privilegierte Rolle hochstufen. Weitere Informationen zu diesem Prozess finden Sie unter Auf eine privilegierte Rolle hochstufen.

Prozedur

1. Navigieren zu **Alle** > **Datenfilterung** > **Datensätze der Datenfilterung**an.
2. Klicken Sie in der Liste **„Datenfilterung“** auf **Neu**.
   Ein neues Formular zur Datenfilterung wird angezeigt.
3. Füllen Sie im Formular die Felder nach Bedarf aus.

Formular zur Datenfilterung

Feld	Beschreibung
Tabelle	Tabelle, für die diese Datenfilterungsregel gilt.
Aktiv	Legt die Datenfilterungsregel als aktiv fest. **Hinweis:** Lassen Sie die Datenfilterungsregeln inaktiv, bis Sie zum Testen bereit sind, um zu vermeiden, dass Anwender unbeabsichtigt für Datensätze gesperrt werden.
Beschreibung	Beschreibung der Datenfilterungsregel.
Kaskadierend	Wählen Sie diese Option aus, um die Datenfilterungsregel festzulegen, die auf erweiterte Tabellen angewendet werden soll.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Sie wählen beispielsweise die Tabelle Task[task] aus und aktivieren die Kaskadierung. In diesem Fall gilt die Datenfilterungsregel auch für alle Tabellen, die aus der Aufgabe erweitert wurden, z. B. Incident [incident] und Change Request [change_request]. Einzelheiten zur Tabellenerweiterung finden Sie unter Tabellenerweiterung und -klassen **Hinweis:** Dieses Feld ist standardmäßig aktiviert.

4. Wählen Sie im Formularmenü **Speichern** aus.
   Nachdem Sie Ihre Datenfilterungsregel gespeichert haben, gilt diese Regel automatisch für alle Datensätze in der ausgewählten Tabelle. Sie können den Geltungsbereich dieser Regel auf bestimmte Datensätze in der Tabelle beschränken, indem Sie Bedingungen auf den Registerkarten **„Datenfilter“** und **„Betreffbedingung** “ verwenden.

Fügen Sie einen Datenfilter für Ihre Datenfilterungsregel hinzu

Sie können optional einen Datenfilter verwenden, um den Bereich Ihrer Datenfilterungsregel so einzugrenzen, dass sie nur für bestimmte Datensätze in einer Tabelle gilt.

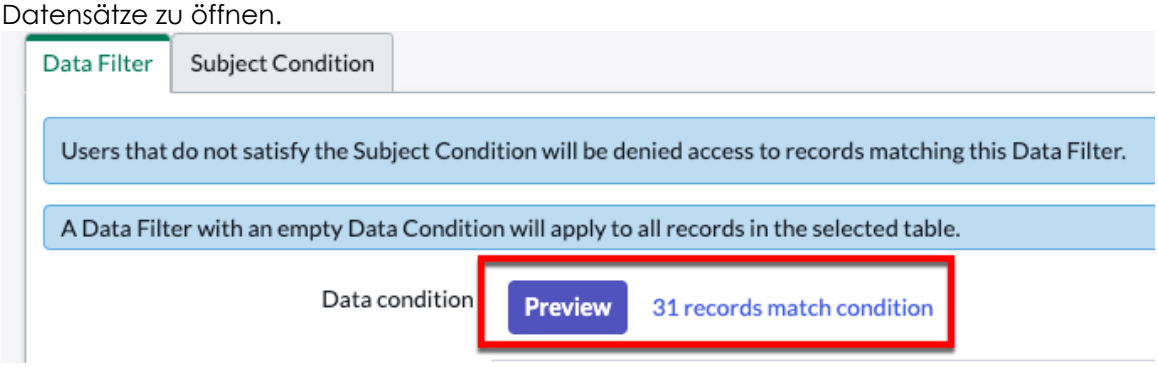
Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Öffnen Sie in Ihrem Datenfilterungsdatensatz die Registerkarte **Datenfilter**.
2. Verwenden Sie den Bedingungsgenerator, um die Tabellendatensätze nach ihren Feldwerten zu filtern.
   Der Datenfilter verwendet den gleichen Bedingungsgenerator wie in anderen Teilen der Plattform. Weitere Informationen zur Verwendung dieser Schnittstelle finden Sie unter Bedingungsgenerator .

   Wichtig: Die Registerkarte „ **Datenfilter** “ erscheint leer, bis Sie eine Tabelle im Feld **Tabelle** auswählen.

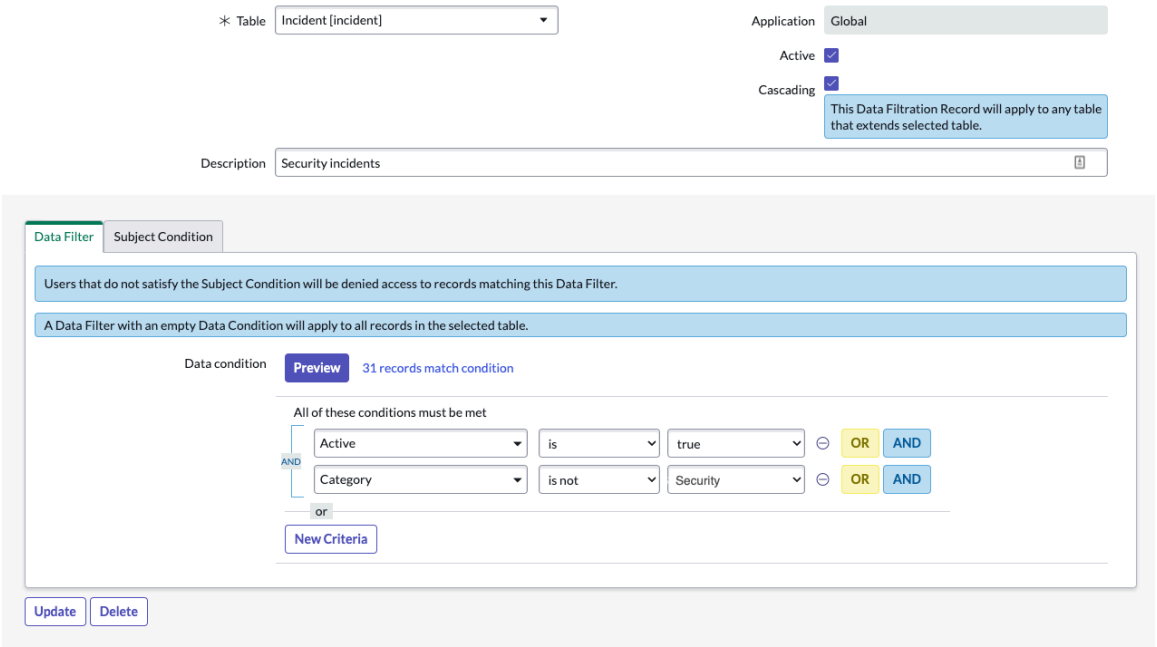
3. Verwenden Sie die Schaltfläche **Vorschau**, um anzuzeigen, wie viele Datensätze Ihrem Datenfilter entsprechen.
4. Wählen Sie die Anzahl der Datensätze aus, um eine Liste der übereinstimmenden Datensätze zu öffnen.



5. Wählen Sie **Speichern**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Example:
Dieses Beispiel zeigt eine Datenfilterregel für die Incident-Tabelle [Incident]. Der Datenfilter ist so eingestellt, dass alle aktiven Datensätze ausgewählt werden, die sich nicht in der Kategorie „ **Sicherheit** “ befinden. Wenn diese Regel aktiv ist, können Anwender diese Datensätze anzeigen. Im folgenden Abschnitt erfahren Sie, wie Sie Kriterien außerhalb des Inhalts des Datensatzes verwenden.



Wichtig:

Der **Not** -Vorgang in Ihren Bedingungen kann je nach Typ der von Ihrer Instanz verwendeten Datenbank unerwartete Ergebnisse zurückgeben. Nehmen Sie als Beispiel die folgende Bedingung an:

Für diese Bedingung wäre das erwartete Ergebnis, dass die Ergebnismenge alle Datensätze umfasst, in denen das Unternehmen nicht `ServiceNow` ist, sowie alle Datensätze, die keinen Wert im Feld **„Unternehmen“** aufweisen. Instanzen, die andere Datenbanken als MySQL und Maria verwenden, geben keine Wertdatensätze mit einem leeren **Unternehmensfeld** zurück. Wenn Sie für diese Instanzen **keine** Abfragen verwenden, schließen Sie Bedingungen ein, um sicherzustellen, dass leere Werte zurückgegeben werden.

Fügen Sie Ihrer Datenfilterungsregel Betreffattribute hinzu

Optional können Sie Betreffattribute verwenden, um den Bereich Ihrer Datenfilterungsregel anhand von Attributen wie IP-Netzwerkadresse, Anwendergruppen und -rollen oder Betreffkriterien einzugrenzen.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Öffnen Sie in Ihrem Datenfilterungsdatensatz die Registerkarte **Betreffkriterien** .
2. Verwenden Sie den Bedingungsgenerator, um die Tabellendatensätze basierend auf einem oder mehreren der folgenden Kriterien zu filtern.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Optionen für Betreffkriterien

Option	Beschreibung
Netzwerkkriterien	Ermöglicht den Zugriff auf Datensätze basierend auf dem IP-Bereich des Netzwerks oder dem IP-Subnetz.
Betreffkriterien	Ermöglicht den Zugriff auf Datensätze basierend auf Betreffkriterien. Wählen Sie einen Betreffkriteriendatensatz aus, um seine Bedingungen auf Ihre Datenfilterungsregel anzuwenden. Einzelheiten zum Erstellen von Betreffkriteriendatensätzen finden Sie unter Betreffkriterien werden erstellt.
Betreffgruppe	Gewähren Sie den Zugriff, wenn der Anwender Mitglied einer bestimmten Gruppe ist. Wählen Sie eine Gruppe aus der Tabelle „ **Gruppen**“ [sys_user_group] aus.
Betreffrolle	Gewähren Sie den Zugriff, wenn der Anwender Mitglied einer bestimmten Gruppe ist. Wählen Sie eine Gruppe aus der Tabelle „ **Rollen**“ [sys_user_role] aus.

Wichtig: Die Bedingungen für Betreffkriterien unterstützen nur den Operator „ **ist** “.

3. Nachdem Sie Ihre Betreffkriterien hinzugefügt haben, klicken Sie auf **Speichern**.

Betreffkriterien werden erstellt

Erstellen Sie Datensätze mit Betreffkriterien zur Verwendung in Datenfilterungsregeln.

Vorbereitungen

Erforderliche Rolle: security_admin

Wichtig: Um Datenfilterungsregeln zu erstellen oder zu ändern, müssen Sie eine privilegierte Rolle zugewiesen haben. Weitere Informationen zu diesem Prozess finden Sie unter Auf eine privilegierte Rolle hochstufen.

Prozedur

1. Navigieren zu **Alle** > **Datenfilterung** > **Betreffkriterien**an.
2. Klicken Sie in der Liste **Betreffkriterien** auf die Schaltfläche **Neu**.
   Ein neues Formular für Betreffkriterien wird angezeigt.
3. Füllen Sie im Formular die Felder nach Bedarf aus.

Felder für Betreffkriterien

Feld	Beschreibung
Name	Name für die Betreffkriterien.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Anwendung	Bereichsbezogene Anwendung für die Betreffkriterien. Dieses Feld ist schreibgeschützt und wird automatisch mit der aktuellen bereichsbezogenen Anwendung gefüllt.
Beschreibung	Beschreibung für die Betreffkriterien.

4. Klicken Sie mit der rechten Maustaste auf den Formular-Header, und klicken Sie im Kontextmenü auf **Speichern**.
   Nach dem Speichern werden die Felder **Kriterieneingaben** und **Kriterienbedingungen angezeigt**.

Erstellt eine Betreffkriterieneingabe

Erstellen Sie eine Betreffkriterieneingabe, um Kriterien zu definieren, nach denen Ihre Datenfilterungsregeln filtern.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Öffnen Sie im **Betreffkriteriendatensatz die Registerkarte Kriterieneingaben**.
2. Klicken Sie in der Liste **Kriterieneingaben** auf **Neu**.
3. Wählen Sie die Richtlinieneingabe für die Kriterien aus, die Sie erstellen möchten.

Richtlinieneingaben

Richtlinieneingabe	Beschreibung
IP-Filterkriterien	Erstellt eine Richtlinieneingabe basierend auf der IP-Adresse
Rollenfilterkriterien	Erstellen Sie eine Richtlinieneingabe basierend auf der Verwendungsrolle
Gruppenfilterkriterien	Erstellt eine Richtlinieneingabe basierend auf einer Benutzergruppe

   Abhängig von Ihrer Auswahl in diesem Schritt wird ein Formular für **IP-Filterkriterien**, **Rollenfilterkriterien**oder **Gruppenfilterkriterien** angezeigt.
4. Füllen Sie im Formular „Filterkriterien“ die Felder nach Bedarf aus.

Filterkriterienfelder

Feld	Beschreibung
Name	Name für die Filterkriterien
Anwendung	Bereichsbezogene Anwendung für die Betreffkriterien. Dieses Feld ist schreibgeschützt und wird automatisch mit der aktuellen bereichsbezogenen Anwendung gefüllt.
Beschreibung	Beschreibung der Filterkriterien

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Unterhalb der Formularfelder befinden sich Registerkarten, auf denen die IP-Adressen, Gruppen oder Rollen für die Filterkriterieneingaben definiert werden.

Filterkriterienfelder für bestimmte Eingabetypen

Eingabetyp für Richtlinie	Beschreibung	Erstellung
IP-Filterkriterien	Anwender-IP-Filterkriterien zum Erstellen eines Bereichs oder Subnetzes von IP-Adressen. Ihre Betreffkriterien können dann mit der IP-Adresse des Anwenders in diesem Bereich oder Subnetz verglichen werden.	Verwenden Sie den **IP** -Bereich oder das **Subnetz (CIDR)**, um IP-Adressen für Ihre Eingabe zu definieren. IP-Bereich Doppelklicken Sie in der Liste **IP** -Bereiche auf **Neue Zeile einfügen**, und geben Sie im Feld **Start-IP**eine IP-Startadresse ein. Drücken Sie dann die Tabulatortaste, und geben Sie im Feld **End-IP** eine End-IP-Adresse ein. Drücken Sie abschließend die Eingabetaste, um den Listeneintrag zu speichern. Subnetz (CIDR) **Doppelklicken Sie in der Liste der Subnetze** auf **Neue Zeile**einfügen, und geben Sie im Feld Netzwerk-IP eine Netzwerk- **IP** ein. Drücken Sie dann die Tabulatortaste, und geben Sie im Feld Netzmaske eine **Netzmaske** ein. Drücken Sie abschließend die Eingabetaste, um den Listeneintrag zu speichern.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingabetyp für Richtlinie	Beschreibung	Erstellung
		Hinweis: Für geplante Aufgaben, die von einem Zeitplaner ausgelöst werden, ist nicht vorgesehen, dass Daten anhand von Netzwerkkriterien gefiltert werden, da sie nicht den Kontext der anfordernden Client-IP haben. Eine geeignetere Art der Filterung kann die Bedingung „Rollen-/ Gruppenbetreff“ sein.
Rollenfilterkriterien	Verwenden Sie Rollenfilterkriterien, um eine Auswahl von Rollen zu erstellen. Ihre Betreffkriterien können dann mit den zugewiesenen Rollen des Anwenders in dieser Auswahl verglichen werden.	Verwenden Sie den Bedingungsgenerator im **Feld Bedingung**, um Rollen für Ihre Eingabe auszuwählen.
Gruppenfilterkriterien	Verwenden Sie Gruppenfilterkriterien, um eine Auswahl von Benutzergruppen zu erstellen. Ihre Betreffkriterien können dann mit den zugewiesenen Gruppen des Anwenders im Rahmen dieser Auswahl verglichen werden.	Doppelklicken Sie in der Tabelle **Gruppen für Kriterien** auf **Neue Zeile einfügen**und wählen Sie eine Benutzergruppe aus. Drücken Sie die Eingabetaste, oder klicken Sie auf das grüne Häkchen, um die Gruppe zu speichern. Klicken Sie auf den Text **Neue Zeile** einfügen unter dem ersten Eintrag, um zusätzliche Einträge zu erstellen.

6. Nachdem Sie Ihre Eingabe definiert haben, klicken Sie auf **Absenden**.

Hinweis: Sie können nicht nur Kriterieneingaben für Ihre Betreffkriterien erstellen, sondern auch vorhandene hinzufügen. Klicken Sie auf der Registerkarte **Kriterieneingaben** auf **Bearbeiten**, und wählen Sie eine vorhandene Eingabe aus.

Erstellen Sie eine Bedingung für Betreffkriterien

Erstellen Sie eine Bedingung, um Anwenderinformationen mit der vorhandenen Betreffkriterieneingabe zu vergleichen.

Vorbereitungen

Erforderliche Rolle: security_admin

Kriterienbedingungen vergleichen Anwenderattribute mit vorhandenen Kriterieneingaben, um zu bestimmen, ob der Zugriff auf Datensätze zulässig sein soll. Um eine Kriterienbedingung zu erstellen, müssen Sie Betreffkriterien erstellt haben. Einzelheiten zu diesem Prozess finden Sie unter Erstellt eine Betreffkriterieneingabe.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Öffnen Sie im Datensatz mit den **Betreffkriterien die Registerkarte Kriterienbedingungen**.
2. Klicken Sie in der Liste **Kriterienbedingungen** auf **Neu**.
3. Füllen Sie im Formular **„Betreffkriterienbedingung“** die Felder nach Bedarf aus.

Formular für Betreffkriterienbedingung

Feld	Beschreibung
Bezeichnung	Eine beschreibende Bezeichnung für Ihre Bedingung
Anwendung	Bereichsbezogene Anwendung für die Betreffkriterien. Dieses Feld ist schreibgeschützt und wird automatisch mit der aktuellen bereichsbezogenen Anwendung gefüllt.

4. Erstellen Sie mit dem Bedingungsgenerator eine Bedingung für Ihre Betreffkriterienbedingung, indem Sie aus den folgenden Bedingungsoptionen auswählen. Diese Bedingungsoptionen umfassen alle von Ihnen erstellten Betreffkriterieneingaben.
5. Wahlweise: Erstellen Sie weitere Bedingungen, indem Sie auf die Schaltflächen **Filterbedingung hinzufügen** oder **„ODER“-Klausel** hinzufügen klicken.

   Hinweis: Sofern Ihre Bedingungen nicht durch eine **-oder** -Klausel getrennt sind, müssen alle Bedingungen als „wahr“ ausgewertet werden, damit die Bedingung der Betreffkriterien als „wahr“ ausgewertet wird.

6. Klicken Sie auf Absenden, um die Bedingung der **Betreffkriterien** zu speichern.

Nächste Maßnahme

Verwenden Sie Betreffkriterien in Ihren Datenfilterungsregeln, um den Zugriff auf Tabellen und Datensätze zu beschränken. Einzelheiten zur Verwendung von Betreffkriterien in Datenfilterungsregeln finden Sie unter Betreffkriterien werden erstellt.

Debugging der Datenfilterung

Sehen Sie im Sitzungsprotokoll, wie sich die Datenfilterung auf Ihre Datensätze auswirkt, und debuggen Sie Probleme mit dem Benutzerzugriff.

Vorbereitungen

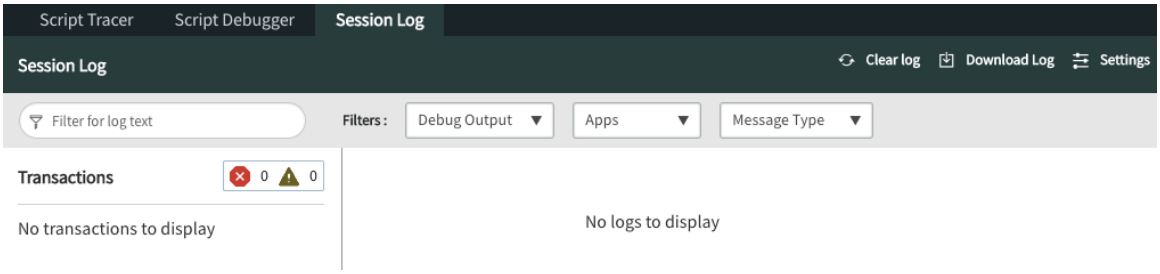
Erforderliche Rolle: admin

Ausgabeinformationen werden in den Sitzungsprotokollen angezeigt, wenn Benutzer auf Datensätze zugreifen. Sie können diese Protokollierungsinformationen zusammen mit dem Identitätswechsel verwenden, um zu erfahren, warum Anwender Datensätze sehen oder nicht. Diese Informationen können Sie dann verwenden, um Ihre Datenfilterungsregeln anzupassen und sicherzustellen, dass die Benutzer nur das sehen, was Sie beabsichtigen.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Debugging** > **Alle Sicherheitseinstellungen debuggen**an.
   Der **Script Debugger** wird in einer neuen Browserregisterkarte oder einem neuen Browserfenster geöffnet.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



2. Wählen Sie im Fenster **„Script Debugger** " die Registerkarte **Sitzungsprotokoll**.
3. Nehmen Sie in einer anderen Browserregisterkarte oder in einem anderen Fenster die Identität eines Benutzers an, um Probleme mit dem Zugriff dieses Benutzers zu beheben.

   Hinweis: Der Identitätswechsel ermöglicht es einem Administrator, eine Instanz mit den Einstellungen und Zugriffen eines anderen Anwenders anzuzeigen. Weitere Informationen zum Identitätswechsel finden Sie unter Identität eines Benutzers annehmen .

4. Greifen Sie beim Annehmen der Identität eines Anwenders auf eine Liste oder einen Datensatz zu, bei der bzw. dem Sie unerwartetes Verhalten beobachten.
   Dieses Verhalten kann ein Datensatz sein, den der Anwender sieht, aber nicht sehen sollte, oder eine Liste von Datensätzen, die für einen Anwender nicht wie erwartet angezeigt werden.
   Nach dem Zugriff auf Datensätze mit dem Anwender, dessen Identität angenommen wurde, sollte im Sitzungs-Debugger eine Ausgabe angezeigt werden.
5. Suchen Sie im Sitzungs-Debugger nach Informationen zur Datenfilterung.

   Dieses Beispiel zeigt zwei Protokollnachrichten, bei denen ein Datenfilter den Zugriff auf Datensätze verweigert hat. Die Protokolleinträge werden als roter Text angezeigt und enthalten den Grund für die Verweigerung des Zugriffs auf den Datenfilter sowie die sys_id des Datenfilters. Sie können auf diese sys_id klicken, um den Datenfilterungsdatensatz zu öffnen.

   Dieses Beispiel zeigt eine Protokollnachricht, bei der ein Datenfilter den Zugriff auf einen Datensatz zugelassen hat. Diese Protokolleinträge werden als grüner Text angezeigt. Wie bei der ersten Nachricht können Sie auf diese sys_id klicken, um den Datenfilterungsdatensatz zu öffnen.

6. Verwenden Sie diese Informationen, um Anpassungen an Ihren Datenfilterungsregeln vorzunehmen.
   Wiederholen Sie diese Schritte, um Ihre Regeln zu verfeinern und Anwendern den erforderlichen Zugriff zu gewähren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitsrollen

Sicherheitsrollen bieten zusätzliche Sicherheit. Jeder Anwender muss über mindestens eine Rolle verfügen, damit die Instanz zwischen internen und externen Anwendern unterscheiden kann.

Erkunden Sie explizite Rollen



Lernen Sie die wichtigsten Funktionen und den Geschäftsnutzen von expliziten Rollen kennen.

Erkunden Sie Erhöhte Berechtigungen



Erfahren Sie, wie die Rolle „Erweiterte Berechtigungen“ sitzungsbasierte Berechtigungen aktiviert.

Explizite Rollen

Sie können internen Benutzern und externen Benutzern Zugriff auf Ihre Instanz gewähren. Möglicherweise möchten Sie jedoch nicht, dass beide Benutzertypen dieselben Zugriffsrechte haben. Um die Sicherheit zu erhöhen, muss jeder Benutzer mindestens eine Rolle besitzen, damit die Instanz zwischen internen und externen Benutzern unterscheiden kann.

Ab Release Paris können Benutzer nicht mehr beide expliziten Rollen (snc_internal und snc_external) haben. Auch durch Gruppen- und Rolleneinschluss dürfen nicht beide Rollen enthalten sein, da dies dazu führen würde, dass jedes Gruppenmitglied oder jeder Benutzer, der einer solchen Gruppe oder Rolle zugeordnet ist, automatisch beide Rollen hätte. Now Platform bricht jeden Vorgang ab, der ein solches Szenario hervorrufen würde.

Externe Benutzer müssen mindestens die Rolle snc_external erhalten. Die Rolle snc_external gibt an, dass es sich gegenüber Ihrer Organisation um einen externen Benutzer handelt. Sie sollten keinen Zugriff auf Ressourcen haben, es sei denn, dies wird ausdrücklich erlaubt durch ACLs für die Rolle snc_external oder zusätzliche Rollen, die die Rolle snc_external erben. Standardmäßig haben Benutzer mit der Rolle snc_external keinen Zugriff auf:

- Scripted REST API-Ressourcen, die nicht als extern markiert sind
- Tabellen ohne die Rolle, die die Rolle snc_external oder public erbt

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ressourcen ohne Datensatztyp, z. B. Prozessoren und UI-Seiten, ohne dass Zugriffsrechte für die Rolle „snc_external“ oder eine Rolle gewährt werden, die die Rolle „snc_external“ erbt.
- Platform Analytics-Dashboards.

Markieren Sie die Rolle snc_internal nicht als erweitert. Andernfalls können interne Benutzer nicht auf die Instanz zugreifen.

Plugin „Explicit Roles“

Wenn das „Explicit Roles“-Plugin aktiviert ist, gilt Folgendes:

- Alle -Benutzer müssen über die Rolle „snc_internal“ verfügen, um auf interne Ressourcen zuzugreifen, oder über die Rolle „snc_external“ für den Zugriff auf externe Ressourcen. Benutzer ohne eine dieser expliziten Rollen können nur auf öffentliche Ressourcen zugreifen.
- Allen vorhandenen Benutzern wird automatisch die Rolle snc_internal zugewiesen. Durch diese Rolle werden die vorhandenen Zugriffsebenen und das Systemverhalten nicht geändert. Stattdessen stellt sie eine Kategorie bereit, um interne Benutzer von externen Benutzern zu unterscheiden. Alle internen Benutzer behalten dieselbe Zugriffsebene bei wie vor der Aktivierung des Plugins.

  Tipp: Um Änderungen an vorhandenen Funktionen für Benutzer zu verhindern, wird durch die Aktivierung des Plugins „Explicit Roles“ die Benutzerrolle snc_internal allen vorhandenen Benutzern in der Instanz zugewiesen. Dies schließt alle externen Benutzer ein, die hinzugefügt wurden, bevor das Plugin „Explicit Roles“ aktiviert wurde. Nachdem das Plugin „Explicit Roles“ aktiviert wurde, gehen Sie für alle externen Benutzer, die vor Aktivierung des Plugins „Explicit Roles“ hinzugefügt wurden, wie folgt vor:

  ◦ Entfernen Sie die Rolle snc_internal.

  ◦ Fügen Sie die Rolle snc_external hinzu.

  Durch die vorstehenden Maßnahmen können Sie sicherstellen, dass externe Benutzer, die vor der Aktivierung des Plugins „Explicit Roles“ hinzugefügt wurden, keinen Zugriff auf interne Ressourcen haben, die nur internen Benutzern zur Verfügung stehen sollten.

- Neu erstellten Benutzern wird automatisch die Rolle snc_internal zugewiesen, wenn sie erstmalig versuchen, sich bei der Instanz anzumelden, es sei denn, ihnen wurde explizit die Rolle snc_external zugewiesen. Sie können die Rolle snc_external einem neuen Benutzer hinzufügen, bevor er sich zum ersten Mal bei der Instanz anmeldet, um externe Benutzerrechte bereitzustellen.

Wichtig:

Aktivieren Sie dieses Plugin während eines Wartungsfensters oder wenn nur wenige Benutzer angemeldet sind. Benutzern, die derzeit bei der Aktivierung des Plugins angemeldet sind, wird die Rolle snc_internal nicht dynamisch zugewiesen. Stattdessen müssen sich Benutzer abmelden und wieder anmelden, um die Rolle snc_internal zu erhalten. Sobald das Plugin aktiviert ist, können Sie die Rollen snc_internal und snc_external jederzeit hinzufügen oder entfernen, um Benutzerrechte zu ändern.

Nach der Aktivierung des Plugins erhält der Benutzer bei jeder Anmeldung die Rolle snc_internal, sofern das Konto diese Rolle noch nicht hatte, oder die Rolle snc_external. Dies schließt per Identitätswechsel angemeldete Benutzer ein.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Allen vorhandenen ACLs ohne Rollenanforderung wird automatisch die Rolle snc_internal zugewiesen. Da sowohl vorhandenen ACLs als auch Benutzern die Rolle „snc_internal“ zugewiesen ist, ändern sich die vorhandenen Zugriffsebenen nicht.
- Neu erstellten ACLs ohne Rollenanforderung wird automatisch die Rolle snc_internal zugewiesen. Diese Rollenzuweisung gilt nicht für neu erstellte ACLs mit zugewiesener Rolle.
- Für alle vorhandenen Prozessor-Datensätze [sys_processor] oder neu erstellte Prozessor-Datensätze [sys_processor] mit **Typ = Skript** wird die Rolle snc_internal automatisch zum Feld **Rollen** hinzugefügt, wenn das Feld leer ist.
- Um den Zugriff auf UI-Seiten auf interne Benutzer zu beschränken, weist das Plugin automatisch die Rolle snc_internal der ***** ACL mit dem **Typ ui_page** zu.
- Um den Zugriff auf Prozessoren auf interne Benutzer zu beschränken, weist das Plugin automatisch die Rolle snc_internal der ***** ACL mit dem **Typ processor** zu.
- Externe Benutzer müssen mindestens die Rolle snc_external erhalten, um auf die Instanz zuzugreifen. Diese Rolle muss externen Benutzern manuell erteilt werden. Der Zugriff auf Datensätze wird über ACLs gewährt.

Verschieben Sie keine System-Update Sets zwischen Instanzen, unabhängig davon, ob das Plugin „Explicit Roles“ aktiviert oder deaktiviert ist. Weitere Informationen finden Sie unter System-Update Sets .

Hinweis: Dieses Plugin erfordert auch das Plugin Contextual Security Manager.

glide.security.explicit_roles.do_not_fix-Verhalten

Ab Release Xanadu wurde „ `glide.security.explicit_roles.do_not_fix` “ mit Änderungen an „snc_internal“ angepasst. Die Rolle „snc_internal“ ist jetzt im Arbeitsspeicher und in „sys_user_has_role“ identisch. Das neue Verhalten für `glide.security.explicit_roles.do_not_fix` lautet:

glide.security.explicit_roles.do_not_fix neues Verhalten

Wert	Ergebnis
Falsch	Fügen Sie die Rolle „snc_internal“ sowohl im Speicher als auch „sys_user_has_role“ hinzu
True	Fügen Sie keine Rolle „snc_internal“ im Speicher oder „sys_user_has_role“ hinzu

Um die Rolle „snc_internal“ für bestimmte Benutzer auszuschließen, verwenden Sie die Eigenschaft „`glide.security.explicit_roles.ignore.snc_internal.exclude_role_list`“.

Tipp: Um das vorherige Verhalten „ `glide.security.explicit_roles.do_not_fix` “ wiederherzustellen, verwenden Sie die Eigenschaft „`glide.security.explicit_roles.do_not_fix_in_memory`“.

Externen Benutzer Zugriff auf Tabellen gewähren

Sie können externen Benutzern Zugriff auf eine Tabelle gewähren, indem Sie der Tabelle eine Rolle hinzufügen, die die Rolle snc_external erbt. Weitere Informationen finden Sie unter Externen Benutzern Zugriff auf eine Tabelle bereitstellen .

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die hasRoles()-Methode

Die Methode `hasRoles()` ist zwar noch verfügbar, wird aber im Geneva-Release abgeschafft. Verwenden Sie stattdessen die Methode `hasRole(role name)`.

Wenn Sie die Methode `hasRoles()` verwenden, beachten Sie die folgenden Änderungen:

- Diese Methode schließt die snc_internal-Standardrolle automatisch aus, wenn sie nach Rollen sucht. Dies bedeutet, dass die Methode `hasRoles()` immer noch **false** zurückgibt, wenn ein Benutzer nur über die Rolle snc_internal verfügt.
- Wenn der Benutzer die Rolle „snc_external“ hat, gibt die Methode **false** zurück, da die Instanz externe Benutzer als ohne Rolle betrachtet.

Gegenseitiger Ausschluss: snc_external und snc_internal

Die Now Platform verhindert, dass Benutzer gleichzeitig über beide Rollen snc_external und snc_internal verfügen. Die Now Platform wendet diesen gegenseitigen Ausschluss überall im System an und schreibt Fehlermeldungen für jeden Konflikt in die Protokolle.

Hinweis: ACLs können beide Rollen haben, wenn die ACL-Ressourcen für alle Benutzer zugänglich sein sollen.

Beispiel: Einem Benutzer beide expliziten Rollen hinzufügen (direkte Kollision):

1. Weisen Sie Benutzer Abel Tuter die Rolle snc_internal zu.
2. Weisen Sie Benutzer Abel Tuter die Rolle snc_external zu.

Ergebnis: Das Hinzufügen der Rolle snc_external schlägt fehl, da Abel Tuter die Rolle snc_internal hat.

Beispiel: Einer Gruppe beide expliziten Rollen hinzufügen (direkte Kollision):

1. Stellen Sie sich eine Gruppe namens Testgruppe vor, der derzeit keine expliziten Rollen zugewiesen sind.
2. Fügen Sie Abel Tuter der Testgruppe hinzu.
3. Fügen Sie die Rolle snc_external der Testgruppe hinzu.

Ergebnis: Das Hinzufügen der Rolle snc_external schlägt fehl, da Abel Tuter die Rolle snc_internal hat und nicht beide Rollen haben kann.

Beispiel: Eine explizite Rolle einer Gruppe zuweisen, in der ein Gruppenmitglied die explizite Rolle hat, die einen Konflikt verursacht (indirekte Kollision):

1. Weisen Sie Benutzer Abel Tuter die Rolle snc_internal zu.
2. Stellen Sie sich eine Gruppe namens Testgruppe vor, der derzeit keine expliziten Rollen zugewiesen sind.
3. Fügen Sie Abel Tuter der Testgruppe hinzu.
4. Fügen Sie die Rolle snc_external der Testgruppe hinzu.

Ergebnis: Das Hinzufügen der Rolle snc_external zur Gruppe schlägt fehl, da Abel Tuter die Rolle snc_external durch seine Zugehörigkeit zur Gruppe erben würde. Beide expliziten Rollen würden demselben Benutzer zugewiesen, was nicht zulässig ist.

Weitere Beispiele finden Sie in der folgenden Tabelle:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rolle	Versuchte Aktion	Ergebnis
Direkte Kollision		
Der Benutzer hat die Rolle snc_internal.	Fügen Sie die Rolle snc_external hinzu.	Die Aktion wird abgebrochen.
Der Benutzer hat die Rolle snc_external.	Fügen Sie die Rolle snc_internal hinzu.	Die Aktion wird abgebrochen.
Der Benutzer hat keine explizite Rolle.	Fügt die Rolle snc_internal oder snc_external hinzu.	Die Rolle wird hinzugefügt.
Der Benutzer hat beide explizite Rollen (vorhandene Kollision).	Fügen Sie den Benutzer einer Gruppe ohne Rollen hinzu.	Die Aktion wird abgebrochen.
Eine Rolle, die keinem Benutzer zugeordnet ist, enthält die Rolle snc_internal.	Fügen Sie die Rolle snc_external hinzu.	Die Aktion wird abgebrochen.
Eine Rolle, die keinem Benutzer zugeordnet ist, enthält die Rolle snc_external.	Fügen Sie die Rolle snc_internal hinzu.	Die Aktion wird abgebrochen.
Der Rolle enthält beide explizite Rollen (vorhandene Kollision).	Fügen Sie die Rolle einem Benutzer, einer Rolle oder einer Gruppe hinzu.	Die Aktion wird abgebrochen.
Eine Gruppe ohne Mitglieder hat die Rolle snc_internal.	Fügen Sie die Rolle snc_external hinzu.	Die Aktion wird abgebrochen.
Eine Gruppe ohne Mitglieder hat die Rolle snc_external.	Fügen Sie die Rolle snc_internal hinzu.	Die Aktion wird abgebrochen.
Eine Gruppe ohne Mitglieder hat keine Rollen.	Fügt die Rolle snc_internal oder snc_external hinzu.	Die Rolle wird hinzugefügt.
Indirekte Kollision		
Rolleneinschluss mit Kollision	**1.** Gewähren Sie einem Benutzer mit der Rolle snc_internal die Testrolle. **2.** Fügen Sie der Testrolle die Rolle snc_external hinzu.	Die Aktion wird abgebrochen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rolle	Versuchte Aktion	Ergebnis
Rolleneinschluss ohne Kollision	**1.** Gewähren Sie einem Benutzer ohne Rolle die Testrolle. **2.** Fügen Sie der Testrolle die Rolle snc_external hinzu.	Die Rolle wird sowohl dem Benutzer als auch der Testrolle hinzugefügt.
Gruppeneinschluss mit Kollision	**1.** Fügen Sie einen Benutzer mit der Rolle snc_internal der „Testgruppe 2“ (untergeordnete Gruppe von Testgruppe 1) hinzu. **2.** Fügen Sie Testgruppe 2 die Rolle snc_external hinzu. **3.** Fügen Sie die Rolle snc_external der übergeordneten Gruppe „Testgruppe 1“ (übergeordnete Gruppe von Testgruppe 2) hinzu.	Die Aktion wird abgebrochen.
Gruppeneinschluss ohne Kollision	**1.** Fügen Sie einen Benutzer ohne Rolle der Gruppe „Testgruppe 2“ (untergeordnete Gruppe von Testgruppe 1) hinzu. **2.** Fügen Sie die Rolle snc_external oder snc_internal der „Testgruppe 1“ (übergeordnete Gruppe der Testgruppe 2) hinzu.	Die Rolle wird der übergeordneten Gruppe, der untergeordneten Gruppe und dem Benutzer hinzugefügt.
Gruppeneinschluss plus Rolleneinschluss mit Kollision	Fügen Sie contains_external der Testgruppe 1, der übergeordneten Gruppe von Testgruppe 2, hinzu.	Testgruppe 1 und Testgruppe 2 erhalten beide contains_external, aber sie erhalten nicht explizit die Rolle snc_external.
	Fügen Sie die Rolle snc_internal der Testgruppe 2, der untergeordneten Gruppe von Testgruppe 1, hinzu.	Die Aktion wird abgebrochen.
Änderung der übergeordneten Gruppe plus Gruppeneinschluss	**1.** Entfernen Sie Testgruppe 1 als übergeordnete Gruppe von Testgruppe 2. **2.** Fügen Sie der Testgruppe 1 die Rolle snc_internal hinzu. **3.** Fügen Sie Testgruppe 2 die Rolle snc_external hinzu. **4.** Legen Sie in Testgruppe 2 die Testgruppe 1 als übergeordnete Gruppe fest, und speichern Sie.	Die Aktion wird abgebrochen. Wiederholen Sie diesen Vorgang für bereits geschachtelte Gruppen, erwarten Sie derselbe Ergebnis.

Die Ursache einer abgebrochenen Aktion wird in der Fehlermeldung angezeigt und muss behoben werden, bevor ein erneuter Versuch erfolgreich verlaufen kann.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für direkte Fälle, z. B. Hinzufügen einer expliziten Rolle zu einem einzelnen Benutzer, überprüfen Sie, welche explizite Rolle der Benutzer haben soll. Wenn der Benutzer über die falsche explizite Rolle verfügt, muss diese zuerst entfernt und dann die richtige explizite Rolle hinzugefügt werden.

Für indirekte Fälle, z. B. Hinzufügen einer expliziten Rolle zu einer Gruppe (sodass einem Gruppenmitglied beide expliziten Rollen zugewiesen werden), überlegen Sie, ob dieser Benutzer in der Gruppe sein soll. Bestimmen Sie auch, ob die explizite Rolle der Gruppe zugewiesen werden soll. Dies schließt auch Fälle ein, in denen die Rolle durch die Gruppenhierarchie und durch Rolleneinschluss geerbt wird.

Beachten Sie, dass die Now Platform nur die erste mögliche Kollision meldet. Wenn nach Aufhebung der Kollision erneute Versuche wieder fehlschlagen, wobei eine andere Ursache vorliegt, sollten Sie die relevanten gegenseitigen Abhängigkeiten von Benutzern/Gruppen/Rollen umfassender analysieren. Dabei sollten Sie gegebenenfalls überdenken, wie Gruppen- und Rolleneinschlüsse aufgebaut sind.

Fordern Sie explizite Rollen an

Aktivieren Sie Explizite Rollen, indem Sie das Plugin „Explicit Roles“ (com.glide.explicit_roles) über den Now Support -Servicekatalog anfordern.

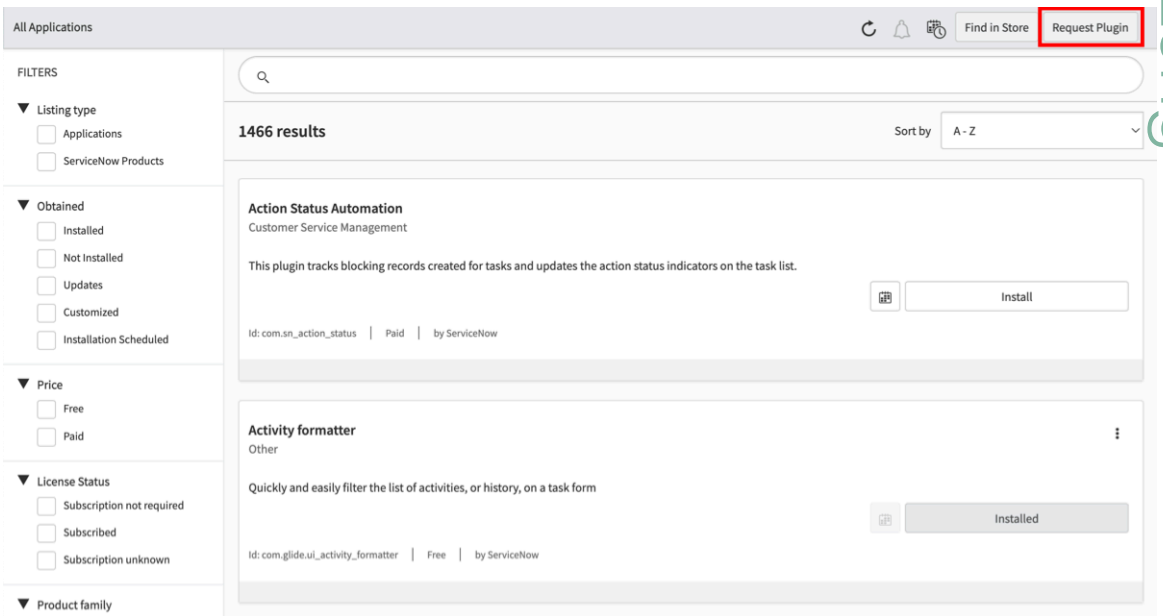
Vorbereitungen

Erforderliche Rolle: admin

Wichtig: Aktivieren Sie dieses Plugin während eines Wartungsfensters oder wenn nur wenige Benutzer angemeldet sind. Benutzern, die derzeit bei der Aktivierung des Plugins angemeldet sind, wird die Rolle snc_internal nicht dynamisch zugewiesen. Stattdessen müssen sich Benutzer abmelden und wieder anmelden, um die Rolle snc_internal zu erhalten. Sobald das Plugin aktiviert ist, können Sie die Rollen snc_internal und snc_external jederzeit hinzufügen oder entfernen, um Benutzerrechte zu ändern.

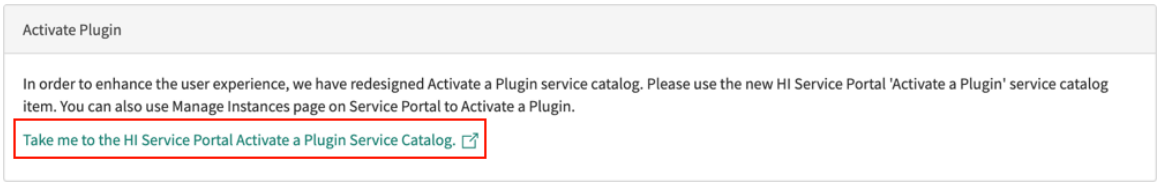
Prozedur

1. Navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Klicken Sie auf der Seite „Alle Anwendungen“ auf **Plugin anfordern**, um das Formular **Plugin aktivieren** auf Now Support zu öffnen.



© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie unter Now Support den Link aus, um auf Now Support Serviceportal Servicekatalog zuzugreifen.



4. Wählen Sie Ihre Instanz aus.
5. Wählen Sie **Aktionen > Plugin aktivieren** aus.
6. Geben Sie im Formular **Plugin aktivieren** die folgenden Informationen an.

Formular „Plugin anfordern“

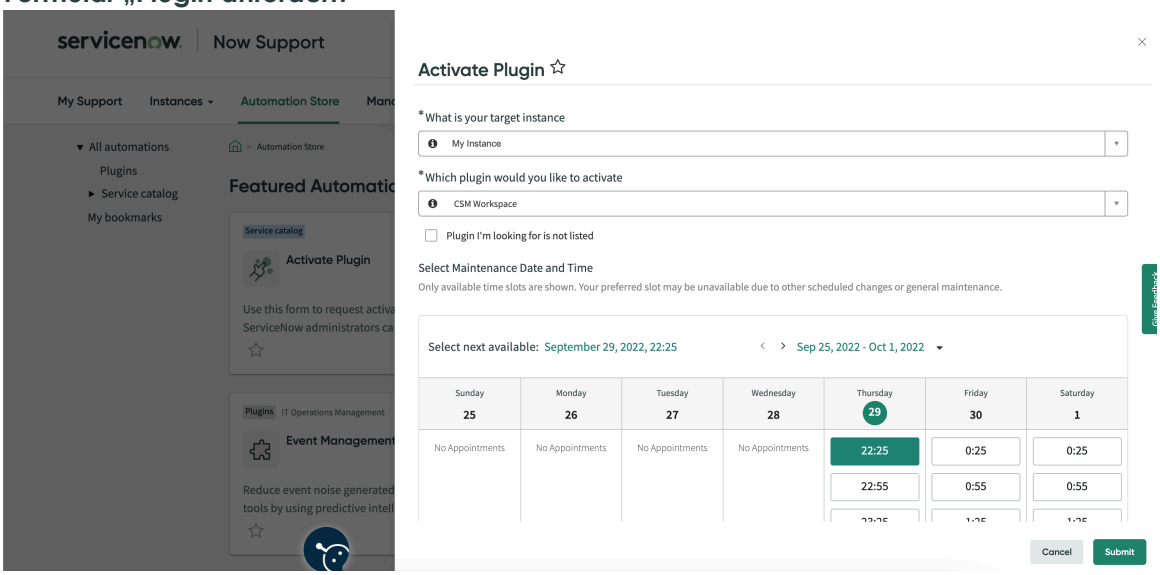
Feld	Beschreibung
What is your target instance (Ihre Zielinstanz)	Instanz, auf der das Plugin aktiviert werden soll.
Which plugin would you like to activate (Welches Plugin möchten Sie aktivieren?)	Name des zu aktivierenden Plugins **Hinweis:** Wenn das System das gewünschte Plugin nicht auflistet oder wenn Sie das Plugin auf einer OEM- oder lokalen Instanz aktivieren, aktivieren Sie das Kontrollkästchen **Plugin I'm looking for is not listed (Gesuchtes Plugin ist nicht aufgelistet)**, und geben Sie dann den Namen des Plugins ein.
Select Maintenance Date and Time (Datum und Uhrzeit der Wartung)	Datum und Uhrzeit zum Aktivieren des Plugins. **Hinweis:** Plugins werden in der pazifischen Zeitzone jeden Werktag in zwei Batches aktiviert, einmal am Morgen und einmal am Abend. Wenn das Plugin zu einem bestimmten Zeitpunkt aktiviert werden muss, geben Sie die Anforderung bei **Grund/ Kommentare** ein.

Example

Betrachten Sie beispielsweise das folgende Formular, um das Plugin „CSM Workspace“ in einer Instanz mit dem Namen „My Instance“ zu aktivieren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Plugin anfordern“



7. Wählen Sie **Absenden**.
   Weitere Informationen zum Anfordern eines Plugins finden Sie im Artikel Plugin aus dem Servicekatalog anfordern [KB0751715] in der Now Support Knowledge Base.

Rollen mit erhöhten Rechten

Rollen mit erweiterten Berechtigungen müssen manuell die Verantwortung für die Verwendung der Rolle übernehmen, bevor Sie auf die Funktionen der Rolle zugreifen können.

Standardmäßig haben Sie bei der Anmeldung keine Rollen mit erhöhten Berechtigungen. Sie müssen manuell auf die Berechtigung der Rolle hochstufen. Eine Rolle mit erhöhten Berechtigungen ist nur für die Dauer Ihrer Benutzersitzung gültig. Bei Zeitüberschreitung der Sitzung oder Abmeldung wird die Rolle entfernt.

Sie können jede Rolle als Rolle mit erweiterten Berechtigungen festlegen und diese Rolle dann einem oder mehreren Benutzern zuweisen. Führen Sie diese Option aus, wenn Sie verhindern möchten, dass Benutzer unmittelbar nach der Anmeldung Zugriff auf die Rechte haben, die die Rolle bietet. Sie können die Berechtigungsrolle im Formular „Rolle“ festlegen. Anweisungen finden Sie unter Rollen erstellen .

Um eine erhöhte Rolle zu verwenden, müssen Sie die folgenden Bedingungen erfüllen:

- Die erhöhte Rolle muss Ihnen zugewiesen werden.
- Sie müssen manuell auf eine bestimmte erhöhte Rolle hochstufen, um deren Berechtigungen zu erhalten, auch wenn Sie bereits auf eine zweite erhöhte Rolle hochgestuft sind, die die erste erhöhte Rolle enthält.

  Wenn beispielsweise die erhöhte Rolle A die erhöhte Rolle B enthält, müssen Sie, selbst wenn Sie auf Rolle A hochstufen, noch auf Rolle B hochstufen, um ihre Berechtigungen zu erhalten.

Die Administratorrolle

Um einem Anwender die Administratorrolle zu gewähren, muss der gewährende Anwender auch über die Administratorrolle verfügen. Beispiel: Ein Benutzer, der nur über die Rolle user_admin verfügt, kann anderen Benutzern die Rolle admin nicht gewähren.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

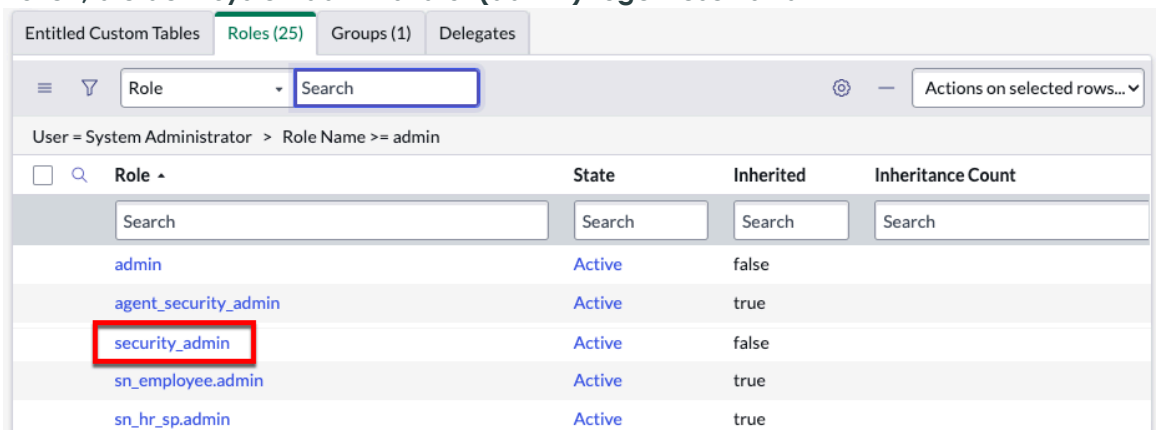
- Nicht-Administratoren können einen Anwender nicht zu einer Gruppe hinzufügen, die die Administratorrolle enthält.
- Um einem Anwender die Rolle „security_admin“ zu gewähren, muss der gewährende Anwender auch über die Administratorrolle verfügen und auf die Rolle „security_admin“ hochstufen, bevor er anderen Anwendern die Rolle „security_admin“ gewährt. Ein Benutzer, der nur über die Rolle „admin“ verfügt, kann anderen Benutzern die Rolle „security_admin“ nicht gewähren.
- Ein Benutzer ohne die Rolle „security_admin“ kann keinen Benutzer zu einer Gruppe hinzufügen, die die Rolle „security_admin“ enthält.

Warnung: Die Verwendung von erweiterten Berechtigungen für die Administratorrolle wird nicht unterstützt und kann zu unerwartetem Verhalten führen. Um von Administratoren eine manuelle Erhöhung zu verlangen, lesen Sie unter Erzwingen Sie eine manuelle Erhöhung durch Administratorennach.

Die Rolle security_admin

Im Basissystem ist die Rolle security_admin die einzige Rolle mit erweiterten Berechtigungen. Diese Rolle wird automatisch dem Benutzer zugewiesen, der der Standardbenutzer des Systemadministrators (admin) ist. Sie bietet Zugriff auf ACLs und Einstellungen für strenge Sicherheit.

Rollen, die dem Systemadministrator (admin) zugewiesen sind



Hinweis: Um diese Rolle anzuzeigen, müssen Sie zuerst auf die Rolle security_admin hochstufen. Wenn Sie nur als Systemadministratorbenutzer (admin) angemeldet sind, wird der Datensatz security_admin nicht in der Liste der Rollen angezeigt.

Rolle Security_admin

Die Rolle „security_admin“ ist eine Rolle mit erweiterten Berechtigungen, die mit „Strenge Sicherheitseinstellungen“ bereitgestellt wird und die es Anwendern ermöglicht, Zugriffssteuerungen zu erstellen und zu ändern und „Strenge Sicherheitseinstellungen“ zu ändern.

Im Basissystem verfügt nur der Standardbenutzer des Systemadministrators (admin) über die Rolle security_admin. Da hierfür eine Erhöhung von Berechtigungen erforderlich ist, verfügt der Administratorbenutzer bei der Anmeldung nicht über diese Rolle. Nach der Erhöhung von Berechtigungen verfügt der Administratorbenutzer für die Dauer der Anwendersitzung über die Rolle security_admin. Weitere Informationen finden Sie unter Auf eine privilegierte Rolle hochstufen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um ein hohes Sicherheitsniveau zu gewährleisten, müssen für die Rolle security_admin Berechtigungen erhöht werden. Schränken Sie die Anwender und Gruppen ein, denen Sie diese Rolle zuweisen.

Auf eine privilegierte Rolle hochstufen

Der Basissystemadministrator kann auf eine privilegierte Rolle hochstufen, um Zugriff auf die Funktionen von „Strenge Sicherheitseinstellungen“ zu erhalten.

Vorbereitungen
Erforderliche Rolle: admin

Hinweis: Wenn Sie zusätzlichen Anwendern die Administratorrolle gewähren, können sie nicht auf eine privilegierte Rolle hochgestuft werden. Nur der Basissystemadministrator kann eine Erhöhung durchführen.

Prozedur

1. Klicken Sie im Bannerframe auf Ihr Bild, oder klicken Sie auf Ihre Initialen, wenn Sie kein Bild hochgeladen haben.
2. Wählen Sie **Rollen erweitern aus**.
   Es wird ein Dialogfeld mit verfügbaren Rollen für die Erhöhung angezeigt.
3. Wählen Sie die zuzuweisenden erhöhten Rollen aus, und klicken Sie auf **OK**.
   Diese Rolle gewährt dem Benutzer für den Rest der Sitzung erweiterte Rechte für alle Ressourcen, die von dieser Rolle gesteuert werden. Wenn sich der Benutzer abmeldet, werden die erweiterten Berechtigungen mit der Sitzung beendet, können jedoch bei der nächsten Anmeldung wiederhergestellt werden.
4. Beenden Sie die Rollenerweiterung, indem Sie zum Dialogfeld in Schritt 2 zurückkehren und die Rolle deaktivieren.

Erzwingen Sie eine manuelle Erhöhung durch Administratoren

Es ist eine Eigenschaft verfügbar, mit der alle Benutzer mit der Administratorrolle aufgefordert werden, die Rolle, auf die sie hochgestuft werden sollen, manuell auszuwählen.

Vorbereitungen
Erforderliche Rolle: security_admin

Prozedur

1. Melden Sie sich als Administrator an.
2. Erhöhen Sie Ihre Rolle auf security_admin.
3. Navigieren Sie zu **sys_properties.list**.
4. Suchen Sie nach der Eigenschaft *`glide.security.strict_elevate_privilege`*, und wählen Sie sie aus.
5. Setzen Sie das Feld Wert auf **true**, und klicken Sie auf **Absenden**.

Ergebnisse
Wenn sich der Benutzer anmeldet, wird ihm ein Dialogfenster angezeigt, in dem er die Rolle auswählen kann, auf die er hochstufen kann.

Verbindung und Anmeldeinformationen

Anmelde- und Verbindungsinformationen sind erforderlich, um auf einen Computer oder ein Netzwerkgerät für Discovery, Service-Mapping und Cloud-Management zuzugreifen oder um

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

mit Orchestration zu arbeiten. Beim Hinzufügen von Inhalten zu Share oder App-Store können Sie für Ihre Umgebung relevante Verbindungen und Anmeldeinformationen konfigurieren, ohne den integrierten Inhalt zu ändern.

Untersuchen	Konfigurieren
	
Erfahren Sie mehr über Anmeldeinformationen.	Anmeldeinformationen konfigurieren

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Referenz



Ruft Details zu Anmeldeinformationen ab.

Problembehandlung



Erfahren Sie, wie Sie Probleme mit Verbindungen und Anmeldeinformationen beheben können.

Anmeldeinformationen, Verbindungen und Aliasse erkunden

Alle Anwendungsintegrationen in Now Platform verwenden Verbindungen, Anmeldeinformationen und Aliasse von , um Anwendungen den Zugriff auf -Ressourcen zu ermöglichen.

Bevor Sie eine Anwendungsintegration in Now Platformausführen können, müssen Sie Verbindungsinformationen und entsprechende Anmeldeinformationen erstellen und konfigurieren und einen Alias hinzufügen. Um zu verstehen, wie ServiceNow diese Begriffe definiert:

Verbindung

Eine Verbindung ist eine Integration in ein System, z. B. eine IP-Adresse oder ein Endpunkt mit Protokollen. Bei der Integration in eine Datenbank enthalten sie bestimmte Daten, z. B. Angaben zur Datenbank.

Anmeldeinformationen

Anmeldeinformationen sind die Authentifizierungsdaten, die zum Herstellen der Verbindung erforderlich sind, z. B. eine ID und ein Passwort.

Alias

Ein Alias ist eine Namenskonvention oder ein Tag, das bzw. der an eine Reihe von Verbindungen oder Anmeldeinformationen in Ihrer Instanz gebunden ist. Ein Alias enthält die erforderlichen Verbindungs- und Anmeldeinformationen für die Integration einer -Anwendung. Anstatt diese Informationen bei jeder Integration einzugeben, können Sie einen Alias verwenden. Sie können beispielsweise einen Alias festlegen, um Ihre QA-, Entwicklungs- und

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Produktionsanmeldeinformationen für dieselbe Anwendungsintegration zu speichern. Der Alias löst die Anwendungsintegration für jede Umgebung auf.

Now Platform unterscheidet verschiedene Arten von Aliassen:

Anmeldeinformationsalias

Dieser Alias wird nur Anmeldeinformationsdaten zugeordnet und während der Laufzeit aufgelöst.

Ungültiger Alias für Verbindungen und Anmeldeinformationen

Dieser Alias wird den Verbindungsinformationen und den Anmeldeinformationen zugeordnet, die zum Abschließen der Integration erforderlich sind, und wird während der Laufzeit aufgelöst.

Innerhalb von Aliassen für Verbindungs- und Anmeldeinformationen können Sie auch zusätzliche Aliasse erstellen, die als untergeordnete Aliassebezeichnet werden. Mit untergeordneten Aliassen können Sie mehrere Verbindungen innerhalb derselben Anwendungsintegration erstellen. Wenn Sie einen untergeordneten Alias erstellen, wird der Alias, unter dem Sie ihn erstellt haben, zu einem übergeordneten Alias. Während untergeordnete Aliasse Eigenschaften von ihrem übergeordneten Alias erben, tragen untergeordnete Aliasse ihre eigenen Verbindungs- und Anmeldeinformationen.

Vorteile der Verwendung von Verbindungen, Anmeldeinformationen und Aliassen

- Zentraler Ort zum Speichern und Verwalten von Anmeldeinformationen für einen externen Service
- Einmal definieren und für mehrere Plattformfunktionen wiederverwenden
- Minimieren Sie die Konfiguration anderer Plattformfunktionen
- Ermöglichen Sie Nicht-Administratoren die Verwendung vordefinierter Verbindungen und Anmeldeinformationen
- Mehr Sicherheit

Funktionen mit Verbindungen, Anmeldeinformationen und Aliassen

Die folgenden Funktionen verwenden Verbindungen, Anmeldeinformationen und Aliasse:

- Flow Designer
- IntegrationHub
- Cloud-Management
- Discovery
- Orchestration
- Service-Mapping

Sie können Aliasse für Now Platform auf zwei Arten einrichten:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Mit dem Modul Verbindungen und Anmeldeinformationen Weitere Informationen finden Sie unter Verbindungs- und Anmeldealias erstellen.
- Im Dashboard „Verbindungen“ von IntegrationHub. Weitere Informationen finden Sie unter Verbindung hinzufügen .

Hinweis: IntegrationHub erfordert ein separates Abonnement. Weitere Informationen finden Sie unter Anforderung IntegrationHub an.

Synchronisierung der Anmeldeinformationen auf MID Servern

Jeder MID-Serverin Ihrem Netzwerk, der mit der -Instanz synchronisiert wird, behält eine Kopie aller von Ihnen erstellten Anmeldeinformationen bei. Der MID-Server (Management, Instrumentation, and Discovery) ist eine Java-Anwendung, die die Kommunikation und die Datenbewegung zwischen einer ServiceNow-Instanz und externen Anwendungen, Datenquellen und Services ermöglicht. Diese Synchronisierung beschleunigt das Lesen von Anmeldeinformationen, wenn Anwendungen wie Discovery oder Service-Mapping im Netzwerk auf mehrere Geräte zugreifen müssen. Die MID Server führen eine Synchronisierung durch, wenn sie einen *credentials_reload*-Auftrag in der ECC-Warteschlange finden. Der Auftrag zum Neuladen weist den MID Server an, einen SOAP-Aufruf an die Instanz auszuführen, um die gesamte Liste der Anmeldeinformationen in der Tabelle „Anmeldeinformationen“ [discovery_credentials] einschließlich aller Feldwerte abzurufen. Weitere Informationen finden Sie unter MID-Server .

Die SOAP-Antwort, die Ihre Instanz an die einzelnen MID Server sendet, enthält auch benutzerdefinierte Felder, die Sie von Ihnen angepassten Formularen für Anmeldeinformationen hinzugefügt haben. Wenn Sie Referenzfelder hinzugefügt haben, werden die Daten in der referenzierten Tabelle ebenfalls als Teil der SOAP-Antwort gesendet. Dies kann zu Leistungsproblemen führen, wenn die Anmeldeinformationen mit mehreren MID Servern synchronisiert werden. Dieses Problem können Sie am besten in den Griff bekommen, wenn Sie der Tabelle „Systemeigenschaften“ [sys_properties] folgende Eigenschaften manuell hinzufügen:

Hinweis: Um die Werte in diesen Eigenschaften zu ändern, fügen Sie sie der Tabelle „Systemeigenschaften“ [sys_properties] hinzu. Wenn Sie sie nicht hinzufügen, verwendet das System den Standardwert.

Eigenschaft	Beschreibung
`com.snc.credentials_user_fields`	Schließt alle benutzerdefinierten Felder in die Synchronisierung der Anmeldeinformationen ein. Legen Sie diese Eigenschaft auf „false“ fest, wenn die Felder, die Sie den Anmeldeinformationsformularen hinzugefügt haben, nicht eingeschlossen werden sollen. • **Typ**: true | false • **Standardwert**: true
`com.snc.credentials_recursion_depth`	Definiert die Anzahl der zu durchlaufenden Tabellen, wenn der Anmeldeinformationssynchronisierungsmechanismus Felder aus Referenztabellen sammelt. Verringern Sie diese Anzahl, wenn Leistungsprobleme auftreten und Sie über angepasste Formulare für Anmeldeinformationen verfügen, die Referenzfelder

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	für Tabellen enthalten, die ebenfalls Referenzfelder enthalten. • **Typ**: Ganzzahl • **Standardwert**: 3

Bereichsschutz für Anmeldeinformationen und Verbindungen

Sie können bestimmte Typen von Verbindungs- und Anmeldeinformationsdatensätzen als zu einem Bereich gehörend klassifizieren und den Schutz des Bereichs darauf erweitern. Diese Bereichsrichtlinien dienen dem Schutz von Datensätzen, die Sie in einer Tabelle erstellen, und verhindern Interaktionen mit Datensätzen, die für einen anderen Bereich privat sind.

In den Tabellen „Verbindung“ [sys_connection] und „Discovery-Anmeldeinformationen“ [discovery_credentials] ist ein **Anwendungsfeld** verfügbar, um diese Datensatztypen bestimmten Bereichen zuzuordnen. Es ist in UI-Formularen in Xanadunicht sichtbar, Sie können es jedoch problemlos hinzufügen. Weitere Informationen zu diesen Datensatztypen und zum Hinzufügen des Felds zu ihren UI-Formularen finden Sie unter:

- Erste Schritte mit Verbindungen
- Erste Schritte mit Anmeldeinformationen
- Anmeldeinformationsaliasse für Discovery
- Formularlayout konfigurieren

Die Beschränkung der Verwendung eines Verbindungs- und Anmeldeinformationsdatensatzes auf einen bestimmten Bereich ist wichtig für die Verwaltung von Anwendungen, die erzwungene Sicherheit erfordern. Diese Anwendungen umfassen 'HR-Servicebereitstellung oder Security Operations Verbindungs- und Anmeldeinformationsdatensätze, die in bereichsbezogenen verwalteten Anwendungen erstellt wurden, sind für Administratorbenutzer nicht sichtbar. Durch das Zuordnen eines Datensatzes mit Verbindungs- und Anmeldeinformationen zu einem bestimmten Anwendungsbereich werden folgende Schutzmaßnahmen gewährt:

- Wendet Zugriffssteuerungslistenregeln (ACLs) auf eingeschränkte Bereiche an. Weitere Informationen zu bereichsbezogenen ACLs finden Sie unter Regeln für Zugriffssteuerungslisten.

  Hinweis: Einige Anwendungen, für die Bereichsverwaltung und erzwungene Sicherheit verwendet werden, erfordern möglicherweise ein zusätzliches Setup. Weitere Informationen finden Sie unter HR-Rollen verwalten

- Schützt Datensätze bei Abfrage mit einem Skript. Wenn Sie eine Abfrage im globalen Bereich durchführen und der Datensatz für Verbindungen und Anmeldeinformationen sich in einem geschützten Bereich befindet, wird er nicht in der Abfrage angezeigt, es sei denn, Sie erhalten Zugriff darauf.

Sie können abfragebeschränkte Datensätze anpassen und den Zugriff auf sie gewähren, indem Sie den eingeschränkten Anruferzugriff verwenden. Weitere Informationen finden Sie unter Einstellungen für eingeschränkte Anruferzugriffsberechtigungen . Einschränkungen bei der Umfangsdefinition gelten auch für alle untergeordneten Tabellen der Tabellen „Verbindung“ [sys_connection] und „Discovery-Anmeldeinformationen“ [discovery_credentials]. Leere Felder und andere Bereiche sind nicht eingeschränkt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Bereichsschutz ist nur für bestimmte gesicherte Bereiche aktiviert, um Verwirrung beim Einrichten neuer Datensätze zu vermeiden. Wenn ein Anwender in seinem bereichsbezogenen Anwendungsbereich eine Verbindung herstellt, erfolgt keine automatische Bereichsbeschränkung.

Domain Separation und Anmeldeinformationen und Verbindungen

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

Support-Stufe: Standard

- Umfasst die **Basis**-Support-Stufe.
- Geschäftslogik: Der Service Provider (SP) erstellt oder ändert Prozesse für einzelne Kunden. Die Anwendungsfälle spiegeln die ordnungsgemäße Verwendung der Anwendung durch mehrere SP-Kunden in einer einzigen Instanz wider.
- Der Besitzer der Instanz muss die MVP-Geschäftslogik (Minimum des lebensfähigen Produkts) und die Datenparameter pro Mandant wie erwartet für die spezifische Anwendung konfigurieren.

Beispiel-Anwendungsfall: Ein Administrator muss in der Lage sein, Kommentare beim Schließen eines Datensatzes für einen Mandanten obligatorisch zu machen, für andere hingegen nicht.

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

Übersicht

Die Anmeldeinformationen sind an verschiedene ServiceNow-Funktionen gebunden, die auf Systeme außerhalb der Instanz zugreifen. Die Anmeldeinformationen folgen der Domain Separation, die an diejenige Funktion gebunden ist, welche die Anmeldeinformationen verwendet.

Verbindungen sind protokollspezifische Informationen, die auf einen Zielhost außerhalb der Instanz verweisen. Eine Verbindung kann die Domäne angeben, um eine Aktivität auszuführen.

Funktionsweise der Domain Separation für Anmeldeinformationen und Verbindungen

Anmeldeinformationen greifen auf Ressourcen außerhalb der Instanz zu und werden von Discovery , Orchestration , verwendet. Service-Mapping , und Cloud Provisioning and Governance Anwendungen. Diese Anmeldeinformationen sind nicht an eine bestimmte Domäne gebunden, sondern können an eine Anwendung gebunden sein und folgen dann der von der Anwendung verwendeten Domain Separation. Anmeldeinformationen können auch einem MID-Server zugewiesen werden und folgen dann der in der Konfiguration MID-Server angegebenen Domänentrennung.

Verbindungen greifen auf einen Zielhost zu, der eine JMS-, JDBC-oder HTTP(s)-Verbindung verwendet. Sie können eine globale oder eine bestimmte Domäne angeben, zu der die Verbindung gehört.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Domänentrennung für Service Provider

Konfigurationsvorlagen für Verbindungen und Anmeldeinformationen

Ermöglichen Sie Benutzern mit der Rolle „admin“ und „flow_designer“, Spoke-Integrationen mit Drittanbietersystemen über ein einzelnes, anpassbares Formular einzurichten.

Sie können beispielsweise eine OAuth-Integration einrichten, die einen OAuth-Anbieter registriert, ein Token generiert und Verbindungs- und Anmeldeinformationsdatensätze erstellt. Aktionsdesigner oder -entwickler können eine Konfigurationsvorlage verwenden, um die Spoke an einem Ort einzurichten. Das System erstellt dann die zugehörigen Datensätze.

Vorteile

Konfigurationsvorlagen ermöglichen:

- Administratoren oder Flow Designer zum Einrichten komplexer Integrationen mit einem einzigen Formular.
- Entwickler können statische Werte in einer Integration festlegen, was den Setup-Prozess für Administratoren und Flow Designer vereinfacht.

Unterstützte Anmeldeinformationstypen

Sie können Konfigurationsvorlagen für Integrationen mit den folgenden Anmeldeinformationstypen erstellen:

- Standardauthentifizierung
- API Key
- Gewährungstyp für OAuth-JWT-Bearer
- Gewährungstyp des OAuth-Autorisierungscodes
- Anwenderdefinierte Authentifizierung

Konfigurationsvorlagenkomponenten

Standarddatenvorlage

Damit werden statische Informationen festgelegt, die für jede Integration gelten. Beispielsweise können Sie die API und die Token-URL festlegen, wenn der Wert für jede Integration gilt.

Dynamische Datenvorlage

Damit werden Informationen festgelegt, die der Benutzer zum Einrichten der Integration eingeben muss. Beispielsweise können Sie Schlüssel-Wert-Paare aus Benutzername und Passwort hinzufügen, um benutzerdefinierte Werte zu erfassen.

Nachbearbeitungsskript

Damit werden zusätzliche Datensätze erstellt, die für die Integration erforderlich sind. Wenn Ihre Spoke beispielsweise benutzerdefinierte Tabellen enthält, können Sie Datensätze in diesen Tabellen auf der Grundlage von Benutzereingaben in der Konfigurationsvorlage erstellen. Dieses Skript wird ausgeführt, nachdem die Verbindungs- und Anmeldeinformationsdatensätze erstellt wurden.

Skript vorab bearbeiten

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Füllt die anwenderdefinierten Felder im Abschnitt „ **Zusätzliche Informationen** “ vorab aus, wenn Sie eine vorhandene Verbindung bearbeiten. Durch Vorabausfüllen der anwenderdefinierten Felder können Sie den aktuellen Wert anzeigen, der dem anwenderdefinierten Feld zugeordnet ist.

Demodaten

Die Tabelle „Vorlagen für Verbindungen und Anmeldeinformationen“ [sys_alias_templates] enthält Beispielvorlagen, die veranschaulichen, wie Vorlagen für gängige Authentifizierungstypen eingerichtet werden. Verwenden Sie diese Beispiele als Leitfaden, wenn Sie eigene erstellen.

Konfigurieren Sie eine Vorlage für den Erteilungstyp „OAuth-JWT-Bearer“.

Diese Beispielkonfigurationsvorlage richtet Datensätze für Anmeldeinformationen und Verbindungen mithilfe des Gewährungstyps „JWT Bearer“ ein, um Anforderungen bei Docusign zu authentifizieren.

Standarddatenvorlage

Jedes Element der obersten Ebene in der Standarddatenvorlage erstellt einen zugehörigen Datensatz. Die Vorlage enthält diese Abschnitte:

- `Anmeldeinformationen`: Erstellt einen Datensatz in der Tabelle „Anmeldeinformationen“.
- `Verbindung`: Erstellt einen Datensatz in der Tabelle „Verbindungen“ [sys_connection] und in allen zugehörigen Verbindungsdatensätzen.
- `Zusätzlich`: Erstellt optional Datensätze in einer benutzerdefinierten Tabelle. Das Nachverarbeitungsskript teilt dem System mit, was mit diesen Datensätzen geschehen soll.

Im folgenden Beispiel werden die für die OAuth-JWT-Bearer-Gewährungstypauthentifizierung erforderlichen Datensätze erstellt.

```
{
  "credential": {
    "oauth_entity": {
      "oauth_entity_profile": [
        {
          "grant_type": "urn:ietf:params:oauth:grant-type:jwt-bearer",
          "name": "Docusign Profile",
          "default": true,
          "oauth_entity_profile_scope": [
            "users:read.email"
          ]
        }
      ],
      "code_challenge_method": "S256",
      "type": "consumer",
      "oauth_entity_scope": [
        {
          "oauth_entity_scope": "users:read.email",
          "name": "email"
        }
      ],
      "client_id": "<provider-client-id>",
      "use_mutual_auth": false,
      "revoke_token_url":
 "https://<provider-domain-name>.com/oauth2/revoke",
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
      "default_grant_type":
 "urn:ietf:params:oauth:grant-type:jwt-bearer",
      "public_client": false,
      "oauth_api_script": "3e3a3a11c333210016194ffe5bba8f70",
      "name": "Docusign Spoke OAuth",
      "client_secret": "<provider-client-secret>",
      "auth_url": "https://<provider-domain-name>.com/oauth2/auth",
      "token_url": "https://<provider-domain-name>.com/oauth2/token",
      "redirect_url":
 "https://<instance-name>.service-now.com/oauth_redirect.do"
    },
    "jwt_provider": {
      "jwt_keystore_aliases": {
        "kid": "<provider-key-id>",
        "name": "Docusign Spoke JWT Key",
        "signing_keystore": "<signing-keystore-sys-id>",
        "signing_algorithm": "rsa_256",
        "signing_key_password": "password"
      },
      "jwt_claim_validation" : [ {
        "name" : "iss",
        "is_standard" : true,
        "data_type" : "string",
        "value":"<docusign-iss-claim>"
      }, {
        "name" : "sub",
        "is_standard" : true,
        "data_type" : "string",
        "value":"<docusign-sub-claim>"
      }, {
        "name" : "aud",
        "is_standard" : true,
        "data_type" : "string",
        "value":"<docusign-aud-claim>"
      }, {
        "name" : "scope",
        "is_standard" : false,
        "data_type" : "string",
        "value" : "signature impersonation"
      } ],
      "name": "Docusign Spoke JWT Provider",
      "jwt_api_script": "9ef6af86ff10330001d3cd6bd53bf144"
    },
    "name": "Docusign Spoke Credential",
    "table": "oauth_2_0_credentials"
  },
  "connection": {
    "use_mid": false,
    "connection_url": "https://<provider-domain-name>.com",
    "name": "Docusign Spoke Connection",
    "table": "http_connection"
  },
"additional":{
    "docusign_account_name": "<docusign-account-name>",
    "docusign_account_email": "<docusign-account-email>"
```

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
}
}
```

Dynamisches Datenschema

Das dynamische Datenschema definiert, was der Benutzer sieht, wenn er einen Alias für Verbindungen und Anmeldeinformationen erstellt, und sammelt seine Eingaben. Verwenden Sie die Dot-Walking-Syntax, um Anwendereingaben Feldern zuzuordnen, die in der Standarddatenvorlage erstellt wurden. Beispiel: `connection_fields` ordnet die Benutzereingabe dem Feld `connection_url` im `Verbindungsobjekt` zu, das von der Standarddatenvorlage erstellt wurde.

```
{
  "connection_fields": [
    {
      "name": "connection.connection_url",
      "label": "Connection URL",
      "type": "text",
      "defaultValue": "https://demo.docusign.net",
      "hint": "Connection URL for Docusign"
    }],
"additional_fields":[
    {
      "name": "additional.docusign_account_id",
      "label": "Docusign Account Number",
      "type": "text",
      "hint": "Docusign Account Number"
    },
    {
      "name": "additional.docusign_account_name",
      "label": "Docusign Account Name",
      "type": "text",
      "hint": "Name to identify the Docusign account"
    },
    {
      "name": "additional.docusign_account_email",
      "label": "Docusign Account Email",
      "type": "text",
      "hint": "Docusign Account Email"
    }
  ],
  "credential_fields": [
    {
      "name": "credential.oauth_entity.client_id",
      "label": "OAuth Client ID",
      "type": "text",
      "hint": "Client ID for Docusign"
    },
    {
      "name": "credential.oauth_entity.redirect_url",
      "label": "OAuth Redirect URL",
      "type": "text",
      "defaultValue":
 "https://<instance-name>.service-now.com/oauth_redirect.do",
      "hint": "Callback URL for Docusign"
    },
 {
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
      "name": "credential.jwt_provider.jwt_claim_validation[0].value",
      "label": "Issuer (iss) Claim value",
      "type": "text",
      "hint": "The integrator key (also known as client ID) of the
 application"
    },
 {
      "name": "credential.jwt_provider.jwt_claim_validation[1].value",
      "label": "Subject (sub) Claim value",
      "type": "text",
      "hint": "The user ID of the user to be impersonated"
    },
 {
      "name": "credential.jwt_provider.jwt_claim_validation[2].value",
      "label": "Audience (aud) Claim value",
      "type": "text",
      "defaultValue": "account-d.docusign.com",
      "hint": "The URI of the authentication service instance to be used
 e.g. account.docusign.com"
    },
    {
      "name": "credential.jwt_provider.jwt_keystore_aliases.kid",
      "label": "Key ID (kid)",
      "type": "text",
      "hint": "Indicates which key was used to secure the JWS"
    },
    {
      "name":
 "credential.jwt_provider.jwt_keystore_aliases.signing_keystore",
      "label": "Key Store",
      "type": "file"
    }
  ]
}
```

Nachbearbeitungsskript

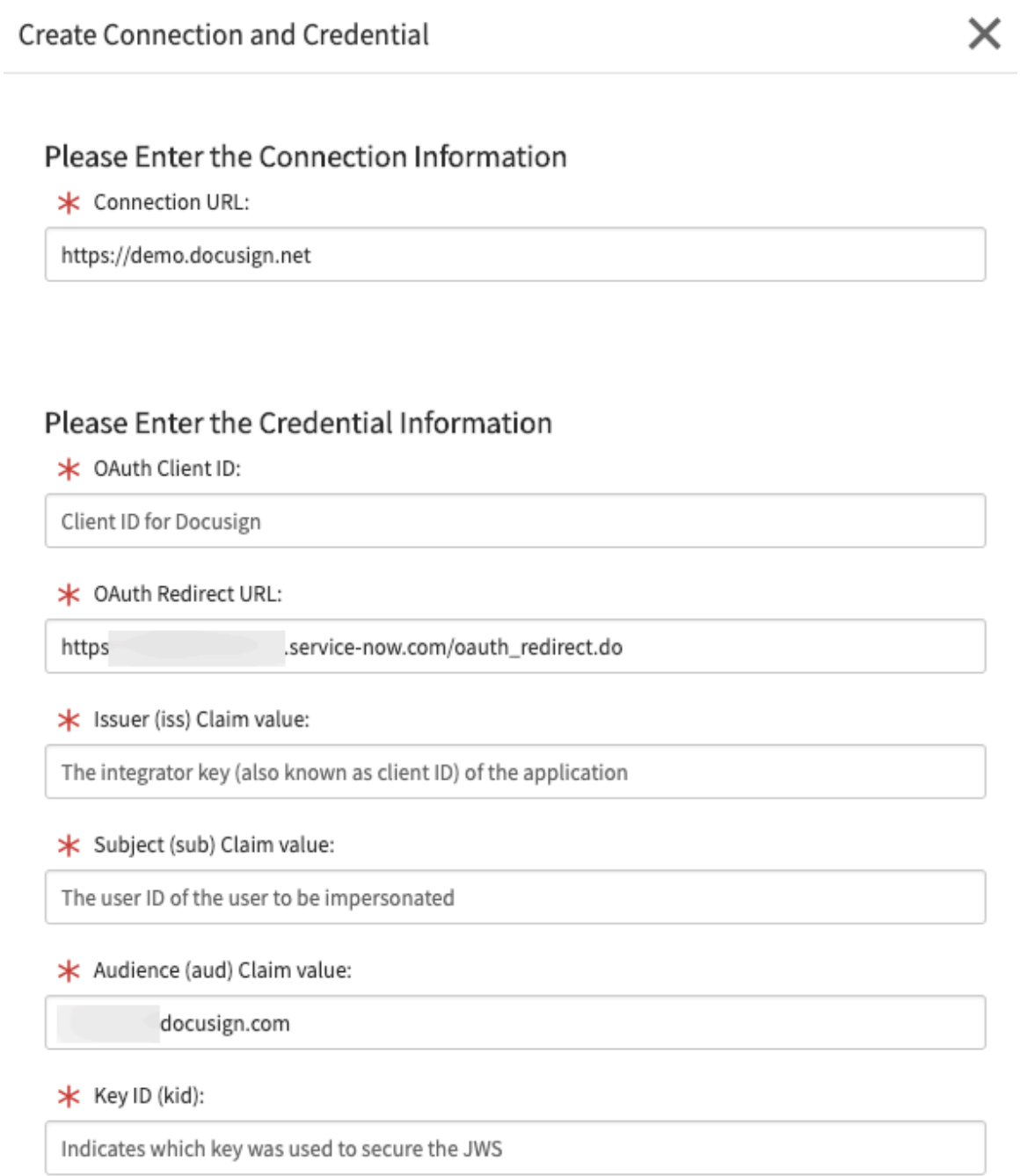
Das folgende Nachbearbeitungsskript ordnet Anwendereingaben Feldern in der Tabelle sn_docusign_spoke_accounts zu.

```
(function execute(aliasId, connectionSysId, jsonDefaultData,
 jsonDynamicData) {
 var jsonDynamicDataP = JSON.parse(jsonDynamicData);
 var accountGR = new GlideRecord("sn_docusign_spoke_accounts");
    accountGR.setValue("account_name",
 jsonDynamicDataP["additional.docusign_account_name"]);
    accountGR.setValue("alias", aliasId);
    accountGR.setValue("email",
 jsonDynamicDataP["additional.docusign_account_email"]);
    accountGR.setValue("id",
 jsonDynamicDataP["additional.docusign_account_id"]);
    accountGR.insert();
})(aliasId, connectionSysId, jsonDefaultData, jsonDynamicData);
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Resultierendes Konfigurationsformular für Verbindungen und Anmeldeinformationen von Docusign

Wenn der Benutzer zum zugehörigen DocuSign-Alias für Verbindungen und Anmeldeinformationen navigiert und **Neue Verbindung und Anmeldeinformationen erstellen**auswählt, wird das folgende Dialogfeld angezeigt.



Erstellen Sie eine Konfigurationsvorlage

Erstellen Sie eine Vorlage, die die Eingaben definiert, die zum Einrichten einer Spoke erforderlich sind. Legen Sie statische Schlüssel-Wert-Paare fest, um Datensätze zu erstellen, und legen Sie Werte fest, die für jede Integration gelten. Legen Sie dynamische Schlüssel-Wert-Paare fest, um Benutzereingaben zu sammeln und Feldwerte festzulegen, die variieren

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

können. Mit dieser Vorlage können Administratoren und Flow-Designer die -Spoke über ein einziges Formular einrichten.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **IntegrationHub** > **Verbindungen und Anmeldeinformationen** > **Konfigurationsvorlagen**an.
2. Wählen Sie **Neu**.
3. Wählen Sie den Typ der Konfigurationsvorlage aus, die Sie erstellen möchten.

Konfigurationstyp	Beschreibung
HTTP-Verbindung mit Gewährungstyp „OAuth-Autorisierungscode“	Erstellt eine Vorlage, um das Drittparteisystem mit einem Autorisierungscode als OAuth-Anbieter zu registrieren.
HTTP-Verbindung mit Gewährungstyp „OAuth JWT Bearer“	Erstellt eine Vorlage, um das Drittparteisystem als OAuth-Anbieter mit einem JSON-Web-Token zu registrieren.
HTTP-OAuth mit Gewährungstyp „Client-Anmeldeinformationen“.	Erstellt eine Vorlage für die Integration mit einer Drittanbieteranwendung über die OAuth 2.0-Authentifizierung, die den Gewährungstyp für Client-Anmeldeinformationen verwendet.
HTTP-Verbindung mit Gewährungstyp für OAuth-Client-Anmeldeinformationen (externer Speicher)	Erstellt eine Vorlage, die das Senden einer OAuth-Token-Anforderung, die von einem externen Speicher gespeicherte Client-Anmeldeinformationen enthält, über den MID-Server an einen OAuth-Server ermöglicht.
HTTP-Verbindung mit Anmeldeinformationsformular für Standardauthentifizierung	Erstellt eine Vorlage zur Integration in das Drittparteisystem mithilfe der Standardauthentifizierung.
HTTP-Verbindung mit Anmeldeinformationen für API-Schlüssel	Erstellt eine Vorlage zur Integration in das Drittparteisystem mithilfe eines API-Schlüssels.
Andere Konfiguration	Erstellt eine leere Vorlage, sodass Sie eine Vorlage für die anwenderdefinierte Authentifizierung einrichten können.

4. Fügen Sie im Feld **Name** einen Namen hinzu, um die Vorlage zu identifizieren.
5. **Nehmen Sie im Feld Standarddatenvorlage** die erforderlichen Änderungen vor.

   Dieses Feld legt statische Informationen fest, die für jede Integration gelten. Beispielsweise können Sie die API und die Token-URL festlegen, wenn der Wert für jede Integration gilt.

   Diese Objekte in der Standarddatenvorlage sind erforderlich:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- `Anmeldeinformationen`: Erstellt einen Anmeldeinformationsdatensatz mit den erforderlichen Feldern.
- `connection`: Erstellt einen Verbindungsdatensatz mit den erforderlichen Feldern. Greifen Sie mit dem untergeordneten Objekt „ `extended_attributes` “ auf Verbindungsattribute zu. Beispiel:

```
"connection": {
            "extended_attributes": {
                "api_version": "v1"

             },
        "connection_url": "https://<provider-domain-name>.com",
        "name": "Spoke Connection",
        "table": "http_connection"
    }
```

Sie können das `zusätzliche` Objekt verwenden, um Daten für eine anwenderdefinierte Tabelle einzurichten, und das Nachverarbeitungsskript verwenden, um die Daten in die Tabelle einzufügen.

Hinweis: In der Standarddatenvorlage für den Erteilungstyp „OAuth-Autorisierungscode“ müssen die Werte für die Schlüssel „ `oauth_entity_profile_scope`“ und „`oauth_entity_scope`“ übereinstimmen. Im folgenden Beispiel haben beide Schlüssel den Wert `E-Mail des Benutzers mit Lesezugriff`.

```
"oauth_entity_profile": [
        {
          "grant_type": "authorization_code",
          "name": "<provider-name> Profile",
          "default": true,
          "oauth_entity_profile_scope": [
            "Read user's email"
          ]
        }
      ],
      "code_challenge_method": "S256",
      "type": "consumer",
      "oauth_entity_scope": [
        {
          "oauth_entity_scope": "Read user's email",
          "name": "email"
        }
      ],
```

6. **Nehmen Sie im Feld Dynamisches Datenschema** die erforderlichen Änderungen vor.

   Dieses Feld Damit werden Informationen festgelegt, die der Benutzer zum Einrichten der Integration eingeben muss. Beispielsweise können Sie Schlüssel-Wert-Paare aus Benutzername und Passwort hinzufügen, um benutzerdefinierte Werte zu erfassen.

   Felder im dynamischen Datenschema enthalten diese Eigenschaften:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- `Name`: Das Feld, dem die Eingabe des Anwenders zugeordnet ist. Um beispielsweise die Benutzereingabe dem Feld Verbindungs-URL im Verbindungsdatensatz zuzuordnen, geben Sie `connection.connection_url`ein.
- `Bezeichnung`: Die Feldbezeichnung, die dem Anwender beim Ausfüllen der Vorlage angezeigt wird.
- `Typ`: Der Feldtyp. Stellen Sie sicher, dass dieser Datentyp mit dem Datentyp des Felds übereinstimmt, dem Sie den Wert zuordnen.
- `defaultValue`: Optional. Standardwert des Felds Wenn kein Standard angegeben ist, wird der Hinweis angezeigt.
- `Tipp`: Optional. Hinweistext, der angezeigt werden soll, wenn kein Standardwert vorhanden ist.

Hinweis: Wenn Sie eine Vorlage für die OAuth-JWT-Bearer-Gewährungstypauthentifizierung einrichten, möchten Sie möglicherweise eine Anwendereingabe für ein einzelnes Schlüssel-Wert-Paar im Array „`jwt_claim_validation`“. Sie können auf ein einzelnes Schlüssel-Wert-Paar im dynamischen Datenschema verweisen, indem Sie auf dessen Index im Array verweisen. Ihre Standarddatenvorlage könnte beispielsweise dieses Fragment enthalten.

```
"jwt_claim_validation" : [ {
        "name" : "iss",
        "is_standard" : true,
        "data_type" : "string",
        "value":"<docusign-iss-claim>"
      }, {
        "name" : "sub",
        "is_standard" : true,
        "data_type" : "string",
        "value":"<docusign-sub-claim>"
      }, {
        "name" : "aud",
        "is_standard" : true,
        "data_type" : "string",
        "value":"<docusign-aud-claim>"
      }, {
        "name" : "scope",
        "is_standard" : false,
        "data_type" : "string",
        "value" : "signature impersonation"
      } ],
```

Verweisen Sie auf das Schlüssel-Wert-Paar von `iss`, indem Sie den nullbasierten Index des Elements verwenden: `createtial.jwt_provider.jwt_claim_validation[0].value`.

7. Wahlweise: **Fügen** Sie im Feld „Nachverarbeitungsskript“ ein Skript hinzu, das Damit werden zusätzliche Datensätze erstellt, die für die Integration erforderlich sind. Wenn Ihre Spoke beispielsweise benutzerdefinierte Tabellen enthält, können Sie Datensätze in diesen Tabellen auf der Grundlage von Benutzereingaben in der Konfigurationsvorlage erstellen. Dieses Skript wird ausgeführt, nachdem die Verbindungs- und Anmeldeinformationsdatensätze erstellt wurden.lautet.
   Das Nachverarbeitungsskript hat Zugriff auf diese globalen Objekte.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Globales Objekt	Beschreibung
aliasId	Sys_id des Aliasdatensatzes aus der Tabelle „Alias für Verbindungen und Anmeldeinformationen“ [sys_alias].
connectionSysId	Sys_id des von der Vorlage erstellten Verbindungsdatensatzes.
jsonDefaultData	JSON-Inhalt aus dem Feld **„Standarddatenvorlage“** im Zeichenfolgenformat.
jsonDynamicData	JSON-Inhalt aus dem Feld **„Dynamische Datenvorlage“** im Zeichenfolgenformat.

8. **Fügen** Sie im Feld Vorbearbeitungsskript ein Skript hinzu, um die zusätzlichen Felder beim Bearbeiten einer Verbindung vorab auszufüllen.

   Dieses Skript gibt ein Array von Objekten zurück. Jedes Objekt verfügt über ein Name-Wert-Paar zum Ausfüllen der zusätzlichen Felder. Wenn beispielsweise die Verbindung Felder erfordert, die sich in einer benutzerdefinierten Tabelle befinden, können Sie diese Felder der benutzerdefinierten Tabelle zuordnen.

   Das **Vorbearbeitungsskript** hat Zugriff auf die folgenden globalen Objekte:

Globales Objekt	Beschreibung
aliasId	Sys_id des Aliasdatensatzes aus der Tabelle „Alias für Verbindungen und Anmeldeinformationen“ [sys_alias].
connectionSysId	Sys_id des von der Vorlage erstellten Verbindungsdatensatzes.
jsonDefaultData	JSON-Inhalt aus dem Feld **„Standarddatenvorlage“** im Zeichenfolgenformat.
jsonDynamicData	JSON-Inhalt aus dem Feld **„Dynamische Datenvorlage“** im Zeichenfolgenformat.

   Jedes Objekt im Skript hat die folgenden Eigenschaften:

   - `name`: Name des anwenderdefinierten Felds, um den Wert in der Verbindung anzugeben.
   - `Wert`: Wert, den Sie zuordnen möchten, um das anwenderdefinierte Feld auszufüllen. Sie können das Feld entweder mithilfe einer Funktion, einer Variable oder durch Hartcodieren zuordnen.

   Die folgenden Datentypen werden für die -Felder unterstützt:

   Unterstützte Datentypen für die -Felder

Typ	Beschreibung
Text	Zeichenfolgenwert.
Boolean	Auswahlfeld. Die Auswahl zeigt den Wert „wahr“ an, und die Abwahl der Auswahl zeigt den Wert „falsch“ an.
Nummer	Numerischer Wert.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typ	Beschreibung
Datum	Datumswert im Format JJJJ-MM-TT. Sie können auch das GlideDate-Objekt verwenden.
Auswahl	Liste der gültigen Auswahlmöglichkeiten, die im Feld **„Dynamisches Datenschema“ definiert**sind.
Referenz	Gültiger GlideRecord
Auswahlgruppe	Gruppen, die einen anderen Satz von Feldern enthalten. Diese Gruppen stehen in einer Dropdown-Liste zur Auswahl, wenn Sie eine Verbindung bearbeiten. Die Felder in jeder Gruppe werden angezeigt, wenn Sie die gewünschte Gruppe aus der Dropdown-Liste auswählen. Betrachten Sie beispielsweise die folgende Struktur der Auswahlgruppe, die im Feld **Dynamisches Datenschema definiert** ist: `{ "name": "radio_groups", "label": "Radio Groups", "type": "radio", "groups": [{ "name": "radio_group1", "label": "Radio Group 1", "fields": [{ "name": "radio_field1", "label": "Radio Field 1", "type": "text", "defaultValue": "efgh", "mandatory": true }] }, { "name": "radio_group2", "label": "Radio Group 2", "fields": [{ "name": "radio_field2", "label": "Radio Field 2", "type": "text", "defaultValue": "abcd", "mandatory": true }], "default_group": true }`  In diesem Beispiel können Sie das folgende Code-Fragment verwenden, um zu verstehen, wie Auswahlgruppen im Skript mithilfe von Dot-Walking verwendet werden:  `{ name: "radio_field.first_radio_group.radio_field1", value: "radio field 1" }, {`

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typ	Beschreibung
	<pre>name: "radio_field.second_radio_group.radio_field 2", value: "radio field 2" }, { name: “radio_groups”, value: gr.getValue(‘radio_groups’) }</pre> Weitere Informationen zur Verwendung von Dot-Walking finden Sie unter Dot-Walking .

Tipp: Wenn die vorab ausgefüllten Werte beim Bearbeiten einer Verbindung nicht in den Feldern angezeigt werden, navigieren Sie zu **Systemdiagnostik** > **Sitzung debuggen** > **Protokoll debuggen** um das Problem zu diagnostizieren.

9. Fügen Sie die Vorlage einem Alias für Verbindungen und Anmeldeinformationen hinzu.
   a. Navigieren zu **IntegrationHub** > **Verbindungen und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen**an.
   b. Öffnen Sie den Aliasdatensatz für die Spoke.
   c. Klicken Sie im Feld **Konfigurationsvorlage** auf das Suchsymbol.
   d. Wählen Sie die von Ihnen erstellte Vorlage aus der Liste aus.
   e. Klicken Sie auf **Aktualisieren**.

Ergebnisse

Wenn der Benutzer zum zugehörigen Alias für Verbindungen und Anmeldeinformationen navigiert und **Neue Verbindung und Anmeldeinformationen erstellen**auswählt, wird ein Dialogfeld angezeigt, in dem die Eingaben erfasst werden. Wenn Sie eine Vorlage für den Gewährungstyp „OAuth-Autorisierungscode“ erstellt haben, können Sie in diesem Dialogfeld auch ein OAuth-Token abrufen.

Nächste Maßnahme

Testen Sie die Vorlage, indem Sie zum zugehörigen Alias für Verbindungen und Anmeldeinformationen navigieren und **Neue Verbindung und Anmeldeinformationen erstellen**wählen. Vergewissern Sie sich, dass das Dialogfeld die erwarteten Daten sammelt und die erforderlichen Datensätze im System erstellt.

Erste Schritte mit Verbindungen

Verwenden Sie die Verbindungstabelle, um eine Basis-, JMS-, JDBC- oder HTTP(s)-Verbindung zu einem Zielhost einzurichten.

Verbindungstabelle

Die Tabelle „Verbindung“ (sys_connection) ist die Basistabelle für alle Verbindungstabellen. Sie können Verbindungen für die folgenden Protokolle einrichten:

- Basisverbindung für PowerShell und SSH
- JDBC

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- JMS
- HTTP(s)

Die Verbindungstabelle verweist auf die Verbindungsalias-Tabelle, die den Verbindungsalias mit Verbindungsinformationen koppelt. Jede Verbindung zeichnet die folgenden Informationen auf:

Basisverbindungseigenschaften

Feld	Beschreibung
Name	Name der Verbindung Dieses Feld muss in der Tabelle eindeutig sein.
Anmeldeinformationen	Geben Sie die Anmeldeinformationen an, die für diese Verbindung verwendet werden sollen. Dies ist optional.
Verbindungsalias	Der Verbindungsalias löst die Verbindung und die Anmeldeinformationen zur Laufzeit auf. Pro Verbindungsalias ist jeweils nur eine Verbindung aktiv.
Aktiv	Aktivieren Sie das Kontrollkästchen, um die aktuelle Verbindung zu aktivieren.
Domäne	Domäne, zu der die Verbindung gehört.

Die Anmeldeinformationen sind für alle aktiven Verbindungen eindeutig, sofern sie nicht leer sind.

Upgrade der Verbindungsinformationen

- Die Tabellen „JDBC-Verbindung“ [jdbc_connection] und „JMS-Verbindung“ [orch_jms_ds] sind vorhandene Orchestration-Verbindungstabellen, die jetzt von der Tabelle „Verbindung“ [sys_connection] erweitert werden. Die Tabellen wurden ursprünglich von „sys_metadata“ erweitert. Die auf „sys_metadata“ bezogenen Daten wurden entfernt.
- Die Tabellen werden aus dem Laufzeit-Plugin „Orchestration“ [com.snc.runbook_automation.runtime] zum Plugin „Anmeldeinformationen und Verbindungen“ verschoben.
- Der Upgrade-Prozess ruft JDBC- und JMS-Verbindungsinformationen ab, erstellt entsprechende Verbindungsaliasnamen und weist den Alias der zugehörigen Verbindung zu.
- JDBC-Feldnamenänderungen:
  - Der JDBC-Server wird in Host umbenannt
  - Der Datenbankport wird in Port umbenannt
  - Daten des JDBC-Servers und der Datenbank werden während des Upgrades zu Host und Port migriert

Basisverbindungen für PowerShell und SSH erstellen

Konfigurieren Sie die Verbindungsinformationen für die Verwendung mit einer benutzerdefinierten Aktivität oder Aktion, die das PowerShell- oder Secure Shell-Protokoll (SSH) verwendet.

Vorbereitungen

Erforderliche Rolle: admin oder connection_admin

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Anmeldeinformationen und Verbindungen** > **Verbindungen**an.
2. Klicken Sie auf **Neu**.
3. Wählen Sie **Basisverbindung für PowerShell und SSH** aus.
4. Füllen Sie das Formular aus.

Feld	Beschreibung
Name	Eindeutiger Name des Verbindungsdatensatzes
Anmeldeinformationen	Wählen Sie den Datensatz mit Anmeldeinformationen aus, der zur Autorisierung der Verbindung verwendet wird.
Verbindungsalias	Wählen Sie den Alias-Datensatz aus, der dieser Verbindung zugeordnet werden soll. Mit einem Alias können Sie den Verbindungsdatensatz aktualisieren, ohne Aktionen oder Aktivitäten, die den Alias verwenden, neu zu konfigurieren.
Host	Vollständig qualifizierter Domänenname des Zielhosts, auf dem das System die Aktivität oder Aktion ausführt. Zum Beispiel: host.domain.com.
Aktiv	Aktivieren Sie das Kontrollkästchen, um diese Verbindung zu aktivieren.
Domäne	Legt die Domäne fest, in der die Aktivität ausgeführt wird. Flow Designer unterstützt keine Domänentrennung und dieses Feld ignoriert.
Standardport überschreiben	Von der Verbindung verwendeter Zielport. Wenn Sie dieses Feld leer lassen, verwendet das System den Wert für den Standardport.
MID-Server verwenden	Aktivieren Sie das Kontrollkästchen, um eine Verbindung mit dem Zielhost über einen MID-Server herzustellen. Falls aktiviert, definieren Sie Felder im Abschnitt „Erweiterte MID Server-Konfiguration“. **Hinweis:** PowerShell erfordert einen MID-Server.
MID Auswahl	Option zum Auswählen des spezifischen MID-Servers oder MID-Clusters. ◦ MID**-Server automatisch auswählen**: Wählt den MID-Server automatisch aus. ◦ **Spezifischer MID-Server**: Verwendet den ausgewählten MID-Server. ◦ **Spezifischer MID-Cluster**: Verwendet den ausgewählten MID-Cluster. Dieses Feld ist verfügbar, wenn **MID-Server verwenden aktiviert** ist. **Hinweis:** Stellen Sie sicher, dass auf den Verbindungsdatensatz IntegrationHub verwiesen wird und nicht auf einen Orchestration -Verbindungsdatensatz.
Fähigkeiten	Die Fähigkeiten, die MID-Server unterstützten muss, um für die Auswahl in Frage zu kommen. Das System führt die Aktion oder Aktivität von einem MID-Server aus, das die ausgewählten

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Fähigkeiten unterstützt. Wird nur angezeigt, wenn **MID-Server verwenden** ausgewählt ist. Erforderliche Fähigkeiten bestimmen, welcher MID-Server zur Laufzeit ausgewählt wird. Weitere Informationen darüber, wie ein MID-Server während der Laufzeit ausgewählt wird, finden Sie unter MID-Server-Auswahl . Dieses Feld ist nur sichtbar, wenn **MID-Server automatisch** auswählen in der Liste MID-Auswahl ausgewählt ist.
MID-Anwendung	Die Anwendung, die MID-Server unterstützten muss, um für die Auswahl in Frage zu kommen. Das System führt die Aktion einem MID-Server aus, das die ausgewählte Anwendung unterstützt. Wird nur angezeigt, wenn **MID-Server verwenden** ausgewählt ist. Um mehr darüber zu erfahren, wie MID-Server während der Laufzeit ausgewählt wird, siehe MID-Server-Auswahl .
MID-Server	Spezifischer MID-Server, für den der Schritt ausgeführt wird. Dieses Feld ist nur sichtbar, wenn **Spezifischer MID-Server** in der Liste MID-Auswahl ausgewählt ist.
MID-Cluster	Der spezifische MID-Cluster, den Sie verwenden möchten. Dieses Feld ist verfügbar, wenn **„MID-Server verwenden" aktiviert** ist und **Spezifischer MID-Cluster** in der Liste „MID-Auswahl" ausgewählt ist.

5. Klicken Sie auf **Absenden**.

HTTP(s)-Verbindung erstellen

Die HTTP(s)-Verbindung stellt die Informationen bereit, mit der benutzerdefinierte HTTP(s)-Aktionen oder -Aktivitäten eine Verbindung herstellen.

Vorbereitungen

Erforderliche Rolle: connection_admin

Prozedur

1. Navigieren zu **Alle** > **Anmeldeinformationen und Verbindungen** > **Verbindungen**, klicken Sie auf **Neu**, und wählen Sie **HTTP(s)-Verbindung**aus.
2. Fügen Sie die folgenden Verbindungsinformationen hinzu, und klicken Sie auf **Absenden**:

Feld	Beschreibung
Name	Eindeutiger Name dieser HTTP(s)-Verbindung.
Anmeldeinformationen	Wählen Sie den Datensatz mit Anmeldeinformationen aus, der zur Autorisierung der Verbindung verwendet wird.
Verbindungsalias	Wählen Sie den Alias-Datensatz aus, der dieser Verbindung zugeordnet werden soll. Mit einem Alias können Sie den Verbindungsdatensatz aktualisieren, ohne Aktionen oder Aktivitäten, die den Alias verwenden, neu zu konfigurieren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
URL-Builder	Geben Sie entweder die Verbindungs-URL manuell ein, oder verwenden Sie das System, um die URL basierend auf den Eingaben zu erstellen. Standardmäßig ist dieses Kontrollkästchen deaktiviert. Wenn diese Option aktiviert ist, wird die Verbindungs-URL aus den folgenden Feldern berechnet: ◦ Gegenseitige Authentifizierung – Aktivieren Sie das Kontrollkästchen, wenn die gegenseitige Authentifizierung verwendet wird. ◦ Protokoll – Wenn keine gegenseitige Authentifizierung verwendet wird, geben Sie das Protokoll ein. Der Standardwert ist HTTPs. ◦ Protokollprofil – Wenn die gegenseitige Authentifizierung verwendet wird, geben Sie das Protokollprofil aus „sys_protocol_profile“ ein. ◦ Host ◦ Port ◦ Basispfad – Pfad der Verbindungszeichenfolge. **Hinweis:** Wenn „Gegenseitige Authentifizierung“ aktiviert ist, wird die Verbindungs-URL erstellt: Protokoll + :// + Host:Port +URL. Wenn „Gegenseitige Authentifizierung“ nicht aktiviert ist, wird die Verbindungs-URL erstellt: Protokollprofil + :// + Host:Port +URL
Verbindungs-URL	Wenn der URL-Builder deaktiviert ist, geben Sie die Verbindungs-URL in dieses Feld ein. **Hinweis:** Wenn „Gegenseitige Authentifizierung“ aktiviert ist, wird die Verbindungs-URL erstellt: Protokoll + :// + Host:Port +URL. Wenn „Gegenseitige Authentifizierung“ nicht aktiviert ist, wird die Verbindungs-URL erstellt: Protokollprofil + :// + Host:Port +URL
Aktiv	Aktivieren Sie das Kontrollkästchen, um diese Verbindung zu aktivieren.
Domäne	Legen Sie die Domäne, fest in der die Aktion oder Aktivität ausgeführt wird.
MID-Server verwenden	Aktivieren Sie dieses Kontrollkästchen, um einen MID Server für diese Aktion oder Aktivität zu verwenden. Falls aktiviert, definieren Sie Felder im Abschnitt „Erweiterte MID Server-Konfiguration“.
MID-Auswahl	Option zum Auswählen des spezifischen MID-Servers oder MID-Clusters.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	◦ MID**-Server automatisch auswählen**: Wählt den MID-Server automatisch aus. ◦ **Spezifischer MID-Server**: Verwendet den ausgewählten MID-Server. ◦ **Spezifischer MID-Cluster**: Verwendet den ausgewählten MID-Cluster. Dieses Feld ist verfügbar, wenn **MID-Server verwenden aktiviert** ist. **Hinweis:** Stellen Sie sicher, dass auf den Verbindungsdatensatz IntegrationHub verwiesen wird und nicht auf einen Orchestration -Verbindungsdatensatz.
Fähigkeiten	Die Fähigkeiten, die MID-Server unterstützten muss, um für die Auswahl in Frage zu kommen. Das System führt die Aktion oder Aktivität von einem MID-Server aus, das die ausgewählten Fähigkeiten unterstützt. Wird nur angezeigt, wenn **MID-Server verwenden** ausgewählt ist. Erforderliche Fähigkeiten bestimmen, welcher MID-Server zur Laufzeit ausgewählt wird. Weitere Informationen darüber, wie ein MID-Server während der Laufzeit ausgewählt wird, finden Sie unter MID-Server-Auswahl . Dieses Feld ist nur sichtbar, wenn **MID-Server automatisch** auswählen in der Liste MID-Auswahl ausgewählt ist.
MID-Anwendung	Die Anwendung, die MID-Server unterstützten muss, um für die Auswahl in Frage zu kommen. Das System führt die Aktion einem MID-Server aus, das die ausgewählte Anwendung unterstützt. Wird nur angezeigt, wenn **MID-Server verwenden** ausgewählt ist. Um mehr darüber zu erfahren, wie MID-Server während der Laufzeit ausgewählt wird, siehe MID-Server-Auswahl .
MID-Server	Spezifischer MID-Server, für den der Schritt ausgeführt wird. Dieses Feld ist nur sichtbar, wenn **Spezifischer MID-Server** in der Liste MID-Auswahl ausgewählt ist.
MID-Cluster	Der spezifische MID-Cluster, den Sie verwenden möchten. Dieses Feld ist verfügbar, wenn **„MID-Server verwenden“ aktiviert** ist und **Spezifischer MID-Cluster** in der Liste „MID-Auswahl“ ausgewählt ist.
Verbindungszeitüberschreitung	Anzahl der Millisekunden, die das System auf eine erfolgreiche Hostverbindung wartet. Wenn während dieser Zeit keine erfolgreiche Verbindung hergestellt wird, läuft die Verbindungsanforderung ab. Lassen Sie dieses Feld leer, um den Standard-Zeitüberschreitungswert für Verbindungen zu verwenden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf **Absenden**.
   Sie können jetzt eine benutzerdefinierte HTTP(s)-Aktion oder -Aktivität erstellen.

JDBC-Verbindung erstellen

Die JDBC-Verbindung enthält die Informationen, mit der benutzerdefinierte JDBC-Aktionen oder -Aktivitäten eine Verbindung zu verschiedenen Zieldatenbanken herstellen.

Vorbereitungen

Sie müssen über eine geeignete JAR-Datei verfügen, unabhängig davon, ob sie mit der Instanz oder mit einer benutzerdefinierten JAR-Datei bereitgestellt wird.

Hinweis: Die ServiceNow-Instanz stellt die Dateien `mysql-connector-java-5.1.21.jar`, `sql-server-jdbc-4.0.jar` und `ojdbc6.jar` als Teil des aktuellen Release bereit, das MySQL-, SQLServer- und Oracle-Datenbanken unterstützt. Andere Datenbanken wie Sybase oder DB2 Universal müssen eine benutzerdefinierte JAR-Datei verwenden, die in die Instanz hochgeladen werden muss, bevor die JDBC-Verbindung festgelegt wird.

Erforderliche Rolle: connection_admin

Warum und wann dieser Vorgang ausgeführt wird

JDBC-Anmeldeinformationen werden von der Aktivitätendesignervorlage separat abgerufen und unterstützen externe Anmeldeinformationsspeicher wie CyberArk.

Prozedur

1. Navigieren zu **Alle** > **Anmeldeinformationen und Verbindungen** > **Verbindungen**, klicken Sie auf **Neu**, und wählen Sie **JDBC-Verbindung**aus.
2. Füllen Sie das Formular anhand der Felder in der Tabelle aus.
   Anhand der Auswahl der Datenbank im Feld **Format** wird festgelegt, welche Felder verfügbar sind.

JDBC-Verbindungsfelder

Feld	Datenbankformat	Beschreibung
Name	Alle	Eindeutiger Name dieser JDBC-Verbindung. Zum Beispiel könnten Sie **JDBC MySQLProd** eingeben.
Berechtigung	Alle	Fügen Sie Anmeldeinformationen für den JDBC-Provider hinzu.
Verbindungsalias	Alle	Wählen Sie den Alias-Datensatz aus, der dieser Verbindung zugeordnet werden soll. Mit einem Alias können Sie den Verbindungsdatensatz aktualisieren, ohne Aktionen oder Aktivitäten, die den Alias verwenden, neu zu konfigurieren.
Abfragezeitüberschreitung	Alle	Maximale Dauer, die die JDBC-Abfrage ohne Antwort ausgeführt werden darf.
Verbindungstimeout	Alle	Anzahl der Millisekunden, die das System auf eine erfolgreiche JDBC-Verbindung wartet. Wenn während dieser Zeit keine erfolgreiche Verbindung hergestellt wird, läuft die Verbindungsanforderung ab. Lassen Sie dieses Feld leer, um den Standard-Zeitüberschreitungswert für Verbindungen zu verwenden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Datenbankformat	Beschreibung
Aktiv	Alle	Aktivieren Sie das Kontrollkästchen, um diese Verbindung zu aktivieren.
Domäne	Alle	Domäne für diese Tabelle. Standardmäßig wird die Tabelle „JDBC-Verbindung“ [jdbc_connection] in der Domäne **global** ausgeführt.
Format	Alle	Datenbanktyp für diese Verbindung. Die Standardoptionen sind: ◦ **MySQL** ◦ **Oracle** ◦ **SQL Server** ◦ **Keine** Sie können **Sybase** oder **DB2 Universal** zur Auswahlliste hinzufügen, indem Sie die entsprechende JAR-Datei für den JDBC-Treiber in die Instanz hochladen. Orchestration erkennt diese Treiber automatisch, wenn sie in das System geladen werden, und fügt sie dieser Liste hinzu.
Host	Oracle, MySQL, SQLServer	Hostname oder IP-Adresse des Datenbankservers.
Oracle-SID	Oracle	Der Site-Identifier der Oracle-Datenbank. Der Standardwert ist **orcl**.
Oracle-Anschluss	Oracle	Port, den die Oracle-Datenbank verwendet. Der Standardwert ist **1521**.
Datenbankname	MySQL, SQLServer	Name der Datenbank.
Port	MySQL, SQLServer	Port, den die ausgewählte Datenbank verwendet.
Instanzname	SQLServer	Instanzname für den ausgewählten SQLServer.
Verbindungs-URL	Alle	URL, mit der der MID Server eine Verbindung zu der angegebenen Datenbank herstellt. Die URL wird beim Speichern des Formulars automatisch erstellt und ist für die Standarddatenbanken schreibgeschützt. **Hinweis:** Wenn das ausgewählte Format keine der Standarddatenbanken ist, müssen Sie die Verbindungs-URL manuell erstellen, damit der MID Server darüber informiert ist, wie die Verbindung erstellt werden soll.
JDBC-Laufwerk	Keiner, DB2 Universal, Sybase	Der für diese Verbindung zu verwendende JDBC-Treiber, wenn es sich nicht um eine Standarddatenbank handelt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Datenbankformat	Beschreibung
		Hinweis: Wenn Sie eine Sybase- oder DB2 Universal-Datenbank hinzufügen, müssen Sie den Treibernamen in dieses Feld eingeben und die Treiber-JAR-Datei in die Instanz hochladen.
MID Server verwenden	Alle	Aktivieren Sie dieses Kontrollkästchen, um einen MID Server für diese Aktion oder Aktivität zu verwenden. Falls aktiviert, definieren Sie Felder im Abschnitt „Erweiterte MID Server-Konfiguration“.
MID Auswahl	Alle	Option zum Auswählen des spezifischen MID-Servers oder MID-Clusters. ◦ MID**-Server automatisch auswählen**: Wählt den MID-Server automatisch aus. ◦ **Spezifischer MID-Server**: Verwendet den ausgewählten MID-Server. ◦ **Spezifischer MID-Cluster**: Verwendet den ausgewählten MID-Cluster. Dieses Feld ist verfügbar, wenn **MID-Server verwenden aktiviert** ist. **Hinweis:** Stellen Sie sicher, dass auf den Verbindungsdatensatz IntegrationHub verwiesen wird und nicht auf einen Orchestration -Verbindungsdatensatz.
Fähigkeiten	Alle	Die Fähigkeiten, die MID-Server unterstützten muss, um für die Auswahl in Frage zu kommen. Das System führt die Aktion oder Aktivität von einem MID-Server aus, das die ausgewählten Fähigkeiten unterstützt. Wird nur angezeigt, wenn **MID-Server verwenden** ausgewählt ist. Erforderliche Fähigkeiten bestimmen, welcher MID-Server zur Laufzeit ausgewählt wird. Weitere Informationen darüber, wie ein MID-Server während der Laufzeit ausgewählt wird, finden Sie unter MID-Server-Auswahl . Dieses Feld ist nur sichtbar, wenn **MID-Server automatisch** auswählen in der Liste MID-Auswahl ausgewählt ist.
MID-Anwendung	Alle	Die Anwendung, die MID-Server unterstützten muss, um für die Auswahl in Frage zu kommen. Das System führt die Aktion einem MID-Server aus, das die ausgewählte Anwendung unterstützt. Wird nur angezeigt, wenn **MID-Server verwenden** ausgewählt ist. Um mehr darüber zu erfahren, wie MID-Server während der Laufzeit ausgewählt wird, siehe MID-Server-Auswahl .

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Datenbankformat	Beschreibung
MID-Server	Alle	Spezifischer MID-Server, für den der Schritt ausgeführt wird. Dieses Feld ist nur sichtbar, wenn **Spezifischer MID-Server** in der Liste MID-Auswahl ausgewählt ist.
MID-Cluster	Alle	Der spezifische MID-Cluster, den Sie verwenden möchten. Dieses Feld ist verfügbar, wenn **„MID-Server verwenden" aktiviert** ist und **Spezifischer MID-Cluster** in der Liste „MID-Auswahl" ausgewählt ist.

3. Klicken Sie auf **Absenden**.

Zugehörige Informationen

JDBC-Anmeldeinformationen

JMS-Verbindung erstellen

Konfigurieren Sie Ihr System für die Verwendung von Java Messaging Service (JMS) mit einer benutzerdefinierten JMS-Aktivität oder -Aktion.

Vorbereitungen

Erforderliche Rolle: connection_admin

Warum und wann dieser Vorgang ausgeführt wird

Der MID Server muss über die richtigen JMS Connection Factorys für Ihre Organisation verfügen. Konfigurieren Sie diese Werte in der Eigenschaft *mid.property.jms.command.allowed_factory_names* in **MID-Server** > **Eigenschaften**an. Die Standardwerte für diese Eigenschaft können in einen beliebigen Wert oder eine durch Kommas getrennte Liste von Werten geändert werden, die der JMS-Provider eines Drittanbieters bekanntgibt.

Prozedur

1. Navigieren zu **Anmeldeinformationen und Verbindungen** > **Verbindungen**an.
2. Klicken Sie auf **Neu**, wählen Sie **JMS-Verbindung**aus, füllen Sie das Formular aus, und klicken Sie dann auf **Absenden**.

Option	Bezeichnung
Name	Eindeutiger Name dieser Connection Factory.
Anmeldeinformationen	Fügen Sie Anmeldeinformationen für den JMS-Provider hinzu.
Verbindungsalias	Wählen Sie den Alias-Datensatz aus, der dieser Verbindung zugeordnet werden soll. Mit einem Alias können Sie den Verbindungsdatensatz aktualisieren, ohne Aktionen oder Aktivitäten, die den Alias verwenden, neu zu konfigurieren.
Ursprüngliche Kontext-Werkseinstellung	Name der JNDI-Klasse, die zum Erstellen des InitialContext verwendet wird.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	Hinweis: Um beispielsweise eine Verbindung zu ActiveMQ V5.10 (JMS-Provider) herzustellen, lautet der Wert `org.apache.activemq.jndi.ActiveMQInitialContextFactory`.
Provider-URL	Speicherort der laufenden JMS-Provider-Installation. **Hinweis:** So stellen Sie beispielsweise eine Verbindung zu ActiveMQ V5.1 her: `tcp://ipAdresseOderHostname:61616`.
Aktiv	Aktivieren Sie das Kontrollkästchen, um diese Verbindung zu aktivieren.
Domäne	Legen Sie die Domäne, fest in der die Aktion oder Aktivität ausgeführt wird.
MID Server verwenden	Aktivieren Sie dieses Kontrollkästchen, um einen MID Server für diese Aktion oder Aktivität zu verwenden. Falls aktiviert, definieren Sie Felder im Abschnitt „Erweiterte MID Server-Konfiguration“.
MID-Auswahl	Option zum Auswählen des spezifischen MID-Servers oder MID-Clusters. ◦ MID-**Server automatisch auswählen**: Wählt den MID-Server automatisch aus. ◦ **Spezifischer MID-Server**: Verwendet den ausgewählten MID-Server. ◦ **Spezifischer MID-Cluster**: Verwendet den ausgewählten MID-Cluster. Dieses Feld ist verfügbar, wenn **MID-Server verwenden aktiviert** ist.
MID-Cluster	Der spezifische MID-Cluster, den Sie verwenden möchten. Dieses Feld ist verfügbar, wenn **„MID-Server verwenden“ aktiviert** ist und **Spezifischer MID-Cluster** in der Liste „MID-Auswahl“ ausgewählt ist.
Fähigkeiten	Die Fähigkeiten, die MID-Server unterstützten muss, um für die Auswahl in Frage zu kommen. Das System führt die Aktion oder Aktivität von einem MID-Server aus, das die ausgewählten Fähigkeiten unterstützt. Wird nur angezeigt, wenn **MID-Server verwenden** ausgewählt ist.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	Um mehr darüber zu erfahren, wie MID-Server während der Laufzeit ausgewählt wird, siehe MID-Server-Auswahl .
MID-Anwendung	Die Anwendung, die MID-Server unterstützten muss, um für die Auswahl in Frage zu kommen. Das System führt die Aktion einem MID-Server aus, das die ausgewählte Anwendung unterstützt. Wird nur angezeigt, wenn **MID-Server verwenden** ausgewählt ist. Um mehr darüber zu erfahren, wie MID-Server während der Laufzeit ausgewählt wird, siehe MID-Server-Auswahl .

3. Navigieren zu **Verbindungen und Anmeldeinformationen** > **Anmeldeinformationen**an.
4. Klicken Sie auf **Neu**, wählen Sie **JMS-Anmeldeinformationen** aus, und geben Sie dann den Benutzernamen und das Passwort ein, die der MID für die Kommunikation mit dem JMS-Provider verwenden soll.
   Weitere Informationen finden Sie unter JMS-Anmeldeinformationen.
5. Klicken Sie auf **Absenden**.
   Sie können jetzt eine benutzerdefinierte JMS-Aktion oder -Aktivität erstellen.

Verbindungsattribute für IntegrationHub erstellen

Definieren Sie verbindungsspezifische Variablen, die Sie in IntegrationHub-Integrationsschritten verwenden können.

Vorbereitungen

Erforderliche Rolle:

- Um Verbindungsattribute zu erstellen, ist die Administratorrolle erforderlich.
- Um Attributwerte zuzuweisen, ist die Rolle „connection_admin“ oder die Administratorrolle erforderlich.
- Die Rolle „action_designer“ oder die Administratorrolle ist erforderlich, Im Attribute in einer benutzerdefinierten Aktion zu verwenden, ist die Rolle „action_designer“ oder die Administratorrolle erforderlich.

Verbindungsattribute werden nur von Integrationsschritten verwendet, für die IntegrationHub abonniert werden muss. Weitere Informationen zur Aktivierung von IntegrationHubfinden Sie unter Fordern Sie eine an IntegrationHub Plugin an.

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie einen Integrationsschritt verwenden, müssen Sie eine Verbindung mit einem externen System herstellen. Verwenden Sie einen Alias für Verbindungen und Berechtigungen, anstatt die Verbindung inline zu definieren. Mit einem Alias können Sie die Verbindungsdetails einmal aktualisieren, ohne jede Aktion neu konfigurieren zu müssen. Jeder Aktionsschritt, bei dem ein Alias verwendet wird, erbt die ihm zugeordneten Attribute. Vom Flow Designer werden Attribute als Datenpillen angezeigt, die Sie in Ihren Aktionsschritt ziehen können. Sie können beispielsweise ein Seitengrößenattribut erstellen, das zu einem Abfrageparameter für den REST-Schritt wird.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zum Erstellen von anwenderdefinierten Flow Designer -Aktionen finden Sie unter Aktionsdesigner an.

Prozedur

1. Navigieren zu **Alle** > **Anmeldeinformationen und Verbindungen** > **Aliasse für Verbindungen und Anmeldeinformationen**an.
2. Erstellen Sie einen Aliasdatensatz, oder wählen Sie einen aus.
3. Klicken Sie in der zugehörigen Liste „Verbindungsattribute“ auf **Neu**.
4. Legen Sie die Attributbezeichnung und den Feldtyp fest.
   Eine Liste der Feldtypen finden Sie unter Feldtypen .
5. Klicken Sie auf den zugehörigen Link „Erweiterte Ansicht“, um erweiterte Dictionary-Voreinstellungen für das Attribut festzulegen.
   Auf diese Weise lässt sich beispielsweise ein Attribut mit einem dynamisch berechneten Wert erstellen. Weitere Informationen finden Sie unter Formular „Wörterbucheintrag“. .
6. Klicken Sie auf **Absenden**.
7. Definieren Sie die Attributwerte im Verbindungsdatensatz.

   a. Navigieren zu **Anmeldeinformationen und Verbindungen** > **Verbindungen**an.

   b. Erstellen Sie einen Verbindungsdatensatz mit demselben Verbindungstyp wie der Alias, oder wählen Sie einen aus.

   c. Wählen Sie unter **Verbindungsalias** den Alias mit Verbindungsattributen aus.

   d. Speichern Sie den Datensatz.
   Die Registerkarte „Attribute“ wird mit den im Aliasdatensatz definierten Verbindungsattributen gefüllt.

   e. Legen Sie Werte für die Attribute fest.
   Wenn für den Alias **Unterstützt mehrere aktive Verbindungen** aktiviert ist, können Sie einem Alias mehrere Verbindungsdatensätze zuordnen und in jedem Verbindungsdatensatz Attributwerte definieren. Wenn mehrere Verbindungsdatensätze mit Attributwerten für denselben Alias vorhanden sind, Die bei der Ausführung des Ablaufs verwendete Verbindung bestimmt die Attributwerte. Angenommen, Sie haben eine Aktion, die einen Alias mit zwei aktiven Verbindungsendpunkten verwendet: Produktion und Test. Das Attribut wird nach dem Wert aufgelöst, der von der zur Laufzeit verwendeten Verbindung festgelegt wird.

8. Fügen Sie den Alias einem Integrationsschritt im Aktionsdesigner hinzu.
   a. Navigieren Sie zu Flow Designer, und erstellen oder wählen Sie eine Aktion.
   b. Fügen Sie der Aktion einen Integrationsschritt hinzu.
   c. Fügen Sie unter „Verbindungsdetails“ den Alias hinzu, für den Sie Attribute erstellt haben.

   Die mit dem Alias verknüpften Verbindungsattribute werden als Datenpillen im Datenbereich angezeigt.

   Hinweis: Das System verfolgt keinen Change an Bezeichnungen und Datentypen von Verbindungsattributen, nachdem Sie den Alias einem Schritt zugeordnet haben. Um die Bezeichnung oder den Datentyp eines Verbindungsattributs zu aktualisieren, löschen Sie den Alias aus dem Schritt, und fügen Sie ihn erneut hinzu.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erste Schritte mit Anmeldeinformationen

Der MID Server verwendet die Anmeldeinformationen, die Sie in der Tabelle „Anmeldeinformationen“ [discovery_credentials] erstellen, um auf Ressourcen für Discovery, Orchestration, Service Mapping und Cloud Management zuzugreifen.

Verwendung von Anmeldeinformationen durch MID Server

Standardmäßig verwenden Windows-MID Server die Anmeldeinformationen des MID Server-Service auf dem Hostcomputer, um Windows-Geräte im Netzwerk zu ermitteln. Sie sollten die Anmeldeinformationen für den Windows-MID-Server-Service so konfigurieren , dass sie mindestens über lokale Administratorrechte verfügen. Für die Computer und Netzwerkgeräte vom Typ Linux und UNIX verwendet der MID-Server die SSH- und SNMP-Anmeldeinformationen, die in der Instanz in konfiguriert sind **Discovery** > **Anmeldeinformationen**an.

Die MID-Server, die von Orchestration verwendet werden, müssen Zugriff auf die erforderlichen Anmeldeinformationen haben, um Befehle auf Computern im Netzwerk auszuführen, wie in den Workflow-Aktivitäten angegeben. Orchestration kann dieselben SSH- und SNMP-Anmeldeinformationen wie Discoveryverwenden, verfügt jedoch über zwei zusätzliche Anmeldeinformationen für bestimmte Workflow-Aktivitäten: Windows (für PowerShell-Aktivitäten) und VMware.

Verschlüsselung und Entschlüsselung

Die Plattform speichert die Anmeldeinformationen in einem verschlüsselten Feld in der Tabelle „Anmeldeinformationen“ [discovery_credentials]. Einmal eingegeben, können sie nicht angezeigt werden.

Wenn der MID-Server Anmeldeinformationen anfordert, entschlüsselt Now Platform die Anmeldeinformationen mit dem folgenden Prozess:

1. Die Anmeldeinformationen werden in der Instanz mit dem festen Schlüssel „password2“ entschlüsselt.
2. Die Anmeldeinformationen werden in der Instanz mit dem öffentlichen Schlüssel des MID Servers erneut verschlüsselt.
3. Die Anmeldeinformationen werden im Lastenausgleichsmodul mit SSL verschlüsselt.
4. Die Anmeldeinformationen werden auf dem MID Server mit SSL entschlüsselt.
5. Die Anmeldeinformationen werden auf dem MID Server mit dem privaten Schlüssel des MID Servers entschlüsselt.

Hinweis: Die Plattform verfügt nicht über separate Verschlüsselungsschlüssel für Instanzen mit mehreren Mandanten.

Reihenfolge der Anmeldeinformationen

Anmeldeinformationen kann ein Wert für die Reihenfolge im Anmeldeinformationsformular zugewiesen werden. Die Anwendung wird so gezwungen, alle verfügbaren Anmeldeinformationen in einer bestimmten Reihenfolge durchzugehen. Wenn Sie keinen Wert für die Reihenfolge angeben, versucht die Anwendung die Anmeldeinformationen in der Tabelle „Anmeldeinformationen“ [discovery_credential] nach dem Zufallsprinzip, bis sie einen geeigneten Wert findet. Beispiel:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Orchestration versucht, einen Befehl auf einem SSH-Server wie einem Linux- oder UNIX-Computer auszuführen.
- Discovery versucht, ein SNMP-Gerät wie einen Drucker, einen Router oder eine USV abzufragen.

Nach der Ermittlung der Anmeldeinformationen für ein Gerät erstellen Discovery und Orchestration anhand der Tabelle „Anmeldeinformationsaffinität“ `[dscy_credentials_affinity]` eine Affinität zwischen den Anmeldeinformationen und dem Gerät. Bei allen nachfolgenden Ermittlungen oder Orchestration-Aktivitäten wird versucht, die Anmeldeinformationen in dieser Tabelle einem Gerät zuzuordnen, für das eine Affinität besteht. Wenn sich die Anmeldeinformationen für ein Gerät ändern, testen Discovery und Orchestration alle verfügbaren Anmeldeinformationen erneut, bis sie eine neue Affinität herstellen.

Hinweis: Wenn Orchestration und Discovery installiert sind und der Anmeldeinformationsalias aktiviert ist, können mehrere Affinitäten vorhanden sein. In diesem Fall sucht die Plattform nach Anmeldeinformationen für jede Affinität und fügt die Anmeldeinformation für die Affinität mit der niedrigsten Reihenfolgenummer in die Probe ein.

Das Angeben einer Reihenfolge für die Anmeldeinformationen ist in den folgenden Situationen hilfreich:

- Die Tabelle „Anmeldeinformationen“ enthält viele Anmeldeinformationen, von denen einige häufiger als andere verwendet werden. Angenommen, die Tabelle enthält 150 SSH-Anmeldeinformationen, und fünf dieser Anmeldeinformationen werden für die Anmeldung bei 90 % der Geräte verwendet. Es empfiehlt sich, diese fünf Anmeldeinformationen mit niedrigen Reihenfolgenummern zu konfigurieren, durch die sie in der Ausführungsliste ganz oben platziert werden. Discovery und Orchestration arbeiten schneller, wenn sie diese allgemeinen Anmeldeinformationen zuerst testen. Nach der ersten erfolgreichen Verbindung weiß Now Platform, welche Anmeldeinformationen beim nächsten Mal für jedes Gerät verwendet werden sollen.
- Now Platform weist eine strenge Anmeldesicherheit auf. Konfigurieren Sie beispielsweise Datenbank-Anmeldeinformationen mit einem niedrigen Reihenfolgewert, wenn Solaris-Datenbankserver im Netzwerk nur nach drei fehlgeschlagenen Anmeldeversuchen den MID-Server sperren.

Anmeldeinformationsaliasse

Aliasse für Anmeldeinformationen sind für Discovery und Orchestrationverfügbar.

Mit Aliassen für Discovery kann ein Administrator:

- ein Filterverhalten für Anmeldeinformationen mit konfigurierbaren Compliance-Stufen einsetzen.
- mehrere Anmeldeinformationsaliase einem Discovery-Zeitplan zuweisen.
- Verhindern Sie die Erstellung von Anmeldeinformationsaffinitäten, die unangemessene oder vertrauliche Anmeldeinformationen verwenden. Weitere Informationen finden Sie unter Anmeldeinformationsaffinitäten.

Mit Aliassen für Orchestration können Workflow-Ersteller:

- jeder Aktivität in einem Orchestration-Workflow individuelle Anmeldeinformationen zuweisen
- jeder Aktion in Flow Designer individuelle Anmeldeinformationen zuweisen

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zuweisen.
- jedem Vorkommen derselben Aktion im Designer-Flow unterschiedliche Anmeldeinformationen zuweisen

Externe Anmeldeinformationsspeicher

Wenn Sie nicht möchten, dass Anmeldeinformationen in Ihrer Instanz gespeichert werden, können Sie externe Repositorien für Anmeldeinformationen verwenden. Externe Anmeldeinformationsspeicher speichern die Anmeldeinformationen an einem externen Standort, auf den Ihre Instanz zugreifen kann. CyberArk ist der einzige externe Anmeldeinformationsspeicher, der unterstützt wird. Andere externe Speicher können jedoch mithilfe der ServiceNow API konfiguriert werden.

Verbindungs- und Anmeldealias erstellen

Definieren Sie einen Alias, um einen Anmelde- oder einen Verbindungsdatensatz zu kennzeichnen.

Vorbereitungen

Erforderliche Rolle:

- Die Administratorrolle ist erforderlich, um einen Alias zu erstellen.
- Die Rollen „credential_admin“ und „connection_admin“ haben Lesezugriff auf den Aliasdatensatz.

Warum und wann dieser Vorgang ausgeführt wird

Der Verbindungs- und Anmeldealias definiert einen Alias, der einen Anmelde- oder einen Verbindungsdatensatz kennzeichnet. Der Alias enthält diese Felder.

Prozedur

1. Navigieren zu **Alle** > **Verbindungen und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular aus.

Aliasse für Verbindungen und Anmeldeinformationen

Feld	Beschreibung
Name	Name des Alias. Ein Alias darf nur Buchstaben, Ziffern und Unterstriche enthalten. Während eines Upgrades wird das Tag im Anmeldedatensatz zu einem Verbindungs- und Anmeldealias migriert. Wenn das Tag der Anmeldeinformationen andere Sonderzeichen als Buchstaben, Ziffern und Unterstriche enthält, wird der Tag-Name nach dem Upgrade beibehalten. Sie können diesen migrierten Alias weiterhin verwenden, Sie können ihn allerdings erst aktualisieren, wenn Sie den Namen den Namensbeschränkungen entsprechend ändern.
ID	Eindeutiger Bezeichner für den Alias für Verbindungen und Anmeldeinformationen, basierend auf dem Format `scope_name.alias_name`.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	◦ Bei „Global“ ist die ID der Aliasname. Wenn Sie beispielsweise einen Workday-Alias im globalen Bereich erstellen, wird die ID auf `workday festgelegt`. ◦ Wenn Sie einen Workday-Alias im Bereich der HR-App erstellen, wird die ID auf `x_hr_app.workday festgelegt`.
Typ	Wählen Sie entweder **Anmeldeinformationen** oder **Verbindung und Anmeldeinformationen aus**. Der Standardwert ist „Verbindung und Anmeldeinformationen“.
Anwendung	Anwendungsbereich, für den der Alias für Verbindungen und Anmeldeinformationen zugewiesen wird. Der aktuelle Sitzungsbereich, den Sie zuletzt in der Anwendungsauswahl ausgewählt haben, wird angezeigt. ◦ **Global** wird beispielsweise angezeigt, wenn dies der aktuelle Bereich für diese Sitzung ist. ◦ Sie können den Bereich in der Anwendungsauswahl ändern, bevor Sie einen Alias erstellen. Weitere Informationen zu Anwendungsbereichen und ihrer Auswahl finden Sie unter: ▪ Anwendungsbereich ▪ Anwendungen aus der Anwendungsauswahl auswählen
Verbindungstyp	Name des Verbindungstyps: entweder Basis, HTTP, JDBC, JMS oder Kafka. Der Standardwert ist HTTP.
Unterstützt mehrere aktive Verbindungen	Bezeichner, der angibt, ob der Alias mehrere aktive Verbindungen unterstützt. Fügen Sie mithilfe der Tabelle „Verbindungen“ Verbindungen hinzu, und verknüpfen Sie sie mithilfe der zugehörigen Liste „Verbindungen“ mit dem Alias.
Standard-Wiederholungsrichtlinie	Wiederholungsrichtlinie für den Alias. Weitere Informationen finden Sie unter Wiederholungsrichtlinie .
Konfigurationsvorlage	Konfigurationsvorlage, die zum Erstellen eines Verbindungs- und Anmeldeinformationsdatensatzes verwendet wird.

4. Klicken Sie auf **Speichern**.
Die zugehörige Liste Verbindungen und Verbindungsattribute wird angezeigt.

Zugehörige Liste	Beschreibung
Verbindungen	Zugehörige Verbindungsdatensätze, die diesem Alias zugeordnet sind. Nachdem Sie den Alias erstellt haben, können Sie Verbindungsdatensätze definieren und diese mit dem Alias verknüpfen. Wenn **Unterstützt mehrere aktive Verbindungen** ausgewählt ist, können Sie einem Alias mehrere Verbindungen zuordnen.
Verbindungsattribute	Attribute für die Verbindung. Definieren Sie für eine Verbindung spezifische Daten, und verwenden Sie sie in einem IntegrationHub-Integrationsschritt. Weitere Informationen finden Sie unter Verbindungsattribute für IntegrationHub erstellen.
Untergeordnete Aliasse	Dem übergeordneten Alias zugeordnete untergeordnete Aliasse. Nachdem Sie einen Alias für Verbindungen und

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Liste	Beschreibung
	Anmeldeinformationen erstellt haben, können Sie einen untergeordneten Alias erstellen, um mehrere Verbindungen für dieselbe Anwendungsintegration zu konfigurieren.

Zugehörige Liste	Beschreibung
Verbindungen	Zugehörige Verbindungsdatensätze, die diesem Alias zugeordnet sind. Nachdem Sie den Alias erstellt haben, können Sie Verbindungsdatensätze definieren und diese mit dem Alias verknüpfen. Wenn **Unterstützt mehrere aktive Verbindungen** ausgewählt ist, können Sie einem Alias mehrere Verbindungen zuordnen.
Verbindungsattribute	Attribute für die Verbindung. Definieren Sie für eine Verbindung spezifische Daten, und verwenden Sie sie in einem IntegrationHub-Integrationsschritt. Weitere Informationen finden Sie unter Verbindungsattribute für IntegrationHub erstellen.

5. Wahlweise: Wenn Sie neue Anmeldeinformationen und eine Verbindung erstellen möchten, die Ihrem Anmeldeinformationsalias zugeordnet sind, klicken Sie unter *Related Links*auf **Neue Verbindung und Anmeldeinformationen erstellen**.
   Die resultierenden Verbindungs- und Anmeldeinformationsdatensätze basieren auf einer vordefinierten Konfigurationsvorlage. Siehe Konfigurationsvorlagen für Verbindungen und Anmeldeinformationen.
6. Wahlweise: Wenn Sie einen untergeordneten Alias für Ihren Alias für Verbindungen und Anmeldeinformationen erstellen möchten, wählen Sie in der zugehörigen Liste **Untergeordnete AliasseNeu**.

   a. Geben Sie einen Namen für den untergeordneten Alias ein, und wählen Sie **Absenden**aus.
   Der untergeordnete Alias erbt Eigenschaften vom übergeordneten Alias. Anschließend können Sie einen untergeordneten Alias so konfigurieren, dass er eigene Verbindungs- und Anmeldeinformationen enthält.

Nächste Maßnahme

Erstellen Sie einen oder mehrere Verbindungsdatensätze, die dem Alias oder untergeordneten Aliassen zugeordnet werden sollen. Weitere Informationen zum Erstellen von Verbindungen finden Sie unter Erste Schritte mit Verbindungen. Fügen Sie dem Alias Verbindungsattribute hinzu, um Verbindungsmetadaten für Abläufe im Flow Designer verfügbar zu machen.

Richten Sie die OAuth-Integration über ein MID-Server

Erstellen Sie einen Verbindungsdatensatz, der das Senden einer OAuth-Tokenanforderung an einen Drittanbieterserver über MID-Serverermöglicht.

Vorbereitungen

Bestätigen Sie, dass Sie das ServiceNow IntegrationHub Standard Pack Installer-Abonnement abonniert haben. Weitere Informationen finden Sie unter https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/legal/snc-addendum-integrationhub.pdf .

Erforderliche Rolle: admin

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

Konfigurieren Sie die Verbindung mit einer Konfigurationsvorlage.

a. Navigieren zu **Alle** > **IntegrationHub** > **Konfigurationsvorlagen**an.

b. Wählen Sie **Neu**.

c. Wählen Sie **den Erteilungstyp „HTTP-Verbindung mit OAuth-Client-Anmeldeinformationen“ aus**.

d. Aktualisieren Sie das Formular nach Bedarf.
Sie können den Umfang beispielsweise in den Feldern `oauth_entity_profile_scope` und `oauth_entity_scope` im Abschnitt „Standarddatenvorlage“ angeben.
Informationen zum Erstellen einer -Konfigurationsvorlage finden Sie unter Erstellen Sie eine Konfigurationsvorlage.

e. Wählen Sie **Absenden**.
Sie haben die Konfigurationsvorlage erstellt.

f. Navigieren zu **Alle** > **IntegrationHub** > **Aliasse für Verbindungen und Anmeldeinformationen**an.

g. Aktualisieren Sie das Formular.

Alias für Verbindungen und Anmeldeinformationen

Feld	Beschreibung
Name	Name des Alias. Ein Alias darf nur Buchstaben, Ziffern und Unterstriche enthalten. Während eines Upgrades wird das Tag im Anmeldedatensatz zu einem Verbindungs- und Anmeldealias migriert. Wenn das Tag der Anmeldeinformationen andere Sonderzeichen als Buchstaben, Ziffern und Unterstriche enthält, wird der Tag-Name nach dem Upgrade beibehalten. Sie können diesen migrierten Alias weiterhin verwenden, Sie können ihn allerdings erst aktualisieren, wenn Sie den Namen den Namensbeschränkungen entsprechend ändern.
Anwendung	Eindeutiger Bezeichner für den Alias für Verbindungen und Anmeldeinformationen, basierend auf dem Format `scope_name.alias_name`.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	◦ Bei „Global“ ist die ID der Aliasname. Wenn Sie beispielsweise einen Workday-Alias im globalen Bereich erstellen, wird die ID auf `workday festgelegt`. ◦ Wenn Sie einen Workday-Alias im Bereich der HR-App erstellen, wird die ID auf `x_hr_app.workday festgelegt`.
Übergeordneter Alias	Option zum Auswählen des Alias, unter dem Sie diesen Alias für Verbindungen und Anmeldeinformationen erstellen. Der Alias für Verbindungen und Anmeldeinformationen, den Sie erstellen, ist ein untergeordneter Alias. Ein untergeordneter Alias wird unter der Registerkarte **Untergeordnete Aliase** auf der Seite des übergeordneten Alias für Verbindungen und Anmeldeinformationen angezeigt. 
Typ	Option zur Angabe des Typs des Alias, den Sie erstellen. Wählen Sie eine der folgenden Optionen aus: ◦ Anmeldeinformationen: Alias, der einen Anmeldeinformationsdatensatz enthält. ◦ Verbindungen und Anmeldeinformationen: Alias, der Verbindungs- und Anmeldeinformationsdatensatz enthält. Diese Option ist standardmäßig ausgewählt. Bestätigen Sie, dass Verbindung und Anmeldeinformationen ausgewählt sind.
Unterstützt mehrere aktive Verbindungen	Bezeichner, der angibt, ob der Alias mehrere aktive Verbindungen unterstützt. Fügen Sie mithilfe der Tabelle „Verbindungen“ Verbindungen hinzu, und verknüpfen Sie sie mithilfe der zugehörigen Liste „Verbindungen“ mit dem Alias.
Standard-Wiederholungsrichtlinie	Wiederholungsrichtlinie für den Alias. Weitere Informationen finden Sie unter Wiederholungsrichtlinie .
Konfigurationsvorlage	Option zum Auswählen der Konfigurationsvorlage, auf deren Grundlage Sie den Alias für Verbindungen und Anmeldeinformationen erstellen. Wählen Sie die Vorlage des

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Berechtigungstyps „ **HTTP-Verbindung mit OAuth-Client-Anmeldeinformationen**“ aus, die Sie erstellt haben.

h. Wählen Sie **Absenden**.
Sie haben den Datensatz des Alias für Verbindungen und Anmeldeinformationen erstellt.

i. Navigieren zu **Alle** > **IntegrationHub** > **Verbindungs-Dashboard**an.

j. Geben Sie im Feld Alle Verbindungen durchsuchen den Namen des von Ihnen erstellten Aliasdatensatzes für Verbindungen und Anmeldeinformationen ein.

k. Wählen Sie im Datensatz des Alias für Verbindungen und Anmeldeinformationen **Details anzeigen**aus.

l. Wählen Sie **Konfigurieren**.

m. Füllen Sie das Formular aus.

Verbindungsdatensatz

Feld	Beschreibung
Verbindungsname	Name des Verbindungsdatensatzes. Sie können den Namen nicht aktualisieren.
Verbindungs-URL	Option zum Bereitstellen der URL, die die Verbindung mit dem Drittpartei-Server herstellt.
MID verwenden	Option, um anzugeben, dass OAuth-Token-Anforderungen über einen MID-Server gesendet werden sollen. **Wichtig:** Bestätigen Sie, dass die Option ausgewählt ist.
MID-Auswahl	Option, um anzugeben, ob Sie einen bestimmten MID-Server verwenden, die automatische Auswahl des MID-Servers aktivieren oder einen MID-Cluster verwenden möchten. Wählen Sie eine der folgenden Optionen aus. ◦ MID-Server automatisch auswählen ◦ Spezifischer MID-Server ◦ Spezifischer MID-Server-Cluster
MID-Server	Option zum Auswählen eines MID-Servers.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Diese Option wird angezeigt, wenn Sie im Feld „MID-Auswahl“ die Option **Spezifischer MID-Server** auswählen.
MID-Cluster	Option zum Auswählen eines MID-Clusters. **Hinweis:** Diese Option wird angezeigt, wenn Sie im Feld „MID-Auswahl“ die Option „ **Spezifischer MID-Server-Cluster** “ auswählen.
OAuth-Client-ID	Option zum Angeben der Client-ID.
Geheimer OAuth-Schlüssel	Option zum Angeben des geheimen Clientschlüssels.
Verbindung mit Auth-Server über MID-Server herstellen	Option, um anzugeben, dass die Verbindung zwischen der ServiceNow-Instanz und dem Auth-Server über den MID-Server hergestellt wird. **Wichtig:** Bestätigen Sie, dass die Option ausgewählt ist.
OAuth-Token-URL	Option zum Angeben der OAuth-Token-URL, die zum Anfordern von OAuth-Token verwendet wird.

n. Wählen Sie **Konfigurieren und OAuth-Token abrufen aus**.
Der Verbindungs- und Anmeldeinformationsdatensatz wird erstellt.

Anmeldeinformationsaliasse für Discovery

Mit Anmeldeinformationsaliassen für Discovery kann ein Administrator bestimmte Anmeldeinformationen in Discovery-Zeitplänen verwenden. Sie können Verhaltensweisen für Ihre Aliasse konfigurieren, die bestimmen, wie strikt das System ihre Nutzung durchsetzt.

Ohne Anmeldeinformationsaliasse können Discovery-Zeitpläne auf alle Anmeldeinformationen zugreifen, die in der Instanz definiert sind. Dieses Verhalten ist unter bestimmten Umständen möglicherweise nicht wünschenswert, insbesondere für Anmeldeinformationen mit erhöhten Berechtigungen. Anmeldeinformationsaliasse bieten mehr Kontrolle darüber, welche Anmeldeinformationen ein Discovery-Zeitplan verwenden darf, und verhindern, dass Anmeldeinformationen mit erhöhten Rechten unnötigerweise offengelegt werden.

Funktionsweise von Anmeldeinformationsaliassen

Wird ein Datensatz in die ECC-Warteschlange eingefügt, wird die Geschäftsregel „ *Discovery-Affinität und Anmeldeinformationen einfügen* “ (zuvor „ *Discovery-Affinität*einfügen“ genannt) ausgeführt. Die Geschäftsregel hängt die Anmeldeinformationsaliasse, die im Discovery-Zeitplan definiert werden, an die Probe an, damit der MID Server Anmeldeinformationen filtern kann. Die erste Aufgabe des MID Servers besteht darin, die Liste der Anmeldeinformationen für die Suche zu erstellen. Filtert die Anmeldeinformationen nach

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Affinität und dann nach Tags, falls vorhanden. Die Affinitäten werden an das obere Ende der Liste und die entsprechenden Tags an das untere Ende der Liste gesetzt. Der MID Server geht immer wieder die Liste durch, bis er funktionierende Anmeldeinformationen findet. Dann erstellt der MID Server eine Affinität für diese Anmeldeinformationen.

Hinweis: Anmeldeinformationen müssen mit allen Anmeldeinformations-Tags übereinstimmen.

Wenn mit der Geschäftsregel festgestellt wird, dass eine Affinität für das Gerät vorhanden ist, wird anhand der Regel die richtige *credential_id* identifiziert, die zu verwenden ist. Dies ist die *sys_id* des Datensatzes in der Tabelle „Anmeldeinformationen“ `[discovery_credentials]`. Wenn die Plattform auf eine Affinität mit einem Aliaswert für Anmeldeinformationen stößt, der in der Geschäftsregel als *credential_alias* definiert ist, ermittelt die Geschäftsregel, ob die von der Affinität referenzierten Anmeldeinformationen den angegebenen Alias aufweisen. Ist dies der Fall, wählt die Geschäftsregel die „ *credential_id*“ des Alias aus und übergibt diesen Wert an den MID Server. Wenn die Anmeldeinformationen nicht über den angegebenen Anmeldeinformationsalias verfügen, werden alle anderen für das Zielsystem vorhandenen Affinitäten geprüft.

Discovery-Anmeldeinformationsalias erstellen

Erstellen Sie den Alias, und fügen Sie diesen Alias dann den Anmeldeinformationen im Anmeldeinformationsdatensatz hinzu. Sie können Anmeldeinformationen mehreren Aliassen und mehrere Anmeldeinformationen einem einzelnen Alias hinzufügen.

Vorbereitungen

Erforderliche Rolle: admin, credential_admin (nur Lesezugriff), connection_admin (nur Lesezugriff)

Warum und wann dieser Vorgang ausgeführt wird

Ein Discovery-Zeitplan verwendet nur Anmeldeinformationen, die in den für den betreffenden Zeitplan definierten Aliassen enthalten sind.

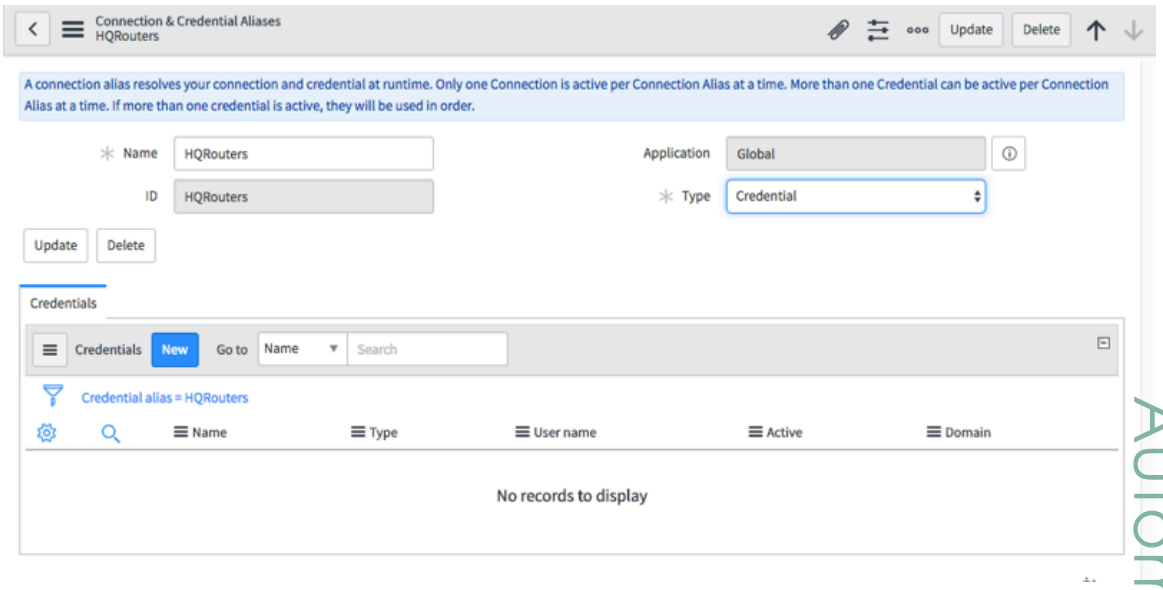
Hinweis: Wenn ein Alias für Anmeldeinformationen für einen Zeitplan definiert ist, ignoriert er alle zuvor vorhandenen Anmeldeinformationsaffinitäten zwischen den Anmeldeinformationen und dem Ziel, die in einem Zeitplan erkannt werden, der für die Verwendung dieses Alias für Anmeldeinformationen eingerichtet ist.

Prozedur

1. Erstellen Sie einen Alias.
   a. Navigieren zu **Verbindungen und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen**an.
   b. Klicken Sie auf **Neu**.
   c. Geben Sie einen eindeutigen Namen für den Alias ein, und wählen Sie **Anmeldeinformationen** für den **Aliastyp**aus.
   d. Klicken Sie auf **Absenden**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die zugehörige Liste „ **Anmeldeinformationen** “ wird angezeigt. Sie können für diesen Alias in dieser Liste neue Anmeldeinformationen hinzufügen, nicht jedoch bestehende Anmeldeinformationen.

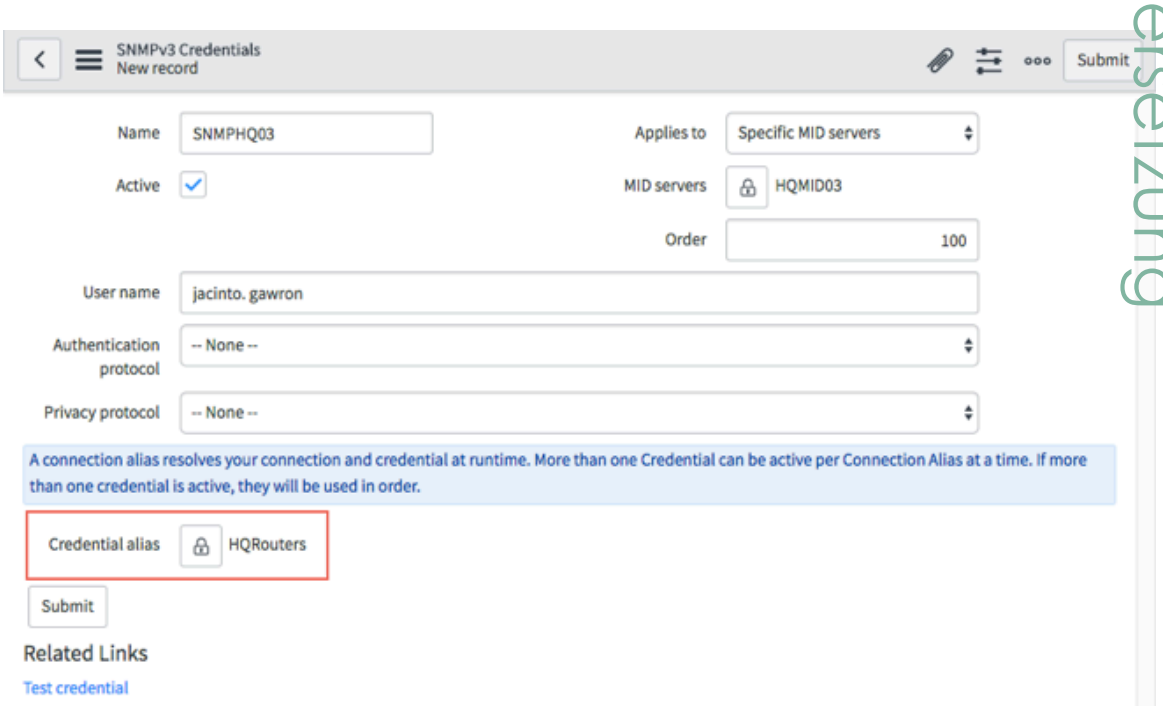


2. Konfigurieren Sie Anmeldeinformationen für den neuen Alias.

a. Navigieren zu **Verbindungen und Anmeldeinformationen** > **Anmeldeinformationen**an.

b. Wählen Sie vorhandene Anmeldeinformationen aus der Liste aus, oder klicken Sie auf **Neu**, um neue Anmeldeinformationen zu erstellen.

c. Entsperren Sie im **Anmeldeinformationsdatensatz** das Feld Anmeldeinformationsalias, und wählen Sie den von Ihnen erstellten Alias aus.

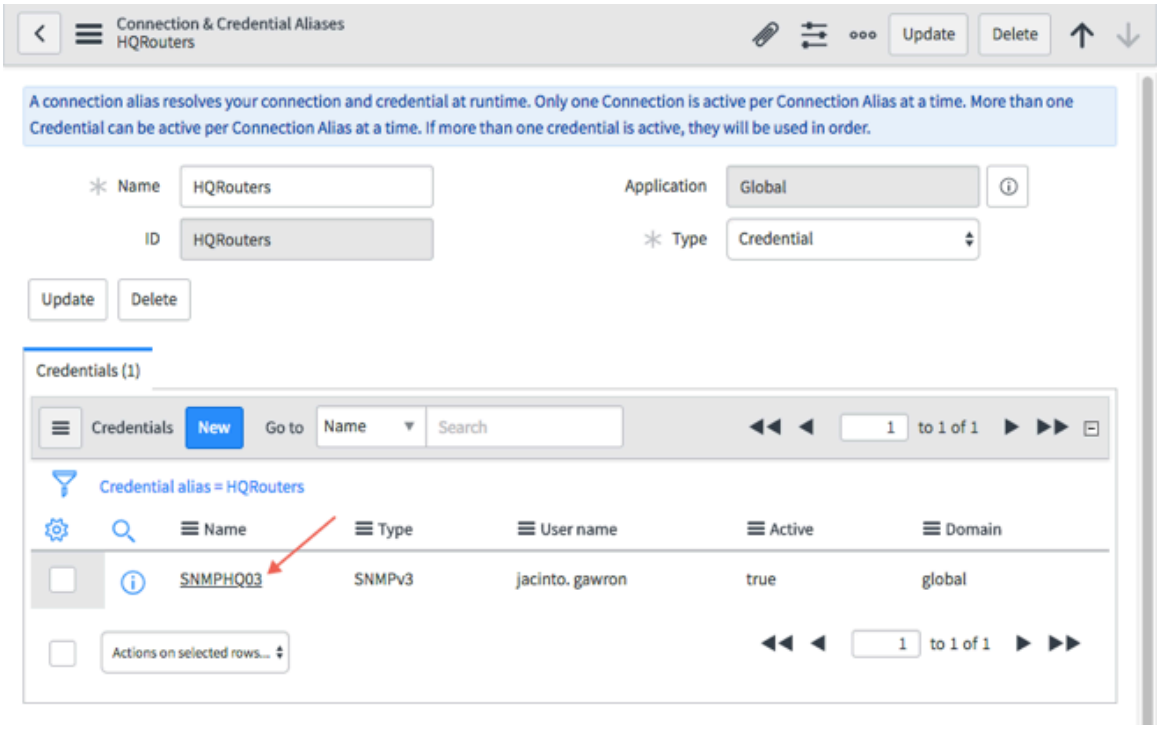


d. Speichern Sie den Datensatz, oder senden Sie ihn ab.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Zurück zu **Verbindungen und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen** und öffnen Sie Ihren neuen Alias.
   Die Anmeldeinformationen, die Sie an den Alias angehängt haben, werden jetzt in der zugehörigen Liste angezeigt.



4. Um zusätzliche Anmeldeinformationen für diesen Alias zu erstellen, klicken Sie in der zugehörigen Liste auf **Neu**, und wählen Sie einen Anmeldeinformationstyp aus.
   Der Aliasname ist im Feld Anmeldeinformationsalias des Anmeldeinformationsdatensatzes vorab **ausgefüllt**.
5. Füllen Sie die Felder im Formular aus, und senden Sie den Datensatz.

Aliasse für Anmeldeinformationen für Orchestration-Aktivitäten

Der Anmeldeinformationsalias ermöglicht einem Administrator mehr Kontrolle über die in Orchestration-Aktivitäten verwendeten Anmeldeinformationen.

Dies ist nützlich, wenn eine Aktivität zur Ausführung einer Aufgabe bestimmte Anmeldeinformationen benötigt. Sie können ein Anmeldeinformations-Tag verwenden, um bestimmten Aktivitäten in einem Orchestration-Workflow einzelne Anmeldeinformationen zuzuweisen, oder jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zuzuweisen.

Der Alias für Anmeldeinformationen interagiert mit der Anmeldeinformationsaffinität, um zu bestimmen, welche Anmeldeinformationen für eine Orchestration-Aktivität verwendet werden sollen.

Funktionsweise des Anmeldeinformationsalias

Eine Geschäftsregel namens „ *Discovery-Affinität* einfügen“ (im Genfer Release von „Berechtigungsnachweis-Affinität einfügen“ umbenannt) wird ausgeführt, wenn ein Datensatz in die ECC-Warteschlange eingefügt wird. Diese Regel bestimmt, ob eine Berechtigungsaffinität für das Gerät besteht, und identifiziert die richtige, zu verwendende *credential_id* (die *sys_id* des Datensatzes in der Tabelle „Anmeldeinformationen“

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

[discovery_credentials]). Wenn die Plattform auf eine Affinität mit einem definierten Aliaswert für Anmeldeinformationen (*credential_alias* in der Geschäftsregel) stößt, ermittelt die Geschäftsregel, ob die von der Affinität referenzierten Anmeldeinformationen den angegebenen Alias haben. Wenn dies der Fall ist, wählt die Geschäftsregel die *credential_id* des Anmeldeinformationsalias aus und übergibt diesen Wert an den MID Server. Wenn der Anmeldeinformationen nicht über den angegebenen Anmeldeinformationsalias verfügen, werden alle anderen für das Zielsystem vorhandenen Affinitäten geprüft. Wenn keine Affinität auf entsprechend gekennzeichnete Anmeldeinformationen verweist, durchläuft der MID Server die Tabelle „Anmeldeinformationen" *[discovery_credentials]* und wählt die Anmeldeinformationen mit dem entsprechenden Tag aus. Der MID Server erstellt dann eine neue Affinität für diese Anmeldeinformationen.

Anmeldeinformationen erstellen und testen

Erstellen und testen Sie die Anmeldeinformationen, die Discovery, Service Mapping, Cloud Management und Orchestration für den Zugriff auf Hardware und Software in Ihrem Netzwerk benötigen.

Vorbereitungen

Erforderliche Rolle: admin
Überprüfen Sie Ihre Sicherheitsrichtlinie und Optionen mit dem Sicherheitsteam Ihrer Organisation.

Warum und wann dieser Vorgang ausgeführt wird

Diese Aufgabe enthält allgemeine Verfahren zum Erstellen von Anmeldeinformationen. Weitere Informationen zu bestimmten Feldern und Anforderungen finden Sie in der Dokumentation zu Ihrem Anmeldeinformationstyp.

Unterstützte Anmeldeinformationstypen

Applicative-Anmeldeinformationen	Virtual Server Interface	Chef-Server-Anmeldeinformationen
CIM-Anmeldeinformationen	Cloud-Anmeldeinformationen	Infoblox-Anmeldeinformationen
JDBC-Anmeldeinformationen	JMS-Anmeldeinformationen	OAuth 2.0-Anmeldeinformationen
SAP-Anmeldeinformationen	SNMP-Anmeldeinformationen	SSH-Anmeldeinformationen
VMware-Anmeldeinformationen	Windows-Anmeldeinformationen	Anmeldeinformationen für das Container-Image-Repository

Hinweis: Beschränken Sie zur Verbesserung der Sicherheit den Bereich der Anmeldeinformationen auf einen bestimmten MID-Server oder Zeitplan, um unnötige Anmeldeinformationen zu vermeiden.

Prozedur

1. Navigieren Sie zu einem dieser Module:
   - **Discovery** > **Berechtigungen**
   - **Service Mapping** > **Berechtigungen**
   - **Orchestration** > **Anmeldeinformationen**
2. Klicken Sie auf **Neu**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf der Seite „Berechtigungen“ auf einen Link für den Anmeldeinformationstyp, und füllen Sie das Formular aus.

   Weitere Informationen finden Sie in der Dokumentation zum ausgewählten Anmeldeinformationstyp.

   Sie können einen Anmeldeinformationsdatensatz zuerst absenden und dann später testen oder die Anmeldeinformationen unmittelbar vor dem Speichern testen.

   Das Testen der Anmeldeinformationen wird für folgende Anmeldeinformationstypen unterstützt:

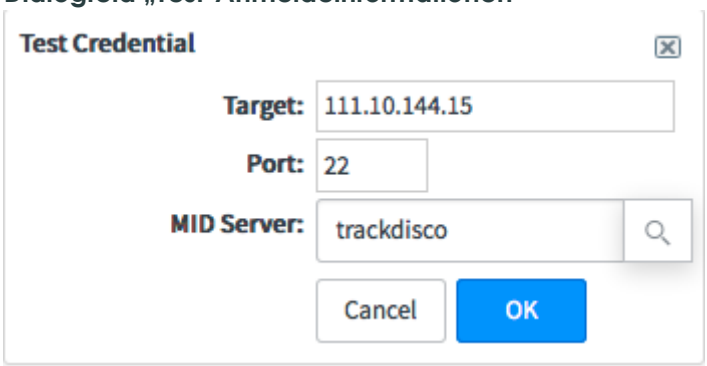
   - Private SSH-Schlüssel
   - Windows
   - SNMP v3
   - VMware
   - JDBC
   - JMS

4. Klicken Sie unter **Zugehörige Links** auf **Test-Anmeldedaten**.

   Hinweis: Die Anmeldeinformationen sind während des Tests stets verschlüsselt.

5. Füllen Sie die Felder im Dialogfeld „Test-Anmeldeinformationen“ aus.

Dialogfeld „Test-Anmeldeinformationen“



Felder im Dialogfeld „Test-Anmeldeinformationen“

Feld	Beschreibung	Anmeldeinformationstyp
Ziel	Zielhost, auf dem diese Anmeldeinformationen ausgeführt werden. Dieser Wert muss für alle Anmeldeinformationstypen eine IP-Adresse sein, mit Ausnahme von VMware, für das die Host-URL angegeben werden kann. Sie können keine MID-Server als Ziel festlegen.	Alle

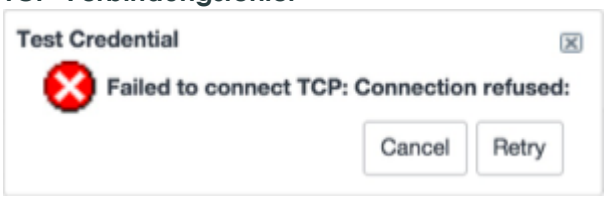
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung	Anmeldeinformationstyp
	Hinweis: Bei JMS ist dies die Provider-URL. Die Informationen in dieser URL teilen JNDI mit, wie der JMS-Provider gefunden und darauf zugegriffen werden kann. Ein Beispielwert für die Verbindung zu ActiveMQ V5.1 ist `tcp://ipAdresseOderHostname:61616`.	
Port	Port des Ziels, der für diesen Test verwendet werden soll. Das System füllt dieses Feld vorab mit dem Standardport für den ausgewählten Anmeldeinformationstyp aus.	Alle
MID Server	Für diesen Test zu verwendender MID Server. Sie müssen einen Windows-MID-Server verwenden, um die Windows-Anmeldeinformationen zu testen. Nur MID-Server, die **In Betrieb** und **Überprüft** sind, stehen zur Verfügung.	Alle
DB-Typ	Typ der Datenbank, für die diese Anmeldeinformationen getestet werden sollen.	JDBC
DB-Name	Name der Datenbank, für die diese Anmeldeinformationen getestet werden sollen.	JDBC
Ursprüngliche Kontext-Werkseinstellung	Name der JNDI-Klasse, die zum Erstellen des InitialContext verwendet wird. Bei Verwendung dieser **Ursprünglichen Kontext-Werkeinstellung** werden verschiedene JMS-Objekte, z. B. JMS-Verbindung, erstellt. Wenn Sie beispielsweise eine Verbindung zu ActiveMQ V5.10 (JMS-Provider) herstellen möchten, lautet der Wert in diesem Feld `org.apache.activemq.jndi.ActiveMQInitialContextFactory`	JMS

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

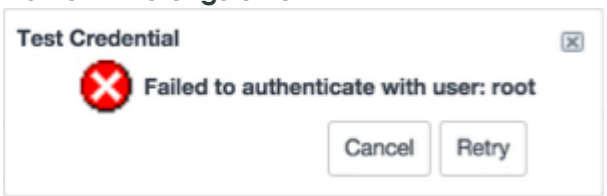
6. Klicken Sie auf **OK**, um den Test zu beginnen.
   Ein Indikator zeigt an, dass das System versucht, das Ziel mit den von Ihnen angegebenen Anmeldeinformationen zu kontaktieren. Wenn die Instanz eine Verbindung zum Ziel herstellt, wird eine Erfolgsmeldung angezeigt. Wenn die Instanz bei den von Ihnen angegebenen Testeingaben auf ein Problem stößt, wird die entsprechende Fehlermeldung angezeigt. Nachfolgend finden Sie einige häufige Fehlermeldungen.
   - Falsches Ziel oder falsche Portnummer:

     TCP-Verbindungsfehler

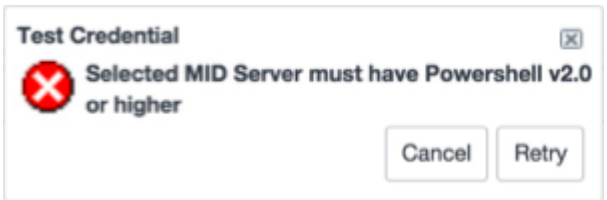
   - Falscher Benutzername oder falsches Passwort:

     Authentifizierungsfehler

   - Falscher MID Server für Windows-Anmeldeinformationen:

     MID Server-Fehler

7. Klicken Sie auf **Neuversuch**, um das Dialogfeld „Test-Anmeldedaten“ zu öffnen und den Eingabefehler zu korrigieren.
8. Wenn der Test der Anmeldeinformationen erfolgreich ist, klicken Sie auf **Absenden**, um den Datensatz zu speichern.

> **Wichtig:** Durch das Testen der Anmeldeinformationen kann nicht sichergestellt werden, dass die Anmeldeinformationen über die erforderlichen Berechtigungen für die beabsichtigten Discovery- oder Orchestration-Workflow-Aufgaben verfügen.

Ansible Tower-Anmeldeinformationen

Ansible Tower-Anmeldeinformationen werden für den Zugriff auf den Account zur Ansible-Konfigurationsverwaltung benötigt. Verwenden Sie diese Anmeldeinformationen zum Verwalten von Ansible-Ressourcen über die Cloud-Management-Anwendung.

Zur Integration von Cloud Provisioning and Governance mit dem Ansible-Konfigurationsverwaltungskonto müssen Benutzername und Passwort für das Administratorkonto in Ansible konfiguriert werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formularfelder für Ansible Tower-Anmeldeinformationen

Feld	Beschreibung
Name	Geben Sie einen beschreibenden Namen an.
Benutzername/ Passwort	Geben Sie die Authentifizierungsinformationen für den Ansible Tower-Benutzer mit Administratorrechten ein.

Hinweis: Sie müssen keine anderen Felder konfigurieren

Anmeldeinformationen für API-Keys

Ein API-Key ist ein eindeutiger Code, der an eine API übergeben wird, um die aufrufende Anwendung oder den aufrufenden Benutzer zu identifizieren.

Anmeldeinformationen für API-Keys

Formularfelder für Anmeldeinformationen für API-Keys

Feld	Eingabewert
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
API Key	Geben Sie den API Key ein.
Anmeldeinformationsalias	Lassen Sie zu, dass Ersteller von Flows und Workflows, jeder Aktivität in einem Flow oder Workflow einzelne Anmeldeinformationen zuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Flow oder Workflow unterschiedliche Anmeldeinformationen zu.
Gilt für	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für **Spezielle MID-Server** angewendet werden sollen. MID Servers angeben, der diese Anmeldeinformationen im Feld „ **MID-Server** “ verwenden soll.
Reihenfolge	Reihenfolge (Reihenfolge), in der Discovery diese Anmeldeinformationen bei dem Versuch, sich bei Geräten anzumelden, ausprobiert. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.

Applicative-Anmeldeinformationen

Einige Anwendungen erfordern zusätzlich zu den vom Host-Computer benötigten weitere Anmeldeinformationen. Anmeldeinformationen, die für den Zugriff auf diese Anwendungen erforderlich sind, werden als Applicative-Anmeldeinformationen bezeichnet.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typische Anmeldeinformationen enthalten einen Anwendernamen und ein Passwort für die Anmeldung bei einem Gerät oder einer Anwendung. Während die meisten Anwendungen nur einen Berechtigungsnachweis für den Zugriff auf sie benötigen, verfügen Hosts und Anwendungen manchmal über separate Anmeldeinformationen für zusätzliche Sicherheit. Beispielsweise benötigen ABAP SAP Central Services (ASCS) zusätzlich zu den SSH- oder Windows-Host-Anmeldeinformationen für den Server, auf dem ASCS gehostet wird, Applicative-Anmeldeinformationen.

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

Wie bei den Host-Anmeldeinformationen weisen Sie MID ServersApplicative-Anmeldeinformationen zu.

Sie erstellen Applicative-Anmeldeinformationen pro CI-Typ. Der CI-Typ für ASCS ist beispielsweise SAP ASCS Application [cmdb_ci_appl_sap_ascs]. Das vorkonfigurierte Muster zum Erkennen von CIs, die zu diesem CI-Typ gehören, enthält Befehle, für die von MID-Server die Verwendung des anwendbaren Berechtigungsnachweises für diesen CI-Typ erfordern. Wenn für diesen CI-Typ mehrere Anmeldeinformationen konfiguriert sind, versucht MID-Server, diese Anmeldeinformationen in der von Ihnen definierten Reihenfolge zu verwenden, bis die passenden Anmeldeinformationen gefunden wurden.

Überprüfen Sie die Informationen zu den Discovery-Anforderungen in der ServiceNow-Dokumentation, um festzustellen, ob Sie Applicative-Anmeldeinformationen für bestimmte Anwendungs-CIs konfigurieren müssen. Es ist nicht erforderlich, Applicative-Anmeldeinformationen zu konfigurieren, wenn dies in den Voraussetzungen für Discovery nicht erwähnt wird.

Felder für Applicative-Anmeldeinformationen

Feld	Beschreibung
Name	Name des Berechtigungsnachweises Verwenden Sie einen beschreibenden Namen wie Oracle DB oder London Oracle DB (für eine Oracle-Datenbank). Verwenden Sie keine Leerzeichen oder Sonderzeichen für den Anmeldeinformationsnamen.
Aktiv	Aktivieren Sie das Kontrollkästchen, um den Berechtigungsnachweis zu verwenden.
Benutzername	Geben Sie den tatsächlichen Benutzernamen des Antragsnachweises ein.
Passwort	Geben Sie das tatsächliche Passwort des Antragsnachweises ein. Verwenden Sie keine Leerzeichen oder Sonderzeichen für den Anmeldeinformationsnamen.
CI-Typ	Wählen Sie einen CI-Typ aus, zu dem das CI gehört.
Anmeldeinformationsalias	Erstellen Sie einen Alias, um bestimmten Discovery-Zeitplänen bestimmte Anmeldeinformationen zuzuweisen. Bei der Zuweisung eines Alias müssen Sie den Tabellennamen für den CI-Typ identifizieren, dessen Applicative-Anmeldeinformationen von der Anwendung verwendet werden. Von Anwendungen können Applicative-Anmeldeinformationen eines CI-Typs verwendet werden, der sich von ihrem eigenen unterscheidet. Informationen zu einer bestimmten Anwendung finden Sie in der entsprechenden Tabelle aus der Liste:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder für Applicative-Anmeldeinformationen (Fortsetzung)

Feld	Beschreibung
	• ABAP SAP Central Services (ASCS): cmdb_ci_appl_sap_ascs • IBM Security Access Manager-Appliance: cmdb_ci_app_server_webseal • SAP Central-Instanz: cmdb_ci_appl_sap_ascs • SAP Central Services (SCS): cmdb_ci_appl_sap_ascs • SAP Evaluated Receipt Settlement (ERS): cmdb_ci_appl_sap_ascs • SAP Java-Cluster: cmdb_ci_appl_sap_ascs • SAP NetWeaver Dialog Instance: cmdb_ci_appl_sap_ascs • Microsoft Exchange Mailbox (für Microsoft Exchange): cmdb_ci_exchange_mailbox • Microsoft SQL-Datenbank: cmdb_ci_db_mssql_instance • MySQL Server: cmdb_ci_db_mysql_instance • Oracle Advanced Queue-Warteschlange: cmdb_ci_db_ora_instance • Oracle-Datenbank: cmdb_ci_db_ora_instance • Oracle E-Business Suite: cmdb_ci_db_ora_instance • Oracle WebLogic-Modul: cmdb_ci_app_server_weblogic • Tibco Enterprise Message Service (EMS): cmdb_ci_appl_tibco_message
Gilt für	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für **Spezielle MID-Server** angewendet werden sollen. MID Servers angeben, der diese Anmeldeinformationen im Feld „ **MID-Server** “ verwenden soll.
Reihenfolge	Reihenfolge (Reihenfolge), in der Discovery diese Anmeldeinformationen bei dem Versuch, sich bei Geräten anzumelden, ausprobiert. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.

Virtual Server Interface

Der Anmeldeinformationstyp für die Standardauthentifizierung verwaltet den Zugriff zum Speichern von Anmeldeinformationen für die Standardauthentifizierung.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Felder stehen im Formular „Anmeldeinformationen“ für die Standardauthentifizierung zur Verfügung.

Anmeldeinformationsformular für die Standardauthentifizierung

Feld	Eingabewert
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein. Zum Beispiel könnten Sie sie **Standardauthentifizierung** nennen.
Benutzername	Geben Sie den Benutzernamen ein.
Passwort	Geben Sie das Passwort ein.
Nachweis-ID	Geben Sie den eindeutigen Schlüssel ein, der für diese Anmeldeinformationen im externen CyberArk-Anmeldeinformationsspeichersystem konfiguriert wurde. Die Nachweis-ID kann als Safe-Überschreibung verwendet werden, wenn mehrere Safes verwendet werden. Standardmäßig lautet die Syntax im Feld „ **Anmeldeinformations-ID** *<safe name>:<Credential ID>*“ . Wenn der Safe-Name weggelassen wird, muss ein Safe-Name in der Datei `config.xml` definiert sein. Um das Trennzeichen vom Standard-Doppelpunkt in ein anderes Zeichen zu ändern, überschreiben Sie den Wert mit dem optionalen Parameter *ext.cred.safe_name*. Das Feld **Nachweis-ID** darf maximal 40 Zeichen lang sein. Dieses Feld ist nur sichtbar, wenn das Kontrollkästchen **Externer Anmeldeinformationsspeicher** aktiviert ist.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn Sie diese Option auswählen, werden die Felder **Benutzername** und **Passwort** durch das Feld **Nachweis-ID** ersetzt. Derzeit ist CyberArk das einzige unterstützte externe Speichersystem.
Reihenfolge	Reihenfolge (Reihenfolge), in der Discovery diese Anmeldeinformationen bei dem Versuch, sich bei Geräten anzumelden, ausprobiert. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.

Chef-Server-Anmeldeinformationen

Chef-Server-Anmeldeinformationen greifen auf Chef-Integrationen mit der Instanz zu.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Felder sind im Formular „Anmeldeinformationen“ für Anmeldeinformationen des Typs „Chef-Server“ verfügbar. Diese Informationen stammen aus den Einstellungen, die Sie bei der Durchführung der Chef-Server-Installation konfiguriert haben.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Administratorname	Geben Sie den Administratornamen an, den Sie während der Chef-Server-Installation erstellt haben.
Administratorschlüssel	Geben Sie den privaten RSA-Schlüssel ein, den der Chef-Server beim Erstellen des Administrators generiert hat.
Validierungsname	Geben Sie den Namen des Prüfers ein.
Bestätigungsschlüssel	Geben Sie den privaten RSA-Schlüssel ein, den der Chef-Server beim Erstellen einer Organisation generiert hat.
Zertifikatname	Geben Sie den Zertifizierungsnamen ein.
Zertifikatschlüssel	Geben Sie den Zertifizierungsschlüssel ein.

CIM-Anmeldeinformationen

Der CIM-Berechtigungstyp verwaltet den Zugriff auf einen CIM-Server (auch als CIMOM - Common Information Model Object Manager bezeichnet), um Informationen zu VMware ESX-Servern zu erhalten. Dieser Anmeldeinformationstyp ist für Discovery verfügbar.

Diese Felder sind im Anmeldeinformationsformular für CIM verfügbar.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Benutzername	Geben Sie den zu erstellenden Benutzernamen in die Tabelle „Berechtigungsnachweise“ ein. Vermeiden Sie führende oder nachgestellte Leerzeichen in Benutzernamen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachgestellte Leerzeichen im Benutzernamen erkennt. Für die CIM-Erkennung muss der Benutzer über die Administratorrolle verfügen.
Passwort	Geben Sie das Passwort ein.
Nachweis-ID	Geben Sie den für externe Anmeldeinformationen konfigurierten eindeutigen Schlüssel in der JAR-Datei ein, die für ein externes Anmeldeinformationssystem auf den MID Server hochgeladen wurde. Das Feld **Nachweis-ID** darf maximal 40 Zeichen lang sein.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Dieses Feld ist nur sichtbar, wenn das Kontrollkästchen **Externer Anmeldeinformationsspeicher** aktiviert ist.
Alias für Anmeldeinformationen	Erlauben Sie Workflow-Erstellern, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuzuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu. Geben Sie den Tabellennamen für den CI-Typ ein, zu dem das CI gehört (z. B. cmdb_ci_apache_web_server), um die Anmeldeinformationen zur Erkennung von CIs zu verwenden, die nicht zu diesem CI-Typ gehören und dafür Service Mapping- und Discovery-Muster nutzen.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn Sie diese Option auswählen, werden die Felder **Benutzername** und **Passwort** durch das Feld **Nachweis-ID** ersetzt. Externe Anmeldeinformationsspeicher stehen nur zur Verfügung, wenn dasPlugin „Externer Anmeldeinformationsspeicher“ aktiviert ist. **Hinweis:** Derzeit ist CyberArk das einzige unterstützte externe Speichersystem.
Betrifft	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für **Spezielle MID-Server** angewendet werden sollen. MID Servers angeben, der diese Anmeldeinformationen im Feld „ **MID-Server** “ verwenden soll.
MID Server verwenden	Wählen Sie einen oder mehrere MID Server aus der Liste der verfügbaren MID Server aus. Die in diesem Datensatz konfigurierten Anmeldeinformationen stehen den MID Servern in dieser Liste zur Verfügung. Dieses Feld ist nur verfügbar, wenn Sie **Spezifische MID-Server** im Feld **Gilt für** auswählen. **Hinweis:** Die Auswahl von Spezifischen **Spezifischen MID-Servern** hat keine Auswirkungen auf die Auswahl der MID-Server. Es wird nur verwendet, um zu entscheiden, welche MID-Server für die Anmeldeinformationen sichtbar sein sollen. **Bestimmte MID-Server** werden in Orchestration-Aktivitäten nicht unterstützt.
Bestellung	Reihenfolge (Reihenfolge), in der Discovery diese Anmeldeinformationen bei dem Versuch, sich bei Geräten anzumelden, ausprobiert. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.
Windows-MID-Server-Servicekonto	Wenn sie aktiv sind, stellen die definierten Anmeldeinformationen das MID-Server-Servicekonto dar.

NetApp-Speichergeräte für CIM-Anmeldeinformationen konfigurieren

NetApp-Speichergeräte erfordern eine zusätzliche Konfiguration, damit Discovery sie erkennt.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Installieren Sie den SMI-S-Agenten auf dem Speichergerät-Host.

   Beachten Sie hinsichtlich Anweisungen und Anforderungen den Data ONTAP SMI-S Agent 5.2 Installation and Configuration Guide .

   Hinweis:

   ServiceNow verwaltet die Dokumentation auf dieser Website nicht. Dieses Dokument kann sich ohne vorherige Ankündigung ändern.

2. Erstellen Sie einen Benutzer-Account und ein Passwort für den SMI-S-Agenten.
3. Erstellen Sie einen Anmeldeinformationsdatensatz für die SMI-S-Agentenanmeldeinformationen.
   Legen Sie den Anmeldeinformationstyp auf **CIM** fest.

Cloud-Anmeldeinformationen

Cloud-Anmeldeinformationstypen verwalten den Zugriff auf cloudbasierte Anwendungen, einschließlich Amazon Web Services und der Microsoft Azure Cloud.

AWS Identity and Access Management-Rollen (IAM).

Wenn Sie einen MID-Server auf Amazon EC2 in einer AWS-Cloud installiert haben und dieser MID-Server für die Erkennung von Ressourcen in der Cloud konfiguriert ist, können Sie anstelle von in verwalteten Anmeldeinformationen Sicherheitsanmeldeinformationen verwenden, die von AWS Identity and Access Management-Rollen (IAM) bereitgestellt werden Ihre Instanz. Diese AWS-Anmeldeinformationen gewähren über ein Instanzprofilbasierend auf Rollen Berechtigungen in der Cloud. Diese Anmeldeinformationen sind vorübergehend und rotieren automatisch in konfigurierbaren Intervallen. Wenn auf dem MID-Server eine IAM-Rolle definiert ist. Einzelheiten finden Sie unter MID-Server für AWS IAM-Rollen konfigurieren .

Discovery ignoriert alle in der Instanz gespeicherten Anmeldeinformationen und verwendet stattdessen die von der Rolle im Instanzprofil gewährten Anmeldeinformationen. Weitere Informationen zu AWS-Instanzprofilen finden Sie unter IAM-Rollen für Amazon EC2 .

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AWS-Anmeldeinformationen

Formularfelder mit AWS-Anmeldeinformationen

Feld	Eingabewert
Name	Eindeutiger und beschreibender Name für die AWS-Anmeldeinformationen.
Aktiv	Option zur Verwendung dieser Anmeldeinformationen.
Zugangsschlüssel-ID	Die **Zugriffsschlüssel-ID**, die Sie in der AWS-Verwaltungskonsole generiert haben, z. B: APIAIOSFODNN7BEISPIEL.
Geheimer Zugangsschlüssel	Der **geheime Zugriffsschlüssel**, den Sie in der AWS-Verwaltungskonsole generiert haben, z. B.: wPalrXUtnFEMI/K7MDENG/bPxRfiCYBEISPIELSCHLÜSSEL.

Anmeldeinformationsfelder für den Azure-Service-Prinzipal

Feld	Wert
Name	Geben Sie den Namen des Service Principals ein, der bei der Instanz registriert werden soll.
Tenant-ID und	Fügen Sie den Wert der Azure-**Verzeichnis-ID** aus dem Azure-Portal in das Feld Cloud-Management **Tenant-ID** ein.
Client-ID	Fügen Sie die Azure-**Anwendungs-ID** der Anwendung, die Sie in Azure registriert haben, im Feld Cloud-Management **Client-ID** ein.
Authentifizierungsmethode	Wählen Sie **Client-Geheimnis**. **Hinweis:** **Client-Zusicherung** wird nicht unterstützt.
Geheimschlüssel	Fügen Sie den geheimen Schlüssel ein, der beim Erstellen des Azure Service Principal generiert wurde. Dieses Feld erscheint, wenn die **Authentifizierungsmethode** **Client-Geheimnis** ist.

Azure Enterprise Agreement-Anmeldeinformationen

Azure Enterprise Agreement-Anmeldeinformationen sind für die Abrechnungsfunktionen der Cloud Management-Anwendung erforderlich.

Formularfelder für Azure Enterprise Agreement-Anmeldeinformationen

Feld	Beschreibung
Name	Geben Sie einen beschreibenden Namen ein.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formularfelder für Azure Enterprise Agreement-Anmeldeinformationen (Fortsetzung)

Feld	Beschreibung
Registrierungsnummer	Geben Sie die Registrierungsnummer von Azure ein.
Zugriffsschlüssel	Fügen Sie den von Azure bereitgestellten Zugriffsschlüssel ein.

Cloud Management-Anmeldeinformationen

Dieser Anmeldeinformationstyp ist für Orchestration verfügbar.

Formularfelder für Cloud Management-Anmeldeinformationen

Feld	Eingabewert
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein. Zum Beispiel könnten Sie sie **Cloud Atlanta** nennen.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Typ	Geben Sie **AWS** an.
Benutzername	Geben Sie den CIM-Benutzernamen ein, um die Tabelle „Anmeldeinformationen“ zu erstellen. Vermeiden Sie in Benutzernamen führende oder nachfolgende Leerzeichen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachgestellte Leerzeichen im Benutzernamen erkennt.
Passwort	Geben Sie das CIM-Passwort ein.
SSH-Passwortsatz	Geben Sie eine einprägsame Phrase für die Schlüsselgenerierung ein. Zum Beispiel könnten Sie **Freitag ist ein guter Tag** eingeben.
Privater SSH-Schlüssel	Geben Sie den privaten SSH-Schlüssel ein.
Authentifizierungsprotokoll	Wählen Sie das **MD5**- oder **SHA**-Authentifizierungsprotokoll aus, mit dem der **Authentifizierungsschlüssel** erstellt wurde.
Authentifizierungsschlüssel	Geben Sie einen von SSH generierten Authentifizierungsschlüssel ein.
Datenschutzprotokoll	Geben Sie eines der folgenden Datenschutzprotokolle ein, das die Verschlüsselung für die **Datenschutzschlüssel** beschreibt: • **3DES** für Triple Data Encryption Standard (DES) • **AES128** für Advanced Encryption Standard (AES) mit 128-Bit-Verschlüsselung • **AES192** für AES mit 192-Bit-Verschlüsselung • **AES256** für AES mit 256-Bit-Verschlüsselung • **DES** für die alte DES-Verschlüsselung
Geben Sie einen zusätzlichen Datenschutzschlüssel ein.	

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formularfelder für Cloud Management-Anmeldeinformationen (Fortsetzung)

Feld	Eingabewert
Anmeldeinformationsalias	Lassen Sie zu, dass Ersteller von Workflows, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn Sie diese Option auswählen, werden die Felder **Benutzername** und **Passwort** durch das Feld **Nachweis-ID** ersetzt. Derzeit ist CyberArk das einzige unterstützte externe Speichersystem.
Gilt für	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für **Spezielle MID-Server** angewendet werden sollen. MID Servers angeben, der diese Anmeldeinformationen im Feld „ **MID-Server** “ verwenden soll.
Klassifizierung	Geben Sie die Anwendungsklassifizierung für die CI-Ermittlung ein.
Reihenfolge	Reihenfolge (Reihenfolge), in der Discovery diese Anmeldeinformationen bei dem Versuch, sich bei Geräten anzumelden, ausprobiert. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.

Anmeldeinformationen für CMP-Knoten (Cloud Management)

Anmeldeinformationen für CMP-Knoten (Cloud Management) verknüpfen Anmeldeinformationen für einen virtuellen Server, die von Cloud Management bereitgestellt werden. Die Cloud Management-Anwendung erstellt diese Anmeldeinformationen automatisch.

Hinweis: Möglicherweise müssen Sie diese Anmeldeinformationen deaktivieren, wenn Sie sie nicht mehr verwenden möchten, die Prioritätsreihenfolge ändern oder einen MID Server auswählen, der darauf zugreifen darf. Andernfalls müssen Sie diesen Anmeldeinformationstyp nicht manuell erstellen oder ändern.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formularfelder für Anmeldeinformationen für CMP-Knoten

Feld	Beschreibung
Name	Der automatisch generierte Name basiert auf dem Rechenzentrum, in dem sich der virtuelle Computer befindet.
Aktiv	Ob die Anmeldeinformationen aktiv sind.
Gilt für	Wählen Sie aus, ob diese Anmeldeinformationen für einen bestimmten MID Server oder für alle MID Server verfügbar sind.
Reihenfolge	Reihenfolge (Reihenfolge), in der Discovery diese Anmeldeinformationen bei dem Versuch, sich bei Geräten anzumelden, ausprobiert. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.
Benutzername und Passwort	Der Benutzername und das Passwort des virtuellen Servers.
SSH-Passwortsatz und Privater SSH-Schlüssel	Der private Schlüssel und der Passwortsatz, der den Schlüssel schützt, falls der virtuelle Server dies erfordert.
Authentifizierungsprotokoll und Authentifizierungsschlüssel	Der private Schlüssel und der Passwortsatz, der den Schlüssel schützt, falls der virtuelle Server dies erfordert.
Datenschutzprotokoll und Datenschutzschlüssel	Wählen Sie das mit dem virtuellen Server verwendete Verschlüsselungsprotokoll aus, und geben Sie den Datenschutzschlüssel ein.
Anmeldeinformationsalias	Lassen Sie zu, dass Ersteller von Workflows, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu.

Anmeldeinformationen für Cloud Management (CMP)-SSH-Schlüsselpaar

Cloud Management (CMP)-SSH-Schlüsselpaare speichern die Schlüssel, die die Cloud Management-Anwendung automatisch generiert, wenn Benutzer Stapelressourcen bereitstellen.

Hinweis: Möglicherweise müssen Sie diese Anmeldeinformationen deaktivieren, wenn Sie sie nicht mehr verwenden möchten. Andernfalls müssen Sie diesen Anmeldeinformationstyp nicht manuell erstellen oder ändern.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formularfelder für Anmeldeinformationen für CMP-SSH-Schlüsselpaare

Feld	Beschreibung
Name	Der automatisch generierte Name
Aktiv	Ob die Anmeldeinformationen aktiv sind.
Öffentlicher SSH-Schlüssel	Der öffentliche Schlüssel
Privater SSH-Schlüssel	Ein sicherer privater Schlüssel, der anstelle eines Passworts für SSH-Anmeldungen verwendet werden kann.

Infoblox-Anmeldeinformationen

Infoblox-Anmeldeinformationen sind erforderlich, um IP-Pools (IPAM) in der Cloud Management-Anwendung einzurichten.

Diese Felder sind im Formular „Anmeldeinformationen“ für Anmeldeinformationen des Typs „Infoblox“ verfügbar.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Gilt für	Wählen Sie aus, ob diese Anmeldeinformationen für einen bestimmten MID Server oder für alle MID Server verfügbar sind.
Reihenfolge	Reihenfolge (Reihenfolge), in der Discovery diese Anmeldeinformationen bei dem Versuch, sich bei Geräten anzumelden, ausprobiert. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert. Reihenfolge (Reihenfolge), in der Discovery diese Anmeldeinformationen bei dem Versuch, sich bei Geräten anzumelden, ausprobiert. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.
wapiversion	Geben Sie die Version von wAPI ein, die Sie verwenden.
Benutzername und Passwort	Geben Sie den InfoBlox-Benutzernamen und das Passwort ein.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

JDBC-Anmeldeinformationen

Der JDBC-Anmeldeinformationstyp verwaltet den Zugriff auf eine JDBC-Verbindung (Java Database Connectivity). Dieser Anmeldeinformationstyp ist für Discovery und Orchestration verfügbar.

Diese Felder sind im Formular „Anmeldeinformationen“ für Anmeldeinformationen des Typs „JDBC“ verfügbar.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Benutzername	Geben Sie den zu erstellenden Benutzernamen in die Tabelle „Berechtigungsnachweise“ ein. Vermeiden Sie führende oder nachgestellte Leerzeichen in Benutzernamen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachgestellte Leerzeichen im Benutzernamen erkennt. Für die CIM-Erkennung muss der Benutzer über die Administratorrolle verfügen.
Passwort	Geben Sie das Passwort ein.
Nachweis-ID	Geben Sie den für externe Anmeldeinformationen konfigurierten eindeutigen Schlüssel in der JAR-Datei ein, die für ein externes Anmeldeinformationssystem auf den MID Server hochgeladen wurde. Das Feld **Nachweis-ID** darf maximal 40 Zeichen lang sein. Dieses Feld ist nur sichtbar, wenn das Kontrollkästchen **Externer Anmeldeinformationsspeicher** aktiviert ist.
Alias für Anmeldeinformationen	Erlauben Sie Workflow-Erstellern, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuzuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu. Geben Sie den Tabellennamen für den CI-Typ ein, zu dem das CI gehört (z. B. cmdb_ci_apache_web_server), um die Anmeldeinformationen zur Erkennung von CIs zu verwenden, die nicht zu diesem CI-Typ gehören und dafür Service Mapping- und Discovery-Muster nutzen.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn Sie diese Option auswählen, werden die Felder **Benutzername** und **Passwort** durch das Feld **Nachweis-ID** ersetzt. Externe Anmeldeinformationsspeicher stehen nur zur Verfügung, wenn dasPlugin „Externer Anmeldeinformationsspeicher“ aktiviert ist.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Derzeit ist CyberArk das einzige unterstützte externe Speichersystem.
Betrifft	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für **Spezielle MID-Server** angewendet werden sollen. MID Servers angeben, der diese Anmeldeinformationen im Feld „ **MID-Server** “ verwenden soll.
MID Server verwenden	Wählen Sie einen oder mehrere MID Server aus der Liste der verfügbaren MID Server aus. Die in diesem Datensatz konfigurierten Anmeldeinformationen stehen den MID Servern in dieser Liste zur Verfügung. Dieses Feld ist nur verfügbar, wenn Sie **Spezifische MID-Server** im Feld **Gilt für** auswählen. **Hinweis:** Die Auswahl von Spezifischen **Spezifischen MID-Servern** hat keine Auswirkungen auf die Auswahl der MID-Server. Es wird nur verwendet, um zu entscheiden, welche MID-Server für die Anmeldeinformationen sichtbar sein sollen. **Bestimmte MID-Server** werden in Orchestration-Aktivitäten nicht unterstützt.
Bestellung	Reihenfolge (Reihenfolge), in der Discovery diese Anmeldeinformationen bei dem Versuch, sich bei Geräten anzumelden, ausprobiert. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.
Windows-MID-Server-Servicekonto	Wenn sie aktiv sind, stellen die definierten Anmeldeinformationen das MID-Server-Servicekonto dar.

JMS-Anmeldeinformationen

Der JMS-Anmeldeinformationstyp verwaltet den Zugriff auf einen Java Message Service (JMS). Dieser Anmeldeinformationstyp ist für Discovery und Orchestration verfügbar.

Diese Felder sind im Anmeldeinformationsformular für JMS verfügbar.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Benutzername	Geben Sie den zu erstellenden Benutzernamen in die Tabelle „Berechtigungsnachweise“ ein. Vermeiden Sie führende oder nachgestellte Leerzeichen in Benutzernamen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachgestellte Leerzeichen im Benutzernamen erkennt. Für die CIM-Erkennung muss der Benutzer über die Administratorrolle verfügen.
Passwort	Geben Sie das Passwort ein.
Nachweis-ID	Geben Sie den für externe Anmeldeinformationen konfigurierten eindeutigen Schlüssel in der JAR-Datei ein, die für ein externes Anmeldeinformationssystem auf den MID Server hochgeladen wurde. Das Feld **Nachweis-ID** darf maximal 40 Zeichen lang sein. Dieses Feld ist nur sichtbar, wenn das Kontrollkästchen **Externer Anmeldeinformationsspeicher** aktiviert ist.
Alias für Anmeldeinformationen	Erlauben Sie Workflow-Erstellern, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuzuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu. Geben Sie den Tabellennamen für den CI-Typ ein, zu dem das CI gehört (z. B. cmdb_ci_apache_web_server), um die Anmeldeinformationen zur Erkennung von CIs zu verwenden, die nicht zu diesem CI-Typ gehören und dafür Service Mapping- und Discovery-Muster nutzen.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn Sie diese Option auswählen, werden die Felder **Benutzername** und **Passwort** durch das Feld **Nachweis-ID** ersetzt. Externe Anmeldeinformationsspeicher stehen nur zur Verfügung, wenn dasPlugin „Externer Anmeldeinformationsspeicher“ aktiviert ist. **Hinweis:** Derzeit ist CyberArk das einzige unterstützte externe Speichersystem.
Betrifft	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für **Spezielle MID-Server** angewendet werden sollen. MID Servers angeben, der diese Anmeldeinformationen im Feld „ **MID-Server** “ verwenden soll.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
MID Server verwenden	Wählen Sie einen oder mehrere MID Server aus der Liste der verfügbaren MID Server aus. Die in diesem Datensatz konfigurierten Anmeldeinformationen stehen den MID Servern in dieser Liste zur Verfügung. Dieses Feld ist nur verfügbar, wenn Sie **Spezifische MID-Server** im Feld **Gilt für** auswählen. **Hinweis:** Die Auswahl von Spezifischen **Spezifischen MID-Servern** hat keine Auswirkungen auf die Auswahl der MID-Server. Es wird nur verwendet, um zu entscheiden, welche MID-Server für die Anmeldeinformationen sichtbar sein sollen. **Bestimmte MID-Server** werden in Orchestration-Aktivitäten nicht unterstützt.
Bestellung	Reihenfolge (Reihenfolge), in der Discovery diese Anmeldeinformationen bei dem Versuch, sich bei Geräten anzumelden, ausprobiert. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.
Windows-MID-Server-Servicekonto	Wenn sie aktiv sind, stellen die definierten Anmeldeinformationen das MID-Server-Servicekonto dar.

OAuth 2.0-Anmeldeinformationen

OAuth 2.0-Anmeldeinformationen ermöglichen ServiceNow den Zugriff auf Benutzer-Accounts in einem HTTP-Service.

Diese Felder sind im Anmeldeinformationsformular für OAuth 2.0 verfügbar.

OAuth 2.0-Anmeldeinformationsformular

Feld	Eingabewert
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein. Zum Beispiel könnten Sie sie **OAuth2-Anmeldeinformationen** nennen.
Aktiv	Geben Sie an, ob diese Anmeldeinformationen aktiv sind.
OAuth-Entitätsprofil	Ein OAuth-Profil ist eine Kombination aus einem Gewährungstyp und mindestens einem Bereich.
Verbindung mit Auth-Server über MID-Server herstellen	Verbindet Ihre Instanz ServiceNow über MID-Server] mit einem lokalen OAuth-Server, der sich hinter einer Firewall befindet. Sie können Ihre Instanz ServiceNow auch über einen MID-Server

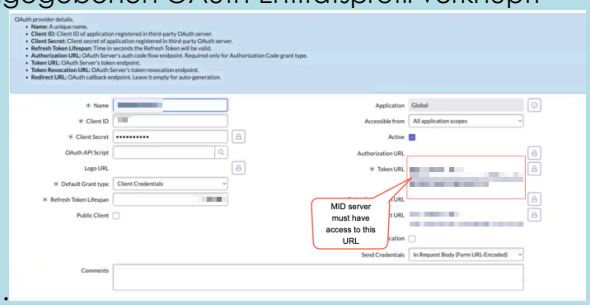
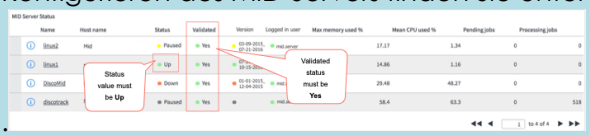
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OAuth 2.0-Anmeldeinformationsformular (Fortsetzung)

Feld	Eingabewert
	mit einem cloudbasierten OAuth-Server verbinden. Wenn diese Option aktiviert ist, wird die Anforderung eines OAuth-Tokens über MID-Servergesendet. **Wichtig:** • Die Option wird angezeigt, wenn der Wert im Feld **Gewährungstyp** im OAuth-Entitätsprofil auf **Client-Anmeldeinformationen**festgelegt ist. Informationen zum Festlegen eines OAuth-Entitätsprofils für einen OAuth-Drittpartei-Anbieter finden Sie unter Stellen Sie eine Verbindung zu einem OAuth-Drittpartei-Anbieter her. • Wenn Sie das Kontrollkästchen **Verbindung mit Auth-Server über MID-Server** herstellen aktivieren, müssen Sie das erforderliche MID-Server oder MID Servers in der Liste **Gilt für** identifizieren.
Betrifft	Geben Sie an, ob der Anmeldeinformationsdatensatz für alle MID-Server oder einen bestimmten MID-Server gilt. Wenn Sie „Spezielle MID Server“ auswählen, fügen Sie die entsprechenden MID Server hinzu.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OAuth 2.0-Anmeldeinformationsformular (Fortsetzung)

Feld	Eingabewert
	Wichtig: Beachten Sie diese Punkte, wenn Sie das Kontrollkästchen **Verbindung mit Auth-Server über MID-Server** herstellen aktiviert haben. • Stellen Sie sicher, dass alle MID Servers, die unter Gilt für ausgewählt sind, mit dem Auth-Server kommunizieren können. Dies ist erforderlich, um die Tokenanforderung für die im OAuth-Provider-Datensatz erwähnte **Token-URL** auszuführen (die mit dem im OAuth 2.0-Anmeldeinformationsdatensatz angegebenen OAuth-Entitätsprofil verknüpft ist).  • Stellen Sie sicher, dass mindestens ein MID-Server (im Feld MID Servers, das unter **Gilt für**ausgewählt ist) mit den folgenden Konfigurationen vorhanden ist: ◦ Der Wert des Felds **Status** lautet **In Betrieb**. ◦ Der Wert des Felds **Validiert** lautet **Ja**. ◦ Die Fähigkeit von MID-Server ist auf **REST** oder **ALL**festgelegt. Informationen zum Konfigurieren des MID-Servers finden Sie unter .  Weitere Informationen zu diesen Status finden Sie unter MID-Server-Dashboard .
Bestellung	Reihenfolge (Reihenfolge), in der Discovery diese Anmeldeinformationen bei dem Versuch, sich bei Geräten anzumelden, ausprobiert. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OAuth 2.0-Anmeldeinformationsformular (Fortsetzung)

Feld	Eingabewert
	Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.
Anmeldeinformationsalias	Geben Sie den Alias für Anmeldeinformationen an, den Sie an die OAuth 2.0-Anmeldeinformationen binden möchten.
Integrationstyp	Gibt den Integrationstyp für die Anmeldeinformationen an. Rufen Sie eine API eines Drittanbieters mit einer OAuth-Anforderung auf, die ein system- oder anwenderspezifisches OAuth-Token generiert. Es folgen die Integrationstypen: • **System**: Rufen Sie die Tokeninformationen basierend auf dem Profil der anfordernden Person ab. • **Persönlich**: Ruft die anwenderspezifischen Tokeninformationen ab. Der Benutzer, der die Sitzung initiiert. Wenn „ **Personal** “ auf der OAuth-Seite „Profil der anfordernden Person“ ausgewählt ist, wird die zusätzliche Kennzeichnung „ **Persönlich** “ angezeigt. **Hinweis:** • Auf alle Informationen, die sich auf einen Anwender beziehen, kann nur mit anwenderspezifischen OAuth-Token zugegriffen werden, deren Integrationstyp **Persönlich**ist. • Um das auf den Sitzungsanwender bezogene Token zu verwenden, müssen Sie unter **Ausführen als** in den Flow-Eigenschaften den **Benutzer, der die Sitzung initiiert**auswählen.

SAP-Anmeldeinformationen

Der SAP-Anmeldeinformationstyp verwaltet den Zugriff auf SAP JCo-Systeme. Dieser Anmeldeinformationstyp ist für Discovery und Orchestration verfügbar.

Diese Felder sind im Formular „Anmeldeinformationen“ für Anmeldeinformationen des Typs „SAP“ verfügbar.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Benutzername	Geben Sie den zu erstellenden Benutzernamen in die Tabelle „Berechtigungsnachweise“ ein. Vermeiden Sie führende oder nachgestellte Leerzeichen in Benutzernamen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachgestellte Leerzeichen im

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Benutzernamen erkennt. Für die CIM-Erkennung muss der Benutzer über die Administratorrolle verfügen.
Passwort	Geben Sie das Passwort ein.
Nachweis-ID	Geben Sie den für externe Anmeldeinformationen konfigurierten eindeutigen Schlüssel in der JAR-Datei ein, die für ein externes Anmeldeinformationssystem auf den MID Server hochgeladen wurde. Das Feld **Nachweis-ID** darf maximal 40 Zeichen lang sein. Dieses Feld ist nur sichtbar, wenn das Kontrollkästchen **Externer Anmeldeinformationsspeicher** aktiviert ist.
Alias für Anmeldeinformationen	Erlauben Sie Workflow-Erstellern, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuzuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu. Geben Sie den Tabellennamen für den CI-Typ ein, zu dem das CI gehört (z. B. cmdb_ci_apache_web_server), um die Anmeldeinformationen zur Erkennung von CIs zu verwenden, die nicht zu diesem CI-Typ gehören und dafür Service Mapping- und Discovery-Muster nutzen.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn Sie diese Option auswählen, werden die Felder **Benutzername** und **Passwort** durch das Feld **Nachweis-ID** ersetzt. Externe Anmeldeinformationsspeicher stehen nur zur Verfügung, wenn dasPlugin „Externer Anmeldeinformationsspeicher“ aktiviert ist. **Hinweis:** Derzeit ist CyberArk das einzige unterstützte externe Speichersystem.
Betrifft	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für **Spezielle MID-Server** angewendet werden sollen. MID Servers angeben, der diese Anmeldeinformationen im Feld „ **MID-Server** “ verwenden soll.
MID Server verwenden	Wählen Sie einen oder mehrere MID Server aus der Liste der verfügbaren MID Server aus. Die in diesem Datensatz konfigurierten Anmeldeinformationen stehen den MID Servern in dieser Liste zur Verfügung. Dieses Feld ist nur verfügbar, wenn Sie **Spezifische MID-Server** im Feld **Gilt für** auswählen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Die Auswahl von Spezifischen **Spezifischen MID-Servern** hat keine Auswirkungen auf die Auswahl der MID-Server. Es wird nur verwendet, um zu entscheiden, welche MID-Server für die Anmeldeinformationen sichtbar sein sollen. **Bestimmte MID-Server** werden in Orchestration-Aktivitäten nicht unterstützt.
Bestellung	Reihenfolge (Reihenfolge), in der Discovery diese Anmeldeinformationen bei dem Versuch, sich bei Geräten anzumelden, ausprobiert. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.
Windows-MID-Server-Servicekonto	Wenn sie aktiv sind, stellen die definierten Anmeldeinformationen das MID-Server-Servicekonto dar.

SNMP-Anmeldeinformationen

Discovery untersucht viele Arten von Geräten (Switches, Router, Drucker usw.) mithilfe des SNMP-Protokolls. Anmeldeinformationen für SNMP enthalten keinen Anwendernamen, nur ein Passwort, das „ *Community-Zeichenfolge*“ genannt wird.

Die standardmäßige schreibgeschützte Community-Zeichenfolge für viele SNMP-Geräte ist öffentlich, und Discovery testet diese automatisch. Geben Sie die entsprechenden SNMP-Anmeldeinformationen ein, falls diese sich von der *öffentlichen* Community-Zeichenfolge unterscheiden.

Beim Ermitteln von SNMP werden alle konfigurierten Community-Zeichenfolgen verwendet. Dieses Verhalten gilt nicht für das Ermitteln von SNMPv3.

Die standardmäßige SNMP-Abfrage der Orchestration-Aktivität gibt den Objektbezeichner (OID) eines Geräts zurück und erfordert SNMP-Anmeldeinformationen.

SNMP-Community Anmeldeinformationen

Der Anmeldeinformationstyp der SNMP-Community verwaltet den Zugriff, um viele Arten von Geräten (Switches, Router, Drucker usw.) mithilfe des SNMP-Protokolls zu ermitteln. Dieser Anmeldeinformationstyp ist für Discovery, Service-Mapping und Orchestration verfügbar.

SNMP-Anmeldeinformationen enthalten keinen Benutzernamen, nur ein Passwort (die Community-Zeichenfolge). Die standardmäßige schreibgeschützte Community-Zeichenfolge für viele SNMP-Geräte ist öffentlich, und das System testet diese automatisch. Geben Sie die entsprechenden SNMP-Anmeldeinformationen ein, falls diese sich von der öffentlichen Community-Zeichenfolge unterscheiden.

Diese Felder sind im Anmeldeinformationsformular für SNMP-Community verfügbar.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Benutzername	Geben Sie den zu erstellenden Benutzernamen in die Tabelle „Berechtigungsnachweise“ ein. Vermeiden Sie führende oder nachgestellte Leerzeichen in Benutzernamen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachgestellte Leerzeichen im Benutzernamen erkennt. Für die CIM-Erkennung muss der Benutzer über die Administratorrolle verfügen.
Passwort	Geben Sie das Passwort ein.
Nachweis-ID	Geben Sie den für externe Anmeldeinformationen konfigurierten eindeutigen Schlüssel in der JAR-Datei ein, die für ein externes Anmeldeinformationssystem auf den MID Server hochgeladen wurde. Das Feld **Nachweis-ID** darf maximal 40 Zeichen lang sein. Dieses Feld ist nur sichtbar, wenn das Kontrollkästchen **Externer Anmeldeinformationsspeicher** aktiviert ist.
Alias für Anmeldeinformationen	Erlauben Sie Workflow-Erstellern, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuzuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu. Geben Sie den Tabellennamen für den CI-Typ ein, zu dem das CI gehört (z. B. cmdb_ci_apache_web_server), um die Anmeldeinformationen zur Erkennung von CIs zu verwenden, die nicht zu diesem CI-Typ gehören und dafür Service Mapping- und Discovery-Muster nutzen.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn Sie diese Option auswählen, werden die Felder **Benutzername** und **Passwort** durch das Feld **Nachweis-ID** ersetzt. Externe Anmeldeinformationsspeicher stehen nur zur Verfügung, wenn dasPlugin „Externer Anmeldeinformationsspeicher“ aktiviert ist. **Hinweis:** Derzeit ist CyberArk das einzige unterstützte externe Speichersystem.
Betrifft	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für **Spezielle MID-Server** angewendet werden sollen. MID Servers angeben, der diese Anmeldeinformationen im Feld „ **MID-Server** “ verwenden soll.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
MID Server verwenden	Wählen Sie einen oder mehrere MID Server aus der Liste der verfügbaren MID Server aus. Die in diesem Datensatz konfigurierten Anmeldeinformationen stehen den MID Servern in dieser Liste zur Verfügung. Dieses Feld ist nur verfügbar, wenn Sie **Spezifische MID-Server** im Feld **Gilt für** auswählen. **Hinweis:** Die Auswahl von Spezifischen **Spezifischen MID-Servern** hat keine Auswirkungen auf die Auswahl der MID-Server. Es wird nur verwendet, um zu entscheiden, welche MID-Server für die Anmeldeinformationen sichtbar sein sollen. **Bestimmte MID-Server** werden in Orchestration-Aktivitäten nicht unterstützt.
Bestellung	Reihenfolge (Reihenfolge), in der Discovery diese Anmeldeinformationen bei dem Versuch, sich bei Geräten anzumelden, ausprobiert. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.
Windows-MID-Server-Servicekonto	Wenn sie aktiv sind, stellen die definierten Anmeldeinformationen das MID-Server-Servicekonto dar.

SNMPv3-Anmeldeinformationen

SNMPv3-Anmeldeinformationen akzeptieren ein Datenschutzprotokoll und einen zusätzlichen Datenschutzschlüssel und sind für Discovery und Orchestration verfügbar. Für externen Speicher in CyberArk können Sie einen Datenschutz-Accountschlüssel auswählen.

Diese Felder sind im Anmeldeinformationsformular für SNMPv3 verfügbar.

SNMPv3-Anmeldeinformationsfelder

Feld	Eingabewert
Name	Eindeutiger und beschreibender Name für diese Anmeldeinformationen. Zum Beispiel könnten Sie sie **SNMP-Community Atlanta** nennen.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Betrifft	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für einen oder mehrere **Spezielle MID-Server** angewendet werden sollen. Geben Sie im Feld

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SNMPv3-Anmeldeinformationsfelder (Fortsetzung)

Feld	Eingabewert
	MID-Server die MID-Server an, die diese Anmeldeinformationen verwenden sollen.
MID-Server	Wählen Sie einen oder mehrere MID Server aus der Liste der verfügbaren MID Server aus. Die in diesem Datensatz konfigurierten Anmeldeinformationen stehen den MID Servern in dieser Liste zur Verfügung. Dieses Feld ist nur verfügbar, wenn Sie **Spezifische MID-Server** im Feld **Gilt für** auswählen.
Reihenfolge	Reihenfolge (Reihenfolge), in der Discovery diese Anmeldeinformationen bei dem Versuch, sich bei Geräten anzumelden, ausprobiert. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.
Benutzername	Geben Sie den SNMP-Benutzernamen ein. Vermeiden Sie in Benutzernamen führende oder nachfolgende Leerzeichen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachfolgende Leerzeichen im Benutzernamen erkennt.
Authentifizierungsprotokoll	Wählen Sie den Authentifizierungstyp aus, der für diese Anmeldeinformationen verwendet werden soll. Die Auswahlmöglichkeiten sind: • MD5 • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512
Authentifizierungsschlüssel	Geben Sie den mit diesen Anmeldeinformationen zu verwendenden Authentifizierungsschlüssel ein.
Datenschutzprotokoll	Wählen Sie das Verschlüsselungsprotokoll für diese Anmeldeinformationen aus. Die Auswahlmöglichkeiten sind: • 3DES • AES128 • AES192 • AES256 • DES

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SNMPv3-Anmeldeinformationsfelder (Fortsetzung)

Feld	Eingabewert
Datenschutzschlüssel	Geben Sie den Schlüssel ein, der dem ausgewählten Datenschutzprotokoll zugeordnet ist.
Nachweis-ID	Geben Sie den für externe Anmeldeinformationen in der JAR-Datei, die für einen externen Anmeldeinformationsanbieter auf den MID Server hochgeladen wurde, konfigurierten eindeutigen Schlüssel ein. Das Feld **Nachweis-ID** darf maximal 40 Zeichen lang sein. Dieses Feld ist nur sichtbar, wenn das Kontrollkästchen **Externer Speicher für Berechtigungsnachweise** aktiviert ist.
Datenschutz-Anmeldeinformations-ID	Geben Sie den für SNMPv3-Anmeldeinformationen konfigurierten Datenschutzkonto-Schlüssel in CyberArk ein. Wenn Sie ein Datenschutzprotokoll in CyberArk verwenden, muss dieses Feld denselben Wert aufweisen wie das Feld **Name** für das CyberArk-SNMPv3-Datenschutzkonto. Dieses Feld ist für SNMPv3 nur sichtbar, wenn Sie im Feld **Anmeldeinformationsspeicher-Typ** die Option **CyberArk** auswählen. Wenn Sie keinen Datenschutzschlüssel für CyberArk verwenden, lassen Sie dieses Feld leer.
Anmeldeinformationsalias	Lassen Sie zu, dass Ersteller von Workflows, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn ein externer Speicher aktiviert ist, wird das Feld **Nachweis-ID** angezeigt. Eine externe Speicherung von Anmeldeinformationen ist nur verfügbar, wenn das External Credential Storage-Plugin aktiviert und die Ansicht **Externer Speicher** ausgewählt ist.
Anmeldeinformationsspeicher-Typ	Wählen Sie den Provider für den externen Speicher aus. Wählen Sie **CyberArk** nur aus, wenn Sie einen SNMPv3-Datenschutzschlüssel für CyberArk verwenden. Das Feld **Datenschutz-Anmeldeinformations-ID** wird zur Eingabe des Schlüssels angezeigt.
Kontext verwenden	Aktivieren Sie dieses Kontrollkästchen, um einen Kontextwert für diese Anmeldeinformationen hinzuzufügen. Dieses Feld wird in der **Discovery**-Ansicht angezeigt. Kontexte werden derzeit für externe Anmeldeinformationsspeicher nicht unterstützt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SNMPv3-Anmeldeinformationsfelder (Fortsetzung)

Feld	Eingabewert
	Hinweis: Ein Kontext ist eine Sammlung von Verwaltungsinformationen, auf die SNMPv3-Anmeldeinformationen zugreifen, in denen auf eine bestimmte OID verwiesen wird. Auf Kontexte wird manchmal verwiesen, damit Informationen über das Gerät gesammelt werden können, auf die mit den normalen Anmeldeinformationen nicht zugegriffen werden kann. Ein Kontext kann vom Hersteller bereitgestellt oder separat konfiguriert werden. Weitere Informationen finden Sie unter Kontextname und Kontext-ID . Wenn Sie über mehrere SNMPv3-Anmeldeinformationen mit demselben Benutzernamen und denselben Schlüsseln verfügen, einige Ihrer Geräte jedoch einen Kontext benötigen und andere nicht, müssen Sie für jedes Gerät separate Datensätze erstellen.
Kontextname	Geben Sie den Kontextnamenswert für diese Anmeldeinformationen ein. Diese Option sollte nur verwendet werden, wenn Sie über Geräte verfügen, die diesen Wert für einen vollständigen Zugriff benötigen. Dieses Feld wird angezeigt, wenn das Kontrollkästchen **Kontext verwenden** aktiviert ist.

SSH-Anmeldeinformationen

Discovery, Orchestration und IntegrationHub erkunden die Geräte UNIX und Linux mithilfe von SSH-Anmeldeinformationen, um Befehle über Secure Shell (SSH) auszuführen. SSH-Befehle müssen mit Stammberechtigungen ausgeführt werden, entweder mit Stamm-Anmeldeinformationen oder mit Sudo. Private SSH-Schlüsselanmeldeinformationen bieten zusätzliche Sicherheit.

Stammberechtigungen erteilen

Bevor Sie Stammberechtigungen gewähren, überprüfen Sie Ihre Sicherheitsrichtlinie und -optionen mit dem Sicherheitsteam Ihrer Organisation.

Verwenden Sie eine dieser Methoden, um Benutzern die Ausführung von SSH-Befehlen mit Stammberechtigungen zu ermöglichen:

- Erteilen Sie andere Anmeldeinformationen für Discovery, Orchestration oder IntegrationHub, aber gewähren Sie dem Benutzer in diesen Anmeldeinformationen das Recht, bestimmte Befehle mit Stammberechtigungen über sudo auszuführen. Dies ist eine sichere Methode zum Gewähren eingeschränkter Berechtigungen. Von Discovery, Orchestration oder IntegrationHub wird „sudo“ für jede Probe verwendet, für die der Parameter `must_sudo` auf **true** gesetzt ist (Standardeinstellung ist **false**). Hierfür muss allerdings jedes System so konfiguriert werden, dass es die Ausführung von sudo gestattet. Dies erfolgt durch Bearbeiten der Datei **/etc/sudoers** mit dem Befehl **visudo**.
- Teilen Sie **Stamm**-Anmeldeinformationen zu. Dies sind offenkundig die leistungsstärksten Anmeldeinformationen, unter Sicherheitsgründen aber möglicherweise nicht erstrebenswert. Wenn Discovery, Orchestration oder IntegrationHub über die Stammanmeldeinformationen für UNIX- oder Linux-Systeme verfügen, ist keine weitere Konfiguration erforderlich.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Privilegierte Befehle

Die Plattform bietet standardisierte privilegierte Befehle, die der MID Server verwenden kann, und die Möglichkeit, dem System zusätzliche Befehle hinzuzufügen. Weitere Informationen zur Verwendung von sudo-Befehlen und anderen privilegierten Befehlen finden Sie unter Privilegierte MID-Server-Befehle .

Anmeldeinformationstyp „Privater SSH-Schlüssel“

Hinweis: Die Anmeldeinformationen mit dem privaten SSH-Schlüssel bieten eine größere Sicherheit als die Anmeldeinformationen mit dem SSH-Passwort.

Feld	Eingabewert
Name	Eindeutiger und beschreibender Name für diese Anmeldeinformationen. Zum Beispiel könnten Sie sie **SSH Atlanta** nennen.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Benutzername	Geben Sie einen UNIX- oder Linux-Benutzernamen ein. Vermeiden Sie in Benutzernamen führende oder nachfolgende Leerzeichen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachgestellte Leerzeichen im Benutzernamen erkennt.
Passwort	Geben Sie das UNIX- oder Linux-Passwort ein. Geben Sie für Anmeldeinformationen vom Typ **Privater SSH-Schlüssel** das sudo-Passwort ein, wenn für den Benutzernamen ein Passwort erforderlich ist.
SSH-Passphrase	Geben Sie einen sicheren SSH-Passwortsatz ein. Dieses Feld ist nur für Anmeldeinformationen mit dem Typ **Privater SSH-Schlüssel** verfügbar.

Privater SSH-Schlüssel	Geben Sie einen sicheren, privaten RSA-, DSA-, ECDSA- oder ED25519-Schlüssel ein.
	
	Der private Schlüssel muss im richtigen Format eingegeben werden, um sicherzustellen, dass er ordnungsgemäß verschlüsselt ist. Der private Schlüssel muss mit der Zeichenfolge `-----BEGIN` beginnen.
	
	Hier ist ein Beispiel für einen korrekt formatierten privaten RSA-Schlüssel:
	`-----BEGIN RSA PRIVATE KEY-----`
	`MIIEogIBAAKCAQEAsEK65scPssPSobpDFMpR+Btv3MS4Q7`
	`NP8ERaStRZsh3IWz+x...`
	`...7hrxV2dbSug60FahyupGWBGtPnXm5PaE2X5WPLuUj94`
	`ue48i1Fs`
	`-----END RSA PRIVATE KEY-----`
	
	Beispiel für einen DSA-Schlüssel:
	`-----BEGIN DSA PRIVATE KEY-----`
	`MIIEogIBAAKCAQEAsEK65scPssPSobpDFMpR+Btv3MS4Q7`
	`NP8ERaStRZsh3IWz+x...`

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Eingabewert
	...7hrxV2dbSug60FahyupGWBGtPnXm5PaE2X5WPLuUj94ue48i1Fs -----END DSA PRIVATE KEY----- Beispiel für einen ECDSA-Schlüssel: -----BEGIN EC PRIVATE KEY----- MIIEogIBAAKCAQEAsEK65scPssPSobpDFMpR+Btv3MS4Q7NP8ERaStRZsh3IWz+x... ...7hrxV2dbSug60FahyupGWBGtPnXm5PaE2X5WPLuUj94ue48i1Fs -----END EC PRIVATE KEY----- Beispiel für einen privaten ED25519-Schlüssel: -----BEGIN OPENSSH PRIVATE KEY----- b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAABAAAAMwAAAAtzc2gtZW QyNTUxOQAAACAlYlqhcdwx8VQzZ5XaIC5ltQpjRr3lIlq/aE66mufmiwAAAKDQUtxZ0FLc WQAAAAtzc2gtZWQyNTUxOQAAACAlYlqhcdwx8VQzZ5XaIC5ltQpjRr3lIlq/aE66mufmiw AAAECuvsTkFUPdpTh0kw23i8TYx19qsFOZ3TRgowkkHBh6wSViWqFx3DHxVDNnldogLmW1 CmNGveUiWr9oTrqa5+aLAAAAGmFiaGluYXYuc3V0YXJATVJFTUE3OTAzMkI3AQID -----END OPENSSH PRIVATE KEY----- **Hinweis:** Für einen privaten ED25519-Schlüssel wird nur das OpenSSH-Schlüsselformat unterstützt, das mit dem Dienstprogramm OpenSSH SSH-keygen generiert wird. Die Now Platform unterstützt private Schlüssel im PEM-Format, das vom OpenSSH-Dienstprogramm ssh-keygen generiert wird. So konvertieren Sie PPK-Schlüssel, die von PuTTY generiert wurden: • Öffnen Sie Ihren privaten Schlüssel in PuTTYGen. • Exportieren Sie sie im OpenSSH-Format aus dem Menü **Konvertierungen** > **Exportieren Sie den OpenSSH-Schlüssel**an. • Speichern Sie den neuen OpenSSH-Schlüssel.
SSH-Zertifikat	Geben Sie ein RSA- oder ED25519-basiertes OpenSSH-Zertifikat ein. Wenn das Zertifikat eingegeben wird, wird ein privater Schlüssel für die zertifikatbasierte Authentifizierung verwendet. Diese Authentifizierung wird ab OpenSSH 7.8 unterstützt.
Anmeldeinformationsalias	• Erlauben Sie Flow Designern die Verwendung von Aliassen zur Verwaltung von Verbindungs- und Berechtigungsinformationen. Wenn

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Eingabewert
	Sie ein Alias verwenden, müssen Sie nicht mehrere Anmeldeinformations- und Verbindungsinformationsprofile konfigurieren, wenn Sie mehrere Umgebungen verwenden. Wenn sich die Verbindungs- oder Anmeldeinformationen ändern, müssen Sie Aktionen, die die Verbindung verwenden, nicht aktualisieren. Weitere Informationen finden Sie unter Verbindung und Anmeldeinformationen. • Erlauben Sie Workflow-Erstellern, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuzuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn Sie diese Option auswählen, werden die Felder **Benutzername** und **Passwort** durch das Feld **Nachweis-ID** ersetzt. Derzeit ist CyberArk das einzige unterstützte externe Speichersystem.
MID Server	Wählen Sie einen oder mehrere MID Server aus der Liste der verfügbaren MID Server aus. Die in diesem Datensatz konfigurierten Anmeldeinformationen stehen den MID Servern in dieser Liste zur Verfügung. Dieses Feld ist nur verfügbar, wenn Sie **Spezielle MID-Server** aus dem Feld **Betrifft** auswählen.
Gilt für	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für einen oder mehrere **Spezielle MID-Server** angewendet werden sollen. Geben Sie im Feld **MID-Server** die MID-Server an, die diese Anmeldeinformationen verwenden sollen.
Bestellung	Die Reihenfolge, in der die Plattform diese Anmeldeinformationen bei der Anmeldung bei Geräten testet. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Anmeldeinformationen ein, wenn Sie eine große Anzahl von Anmeldeinformationen verwenden oder wenn Benutzer nach drei fehlgeschlagenen Anmeldeversuchen von den Sicherheitsfunktionen gesperrt werden. Wenn alle Anmeldeinformationen dieselbe Nummer (oder keine) in der Reihenfolge haben, testet Discovery oder Orchestration die Anmeldeinformationen in zufälliger Reihenfolge.

SSH-Anmeldeinformationstyp

Diese Felder sind im SSH-Anmeldeinformationsformular verfügbar.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Benutzername	Geben Sie den zu erstellenden Benutzernamen in die Tabelle „Berechtigungsnachweise“ ein. Vermeiden Sie führende oder nachgestellte Leerzeichen in Benutzernamen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachgestellte Leerzeichen im Benutzernamen erkennt. Für die CIM-Erkennung muss der Benutzer über die Administratorrolle verfügen.
Passwort	Geben Sie das Passwort ein.
Nachweis-ID	Geben Sie den für externe Anmeldeinformationen konfigurierten eindeutigen Schlüssel in der JAR-Datei ein, die für ein externes Anmeldeinformationssystem auf den MID Server hochgeladen wurde. Das Feld **Nachweis-ID** darf maximal 40 Zeichen lang sein. Dieses Feld ist nur sichtbar, wenn das Kontrollkästchen **Externer Anmeldeinformationsspeicher** aktiviert ist.
Alias für Anmeldeinformationen	• Erlauben Sie Flow Designern die Verwendung von Aliassen zur Verwaltung von Verbindungs- und Berechtigungsinformationen. Wenn Sie ein Alias verwenden, müssen Sie nicht mehrere Anmeldeinformations- und Verbindungsinformationsprofile konfigurieren, wenn Sie mehrere Umgebungen verwenden. Wenn sich die Verbindungs- oder Anmeldeinformationen ändern, müssen Sie Aktionen, die die Verbindung verwenden, nicht aktualisieren. Weitere Informationen finden Sie unter Verbindung und Anmeldeinformationen. • Erlauben Sie Workflow-Erstellern, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuzuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu. Geben Sie den Tabellennamen für den CI-Typ ein, zu dem das CI gehört (z. B. cmdb_ci_apache_web_server), um die Anmeldeinformationen zur Erkennung von CIs zu verwenden, die nicht zu diesem CI-Typ gehören und dafür Service Mapping- und Discovery-Muster nutzen.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn Sie diese Option auswählen, werden die Felder **Benutzername** und **Passwort** durch das Feld **Nachweis-ID** ersetzt. Externe Anmeldeinformationsspeicher stehen nur zur Verfügung, wenn dasPlugin „Externer Anmeldeinformationsspeicher“ aktiviert ist.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Derzeit ist CyberArk das einzige unterstützte externe Speichersystem.
Betrifft	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für **Spezielle MID-Server** angewendet werden sollen. MID Servers angeben, der diese Anmeldeinformationen im Feld „ **MID-Server** “ verwenden soll.
MID Server verwenden	Wählen Sie einen oder mehrere MID Server aus der Liste der verfügbaren MID Server aus. Die in diesem Datensatz konfigurierten Anmeldeinformationen stehen den MID Servern in dieser Liste zur Verfügung. Dieses Feld ist nur verfügbar, wenn Sie **Spezifische MID-Server** im Feld **Gilt für** auswählen.
Bestellung	Reihenfolge (Reihenfolge), in der Discovery diese Anmeldeinformationen bei dem Versuch, sich bei Geräten anzumelden, ausprobiert. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.

Befehle, die Stammberechtigungen für Discovery, Orchestration und IntegrationHub erfordern

Diese Beispiele setzen voraus, dass der Benutzername **Disco** lautet. Setzen Sie den tatsächlichen Benutzernamen ein, und stellen Sie sicher, dass die Pfade für die Befehle mit den Pfaden im System übereinstimmen.

Hinweis: Sudo-Befehle funktionieren nicht mit Anmeldeinformationen mit privaten Schlüsseln, da für den Sudo-Befehl kein Passwort angegeben werden muss. Eine Lösung ist das Hinzufügen der Option *NOPASSWD* zur Sudo-Konfiguration. Zum Beispiel könnten Sie Folgendes eingeben: `disco ALL=(root) NOPASSWD:/usr/sbin/dmidecode,/usr/sbin/lsof,/sbin/ifconfig`.

UNIX- und Linux-Befehle, für die Stammberechtigungen erforderlich sind

Befehl	Zweck
HP-UX	
adb	Erfasst CPU-Geschwindigkeit und Speicher. • **Beispiel einer /etc/sudoers-Zeile**: Disco ALL=(root) /usr/bin/adb • **Verwendet von:** Discovery

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

UNIX- und Linux-Befehle, für die Stammberechtigungen erforderlich sind (Fortsetzung)

Befehl	Zweck
Alle Linux- und UNIX-Versionen	
chage	Ändert die Anzahl der Tage zwischen Passwortänderungen und dem Datum der letzten Passwortänderung. • **Beispiel einer /etc/sudoers-Zeile**: Disco ALL=(root) /usr/bin/chage • **Verwendet von**: Orchestration und IntegrationHub
chpasswd	Ändert Benutzerpasswörter. • **Beispiel einer /etc/sudoers-Zeile**: Disco ALL=(root) /etc/chpasswd • **Verwendet von**: Orchestration und IntegrationHub
Alle Linux-Versionen	
dmidecode	Sammelt Informationen über die Hardware, einschließlich der Seriennummer des Motherboard. • **Beispiel einer /etc/sudoers-Zeile**: Disco ALL=(root) /sbin/ dmidecode • **Verwendet von:** Discovery
fdisk	Sammelt die Informationen über Datenträger und Größen im System. • **Beispiel einer /etc/sudoers-Zeile**: Disco ALL=(root) /usr/bin/fdisk -l • **Verwendet von:** Discovery
multipath	Sammelt Gerätezuordnungen für MPIO. • **Beispiel einer /etc/sudoers-Zeile**: Disco ALL=(root) /usr/bin/ multipath -ll • **Verwendet von:** Discovery
Linux und Solaris	
dmsetup	Untersucht einen Low-Level-Datenträger. • **Beispiel einer /etc/sudoers-Zeile**: ◦ Disco ALL=(root) /usr/bin/dmsetup table * ◦ Disco ALL=(root) /usr/bin/dmsetup ls • **Verwendet von:** Discovery
Alle UNIX-Versionen	
lsof	Ermittelt die Beziehung zwischen Prozessen und den Verbindungen, die zum System hergestellt werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

UNIX- und Linux-Befehle, für die Stammberechtigungen erforderlich sind (Fortsetzung)

Befehl	Zweck
	• **Beispiel einer /etc/sudoers-Zeile**: Disco ALL=(root) /sbin/lsof • **Verwendet von:** Discovery
oratab	Ermöglicht den Lesezugriff auf die oratab-Datei zum Auffinden von Oracle Home und der Parameterdatei (pfile). • **Beispiel einer /etc/sudoers-Zeile**: Nicht zutreffend • **Verwendet von:** Discovery
Solaris	
iscsiadm	Ruft iSCSI-IQNs ab • **Beispiel einer /etc/sudoers-Zeile**: ${sudo:iscsiadm list target -S} • **Verwendet von:** Discovery
fcinfo	Ruft WWPNs für Ports ab. • **Beispiel einer /etc/sudoers-Zeile**: ${sudo:fcinfo remote-port -sl -p $port} • **Verwendet von:** Discovery
prtvtoc	Liefert Informationen zu Datenträgerpartitionen. • **Beispiel einer /etc/sudoers-Zeile**: Disco ALL=(root) /usr/bin/prtvtoc • **Verwendet von:** Discovery
pfiles	Wird zum Sammeln von TCP-Verbindungsinformationen verwendet. • **/etc/sudoers** Zeilenbeispiel: Disco ALL=(root) /usr/bin/pfiles • **Verwendet von:** Discovery
pgrep	Wird verwendet, um Prozess-IDs einer bestimmten Region aufzulisten, für die Profile ausgeführt werden sollen. • **/etc/sudoers Zeilenbeispiel** : Disco ALL=(root) /usr/bin/pgrep • **Verwendet von:** Discovery
/usr/bin/ps	Führt laufende Prozesse auf. Fügen Sie als Alternative zur Ausführung mit Stammzugriff eine proc_owner-Rolle hinzu.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

UNIX- und Linux-Befehle, für die Stammberechtigungen erforderlich sind (Fortsetzung)

Befehl	Zweck
	• **Beispiel einer /etc/sudoers-Zeile**: Disco ALL=(root) /usr/bin/ps • **Verwendet von:** Discovery
/usr/ucb/ps	Führt laufende Prozesse auf. Fügen Sie als Alternative zur Ausführung mit Stammzugriff eine proc_owner-Rolle hinzu. Die Verwendung des Befehls `/usr/ucb/ps` ist ab Solaris 11 veraltet. Weil Discovery, Orchestration und IntegrationHub die Verwendung dieses Befehls für alle Solaris-Versionen erfordern, müssen Sie das ucb-Dienstprogramm auf Solaris 11-Systemen manuell installieren. Anweisungen dazu finden Sie in KB0564262 . • **Beispiel einer /etc/sudoers-Zeile**: Disco ALL=(root) /usr/ucb/ps • **Verwendet von:** Discovery

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service-Mappingbenötigen, finden Sie unter Service-Mapping -Befehle, die einen privilegierten Benutzer erfordern . Hier finden Sie auch eine Liste der Befehle, die erhöhte Berechtigungen zum Erkennen und Zuordnen von Unix-basierten Hosts in Ihrer Organisation erfordern.

Zugriffsanforderungen für Anmeldeinformationen ohne Root-Berechtigungen

Wenn Sie Discovery Anmeldeinformationen ohne Root-Zugriffsrechte erteilen, müssen Sie die folgenden Zugriffsanforderungen angeben.

Anwendung	Datei oder Verzeichnis	Erforderlicher Zugriff
Apache	httpd.conf	Lesen
Hbase	hbase-site.xml	Lesen
JBoss	jboss-service.xml	Lesen
	JBoss-Stammverzeichnis	Lesen
	web.xml	Lesen
MySQL	my.cnf	Lesen
NGINX	nginx.conf	Lesen
Oracle	oratab	Lesen
	Zugehörige Parameterdateien/ Serverparameterdateien	Lesen
Oracle-Listener	lsnrctl	Ausführen
	listener.ora	Lesen
Tomcat	catalina.jar	Lesen
	server.xml	Lesen
	web.xml	Lesen

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendung	Datei oder Verzeichnis	Erforderlicher Zugriff
Unix	/etc/*release	Lesen
	/etc/bashrc	Lesen
	/etc/profile	Lesen
	/proc/cpuinfo	Lesen
	/proc/vmware/sched/ncpus	Lesen
	/var/log/dmesg	Lesen
	APD-Verzeichnis	Lesen
WebSphere	cell.xml	Lesen
	server.xml	Lesen
	serverindex.xml	Lesen

VMware-Anmeldeinformationen

Der VMware-Anmeldeinformationstyp verwaltet den Zugriff auf vCenter-Anmeldeinformationen.

Anwendungen, mit denen auf VMware-Cloud-Ressourcen zugegriffen wird, benötigen Zugriff auf VMware-Anmeldeinformationen. Beispielsweise ermöglicht der Anmeldeinformationstyp „VMware“ Discovery, das auf einem Windows-Computer ausgeführte vCenter von VMware zu untersuchen, um ESX-Maschinen, virtuelle Maschinen und Ressourcenpools zu erkennen. VMware Discovery und die Automatisierungs-API (vCenter-API) stellen jetzt die global eindeutige Seriennummer für Computer-CIs bereit. CIM-Anmeldeinformationen sind nicht erforderlich, um den Zugriff auf jeden VMware-Host zu aktivieren.

Hinweis: Windows-Anmeldeinformationen sind für vCenter Discoverynicht erforderlich, wenn gültige VMware-Anmeldeinformationen verwendet werden.

Wichtig: Verwenden Sie Anmeldeinformationen vom Typ **VMware** nicht für Orchestration-Aktivitäten, die auf den einzelnen von vCenter geklonten virtuellen Maschinen Aufgaben ausführen (z. B. Neustarten einer Linux-VM). Für diese Aktivitäten hängt der **Typ** der Anmeldeinformationen vom Betriebssystem der virtuellen Maschine ab (entweder **SSH** oder **Windows**).

Formular für VMWare-Anmeldeinformationen

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für die VMware-Anmeldeinformationen ein.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Anwendername	Geben Sie den Anwendernamen ein, den Sie für Ihr VMware-Konto verwenden. Vermeiden Sie führende oder nachgestellte Leerzeichen in Benutzernamen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachgestellte Leerzeichen im Benutzernamen erkennt. Die VMware-Anmeldeinformationen müssen in vCenter über die Rolle mit Lesezugriff verfügen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular für VMWare-Anmeldeinformationen (Fortsetzung)

Feld	Beschreibung
Passwort	Geben Sie das Passwort für das VMware-Konto ein.
Betrifft	Wählen Sie einen oder mehrere MID Servers aus der Liste der verfügbaren MID Serversaus. Die in diesem Datensatz konfigurierten Anmeldeinformationen sind für MID Servers in dieser Liste verfügbar. Dieses Feld ist nur verfügbar, wenn Sie **Spezifische MID-Server** im Feld **Gilt für** auswählen.
Bestellung	Reihenfolge (Reihenfolge), in der Discovery diese Anmeldeinformationen bei dem Versuch, sich bei Geräten anzumelden, ausprobiert. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.

Windows-Anmeldeinformationen

Windows-Anmeldeinformationen ermöglichen den Zugriff auf Windows-Computer. Dieser Anmeldeinformationstyp ist für Discovery und Orchestration verfügbar.

Anforderungen für Anmeldeinformationen

Für Discovery und Orchestration gelten die folgenden Anforderungen für Windows-Anmeldeinformationen:

- Installieren Sie einen MID Server auf einem Windows-Host als Service.
- Fügen Sie einer der folgenden Stellen Windows-Anmeldeinformationen hinzu:
  - Einem Eintrag in der Tabelle „Anmeldeinformationen“ `[windows_credentials]`
  - Einem MID Server-Service-Account, der als bestimmter Windows-Benutzer oder als Domänen-Account ausgeführt werden soll.

Richtige Berechtigungen erteilen

Um ausreichende Berechtigungen bereitzustellen, müssen Windows-Anmeldeinformationen eines der folgenden sein:

- Ein Domänenbenutzer mit lokalem Administratorzugriff auf Windows-Zielhosts
- Ein lokaler Account mit Administratorrechten und deaktivierter Benutzerzugriffssteuerung (User Access Control, UAC) auf demselben Zielhost
- Ein Benutzer, der die Anforderungen von Windows Probes und Berechtigungen erfüllt (nurDiscovery).
- Ein Benutzer, der die Anforderungen der auszuführenden Orchestration-Aktivität erfüllt (nur Orchestration)

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Es sind keine Anmeldeberechtigungen erforderlich. Account muss NICHT interaktiv sein.

Die Sicherheit bei der Gewährung privilegierter Zugriffsrechte kann durch die Verwendung von JEA-Profilen zum Ausführen von Discoveryerhöht werden. Weitere Informationen finden Sie unter Microsoft Just Enough Administration (JEA) for Discovery .

Arbeitsgruppencomputer

Konfigurieren Sie die MID Server-Anmeldeinformationen für einen dieser Benutzer, um PowerShell-Befehle zum Ermitteln eines Arbeitsgruppencomputers auszuführen:

- Integrierter Administrator-Account auf dem Arbeitsgruppencomputer
- Domänenbenutzer auf dem Arbeitsgruppencomputer

Konfiguration für mehrere Domänen

Stellen Sie sicher, dass Sie die richtigen Namensformate und die richtige MID-Server-Konfiguration verwenden, damit Windows-Anmeldeinformationen für mehrere Domänen genutzt werden können.

Discovery und Orchestration unterstützen Windows-Domänenanmeldeinformationen der Benutzernamensformate **Benutzerprinzipalname** und **Kompatibler Anmeldename**. Zum Beispiel: **Domäne\Benutzername** oder **Benutzername@beispiel.domäne.com**. Sie können Anmeldeinformationen für Windows-Arbeitsgruppen im folgenden Format angeben: ARBEITSGRUPPE\Benutzername.

Hinweis: Sie können auch einen lokalen Account angeben, indem Sie den Benutzernamen **.** verwenden.

Diese zusätzlichen Aktionen sind erforderlich, damit die Anmeldeinformationen für mehrere Windows-Domänen verwendet werden können.

Bedingung	Zusätzlich erforderliche Aktionen
MID Server-Host in derselben Domäne wie das Windows-Ziel	Keine
MID Server-Host in einer anderen Domäne als das Windows-Ziel	Stellen Sie sicher, dass PowerShell 3.0 (oder höher bis 5.1) auf dem MID Server-Host installiert ist.
MID Server-Host in einer anderen Domäne als das Microsoft SQL Server-Ziel	Weitere Informationen finden Sie unter MSSQL-Server-Discovery .

Windows-Anmeldeinformationstyp

Diese Felder sind im Anmeldeinformationsformular für Windows verfügbar:

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Benutzername	Geben Sie den zu erstellenden Benutzernamen in die Tabelle „Berechtigungsnachweise“ ein. Vermeiden Sie führende oder nachgestellte Leerzeichen in Benutzernamen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachgestellte Leerzeichen im Benutzernamen erkennt. Für die CIM-Erkennung muss der Benutzer über die Administratorrolle verfügen.
Passwort	Geben Sie das Passwort ein.
Nachweis-ID	Geben Sie den für externe Anmeldeinformationen konfigurierten eindeutigen Schlüssel in der JAR-Datei ein, die für ein externes Anmeldeinformationssystem auf den MID Server hochgeladen wurde. Das Feld **Nachweis-ID** darf maximal 40 Zeichen lang sein. Dieses Feld ist nur sichtbar, wenn das Kontrollkästchen **Externer Anmeldeinformationsspeicher** aktiviert ist.
Alias für Anmeldeinformationen	Erlauben Sie Workflow-Erstellern, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuzuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu. Geben Sie den Tabellennamen für den CI-Typ ein, zu dem das CI gehört (z. B. cmdb_ci_apache_web_server), um die Anmeldeinformationen zur Erkennung von CIs zu verwenden, die nicht zu diesem CI-Typ gehören und dafür Service Mapping- und Discovery-Muster nutzen.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn Sie diese Option auswählen, werden die Felder **Benutzername** und **Passwort** durch das Feld **Nachweis-ID** ersetzt. Externe Anmeldeinformationsspeicher stehen nur zur Verfügung, wenn dasPlugin „Externer Anmeldeinformationsspeicher“ aktiviert ist. **Hinweis:** Derzeit ist CyberArk das einzige unterstützte externe Speichersystem.
Betrifft	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für **Spezielle MID-Server** angewendet werden sollen. MID Servers angeben, der diese Anmeldeinformationen im Feld „ **MID-Server** “ verwenden soll.
MID Server verwenden	Wählen Sie einen oder mehrere MID Server aus der Liste der verfügbaren MID Server aus. Die in diesem Datensatz konfigurierten Anmeldeinformationen stehen den MID Servern in dieser Liste zur Verfügung. Dieses Feld ist nur verfügbar, wenn Sie **Spezifische MID-Server** im Feld **Gilt für** auswählen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Die Auswahl von Spezifischen **Spezifischen MID-Servern** hat keine Auswirkungen auf die Auswahl der MID-Server. Es wird nur verwendet, um zu entscheiden, welche MID-Server für die Anmeldeinformationen sichtbar sein sollen. **Bestimmte MID-Server** werden in Orchestration-Aktivitäten nicht unterstützt.
Bestellung	Reihenfolge (Reihenfolge), in der Discovery diese Anmeldeinformationen bei dem Versuch, sich bei Geräten anzumelden, ausprobiert. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.
Windows-MID-Server-Servicekonto	Wenn sie aktiv sind, stellen die definierten Anmeldeinformationen das MID-Server-Servicekonto dar.

Windows-Anmeldeinformationen für den MID Server konfigurieren

Konfigurieren Sie den MID Server für die Verwendung der Anmeldeinformationen seines Windows-Service oder der Anmeldeinformationen aus der Tabelle „Anmeldeinformationen“ [discovery_credentials].

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Konfigurieren Sie den MID Server für die Verwendung von Anmeldeinformationen aus dem Service-Account des MID Servers.
   a. Legen Sie die Anmeldeinformationen für den Service MID-Server-Konfiguration für einen Benutzer fest, der die Berechtigungsanforderungen erfüllt.
   b. Stellen Sie sicher, dass der Benutzername den Namensformatanforderungen entspricht.
   c. Füllen Sie die entsprechenden Felder im Formular aus.
   d. Stellen Sie sicher, dass die Anmeldeinformationen den Anforderungen der Domäne entsprechen.
2. Konfigurieren Sie den MID Server für die Verwendung der Anmeldeinformationen aus der Tabelle „Anmeldeinformationen“ [discovery_credentials].

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Fügen Sie der Tabelle „Anmeldeinformationen“ `[windows_credentials]` Windows-Anmeldeinformationen hinzu.
   - Stellen Sie sicher, dass jede Anmeldeinformation die Berechtigungsanforderungen erfüllt.
   - Stellen Sie sicher, dass jeder Benutzername den Namensformatanforderungen entspricht.
   - Stellen Sie sicher, dass jede Anmeldeinformation den Windows-Domänenanforderungen entspricht.

b. Wahlweise: Konfigurieren Sie den MID-Server für die Verwendung von PowerShell, indem Sie den Parameter `mid.use_powershell` auf den Wert **true**festlegen.
Weitere Informationen finden Sie unter MID-Server konfigurieren .

c. Aktivieren Sie das Kontrollkästchen Windows-MID-Server-Service-Account, um Anmeldeinformationen zu erstellen, die den Windows-MID-Server-Service-Account so darstellen, dass er als bestimmter Windows-Anwender oder Domänen-Account ausgeführt wird.

Anmeldeinformationen für das Container-Image-Repository

Die Anmeldeinformationen für das Container-Image-Repository verwalten den Zugriff auf private Repositorys für das Scannen von Container-Images. Dieser Anmeldeinformationstyp ist für Discoveryverfügbar.

Diese Felder sind im Formular „Anmeldeinformationen“ für Anmeldeinformationen vom Typ „Image-Repository“ verfügbar.

Formular „Anmeldeinformationen für Container-Image-Repository“.

Feld	Beschreibung
Name	Vom Benutzer zugewiesener Anmeldeinformationsname.
Anwendername	Name des Anwenders mit Leseberechtigungen für das Repository.
Passwort	Passwort mit Leseberechtigungen für das Repository.
Repository	Vollqualifizierter Domänenname des Repositorys Beispiel: `docker.io/snow_images`.

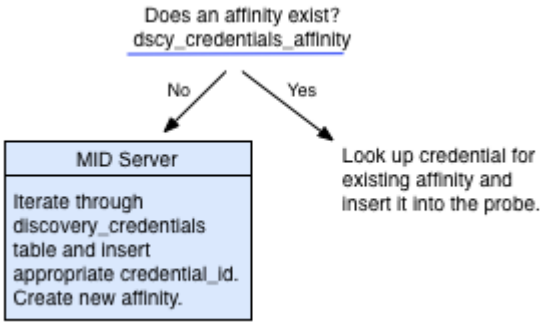
Berechtigungsaffinität für Discovery und Orchestration

Berechtigungsaffinität ist eine Verbindung zwischen einer Reihe von Anmeldeinformationen und einem Gerät im Netzwerk.

Beim ersten Versuch von Discovery oder Orchestration auf ein Gerät zuzugreifen, werden alle verfügbaren Anmeldeinformationen getestet, bis die richtigen gefunden werden. Nach der Ermittlung der Anmeldeinformationen für ein Gerät erstellen Discovery und Orchestration anhand der Tabelle „Anmeldeinformationsaffinität“ `[dscy_credentials_affinity]` eine Affinität zwischen den Anmeldeinformationen und dem Gerät. Bei allen nachfolgenden Ermittlungen oder Orchestration-Aktivitäten wird versucht, die Anmeldeinformationen in dieser Tabelle einem Gerät zuzuordnen, für das eine Affinität besteht. Wenn sich die Anmeldeinformationen für ein Gerät ändern, testen Discovery und Orchestration alle verfügbaren Anmeldeinformationen erneut, bis sie eine neue Affinität herstellen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Berechtigungsaffinitäts-Diagramm



Hinweis: Wenn Orchestration und Discovery installiert sind und der Anmeldeinformationsalias aktiviert ist, können mehrere Affinitäten vorhanden sein. In diesem Fall sucht die Plattform nach Anmeldeinformationen für jede Affinität und fügt die Anmeldeinformation für die Affinität mit der niedrigsten Reihenfolgenummer in die Probe ein.

Behebung von Fehlern bei Anmeldeinformationen

Überprüfen Sie den Abschnitt `<credentials_debug>` des ECC-Warteschlangen-Payload, um Probleme mit Anmeldeinformationen zu beheben.

Bestimmte Proben unterstützen das Debuggen von Anmeldeinformationen. Beim Debugging von Anmeldeinformationen wird der Abschnitt `<credentials_debug>` in das Payload eingefügt, das der MID Server an die Instanz-ECC-Warteschlange zurückgibt. Sie können den Abschnitt `<credentials_debug>` anzeigen, um detaillierte Informationen zur Suche nach Anmeldeinformationen zu erhalten.

Der Abschnitt `<credentials_debug>` erscheint im Payload, wenn:

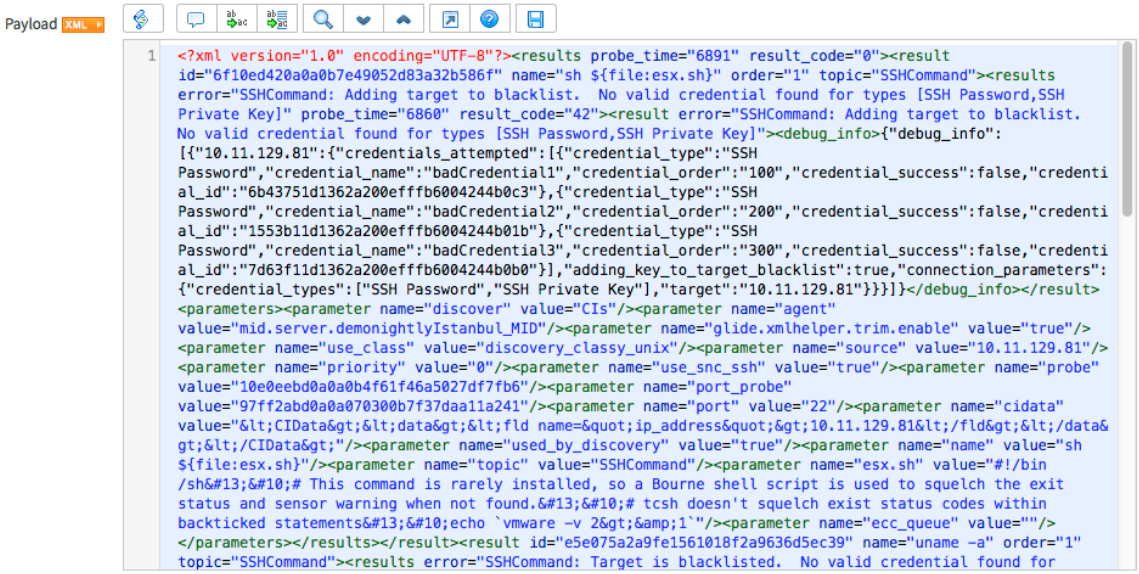
- Anmeldeinformationen für WMIRunner-Probe , PowerShell-Probe , JMS-oder SSHCommand-Probe fehl .
- Setzen Sie den Parameter *credentials_debug* für die WMIRunner-, PowerShell- oder SSHCommand-Proben auf **true**. Wenn Sie diesen Parameter auf „true“ setzen, wird der Abschnitt `<credentials_debug>` auch dann angezeigt, wenn die Suche nach Anmeldeinformationen erfolgreich war.

Der Abschnitt `<credentials_debug>` enthält:

- Informationen über die Suche nach Anmeldeinformationen, z. B. Anmeldeinformationstypen, Tags und Affinitäten.
- Die Ziel-IP-Adresse.
- Informationen zu allen Anmeldeinformationen (in der Reihenfolge), die der MID-Server verwendet hat, einschließlich Typ, Klassifizierung, Tag, Name, Sys-ID und der externen Anmeldeinformations-ID, falls vorhanden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel-Payload mit ungültigen Anmeldeinformationen



Details werden für den PowerShell-Parameter angezeigt:

- Wenn die lokalen MID-Server-Anmeldeinformationen verwendet wurden, nachdem alle Windows-Anmeldeinformationen fehlgeschlagen sind.
- Wenn die Anmeldeinformationen übersprungen wurden, da Sie versuchen, den Computer zu erkennen, auf dem sich der MID-Server befindet.
- Wenn der Parameter „mid.powershell.use_credentials“ auf „ `true`“ festgelegt ist.

Details werden für den SSH-Befehl angezeigt:

- Ob die Suche nach Anmeldeinformationen übersprungen wurde, da die Ziel-IP ausgeschlossen ist.
- Ob die Ziel-IP der Ausschlussliste hinzugefügt wurde.

Hinweis: Der MID-Server speichert IP-Adressen für fehlgeschlagene Anmeldeinformationssuchen in einer Ausschlussliste im Cache. Diese Ausschlussliste gibt an, auf welche Geräte der MID-Server keinen Zugriff versuchen soll. IP-Adressen werden der Ausschlussliste hinzugefügt, nachdem alle Anmeldeinformationen fehlgeschlagen sind. Die IP-Adressen werden entweder nach fünf Minuten aus dem Cache der Ausschlussliste gelöscht, wenn der MID-Server neu gestartet wird oder wenn die Anmeldeinformationsdatensätze in der Instanz aktualisiert werden.

Externer Anmeldeinformationsspeicher

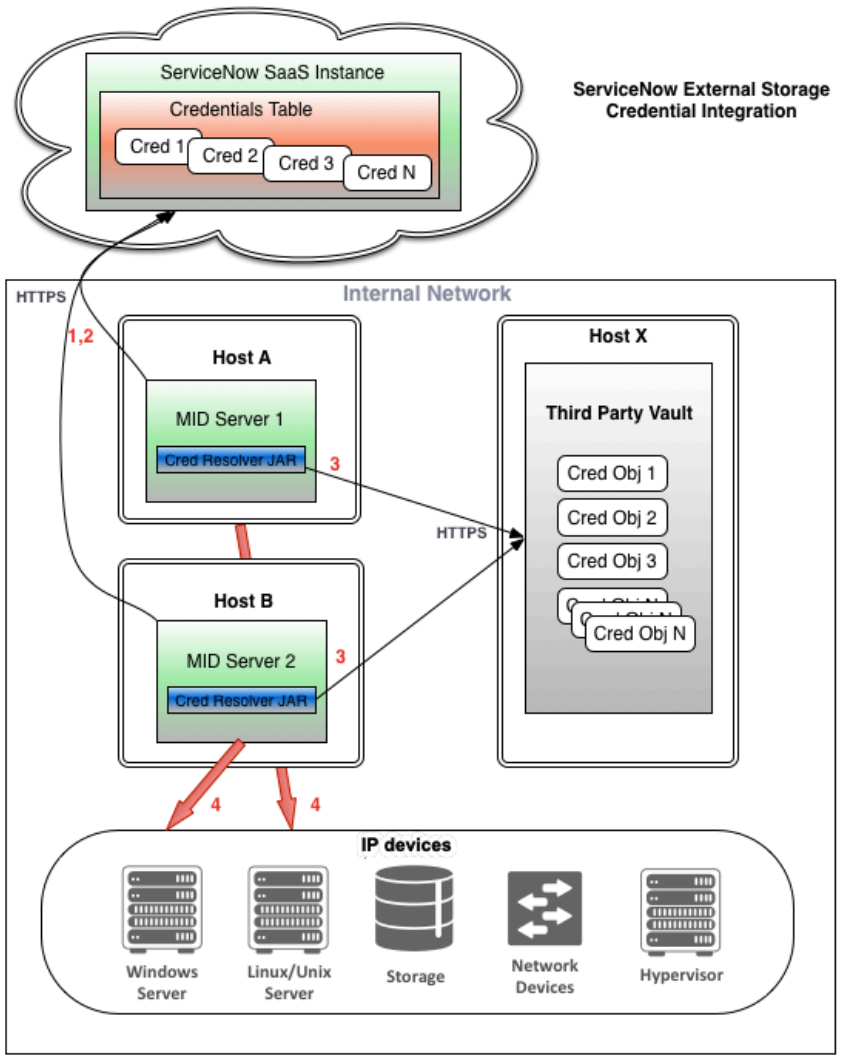
Eine Instanz kann Anmeldeinformationen, die von Discovery, Orchestration und Service-Mapping verwendet werden, in einem externen Anmeldeinformations-Repository anstatt direkt in einem ServiceNow-Anmeldeinformationsdatensatz speichern.

Die Instanz verwaltet einen eindeutigen Bezeichner für jede Anmeldeinformation, den Anmeldeinformationstyp (z. B. SSH, SNMP oder Windows) und alle Berechtigungsaffinitäten. Der MID Server erhält den Nachweis-Bezeichner von der Instanz und löst dann mithilfe einer vom Kunden bereitgestellten JAR-Datei den Bezeichner aus dem Repository in verwendbare Anmeldeinformationen auf. Derzeit unterstützt die Plattform ServiceNow® die Verwendung von CyberArk Vault oder „BeyondTrust“ für externen Anmeldeinformationsspeicher.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Architektur des externen Anmeldeinformationsspeichers

Architektur des externen Anmeldeinformationsspeichers



Prozessablauf für Anmeldeinformationen

Der MID Server ruft Anmeldeinformationen anhand dieses Prozesses aus einem externen Speicher ab:

1. Der MID Server lädt Anmeldeinformationsobjekte aus der ServiceNow-Tabelle „Anmeldeinformationen“ [discovery_credentials] herunter, die die entsprechende Nachweis-ID aus dem Zieltresor enthalten.
2. Während die Probes und Muster von den Aufträgen Discovery oder Orchestration ausgeführt werden, fordert der MID-Server die Anmeldeinformationen an, indem er Informationen wie Anmeldeinformations-ID, Ziel-IP-Adresse und Typ der Anmeldeinformationen an die Java-Jar-Datei des Anmeldeinformations-Resolvers übergibt. Die Details zum richtigen Anmeldeinformationsobjekt, das aus dem Tresor abgerufen werden soll, werden vom Resolver für Anmeldeinformationen bestimmt.

   Viele Resolver für Anmeldeinformationen wie CyberArk nennen eine Anwendung, die vom Drittanbieter-Vault-Anbieter bereitgestellt wird und auf demselben Computer wie der MID-Server ausgeführt wird. Diese Anwendung kann häufig so konfiguriert werden, dass Anmeldeinformationen zwischengespeichert werden, und weiß, dass der Cache

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aktualisiert wird, wenn sich Anmeldeinformationen im Tresor ändern. Dies ist sehr wichtig, um unnötige Netzwerkaufrufe beim Tresor zu vermeiden, wenn der MID-Server jedes Mal Anmeldeinformationen anfordert. Der Resolver für Anmeldeinformationen (unter Verwendung der optionalen Lieferantenanwendung, falls vorhanden) ruft den Tresor auf, um den tatsächlichen Anwendernamen, das Passwort usw. abzurufen.

Bei vordefinierten Resolvern für Anmeldeinformationen (heute nur CyberArk) speichert der MID Server Anmeldeinformationen nur bis zu mehreren Sekunden mithilfe der Verschlüsselung im Prozessspeicher des MID Servers. Dies bedeutet, dass der MID-Server für dieselben Anmeldeinformationen mehrere Anforderungen an den Resolver für Anmeldeinformationen stellen kann, selbst wenn ein einzelnes Gerät erkannt wird. Wenden Sie sich an Drittanbieter, um Informationen zum Zwischenspeichern von Implementierungen für andere Resolver für Anmeldeinformationen zu erhalten.

3. Der MID Server führt die Probe mit den entsprechenden Anmeldeinformationen aus.

Hinweis: Berechtigungsaffinitäten gelten weiterhin. Der Mechanismus bleibt derselbe, da der einzige wirkliche Unterschied aus Sicht des MID Servers darin besteht, dass die tatsächlichen Anmeldeinformationen (Benutzername und Passwort) aus dem Tresor einer Drittpartei stammen.

Protokollierung des externen Anmeldeinformationsspeichers

Der MID Server gibt Protokollnachrichten über den externen Anmeldeinformationsspeicher aus.

Wenn vom Repository beim Versuch, eine Anforderung für Anmeldeinformationen zu lösen, ein Fehler festgestellt wird, werden vom MID-Server Protokollnachrichten mit diesem Präfix ausgegeben: `Problem with client's CredentialResolver:` (Problem mit dem CredentialResolver des Clients).

Mit dem externen Anmeldeinformationsspeicher installierte Komponenten

Geschäftsregel

Mit der Geschäftsregel für externe Anmeldeinformationsspeicher werden die folgenden Aufgaben ausgeführt, wenn ein Administrator Änderungen an der Eigenschaft „Externen Anmeldeinformationsspeicher aktivieren“ vornimmt:

- Ändern der Ansicht für die Datensatzliste und des Formulars für Anmeldeinformationen in die Ansicht „Externer Speicher“. In dieser Ansicht können Anwender die Spalte **„Anmeldeinformations-ID** “ in der Liste anzeigen.
- Weist den MID-Server an, den Cache für Anmeldeinformationen zu aktualisieren. Dies dient der Vorbereitung auf eine geänderte Vorgehensweise zum Abrufen von Anmeldeinformationen.

Eigenschaft

Eine Eigenschaft namens Externen Anmeldeinformationsspeicher [com.snc.use_external_credentials] aktiviert oder deaktiviert das Plugin „Externer Anmeldeinformationsspeicher“, nachdem es aktiviert wurde. Die Eigenschaft befindet sich in **Discovery-Definition** > **Eigenschaften** und **Orchestration** > **MID-Server-Eigenschaften**, und werden aktiviert, wenn Sie das Plugin aktivieren.

Wenn Sie die Speicherung von externen Anmeldeinformationen mit der Systemeigenschaft deaktivieren, werden alle externen Anmeldeinformationen in der Instanz vom System automatisch auf inaktiv festgelegt. Wenn Sie die Funktion

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

mit dieser Eigenschaft erneut aktivieren, setzt das System die Datensätze für externe Anmeldeinformationen nicht auf „Aktiv“ zurück. Sie müssen jeden Anmeldeinformationsdatensatz manuell erneut aktivieren.

Fordern Sie einen externen Anmeldeinformationsspeicher für Discovery und Orchestration an

Das Plugin „Externer Anmeldeinformationsspeicher“ ist auf Anfrage erhältlich.

Vorbereitungen

Erforderliche Rolle: admin

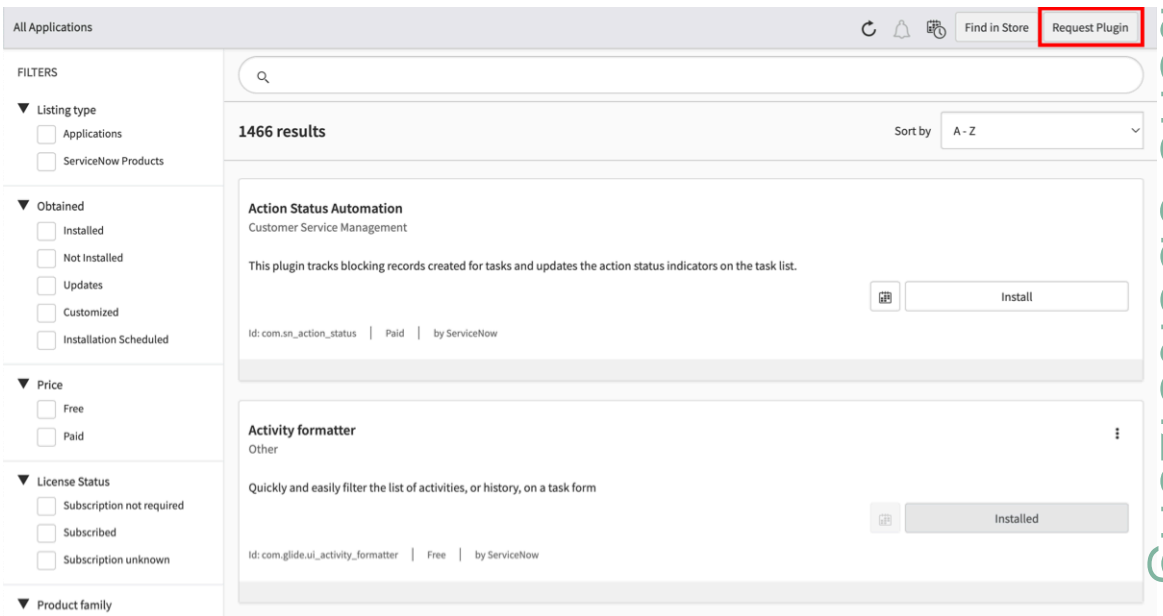
Warum und wann dieser Vorgang ausgeführt wird

Es gibt zwei Möglichkeiten, ein Plugin anzufordern:

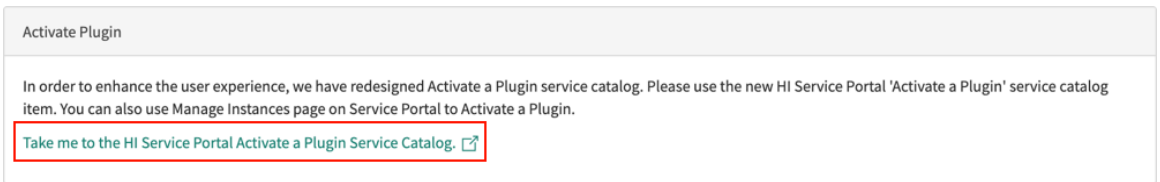
- Greifen Sie direkt auf den Now Support-Servicekatalog zu, indem Sie in Now Support auf **Alle** > **Servicekatalog** > **Plugin aktivieren** klicken.
- Greifen Sie über die Seite „Alle Anwendungen“ in Ihrer Instanz auf den Now Support-Servicekatalog zu, indem Sie die folgenden Schritte ausführen.

Prozedur

1. Navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Klicken Sie auf der Seite „Alle Anwendungen“ auf **Plugin anfordern**, um das Formular **Plugin aktivieren** auf Now Support zu öffnen.



3. Wählen Sie unter Now Support den Link aus, um auf Now Support Serviceportal Servicekatalog zuzugreifen.



4. Wählen Sie Ihre Instanz aus.
5. Wählen Sie **Aktionen > Plugin aktivieren** aus.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Geben Sie im Formular **Plugin aktivieren** die folgenden Informationen an.

Formular „Plugin anfordern“

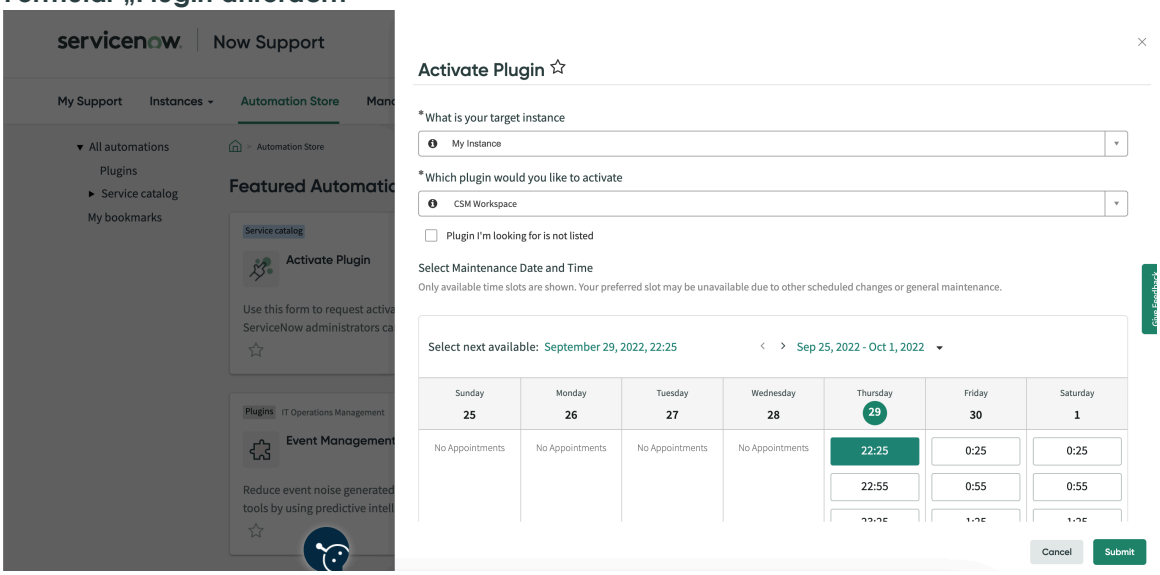
Feld	Beschreibung
What is your target instance (Ihre Zielinstanz)	Instanz, auf der das Plugin aktiviert werden soll.
Which plugin would you like to activate (Welches Plugin möchten Sie aktivieren?)	Name des zu aktivierenden Plugins **Hinweis:** Wenn das System das gewünschte Plugin nicht auflistet oder wenn Sie das Plugin auf einer OEM- oder lokalen Instanz aktivieren, aktivieren Sie das Kontrollkästchen **Plugin I'm looking for is not listed (Gesuchtes Plugin ist nicht aufgelistet)**, und geben Sie dann den Namen des Plugins ein.
Select Maintenance Date and Time (Datum und Uhrzeit der Wartung)	Datum und Uhrzeit zum Aktivieren des Plugins. **Hinweis:** Plugins werden in der pazifischen Zeitzone jeden Werktag in zwei Batches aktiviert, einmal am Morgen und einmal am Abend. Wenn das Plugin zu einem bestimmten Zeitpunkt aktiviert werden muss, geben Sie die Anforderung bei **Grund/ Kommentare** ein.

Example

Betrachten Sie beispielsweise das folgende Formular, um das Plugin „CSM Workspace“ in einer Instanz mit dem Namen „My Instance“ zu aktivieren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Plugin anfordern“



7. Wählen Sie **Absenden**.
   Weitere Informationen zum Anfordern eines Plugins finden Sie im Artikel Plugin aus dem Servicekatalog anfordern [KB0751715] in der Now Support Knowledge Base.

Konfiguration des externen Anmeldeinformationsspeichers

Konfigurieren Sie Ihre Instanz so, dass Anmeldeinformationen von einem Remote-Repository abgerufen werden.

Bei diesen Verfahren wird davon ausgegangen, dass Sie bereits ein externes Repository mit den Anmeldeinformationen konfiguriert haben, die Sie schützen möchten. Der in der ServiceNow-Instanz konfigurierte Nachweis-Bezeichner muss über die JAR-Datei den tatsächlichen Anmeldeinformationen im Repository zugeordnet werden.

Hinweis: ServiceNow unterstützt zwei externe Tresore gleichzeitig: einen standardmäßigen CyberArk-Anmeldeinformationslöser und einen anwenderdefinierten externen Anmeldeinformationslöser. Beim Erstellen eines anwenderdefinierten Resolvers für CyberArk-Anmeldeinformationen wird weiterhin der zweite, benutzerdefinierte externe Tresor verwendet, und es können keine zusätzlichen benutzerdefinierten externen Tresore verwendet werden.

Führen Sie zum Konfigurieren des externen Anmeldeinformationsspeichers die folgenden Aufgaben in der angegebenen Reihenfolge aus.

JAR-Datei zum Auflösen der Anmeldeinformationen erstellen

Erstellen Sie eine JAR-Datei, um die vom MID Server gesendeten Anmeldeinformationen in tatsächliche Anmeldeinformationen aus dem Repository aufzulösen.

Vorbereitungen

Erforderliche Rolle: agent_admin oder admin

Stellen Sie sicher, dass alle Anmeldeinformationen enthalten sind, die die Instanz erwartet, wie z. B. der private Schlüssel.

So erstellen Sie eine JAR-Datei zum Auflösen von Anmeldeinformationen:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

Verwenden Sie entweder die in GitHub ServiceNow bereitgestellten Vorlagen oder die Java-Beispieldatei.

⚠ **Vorsicht:** Diese Beispiele dienen nur als Vorlage. Verwenden Sie diesen Code **NICHT** in der Produktion, ohne ihn für Ihre Umgebung zu ändern.

a. Laden Sie die Open-Source-JAR-Dateien mit Anweisungen von GitHub ServiceNow herunter:

- HshiCorp-Resolver für externe Anmeldeinformationen
- CyberArk-Resolver für externe Anmeldeinformationen

b. Verwenden Sie die folgende Java-Beispieldatei als Vorlage, und passen Sie sie an Ihre Umgebung an:

Example

```
package com.snc.discovery;

import java.util.*;
import java.io.*;

/**
 * Basic implementation of a CredentialResolver that uses a properties
 file.
 */

public class CredentialResolver {

 private static String ENV_VAR = "CREDENTIAL_RESOLVER_FILE";
 private static String DEFAULT_PROP_FILE_PATH =
 "C:\\dummycredentials.properties";

 // These are the permissible names of arguments passed INTO the
 resolve()
 // method.

 // the string identifier as configured on the ServiceNow instance...
 public static final String ARG_ID = "id";

 // a dotted-form string IPv4 address (like "10.22.231.12") of the
 target
 // system...
 public static final String ARG_IP = "ip";

 // the string type (ssh, snmp, etc.) of credential as configured on
 the
 // instance...
 public static final String ARG_TYPE = "type";

 // the string MID server making the request, as configured on the
 // instance...
 public static final String ARG_MID = "mid";
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
// These are the permissible names of values returned FROM the
resolve()
// method.

// the string user name for the credential, if needed...
public static final String VAL_USER = "user";

// the string password for the credential, if needed...
public static final String VAL_PSWD = "pswd";

// the string pass phrase for the credential if needed:
public static final String VAL_PASSPHRASE = "passphrase";

// the string private key for the credential, if needed...
public static final String VAL_PKEY = "pkey";

// the string authentication protocol for the credential, if needed...
public static final String VAL_AUTHPROTO = "authprotocol";

// the string authentication key for the credential, if needed...
public static final String VAL_AUTHKEY = "authkey";

// the string privacy protocol for the credential, if needed...
public static final String VAL_PRIVPROTO = "privprotocol";

// the string privacy key for the credential, if needed...
public static final String VAL_PRIVKEY = "privkey";


private Properties fProps;

public CredentialResolver() {
}

private void loadProps() {
 if(fProps == null)
  fProps = new Properties();

 try {
  String propFilePath = System.getenv(ENV_VAR);
  if(propFilePath == null) {
   System.err.println("Environment var "+ENV_VAR+" not found. Using
default file: "+DEFAULT_PROP_FILE_PATH);
   propFilePath = DEFAULT_PROP_FILE_PATH;
  }

  File propFile = new File(propFilePath);
  if(!propFile.exists() || !propFile.canRead()) {
   System.err.println("Can't open "+propFile.getAbsolutePath());
  }
  else {
   InputStream propsIn = new FileInputStream(propFile);
   fProps.load(propsIn);
  }
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
 //fProps.load(CredentialResolver.class.getClassLoader().getResourceAsS
tream("dummycredentials.properties"));
  } catch (IOException e) {
   System.err.println("Problem loading credentials file:");
   e.printStackTrace();
  }
 }

 /**
  * Resolve a credential.
  */
 public Map resolve(Map args) {
  loadProps();
  String id = (String) args.get(ARG_ID);
  String type = (String) args.get(ARG_TYPE);
  String keyPrefix = id+"."+type+".";

  if(id.equalsIgnoreCase("misbehave"))
   throw new RuntimeException("I've been a baaaaaaaaad
 CredentialResolver!");

  // the resolved credential is returned in a HashMap...
  Map result = new HashMap();
  result.put(VAL_USER, fProps.get(keyPrefix + VAL_USER));
  result.put(VAL_PSWD, fProps.get(keyPrefix + VAL_PSWD));
  result.put(VAL_PKEY, fProps.get(keyPrefix + VAL_PKEY));
  result.put(VAL_PASSPHRASE, fProps.get(keyPrefix + VAL_PASSPHRASE));
  result.put(VAL_AUTHPROTO, fProps.get(keyPrefix + VAL_AUTHPROTO));
  result.put(VAL_AUTHKEY, fProps.get(keyPrefix + VAL_AUTHKEY));
  result.put(VAL_PRIVPROTO, fProps.get(keyPrefix + VAL_PRIVPROTO));
  result.put(VAL_PRIVKEY, fProps.get(keyPrefix + VAL_PRIVKEY));

  System.err.println("Error while resolving credential
 id/type["+id+"/"+type+"]");

  return result;
 }


 /**
  * Return the API version supported by this class.
  */
 public String getVersion() {
  return "1.0";
 }

 public static void main(String[] args) {
  CredentialResolver obj = new CredentialResolver();
  obj.loadProps();

  System.err.println("I spy the following credentials: ");
  for(Object key: obj.fProps.keySet()) {
   System.err.println(key+": "+obj.fProps.get(key));
  }
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
  }
}
```

JAR-Datei zum Auflösen der Anmeldeinformationen importieren

Importieren Sie eine JAR-Datei, um die vom MID Server gesendeten Nachweis-Bezeichner in tatsächliche Anmeldeinformationen aus dem Repository aufzulösen.

Vorbereitungen

Erforderliche Rolle: agent_admin oder admin

Nach dem Erstellen der JAR-Datei importieren Sie sie in die Instanz; dort kann der MID Server darauf zugreifen.

Prozedur

1. Kopieren Sie nach dem Erstellen der JAR- und Eigenschaftendateien die Eigenschaftendatei auf den MID Server.
2. Navigieren zu **MID-Server** > **JAR-Dateien**an.
3. Klicken Sie auf **Neu**.
4. Füllen Sie die folgenden Felder aus:

Feld	Beschreibung
Name	Ein eindeutiger und beschreibender Name zum Identifizieren der Datei in der Instanz.
Version	Eine Versionsnummer für die Datei, sofern verfügbar.
Quelle	Speicherort der JAR-Datei zu Referenzzwecken. Quellinformationen werden vom System nicht verwendet.
Beschreibung	Kurzbeschreibung der JAR-Datei und ihres Zwecks in der Instanz.

5. Klicken Sie auf das Büroklammersymbol im Banner, und hängen Sie die JAR-Datei an den Datensatz an.

   Example

   Eine JAR-Datei anhängen

6. Klicken Sie auf **Absenden**.
7. Starten Sie den MID-Server-Service neu.
   Die Plattform stellt die JAR-Datei jedem MID Server zur Verfügung, der für die Kommunikation mit der Instanz konfiguriert ist.

Nachweis-Bezeichner konfigurieren

Konfigurieren Sie den Nachweis-Bezeichner in der Instanz.

Vorbereitungen

Erforderliche Rolle: admin
Überprüfen Sie Folgendes:

- Das Plugin Externer Anmeldeinformationsspeicher muss aktiv sein.
- Die Discovery-Eigenschaft Externen Anmeldeinformationsspeicher aktivieren ist aktiviert.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Anmeldeinformationen** oder **Orchestration** > **Anmeldeinformationen**an.
2. Klicken Sie auf **Neu**.
3. Wählen Sie einen Anmeldeinformationstyp aus.
4. Aktivieren Sie das Kontrollkästchen **Externer Anmeldeinformationsspeicher**.
   Die Felder **Anwendername** und **Passwort** werden ausgeblendet, das Feld **Anmeldeinformations-ID** und das Menü „ **Anmeldeinformationsspeicherung – Tresor** “ werden angezeigt.
5. Wählen Sie im Menü Tresor für den **Anmeldeinformationsspeicher** entweder Keine, den CyberArk-Tresor oder einen anwenderdefinierten externen Anmeldeinformationsspeicher aus.

   Hinweis:

   Wenn CyberArk Vault ausgewählt ist, wird das Menü „ **Suchschlüssel** “ mit vier Suchschlüsseloptionen angezeigt: Anmeldeinformations-ID, IP-Adresse, FQDN usw. Wenn Sie Alle Optionen auswählen, kann dies die Leistung beeinträchtigen, da mehrmals auf den Tresor zugegriffen werden muss.

   a. Um einen anwenderdefinierten externen Anmeldeinformationsspeicher zu verwenden, navigieren Sie in der Instanz zu Tresorkonfigurationen [vault_configuration.list].

   b. Erstellen Sie einen neuen Datensatz mit einem Namen, der einer importierten JAR-Datei für einen anwenderdefinierten Resolver für Anmeldeinformationen zugeordnet ist.

   Informationen zum Erstellen eines anwenderdefinierten externen Anmeldeinformationsspeicher-Tresors finden Sie in den Verfahren JAR-Datei zum Auflösen der Anmeldeinformationen erstellen und JAR-Datei zum Auflösen der Anmeldeinformationen importieren.

6. Füllen Sie das Anmeldeinformationsformular mit den Feldern aus der folgenden Tabelle aus.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Nachweis-ID	Geben Sie den für externe Anmeldeinformationen in der JAR-Datei, die für ein externes Anmeldeinformationssystem auf den MID Server hochgeladen wurde, konfigurierten eindeutigen Schlüssel ein. Dies ist die ID, die an die Java-Klasse in der Parameterzuordnung übergeben wird: `public static final String ARG_ID = "id";` Der MID-Server verwendet diesen Identifier, um die tatsächlichen Anmeldeinformationen im Repositorium aufzulösen. **Hinweis:** Dieses Feld ist nur sichtbar, wenn das Kontrollkästchen **Externer Anmeldeinformationsspeicher** aktiviert ist.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Tag	Lassen Sie zu, dass Ersteller von Workflows, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn Sie diese Option auswählen, werden die Felder **Benutzername** und **Passwort** durch das Feld **Nachweis-ID** ersetzt. Externe Anmeldeinformationsspeicher stehen nur zur Verfügung, wenn das Plugin „Externer Anmeldeinformationsspeicher“ aktiviert ist.
Anmeldeinformationsspeicher-Tresor	Wählen Sie den Tresor mit externen Anmeldeinformationen aus einer Liste verfügbarer Tresore aus. Das Menü besteht aus Datensätzen aus den Tresorkonfigurationen [vault_configuration.list]. Neue Datensätze können hinzugefügt werden und Namen verwenden, die anwenderdefinierten JAR-Dateien des Anmeldeinformations-Resolvers zugeordnet sind. Informationen zum Erstellen eines anwenderdefinierten externen Anmeldeinformationsspeicher-Tresors finden Sie in den Verfahren JAR-Datei zum Auflösen der Anmeldeinformationen erstellen und JAR-Datei zum Auflösen der Anmeldeinformationen importieren.
Betrifft	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für einen oder mehrere **Spezielle MID-Server** angewendet werden sollen. Geben Sie im Feld **MID-Server** die MID-Server an, die diese Anmeldeinformationen verwenden sollen.
MID-Server	Wählen Sie einen oder mehrere MID Server aus der Liste der verfügbaren MID Server aus. Die in diesem Datensatz konfigurierten Anmeldeinformationen stehen den MID Servern in dieser Liste zur Verfügung. Dieses Feld ist nur verfügbar, wenn Sie **Spezifische MID-Server** im Feld **Gilt für** auswählen.
Bestellung	Geben Sie die Reihenfolge ein, in der die Plattform diese Anmeldeinformationen bei der Anmeldung bei Geräten testet. Je kleiner die Zahl, desto weiter oben werden diese Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Anmeldeinformationen ein, wenn Sie eine große Anzahl von Anmeldeinformationen verwenden oder wenn Benutzer nach drei fehlgeschlagenen Anmeldeversuchen von den Sicherheitsfunktionen gesperrt werden. Wenn alle Anmeldeinformationen dieselbe Nummer (oder keine) in der Reihenfolge haben, testet Discovery oder Orchestration die Anmeldeinformationen in zufälliger Reihenfolge.

7. Klicken Sie auf **Absenden**.

Nachweis-Bezeichner für AWS konfigurieren

Konfigurieren Sie Ihre Instanz so, dass Anmeldeinformationen von einem Remote-Repository abgerufen werden.

Vorbereitungen

Erforderliche Rolle: cloud_admin

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Stellen Sie sicher, dass diese Plugins aktiv sind und der MID-Server installiert wurde:

- Discovery [com.snc.discovery]
- Cloud Provisioning and Governance [com.snc.cloud.mgmt]
- Externer Anmeldeinformationsspeicher [com.snc.discovery.external_credentials]

Warum und wann dieser Vorgang ausgeführt wird

Bei diesen Verfahren wird davon ausgegangen, dass Sie bereits ein externes Repository mit den Anmeldeinformationen konfiguriert haben, die Sie schützen möchten. Der in der ServiceNow-Instanz konfigurierte Nachweis-Bezeichner muss über die JAR-Datei den tatsächlichen Anmeldeinformationen im Repository zugeordnet werden.

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Anmeldeinformationen**an.
2. Wählen Sie Anmeldeinformationen aus, die von Ihrem externen Anmeldeinformationsspeicher-Anbieter unterstützt werden.
3. Füllen Sie das Formular mit den Feldern aus der Tabelle aus.

Feld	Beschreibung
Name	Ein eindeutiger und beschreibender Name für diese Anmeldeinformationen. Zum Beispiel „Amazon Web Services“.
Betrifft	Wählen Sie die MID-Server aus, die diese Anmeldeinformationen verwenden können. Die Auswahlmöglichkeiten sind **Alle MID-Server** und **Bestimmte MID-Server**. Wenn Sie Letzteres auswählen, wird das Feld **MID-Server** angezeigt.
Aktiv	Kontrollkästchen zum Aktivieren oder Deaktivieren der Anmeldeinformationen.
AWS-Konto	Geben Sie Ihre AWS-Account-ID ein, wenn sich Ihre AWS-Anmeldeinformationen bei einem externen Speicheranbieter befinden.
MID-Server	Wählen Sie einen oder mehrere MID-Server aus, die diese Anmeldeinformationen verwenden können.
Anmeldeinformations-ID	Geben Sie den Namen ein, unter dem diese Anmeldeinformationen im externen Anmeldeinformationsspeicheranbieter gespeichert sind.
Datenschutz-Anmeldeinformations-ID	Geben Sie den Namen eines SNMPv3-Datenschutzschlüssels aus CyberArk ein. Dieses Feld ist für SNMPv3 nur sichtbar, wenn Sie im Feld **Anmeldeinformationsspeicher-Typ** die Option **CyberArk** auswählen. Wenn Sie keinen Datenschutzschlüssel für CyberArk verwenden, lassen Sie dieses Feld leer.
Anmeldeinformationsalias	Wählen Sie einen Alias für diese Anmeldeinformationen aus, der bestimmte Verhaltensweisen enthält. Weitere Informationen finden Sie unter Anmeldeinformationsaliasse für Discovery.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn ein externer Speicher aktiviert ist, wird das Feld

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Nachweis-ID angezeigt. Wenn dieses Kontrollkästchen nicht sichtbar ist, klicken Sie auf das Menüsymbol in der Kopfzeile, und wählen Sie **Ansicht** > **Externer Speicher** aus dem Kontextmenü.
Anmeldeinformationsspeicher Typ	Wählen Sie **CyberArk** nur aus, wenn Sie einen SNMPv3-Datenschutzschlüssel für CyberArk verwenden. Das Feld **Datenschutz-Anmeldeinformations-ID** wird zur Eingabe des Schlüssels angezeigt.

4. Klicken Sie auf **Absenden**.

CyberArk Integration des Anmeldeinformationsspeichers

Durch die Integration von MID-Server mit dem Tresor ServiceNow® OrchestrationCyberArk können [], ServiceNow® Discoveryund ServiceNow® Service-Mapping ausgeführt werden, ohne dass Anmeldeinformationen in der Instanz gespeichert werden.

Einführung in CyberArk

Das ProduktCyberArk Application Identity Management (AIM) nutzt die Lösung für die Sicherheit privilegierter Konten, um zu verhindern, dass Anwendungspasswörter eingebettet in Anwendungen, Skripts oder Konfigurationsdateien gespeichert werden, und ermöglicht die zentrale Speicherung, Protokollierung und Verwaltung dieser vertraulichen Passwörter im CyberArk.] Tresor. Dieser Ansatz ermöglicht es Organisationen, die internen und behördlichen Anforderungen hinsichtlich der periodischen Ersetzung von Passwörtern zu erfüllen und Aktivitäten zu überwachen, die mit allen Arten von privilegierten Identitäten verbunden sind, ob vor Ort oder in der Cloud.

Die Instanz verwaltet einen eindeutigen Bezeichner für jede Anmeldeinformation, den Anmeldeinformationstyp (z. B. SSH, SNMP oder Windows) und alle Anmeldeinformationsaffinitäten. MID-Server ruft den Bezeichner der Anmeldeinformationen, den Typ der Anmeldeinformationen und die IP-Adresse von der Instanz ab und verwendet dann den Tresor CyberArk, um diese Elemente in verwendbare Anmeldeinformationen zu konvertieren. Der Resolver für Anmeldeinformationen kann auch den Hostnamen und den FQDN suchen und die umgekehrte DNS-Suche verwenden, um den FQDN abzurufen.

Die Integration CyberArk erfordert das ServiceNow® Plugin Externer Anmeldeinformationsspeicher, das in verfügbar ist **Systemdefinitionen** > **Plugins**an. Der AIM/API-Client MID-Server und CyberArk müssen auf demselben Computer installiert sein. CyberArk Application Access Manager (AAM) Version 12.0.1 und höher für Anmeldeinformationsanbieter wird unterstützt.

Mit CyberArk installierte Komponenten

- **Business-Regel**: Die Business-Regel „Externer Anmeldeinformationsspeicher“ führt die folgenden Aufgaben aus, wenn ein Administrator Änderungen an der Eigenschaft „Externer Anmeldeinformationsspeicher“ vornimmt:
  - Ändern der Ansicht für die Datensatzliste und des Formulars für Anmeldeinformationen in die Ansicht „Externer Speicher“. In dieser Ansicht können Benutzer die Spalte „Nachweis-ID“ in der Liste sehen.
  - Weist MID-Server an, den Cache für nicht externe Anmeldeinformationen zu aktualisieren, als Vorbereitung auf eine Änderung der Art und Weise, wie Anmeldeinformationen abgerufen werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Systemeigenschaft**: Die Eigenschaft „Externen Anmeldeinformationsspeicher aktivieren“ [com.snc.use_external_credentials] aktiviert oder deaktiviert das Plugin „Externer Anmeldeinformationsspeicher“, nachdem es aktiviert wurde. Diese Eigenschaft befindet sich in**Discovery-Definition** > **Eigenschaften**und**Orchestration** > **MID-Server-Eigenschaften**, und werden aktiviert, wenn Sie das Plugin aktivieren.

  Hinweis: Wenn Sie die Einsatzbereitschaft des externen Anmeldeinformationsspeichers über die Systemeigenschaft widerrufen, setzt das System automatisch alle externen Anmeldeinformationen in der Instanz auf „Inaktiv“. Wenn Sie die Funktion mithilfe dieser Eigenschaft erneut in Einsatzbereitschaft versetzen, setzt das System die externen Anmeldeinformationsdatensätze nicht wieder auf „Aktiv“. Sie müssen jeden Anmeldeinformationsdatensatz manuell neu aktivieren.

Unterstützte Anmeldeinformationstypen

Die CyberArk -Integration unterstützt die folgenden ServiceNow -Anmeldeinformationstypen:

- GCP
- Azure
- CIM
- JMS
- SNMP-Forum
- SNMPv3
- Basisauth.
- SSH-Schlüsselpaar
- Privater SSH-Schlüssel (mit Schlüssel, Passphrase und Passwort)
- VMware
- Windows
- Applicative-Anmeldeinformationen

Hinweis: Um die Integration CyberArk mit dem Anmeldeinformationstyp GCP zu verwenden, müssen Sie die JAR-Datei für den externen Anmeldeinformationsspeicher ändern. Einzelheiten hierzu finden Sie unter ServiceNow GCP Credential Resolver with CyberArk (Resolver für Anmeldeinformationen von ServiceNow GCP mit CyberArk) .

Die FunktionenNow Platform, die diese Netzwerkprotokolle verwenden, unterstützen auch die Verwendung von Anmeldeinformationen, die in einem CyberArk -Tresor gespeichert sind.

Vom Netzwerkprotokoll unterstützte Anmeldeinformationen

Netzwerkprotokoll	ServiceNow® Flow Designer **Unterstützung**	Orchestration **-Unterstützung**
SOAP	SOAP-Schritt	Erstellt eine SOAP-Webservice-Aktivität mit Außerkraftsetzung der Standardauthentifizierung
REST	REST-Schritt	Erstellen Sie eine REST-Webservice-Aktivität mit Außerkraftsetzung der Standardauthentifizierung
JDBC	JDBC-Schritt	JDBC-Aktivität
SSH	SSH-Schritt	SSH-Aktivität

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vom Netzwerkprotokoll unterstützte Anmeldeinformationen (Fortsetzung)

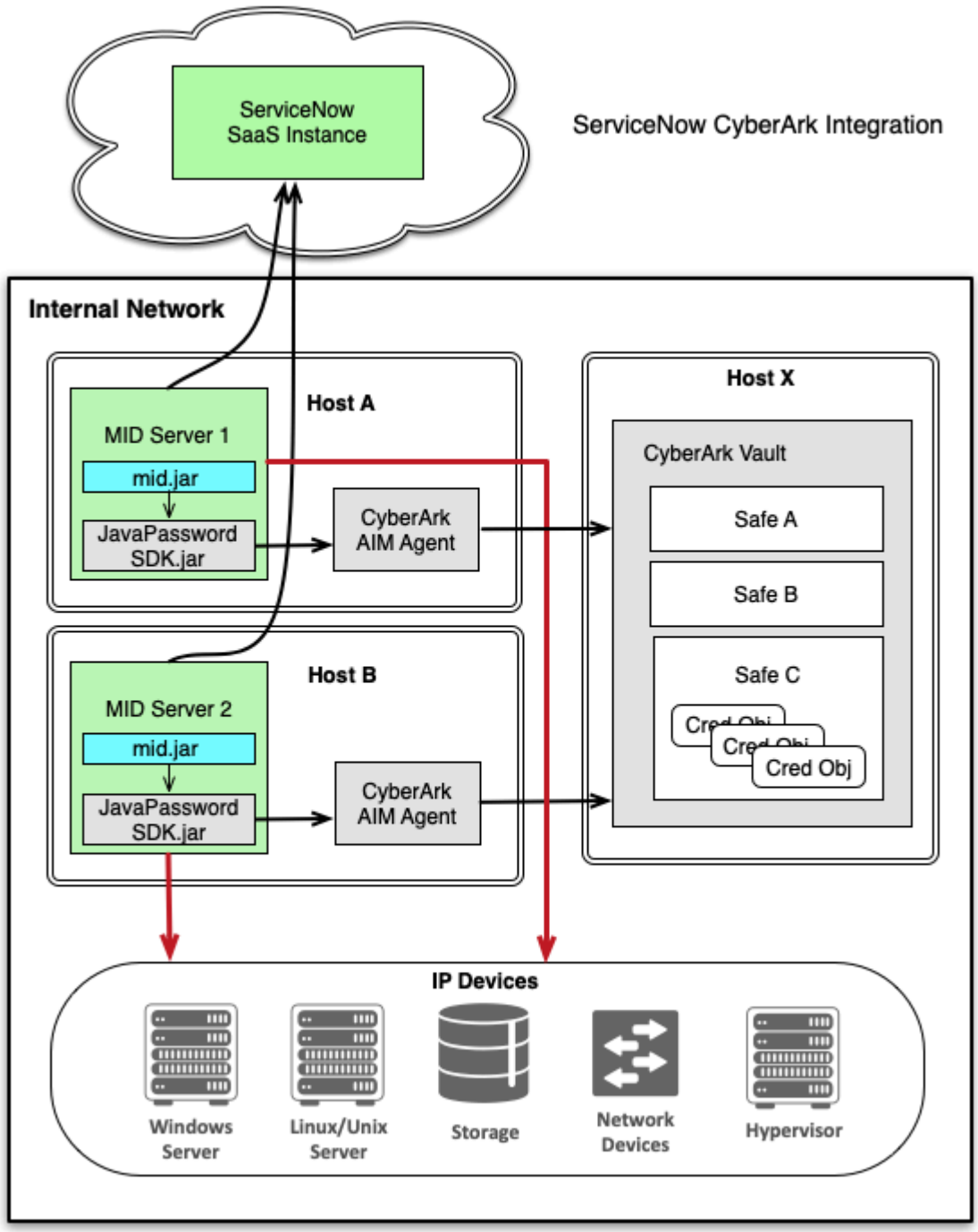
Netzwerkprotokoll	ServiceNow® Flow Designer **Unterstützung**	Orchestration **-Unterstützung**
PowerShell	PowerShell-Schritt	PowerShell-Aktivität
SFTP	SFTP-Schritt	SFTP-Aktivität
JMS		JMS-Aktivität

Wichtig: Sie können Anmeldeinformationen, die in einem CyberArk Tresor und einem anwenderdefinierten externen Anmeldeinformationsspeichersystem gespeichert sind, nicht mit demselben MID-Serververwalten. Der AIM/API-Client MID-Server und CyberArk müssen auf demselben Computer installiert sein.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CyberArk-Architektur

CyberArk Speicherarchitektur



Hinweis: CyberArk verwendet die *Basissystemdatei mid.jar* zum Auflösen von Anmeldeinformationen.

Wie der MID-Server mit den Accounts Windows umgeht

Die Suche nach Anmeldeinformationen versucht zunächst, die angegebene Anmeldeinformations-ID einem vorhandenen Wert im Feld **Name** des Tresors CyberArk zuzuordnen. Wenn eine Übereinstimmung gefunden wird, werden die

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anmeldeinformationen ausgegeben. Wenn keine Übereinstimmung gefunden wird, versucht die Anmeldeinformationssuche, mithilfe der IP-Adresse eine Übereinstimmung zu finden. Wenn die IP-Adressensuche mit mehreren Anmeldeinformationen übereinstimmt, z. B. Windows und Tomcat auf demselben Server, schlägt die Suche fehl. Um dieses Problem zu vermeiden, legen Sie den Parameter *ext.cred.type_specifier* in der Datei MID-Server config.xml auf „ **true** “ fest, um zu erzwingen, dass CyberArk Anmeldeinformationen zurückgibt, die dem Anmeldeinformationstyp und der IP-Adresse entsprechen. Wenn beispielsweise eine IP-Adresse von Windows und Tomcatgemeinsam genutzt wird, gibt der Anmeldeinformationstyp Windows nur die Anmeldeinformationen Windows zurück.

Aktualisieren Sie die Bibliothek CyberArk

Sie können die Bibliothek CyberArk upgraden, wenn ein gesicherter Konfigurationsparameter benötigt wird.

Überprüfen Sie die folgenden Konfigurationsparameter in der
Datei config.xml : <parameter name="mid.secure_config.provider" value="com.service_now.mid.services.config.CyberArkSecuredConfigProvider"/>

Führen Sie die folgenden Schritte aus, um das Upgrade durchzuführen, wenn ein gesicherter Konfigurationsparameter-Provider konfiguriert ist.

1. Benennen Sie die Client-Version CyberArk in `JavaPasswordSDK_MajorVersion_minorVersion_patchNum.jar`um.
2. Erstellen Sie einen neuen JAR-Eintrag in der Tabelle `„ecc_agent“`, in dem die umzubenennende JAR-Datei angehängt werden kann. Dieser neue Eintrag wird in MID-Serverheruntergeladen. Dieser Schritt führt zu zwei JAR-Dateien (Passworsdk.jar und JavaPasswordSDK _12_X_X.jar).
3. Löschen Sie den alten ecc_agent-Eintrag aus der Instanz. Dieser Schritt löscht PasswordSDK.jar aus MID-Server, und JavaPasswordSDK _12_X_X.jar verbleibt im System.

Konfiguration der CyberArk-Integration

Diese Verfahren umfassen sowohl Konfigurationsaufgaben für CyberArk als auch ServiceNow, einschließlich Verweisen auf die entsprechende CyberArk-Dokumentation.

Der in der ServiceNow-Instanz konfigurierte Nachweis-Bezeichner muss dem Anmeldeinformationsnamen im CyberArk-Tresor zugeordnet sein. Bei der Suche nach Anmeldeinformationen ermittelt der MID Server die Anmeldeinformationen durch den Abgleich des Nachweis-Bezeichners mit einem Namen im Tresor, der eindeutig sein muss. Wenn der Nachweis-Bezeichner leer ist, ermittelt der MID Server die Anmeldeinformationen anhand der IP-Adresse. Um die Anmeldeinformationen anhand der IP-Adresse zu ermitteln, prüft das System den Anmeldeinformationstyp, um sicherzustellen, dass sich an dieser Adresse nur eine Anmeldeinformation dieses Typs befindet. Ein Beispiel hierfür könnte die Ausführung eines Windows-Servers und von vCenter auf derselben IP-Adresse sein. Um die strengen Anforderungen für Anmeldeinformationen in einer SSH-Umgebung zu unterstützen, können Sie in einem MID Server-Konfigurationsparameter angeben, dass der angeforderte Anmeldeinformationstyp dem von CyberArk zurückgegebenen Typ entsprechen muss.

Hinweis: Das Feld **Anmeldeinformations-ID** ist in allen Fällen außer SNMPv3 das einzige Feld, das zum Zuordnen Ihrer Anmeldeinformationen zu CyberArk erforderlich ist. Das Feld **Datenschutz-Anmeldeinformations-ID** ist optional und nur erforderlich, wenn SNMPv3-Anmeldeinformationen verwendet werden und ein Datenschutzprotokoll für die Anmeldeinformationen verwendet wird. Unter CyberArk-Nachweis-Bezeichner konfigurieren finden Sie weitere Details.

Um Ihre Instanz so zu konfigurieren, dass Anmeldeinformationen von einem CyberArk-Tresor abgerufen werden, führen Sie diese Aufgaben in der angegebenen Reihenfolge aus.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CyberArk-Tresor konfigurieren und die AIM-API installieren

Konfigurieren Sie den CyberArk-Tresor so, dass er dem MID Server Zugriff gewährt, und installieren Sie die CyberArk AIM-API auf dem MID Server-Computer.

Vorbereitungen

Erforderliche Rolle: admin
Bevor Sie mit diesem Verfahren beginnen, stellen Sie sicher, dass das Plugin „Externer Anmeldeinformationsspeicher“ aktiviert ist. CyberArk Application Access Manager (AAM) Version 12.0.1 und höher für Anmeldeinformationsanbieter wird unterstützt.

Prozedur

1. Konfigurieren Sie den CyberArk-Tresor mit der Anwendungs-ID und den Authentifizierungsdetails, die alle MID Server, die Anmeldeinformationen anfordern, verwenden.
   Weitere Informationen finden Sie im Handbuch „CyberArk Credential Provider and ASCP Implementation“.

   a. Konfigurieren Sie CyberArk so, dass der MID Server auf den Tresor zugreifen kann, indem Sie in CyberArk die App-ID *ServiceNow_MID_Server* erstellen.

   b. Stellen Sie sicher, dass jede Anmeldeinformation, die der MID Server benötigt, Zugriff auf die App-ID *ServiceNow_MID_Server* erhält.

      Hinweis: Sie können die Standard-App-ID **ServiceNow_MID_Server** in der MID-Server-Datei `config.xml` mit dem Parameter ext.cred.app_id überschreiben. Wenn Sie den Wert in diesem Parameter ändern, müssen Sie einen entsprechenden Wert im Tresor konfigurieren.

2. Installieren Sie den Credential Provider von CyberArk, einschließlich der AIM-API, auf jedem Computer, der einen für den Zugriff auf den Anmeldeinformationsspeicher verwendeten MID Server-Service hostet.
3. Stellen Sie CyberArk-Accounts bereit, und legen Sie Berechtigungen für den Anwendungszugriff fest.
   Weitere Informationen finden Sie im Handbuch „CyberArk Privileged Account Security Implementation“.

   a. Erstellen Sie in CyberArk-Passwortsafe die privilegierten Accounts, die von Discovery, Orchestration oder Service Mapping für den Zugriff auf verschiedene Geräte benötigt werden, und stellen Sie sicher, dass diese Accounts zu den Safes gehören, in denen die erforderlichen Anmeldeinformationen gespeichert sind.

   b. Fügen Sie den Credential Provider und die Anwendungsbenutzer als Mitglieder der Passwortsafes hinzu, in denen die Anwendungspasswörter gespeichert werden.

CyberArk-JAR-Datei importieren

Importieren Sie die CyberArk-Datei „JavaPasswordSDK.jar“ in die Instanz, damit der MID Server darauf zugreifen kann.

Vorbereitungen

Erforderliche Rolle: agent_admin oder admin
Bevor Sie mit diesem Verfahren beginnen, müssen Sie CyberArk so konfigurieren, dass der MID Server auf Anmeldeinformationen zugreifen kann. Stellen Sie sicher, dass die CyberArk AIM-API auf jedem Server installiert ist, auf dem sich ein MID Server befindet, der für den Zugriff auf den Tresor verwendet wird.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Verwenden Sie diesen Prozess auch, wenn die Datei „JavaPasswordSDK.jar“ bereits auf dem MID Server vorhanden ist.

Prozedur

1. Navigieren zu **Alle** > **MID-Server** > **JAR-Dateien**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie das Formular aus, indem Sie die Felder in der Tabelle verwenden.

Formularfelder für die JAR-Datei

Feld	Beschreibung
Name	Eindeutiger und beschreibender Name zur Identifizierung der Datei in der Instanz.
Version	Optionale Versionsnummer für die Datei, sofern verfügbar.
Quelle	Provider der JAR-Datei. Quellinformationen werden vom System nicht verwendet.
Beschreibung	Optionale Kurzbeschreibung der JAR-Datei und ihres Zwecks in der Instanz.

4. Hängen Sie die JAR-Datei an diesen Datensatz an.
   Die AIM-Datei `JavaPasswordSDK.jar` wird mit den AIM-SDK-Installationsdateien geliefert und befindet sich normalerweise auf dem MID-Server im AIM-Installationsverzeichnis unter `<Installationsverzeichnis>/CyberArk/ApplicationPasswordSdk`.
5. Klicken Sie auf **Absenden**.
6. Starten Sie den MID-Server-Service neu.
   Die Plattform stellt die JAR-Datei jedem MID Server zur Verfügung, der für die Kommunikation mit der Instanz konfiguriert ist.

MID Server für CyberArk konfigurieren

Konfigurieren Sie die Datei `config.xml`, um dem MID Server Zugriff auf den CyberArk-Tresor zu gewähren.

Vorbereitungen

Erforderliche Rolle: admin
Bevor Sie dieses Verfahren beginnen, müssen Sie die Datei `JavaPasswordSDK.jar` in die Instanz importieren.

Prozedur

MID-Server manuell konfigurieren Fügen Sie eine MID-Server-Parameterdatei mit diesen Parametern hinzu.

Diese Konfiguration kann nicht von der Instanz vorgenommen werden.

Erforderliche Konfigurationsparameter

Parameter	Wert	Beschreibung
ext.cred.safe_folder	NameOfFolder	Ordner für alle Suchen nach Anmeldeinformationen. Zum Beispiel: **root**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Wert	Beschreibung
ext.cred.use_cyberark	true	Boolescher Parameter, der angibt, dass dieser MID Server in CyberArk integriert ist.

Optionale Konfigurationsparameter

Parameter	Wert	Beschreibung
ext.cred.safe_timeout	5 (Sek.)	Zeitüberschreitung in Sekunden für jede Suche nach Anmeldeinformationen im Tresor.
ext.cred.safe_name	NameOfSafe	Standardname des Safes, der für alle Suchen nach Anmeldeinformationen verwendet wird. Wenn sich Parameter in mehreren Safes befinden, kann die Nachweis-ID im Format *<safeName>:<CredentialID>* angegeben werden. Bei dieser Konfiguration wird das Feld **NameOfSafe** ignoriert. Wenn für alle externen Anmeldeinformationen die Nachweis-IDs in diesem Format angegeben sind, lassen Sie das Feld **NameOfSafe** aus. **Hinweis:** Standardmäßig ist das Trennzeichen in diesem Format ein Doppelpunkt. Um ein beliebiges Zeichen als Trennzeichen zuzuweisen, fügen Sie diese Zeile der Datei `CredMap.properties` hinzu: `safe.cred.split.string = <Zeichenfolge>`.
ext.cred.app_id	ServiceNow_MID_Server	Gibt die App-ID an, mit der dem MID-Server die Berechtigung zum Zugriff auf den CyberArk-Tresor erteilt wird. Der Standardwert **ServiceNow_MID_Server** muss im CyberArk-Tresor definiert sein. Mit diesem Parameter können Sie den Standardwert überschreiben und eine eigene App-ID angeben. Wenn Sie die App-ID in diesem Parameter bearbeiten, müssen Sie CyberArk entsprechend konfigurieren.
ext.cred.type_specific	wahr	Erzwingt, dass die IP-Adressen-Suche Anmeldeinformationen ausgibt, die sowohl mit der CyberArk-Plattform-ID als auch mit der IP-Adresse übereinstimmen. Wenn zum Beispiel eine IP-Adresse von Windows und Tomcat gemeinsam genutzt wird, geben Anmeldeinformationen mit einer Plattform-ID, die mit **Win** beginnt, nur die Windows-Anmeldeinformationen zurück. Wenn dieser Parameter auf „true“ festgelegt ist,

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Wert	Beschreibung
		sucht CyberArk nach Plattform-IDs, die mit Folgendem beginnen: • Win: Windows • Unix: SSH • VMWare: VMware
ext.cred.check_ssh_type	false	Ist der Wert auf „true“ festgelegt, müssen die von CyberArk zurückgegebenen SSH-Anmeldeinformationen mit dem angeforderten Anmeldeinformationstyp übereinstimmen. Wenn beispielsweise normale SSH-Anmeldeinformationen mit Benutzername/Passwort angefordert werden und nur SSH-Schlüssel verfügbar sind, schlägt die Suche nach Anmeldeinformationen fehl.

CyberArk für SNMPv2-Anmeldeinformationen konfigurieren

Wenn Ihr System SNMPv2 verwendet, können Sie eine spezielle Datei erstellen, um das Attribut in Anmeldeinformationen der Community-Zeichenfolge zuzuordnen.

Vorbereitungen

Erforderliche Rolle: admin
Bevor Sie dieses Verfahren beginnen, müssen Sie den MID Server für den Zugriff auf den CyberArk-Tresor konfigurieren.

Warum und wann dieser Vorgang ausgeführt wird

Hinweis: Wenn die Community-Zeichenfolge im Passwortfeld der CyberArk-Anmeldeinformationen angezeigt wird, ist es nicht erforderlich, dieses Verfahren auszuführen.

SNMPv2 wird in CyberArk nicht nativ unterstützt. Wenn Ihre Organisation benutzerdefinierte SNMPv2-Anmeldeinformationen erstellt hat, bei denen die Community-Zeichenfolge nicht im Passwortfeld der Anmeldeinformationen angezeigt wird, verwenden Sie dieses Verfahren, um das Attribut in den Anmeldeinformationen der Community-Zeichenfolge zuzuordnen.

Prozedur

1. Erstellen Sie in einem Texteditor eine Datei mit dem Namen `CredMap.properties` mit diesem Code:
   `SNMPv2.Community=attribute_name`
2. Speichern Sie die Datei im Verzeichnis `/agent` Ihrer MID Server-Installation.
   Beim Suchen nach Anmeldeinformationen versucht der MID Server, dieses Attribut für die Anmeldeinformationen zu finden. Wenn das Attribut nicht gefunden wird, sucht der MID Server im Passwortfeld. Wenn das Passwortfeld leer ist, schlägt die Suche nach Anmeldeinformationen fehl.

CyberArk-Nachweis-Bezeichner konfigurieren

Erstellen Sie den eindeutigen Schlüssel, mit dem CyberArk bestimmte Anmeldeinformationen im externen Repository identifizieren kann.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: admin

Bevor Sie mit diesem Verfahren beginnen, müssen Sie das Plugin „Externer Anmeldeinformationsspeicher“ aktivieren und die Systemeigenschaft com.snc.use_external_credentials auf „true“ setzen.

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Anmeldeinformationen** oder **Orchestration** > **Anmeldeinformationen**an.
2. Klicken Sie auf **Neu**.
3. Wählen Sie aus der Liste der Anmeldeinformationstypen einen Typ aus, der den externen Speicher von CyberArk unterstützt.
4. Füllen Sie das Formular mit den Feldern des Anmeldeinformationstyps aus.
5. Aktivieren Sie das Kontrollkästchen **Externer Anmeldeinformationsspeicher**.
   Die Felder **Benutzername** und **Passwort** werden durch das Feld **Nachweis-ID** ersetzt.

   Hinweis: Wenn das Kontrollkästchen nicht sichtbar ist, klicken Sie auf das Menüsymbol in der Kopfzeile, und wählen Sie **Ansicht** > **Externer Speicher**an.

6. Geben Sie im Feld **Nachweis-ID** einen Ausdruck in einem der folgenden Formate ein:
   - Wenn sich alle Anmeldeinformationen im selben Safe befinden, konfigurieren Sie diesen Safe-Namen in der MID-Server-Datei `config.xml` mit dem Parameter ext.cred.safe_name, und geben Sie die Nachweis-ID nur mit dem Namen als **<Nachweis-ID>** an.
   - Um die Anmeldeinformationen für eine Plattform zu benennen, die sich in einem bestimmten Safe befinden, definieren Sie die Nachweis-ID als **<Safe>:<Nachweis-ID>:<Plattform-ID>**.
   - Wenn sich die Anmeldeinformationen in mehreren Safes befinden, geben Sie die Nachweis-ID in diesem Format an: **<Safe>:<Nachweis-ID>**.
   - Wenn CyberArk die Anmeldeinformationen anhand der IP-Adresse suchen soll, verwenden Sie einen alternativen Safe, und geben Sie die Nachweis-ID in diesem Format an: **<Safe>:**.
   - Wenn CyberArk die Anmeldeinformationen für eine alternative Plattform-ID im selben Safe suchen soll, verwenden Sie dieses Format: **::<Plattform-ID>**
   - Wenn CyberArk die Anmeldeinformationen in einem konfigurierten Safe anhand der IP-Adresse anstelle der Nachweis-ID suchen soll, lassen Sie dieses Feld leer. Dies ist die Best Practice für Installationen, bei denen jeder Server über eindeutige Anmeldeinformationen verfügt. Ohne diese Art von Suche müssen Sie in Ihrer Instanz für jeden Server in der Umgebung einen Nachweis-ID-Datensatz erstellen.

   Hinweis: Die Anmeldeinformations-ID muss mit dem Wert im Feld „ **Name** “ für das CyberArk-Konto übereinstimmen. Das Feld **„Anmeldeinformations-ID“ darf maximal** 180 Zeichen lang sein.

7. Wenn Sie SNMPv3-Anmeldeinformationen in CyberArk speichern und das Datenschutzprotokoll und den Datenschutzschlüssel verwenden, konfigurieren Sie die ID wie folgt:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie im Feld **Anmeldeinformationsspeicher-TypCyberArk aus**.
Das Feld **Datenschutz-Anmeldeinformations-ID** wird angezeigt.

b. Geben Sie im Feld **Datenschutz-Anmeldeinformations-ID** den **Namen** des CyberArk SNMPv3-Datenschutzkontos ein.

8. Klicken Sie auf **Absenden**.

AWS-Anmeldeinformationen in einem CyberArk-Tresor konfigurieren

Konfigurieren Sie Ihren CyberArk-Tresor mit den AWS-Anmeldeinformationen, die für die Verwendung durch Ihre Instanz abgerufen werden sollen.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Speichern Sie die Anmeldeinformationen im CyberArk-Tresor als SSH-Schlüssel. Wenn Sie den Zugriff auf den Tresor in Ihrer Instanz konfigurieren, muss der Name, den Sie dem SSH-Schlüssel geben, auch als Nachweis-ID verwendet werden.

Prozedur
1. Wechseln Sie in CyberArk zu **Accounts** > **SSH-Schlüssel hinzufügen**an.
2. Geben Sie die folgenden Informationen ein:

CyberArk-Anmeldeinformationen

Feld	Wert
Gerätetyp	Wählen Sie **Cloud Service** aus.
Plattformname	Wählen Sie **Amazon Web Services - AWS - Access Keys** aus.
AWS Zugangsschlüssel-ID	Geben Sie den AWS-Zugriffsschlüssel, wie von AWS bereitgestellt, ein.
AWS IAM-Anwendername	Geben Sie den AWS-Zugriffsschlüssel erneut ein, wie von AWS bereitgestellt.
Passwort	Geben Sie den geheimen AWS-Zugangsschlüssel, wie von AWS bereitgestellt, ein.
Name	Geben Sie einen Namen für diesen Schlüssel ein.

3. Klicken Sie auf **Save**.

Nächste Maßnahme
Wenn Sie dies noch nicht getan haben, erstellen Sie in Ihrer Instanz einen Nachweis-Identifier, um den Zugriff auf den CyberArk-Tresor zu konfigurieren. Weitere Einzelheiten finden Sie unter Zugriff auf den externen Anmeldeinformationsspeicher für AWS konfigurieren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie Azure-Anmeldeinformationen in einem CyberArk-Vault

Konfigurieren Sie Ihren CyberArk-Tresor mit den Azure-Anmeldeinformationen, die zur Verwendung durch Ihre -Instanz abgerufen werden sollen.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Um Azure-Anmeldeinformationen zu speichern, erstellen Sie zuerst eine Azure-Anmeldeinformationsvorlage im CyberArk-Tresor. Dieser Prozess muss für den Tresor nur einmal abgeschlossen werden.

Prozedur

1. Melden Sie sich im Administrationsmodus bei CyberArk an.
2. Navigieren Sie zur Registerkarte **Administration**.
3. Bearbeiten Sie in **SystemkonfigurationPlattformmanagement**.
4. Navigieren Sie zu **Cloud-Provider Vorlage** und duplizieren Sie sie.
5. Bearbeiten Sie die Vorlage für Azure-Anmeldeinformationen.
6. Fügen Sie die folgenden beiden Eigenschaften hinzu:
   - *Name* als *Username* und *Display Name* als *Client ID*
   - *Name* als *Address* und *DisplayName* als *Tenant ID*
7. Wenden Sie die Änderungen an.
8. Navigieren Sie zum Abschnitt „ **Account** “, und wählen **Sie Account hinzufügen**aus.
9. Wählen Sie **Sicher aus**.
10. Legen Sie den **Gerätetyp** auf **Cloud-Service fest**.
11. Wählen Sie die zuvor bearbeitete Azure-Vorlage aus.
12. Füllen Sie die Informationen in für die Felder **Client-ID**, **Mandanten-ID**und **Passwort** aus.
13. Wählen Sie **Speichern**.

OAuth 2.0-Authentifizierung über MID-Server mit externem Anmeldeinformationsspeicher

Speichern Sie die OAuth 2.0-Anmeldeinformationen – Client-ID und Clientschlüssel – im Tresor CyberArk anstelle der Instanz ServiceNow. MID-Server ruft die Anmeldeinformationen aus dem Tresor CyberArk ab, wenn dies zum Abrufen des OAuth-Tokens erforderlich ist. Das Token wird auf dem MID Server gespeichert und bei Ablauf automatisch aktualisiert.

Das Produkt CyberArk Application Identity Management (AIM) nutzt die Lösung für die Sicherheit privilegierter Konten, um zu verhindern, dass Anwendungspasswörter eingebettet in Anwendungen, Skripts oder Konfigurationsdateien gespeichert werden, und ermöglicht die zentrale Speicherung, Protokollierung und Verwaltung dieser Passwörter in der CyberArk Tresor. Sie können den Tresor CyberArk so konfigurieren, dass OAuth 2.0-Anmeldeinformationen anstatt direkt in einem ServiceNow -Anmeldeinformationsdatensatz gespeichert werden. Weitere Informationen zu CyberArk finden Sie unter CyberArk Integration des Anmeldeinformationsspeichers.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Architektur der OAuth 2.0-Authentifizierung der MID-Server -Anforderung

Sie besteht aus zwei Teilen: der Instanz ServiceNow und der Umgebung, in der der AIM-Client (Application Identity Manager) und der MID Server konfiguriert werden. Beispiele für Umgebungen sind die Cloud oder eine Kundenumgebung.

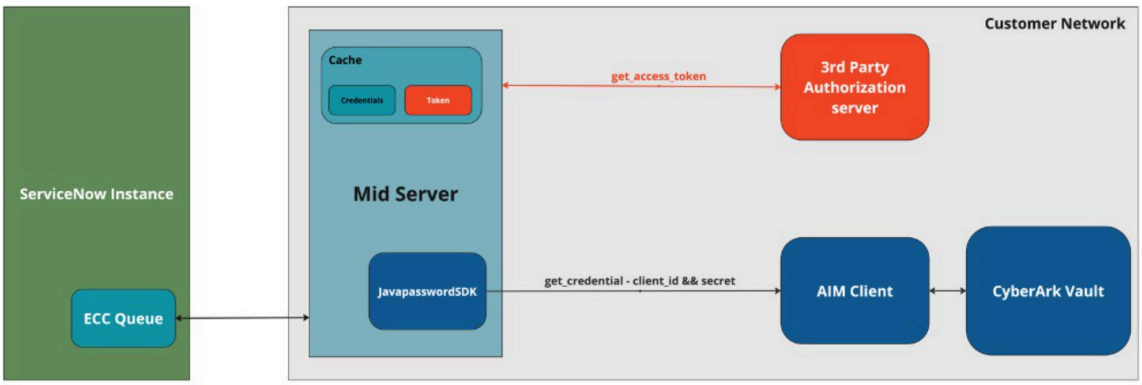
MID-Server und der Application Identity Manager (AIM) -Client müssen in derselben Umgebung konfiguriert sein, und Application Identity Manager (AIM) muss für die Interaktion mit dem externen Tresor CyberArk konfiguriert sein. Der externe Tresor CyberArk kann in der gleichen Umgebung wie der MID-Server und Application Identity Manager (AIM) oder in einer anderen Umgebung gehostet werden.

Die Instanz ServiceNow verwaltet Anmeldeinformations-IDs, die bestimmten OAuth 2.0-Anmeldeinformationen zugeordnet sind, die im Tresor CyberArk gespeichert sind. Vor dem Senden einer OAuth-Token-Anforderung ruft der MID-Server den Bezeichner der Anmeldeinformationen von der Instanz ab und verwendet dann eine vom Kunden bereitgestellte JAR-Datei, um den Bezeichner an den AIM-Client zu senden. Der AIM-Client sendet die Anforderung an Tresor CyberArk. Der Tresor CyberArk sendet die OAuth 2.0-Anmeldeinformationen über den AIM-Client an den MID-Server zurück. Nach dem Empfang der OAuth 2.0 -Anmeldeinformationensendet der MID-Server die OAuth-Token-Anforderung an den Autorisierungsserver des Drittanbieters. Die Tokenanforderung enthält Informationen wie den Client und den geheimen Clientschlüssel, den CyberArk speichert, den OAuth-Bereich und die Token-URL, die die Instanz speichert. Nachdem der Autorisierungsserver das OAuth-Token ausgegeben hat, speichert der MID-Server das Token im Cache.

Hinweis: Diese Funktion unterstützt den Client-Anmeldeinformations-Gewährungstyp.

Die Abbildung zeigt den Authentifizierungsprozess der MID-Server-Anforderung.

Hinweis: Es wird davon ausgegangen, dass der Autorisierungsserver der Drittpartei und der Tresor CyberArk im Kundennetzwerk gehostet werden.



Konfigurieren Sie eine JAR-Datei und Anmeldeinformationsbezeichner

Konfigurieren Sie eine JAR-Datei und Anmeldeinformationsbezeichner, damit die JAR-Datei die Anmeldeinformationsbezeichner in tatsächliche Anmeldeinformationen aus dem externen Tresor CyberArk auflöst. Der Prozess ermöglicht es dem MID Server, OAuth 2.0-Anmeldeinformationen abzurufen und in die OAuth-Token-Anforderung aufzunehmen.

Vorbereitungen

Erforderliche Rolle: agent_admin oder admin

Der externe Tresor CyberArk speichert vertrauliche Anmeldeinformationen, und die Instanz ServiceNow speichert Anmeldeinformationsbezeichner, die den spezifischen Anmeldeinformationsnamen zugeordnet sind, die der Tresor speichert. Die JAR-Datei ermöglicht die Zuordnung eines Anmeldeinformationsbezeichners zu einem bestimmten

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anmeldeinformationsnamen im externen Tresor. Die Zuordnung ermöglicht es MID-Server, die erforderlichen Anmeldeinformationen abzurufen und in die OAuth-Token-Anforderung aufzunehmen. Sie müssen die Anmeldeinformationsbezeichner und die JAR-Datei in der ServiceNow-Instanz bzw. dem MID-Server konfigurieren.

Prozedur

1. CyberArk-JAR-Datei importieren.
2. Konfigurieren Sie eine Verbindung zum Senden der OAuth-Anforderung über MID-Server mithilfe eines externen Tresors.

Konfigurieren Sie CyberArk

Konfigurieren Sie den Tresor CyberArk zum Speichern von OAuth 2.0-Anmeldeinformationen und zur Beantwortung von Anforderungen für OAuth 2.0-Anmeldeinformationen von MID-Server.

Vorbereitungen

Bestätigen Sie, dass Sie das ServiceNow IntegrationHub Standard Pack Installer-Abonnement abonniert haben. Weitere Informationen finden Sie unter https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/legal/snc-addendum-integrationhub.pdf .

Erforderliche Rolle: agent_admin oder admin

Prozedur

1. CyberArk-Tresor konfigurieren und die AIM-API installieren.
2. CyberArk-JAR-Datei importieren.
3. Konfigurieren Sie OAuth 2.0-Anmeldeinformationen in CyberArk.
4. Konfigurieren Sie eine Verbindung zum Senden der OAuth-Anforderung über MID-Server mithilfe eines externen Tresors.

Konfigurieren Sie OAuth 2.0-Anmeldeinformationen in CyberArk

Konfigurieren Sie Ihren CyberArk-Tresor mit OAuth 2.0-Anmeldeinformationen, die von der Instanz ServiceNow angefordert werden.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Um OAuth 2.0-Anmeldeinformationen zu speichern, erstellen Sie zuerst eine OAuth 2.0-Anmeldeinformationsvorlage im CyberArk-Tresor. Dieser Prozess muss für den Tresor nur einmal abgeschlossen werden.

Prozedur

1. Führen Sie die folgenden Schritte aus, wenn Sie die OAuth 2.0-Anmeldeinformationen zum ersten Mal konfigurieren.

   a. Melden Sie sich im Administrationsmodus bei CyberArk an.

   b. Navigieren Sie zur Registerkarte **Administration**.

   c. Wählen Sie **Plattformmanagement aus**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auf der Seite „Plattformmanagement“ werden die Plattformen unter der Registerkarte Ziele angezeigt.

d. Erweitern Sie einen Plattformtyp.

e. Wählen Sie das Einstellungssymbol (Symbol für), das einer Plattformvorlage entspricht, und anschließend **Duplizieren**.

f. Geben Sie im Fenster „Duplicate Platform“ (Plattform duplizieren) einen Namen für die Vorlage ein, und wählen **Sie Erstellen**aus.

Hinweis: Notieren Sie sich den Systemtyp, unter dem Sie eine doppelte Vorlage erstellt haben. Zum Beispiel ist Cloud-Service ein Systemtyp.

g. Wählen Sie das Einstellungssymbol ( ), das der von Ihnen erstellten doppelten Plattformvorlage entspricht, und wählen Sie **Bearbeiten**aus.

h. Fügen Sie die Eigenschaft hinzu.
Name als Anwendername und Anzeigename als Client-ID.

i. Benennen Sie die anderen Eigenschaften um.

Tipp: Wählen Sie für OAuth 2.0 relevante Eigenschaftsnamen aus.

j. Wählen Sie **Übernehmen**.
Die Updates werden angewendet.

k. Wählen Sie **OK**.

l. Navigieren Sie im linken Bereich zu Accounts.

m. Wählen **Sie Account hinzufügen**.

n. Wählen Sie unter der Überschrift Systemtyp den Systemtyp aus, unter dem Sie die Plattformvorlage erstellt haben.
Der Systemtyp zeigt die Plattformvorlagen.

o. Wählen Sie unter der Überschrift Select Platform (Plattform auswählen) die von Ihnen erstellte Plattformvorlage aus.

p. Wählen Sie Sicher aus.
Speichern Sie den Wert Sicher zur späteren Verwendung.

q. Füllen Sie die Informationen für Client-ID, Passwort (Client-Geheimnis als Wert angeben) und andere Felder nach Bedarf aus.

r. Wählen Sie **Hinzufügen**.
Der Account wird hinzugefügt.

s. Öffnen Sie auf der Seite „Accountansicht“ einen Account.

t. Wählen Sie die Registerkarte **Details** aus.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

u. Kopieren Sie den im Abschnitt „Account-Name“ gespeicherten Wert, und speichern Sie ihn zur späteren Verwendung.
Der von Ihnen kopierte und gespeicherte Wert wird als Bezeichner für Anmeldeinformationen in der ServiceNow-Instanz verwendet.

2. Führen Sie die folgenden Schritte aus, wenn Sie die OAuth 2.0-Anmeldeinformationen nicht zum ersten Mal konfigurieren.

a. Melden Sie sich im Administrationsmodus bei CyberArk an.

b. Navigieren Sie zum Abschnitt „ **Account** “, und wählen **Sie Account hinzufügen**aus.

c. Wählen Sie den Systemtyp unter **Systemtyp** aus, unter dem die Vorlage zum Speichern von OAuth 2.0 vorhanden ist.

d. Wählen Sie die erforderliche Plattformvorlage aus, die Sie erstellt haben, und wählen Sie **Sicher**aus.
Speichern Sie den Wert Sicher zur späteren Verwendung.

e. Füllen Sie die Informationen für Client-ID, Passwort (Client-Geheimnis als Wert angeben) und andere Felder nach Bedarf aus.

f. Wählen Sie **Hinzufügen**.
Der Account wird hinzugefügt.

g. Öffnen Sie auf der Seite „Accountansicht“ einen Account.

h. Wählen Sie die Registerkarte **Details** aus.

i. Kopieren Sie den im Abschnitt „Account-Name“ gespeicherten Wert, und speichern Sie ihn zur späteren Verwendung.
Der von Ihnen kopierte und gespeicherte Wert wird als Anmeldeinformationsbezeichner in der Instanz ServiceNow verwendet.

Konfigurieren Sie eine Verbindung zum Senden der OAuth-Anforderung über MID-Server mithilfe eines externen Tresors

Konfigurieren Sie eine Verbindung, um Anforderungen für OAuth 2.0-Token an einen Drittanbieter-Authentifizierungsserver über MID-Serverzu senden. Der MID-Server fügt der Anforderung OAuth 2.0-Anmeldeinformationen (Client-ID und geheimer Clientschlüssel) aus dem externen Tresor CyberArk, den OAuth-Bereich und die Token-URL aus der Instanz hinzu und sendet sie an den Authentifizierungsserver des Drittanbieters.

Vorbereitungen

Überprüfen Sie die folgenden Elemente.

- Bestätigen Sie, dass Sie das ServiceNow IntegrationHub Standard Pack Installer-Abonnement abonniert haben. Weitere Informationen finden Sie unter https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/legal/snc-addendum-integrationhub.pdf .
- Sie haben eine JAR-Datei erstellt, die es dem MID Server ermöglicht, Anmeldeinformationen mit dem externen Tresor CyberArk aufzulösen. Weitere

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen finden Sie unter JAR-Datei zum Auflösen der Anmeldeinformationen erstellen.

- Sie haben die JAR-Datei auf den MID Server importiert.
- Der MID Server wird für CyberArk eingerichtet. Weitere Informationen finden Sie unter MID Server für CyberArk konfigurieren.
- OAuth 2.0 wird im externen CyberArk-Speicher konfiguriert. Weitere Informationen finden Sie unter Konfigurieren Sie OAuth 2.0-Anmeldeinformationen in CyberArk.

Erforderliche Rolle: keine

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Verbindung und die Anmeldeinformationen mit einer Konfigurationsvorlage oder manuell konfigurieren. Eine Konfigurationsvorlage definiert die Komponenten des Verbindungsdatensatzformulars und kann für andere Verbindungsdatensätze wiederverwendet werden. Manuell können Sie die Verbindung nur zu diesem Zweck konfigurieren. Das Thema zeigt beide Ansätze.

Prozedur

1. Konfigurieren Sie die Verbindung mit einer Konfigurationsvorlage.

   a. Navigieren zu **Alle** > **IntegrationHub** > **Konfigurationsvorlagen**an.

   b. Wählen Sie **Neu**.

   c. Wählen Sie **den Gewährungstyp „HTTP-Verbindung mit OAuth-Client-Anmeldeinformationen“ (externer Speicher) aus**.

   d. Aktualisieren Sie das Formular nach Bedarf.
   Sie können den Umfang beispielsweise in den Feldern `oauth_entity_profile_scope` und `oauth_entity_scope` im Abschnitt „Standarddatenvorlage“ angeben.
   Informationen zum Erstellen einer -Konfigurationsvorlage finden Sie unter Erstellen Sie eine Konfigurationsvorlage.

   e. Wählen Sie **Absenden**.
   Sie haben die Konfigurationsvorlage erstellt.

   f. Navigieren zu **Alle** > **IntegrationHub** > **Aliasse für Verbindungen und Anmeldeinformationen**an.

   g. Aktualisieren Sie das Formular.

Alias für Verbindungen und Anmeldeinformationen

Feld	Beschreibung
Name	Name des Alias. Ein Alias darf nur Buchstaben, Ziffern und Unterstriche enthalten. Während eines Upgrades wird das Tag im Anmeldedatensatz zu einem Verbindungs- und Anmeldealias migriert. Wenn das Tag der Anmeldeinformationen andere

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Sonderzeichen als Buchstaben, Ziffern und Unterstriche enthält, wird der Tag-Name nach dem Upgrade beibehalten. Sie können diesen migrierten Alias weiterhin verwenden, Sie können ihn allerdings erst aktualisieren, wenn Sie den Namen den Namensbeschränkungen entsprechend ändern.
Anwendung	Eindeutiger Bezeichner für den Alias für Verbindungen und Anmeldeinformationen, basierend auf dem Format `scope_name.alias_name`. ▪ Bei „Global“ ist die ID der Aliasname. Wenn Sie beispielsweise einen Workday-Alias im globalen Bereich erstellen, wird die ID auf `workday festgelegt`. ▪ Wenn Sie einen Workday-Alias im Bereich der HR-App erstellen, wird die ID auf `x_hr_app.workday festgelegt`.
Übergeordneter Alias	Option zum Auswählen des Alias, unter dem Sie diesen Alias für Verbindungen und Anmeldeinformationen erstellen. Der Alias für Verbindungen und Anmeldeinformationen, den Sie erstellen, ist ein untergeordneter Alias. Ein untergeordneter Alias wird unter der Registerkarte **Untergeordnete Aliase** auf der Seite des übergeordneten Alias für Verbindungen und Anmeldeinformationen angezeigt. 
Typ	Option zur Angabe des Typs des Alias, den Sie erstellen. Wählen Sie eine der folgenden Optionen aus: ▪ Anmeldeinformationen: Alias, der einen Anmeldeinformationsdatensatz enthält. ▪ Verbindungen und Anmeldeinformationen: Alias, der Verbindungs- und Anmeldeinformationsdatensatz enthält. Diese Option ist standardmäßig ausgewählt. Bestätigen Sie, dass Verbindung und Anmeldeinformationen ausgewählt sind.
Unterstützt mehrere aktive Verbindungen	Bezeichner, der angibt, ob der Alias mehrere aktive Verbindungen

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	unterstützt. Fügen Sie mithilfe der Tabelle „Verbindungen“ Verbindungen hinzu, und verknüpfen Sie sie mithilfe der zugehörigen Liste „Verbindungen“ mit dem Alias.
Standard-Wiederholungsrichtlinie	Wiederholungsrichtlinie für den Alias. Weitere Informationen finden Sie unter Wiederholungsrichtlinie .
Konfigurationsvorlage	Option zum Auswählen der Konfigurationsvorlage, auf deren Grundlage Sie den Alias für Verbindungen und Anmeldeinformationen erstellen. Wählen Sie die Vorlage des **Gewährungstyps „HTTP-Verbindung mit OAuth-Client-Anmeldeinformationen“ (externer Speicher)**, die Sie erstellt haben.

h. Wählen Sie **Absenden**.
Sie haben den Datensatz des Alias für Verbindungen und Anmeldeinformationen erstellt.

i. Navigieren zu **Alle** > **IntegrationHub** > **Verbindungs-Dashboard**an.

j. Geben Sie im Feld Alle Verbindungen durchsuchen den Namen des von Ihnen erstellten Aliasdatensatzes für Verbindungen und Anmeldeinformationen ein.

k. Wählen Sie im Datensatz des Alias für Verbindungen und Anmeldeinformationen **Details anzeigen**aus.

l. Wählen Sie **Konfigurieren**.

m. Füllen Sie das Formular aus.

Formular „Verbindung konfigurieren“.

Feld	Beschreibung
Verbindungsname	Name der Verbindung Sie können den Namen nicht aktualisieren.
Verbindungs-URL	URL zum Server der Drittpartei.
MID verwenden	Option zum Aktivieren des MID-Servers. **Wichtig:** Bestätigen Sie, dass die Option ausgewählt ist.
MID-Auswahl	Option zum Angeben der MID-Konfiguration für die Verbindung.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	▪ **Spezifischer MID-Server**: Option zur Angabe der manuellen Auswahl eines bestimmten MID-Servers. ▪ **MID-**Server automatisch auswählen: Option, um anzugeben, dass der MID-Server automatisch ausgewählt werden soll. ▪ **Spezifischer MID-Cluster**: Option zur Angabe der manuellen Auswahl eines MID-Clusters von MID-Servern. **Wichtig:** Stellen Sie sicher, dass sich der von Ihnen ausgewählte MID-Server auf demselben Computer befindet wie der CyberArk-AIM-Client, der für den Zugriff auf den CyberArk-Tresor konfiguriert ist. Weitere Informationen finden Sie unter CyberArk-Tresor konfigurieren und die AIM-API installieren.
MID-Server	Option zum manuellen Angeben eines MID-Servers. Diese Option wird angezeigt, wenn Sie im Feld „ **MID-Auswahl** “ die Option **Spezifischer MID-Server** auswählen.
MID-Cluster	Option zum manuellen Angeben eines MID-Clusters. Diese Option wird angezeigt, wenn Sie im Feld „ **MID-Auswahl** “ die Option „ **Spezifischer MID-Server-Cluster** “ auswählen.
Externer Anmeldeinformationsspeicher	Option zur Verwendung des externen Anmeldeinformationsspeichers von CyberArk. Wenn Sie die Option auswählen, ruft der MID-Server die OAuth 2.0-Anmeldeinformationen (Client-ID und geheimer Clientschlüssel) vom externen Anmeldeinformationsspeicher ab. **Wichtig:** Bestätigen Sie, dass die Option ausgewählt ist.
Anmeldeinformations-ID	Bezeichner für den CyberArk-Account, der die Details zur Client-ID und zum geheimen Clientschlüssel enthält. Informationen zum Verfahren zum Abrufen des Anmeldeinformationsbezeichners finden Sie unter Konfigurieren Sie OAuth 2.0-Anmeldeinformationen in CyberArk. Geben Sie im Feld „Anmeldeinformations-ID“ einen Ausdruck in einem dieser Formate ein.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	▪ Wenn sich alle Anmeldeinformationen im selben Safe befinden, konfigurieren Sie diesen Safe-Namen in der MID-Server-Datei `config.xml` mit dem Parameter ext.cred.safe_name, und geben Sie die Nachweis-ID nur mit dem Namen als **<Nachweis-ID>** an. ▪ Um die Anmeldeinformationen für eine Plattform zu benennen, die sich in einem bestimmten Safe befinden, definieren Sie die Nachweis-ID als **<Safe>:<Nachweis-ID>:<Plattform-ID>**. ▪ Wenn sich die Anmeldeinformationen in mehreren Safes befinden, geben Sie die Nachweis-ID in diesem Format an: **<Safe>:<Nachweis-ID>**.
OAuth-Token-URL	URL, die den Endpunkt angibt, um das Zugriffstoken vom OAuth-Server abzurufen.

n. Wählen Sie **Verbindung konfigurieren aus**.

2. Konfigurieren Sie manuell eine Verbindung.

a. Navigieren zu **Alle** > **System-OAuth** > **Applikationsregistrierung**an.

b. Wählen Sie **Neu**.

c. Wählen Sie **Verbindung mit OAuth-Drittpartei über externen Tresor herstellen aus**.

d. Füllen Sie das Formular aus.

Details zur neuen Anwendungsregistrierung

Feld	Beschreibung
Name	Name zur Identifizierung des Anwendungsregistrierungsdatensatzes. Geben Sie beispielsweise Folgendes ein: OAuth 2.0-Tokenanforderung über MID-App.
Anwendung	Option zum Angeben der Namen von Anwendungen, die auf diese Anwendungsregistrierung zugreifen können. Das Feld ist schreibgeschützt.
Standardgewährungstyp	Standardmethode zum Abrufen des Zugriffstokens durch die Clientanwendung vom OAuth-Server. Der standardmäßige und schreibgeschützte Gewährungstyp ist „Client-Anmeldeinformationen“.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zugänglich von	Option, um anzugeben, welche Anwendungen auf diese Anwendungsregistrierung zugreifen können.
Token-URL	URL, die den Endpunkt angibt, um das Zugriffstoken vom OAuth-Server abzurufen.
Anmeldeinformationen senden	Option zum Angeben der Methode zum Senden von OAuth 2.0 im Anforderungstext.
Kommentare	Geben Sie zugehörige Kommentare ein.

e. Erstellen Sie unter der Spalte **„OAuth-Bereich** " einen oder mehrere OAuth-Bereiche, indem Sie die folgenden Schritte ausführen.

i. Doppelklicken Sie in der Spalte Name auf das Feld, und geben Sie den Namen des OAuth-Bereichs ein.

ii. Doppelklicken Sie unter der Spalte „OAuth-Bereich" auf das Feld, und geben Sie den Bereich ein.

f. Wählen Sie **Absenden**.
Sie haben ein OAuth-Entitätsprofil und die Anwendungsregistrierung erstellt.

g. Navigieren zu **Alle** > **IntegrationHub** > **Verbindungen und Anmeldeinformationen** > **Anmeldeinformationen**an.

h. Wählen Sie **Neu**.

i. Wählen Sie **OAuth 2.0-Anmeldeinformationen** aus.

j. Wählen Sie **Externe Speicheransicht aus**.

Wichtig: Wählen Sie „ **Externe Speicheransicht"** nur aus, wenn sich die Ansicht von der eines externen Speicherformulars für OAuth 2.0-Anmeldeinformationen unterscheidet.

k. Füllen Sie das Formular aus.

OAuth 2.0-Anmeldeinformationen

Feld	Beschreibung
Name	Name des Anmeldeinformationsdatensatzes.
Betrifft	Option zum Angeben, ob der Anmeldeinformationsdatensatz für alle MID-Server oder einen bestimmten MID-Server gilt. Wenn dies der Fall ist, fügen Sie die MID Server hinzu. Wählen Sie eine der folgenden Optionen aus.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	▪ Alle MID-Server: Der MID-Server wird automatisch aus einer Sammlung von MID-Servern ausgewählt. ▪ Spezifische MID-Server: Option zum Angeben eines oder mehrerer MID-Server.
MID-Server	Option zum Angeben eines oder mehrerer MID-Server. **Hinweis:** Dieses Feld wird angezeigt, wenn Sie im Feld Gilt für die Option **Spezifische MID-Server** auswählen.
Aktiv	Option zum Angeben, ob der Anmeldeinformationsdatensatz zur Verwendung verfügbar ist. Standardmäßig ist es verfügbar.
OAuth-Einheitenprofil	Option zum Angeben eines OAuth-Entitätsprofils, das von den Anmeldeinformationen verwendet wird. Wählen Sie das OAuth-Entitätsprofil aus, das Sie oben erstellt haben. Weitere Informationen finden Sie unter OAuth-Entitätsprofil konfigurieren.
Externer Anmeldeinformationsspeicher	Option zum Festlegen, dass die Anmeldeinformationen in einem externen Speicher und nicht in der ServiceNow-Instanz gespeichert werden. **Wichtig:** Bestätigen Sie, dass die Option ausgewählt ist.
Anmeldeinformations-ID	Option zum Angeben des Anmeldeinformationsbezeichners für das CyberArk-Konto, das die Client-ID und den geheimen Clientschlüssel enthält. Informationen zum Verfahren zum Abrufen des Anmeldeinformationsbezeichners finden Sie unter Konfigurieren Sie OAuth 2.0-Anmeldeinformationen in CyberArk.
Anmeldeinformationsspeicher – Tresor	Option zum Angeben des Namens des Tresors mit externen Anmeldeinformationen. Stellen Sie sicher, dass Sie CyberArkausgewählt haben.

l. Wählen Sie **Absenden**.
Sie haben den Anmeldeinformationsdatensatz erstellt.

m. Erstellen Sie einen Alias für Verbindungen und Anmeldeinformationen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einzelheiten zu den Schritten erfahren Sie unter Verbindungs- und Anmeldealias erstellen.

n. Navigieren zu **Alle** > **IntegrationHub** > **Verbindungen**an.

o. Wählen Sie **Neu**.

p. Wählen Sie **HTTP(s)-Verbindung aus**.

q. Füllen Sie das Formular aus.

Verbindungsformular

Feld	Beschreibung
Name	Eindeutiger Name dieser HTTP(s)-Verbindung.
Aktiv	Mit dieser Option können Sie die von Ihnen erstellte Verbindung als aktiv festlegen. Die Option ist standardmäßig ausgewählt.
Anmeldeinformationen	Wählen Sie den Datensatz mit Anmeldeinformationen aus, der zur Autorisierung der Verbindung verwendet wird. Wählen Sie die Anmeldeinformationen aus, die Sie oben erstellt haben.
Verbindungsalias	Wählen Sie den Alias-Datensatz aus, der dieser Verbindung zugeordnet werden soll. Mit einem Alias können Sie den Verbindungsdatensatz aktualisieren, ohne Aktionen oder Aktivitäten, die den Alias verwenden, neu zu konfigurieren.
URL-Builder	Geben Sie entweder die Verbindungs-URL manuell ein, oder verwenden Sie das System, um die URL basierend auf den Eingaben zu erstellen. Standardmäßig ist dieses Kontrollkästchen deaktiviert. Wenn diese Option aktiviert ist, wird die Verbindungs-URL aus den folgenden Feldern berechnet: ▪ Gegenseitige Authentifizierung – Aktivieren Sie das Kontrollkästchen, wenn die gegenseitige Authentifizierung verwendet wird. ▪ Protokoll – Wenn keine gegenseitige Authentifizierung verwendet wird, geben Sie das Protokoll ein. Der Standardwert ist HTTPs. ▪ Protokollprofil – Wenn die gegenseitige Authentifizierung verwendet wird, geben Sie das Protokollprofil aus „sys_protocol_profile“ ein. ▪ Host

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	▪ Port ▪ Basispfad – Pfad der Verbindungszeichenfolge. **Hinweis:** Wenn „Gegenseitige Authentifizierung“ aktiviert ist, wird die Verbindungs-URL erstellt: Protokoll + :// + Host:Port +URL. Wenn „Gegenseitige Authentifizierung“ nicht aktiviert ist, wird die Verbindungs-URL erstellt: Protokollprofil + :// + Host:Port +URL
Verbindungs-URL	Wenn der URL-Builder deaktiviert ist, geben Sie die Verbindungs-URL in dieses Feld ein. **Hinweis:** Wenn „Gegenseitige Authentifizierung“ aktiviert ist, wird die Verbindungs-URL erstellt: Protokoll + :// + Host:Port +URL. Wenn „Gegenseitige Authentifizierung“ nicht aktiviert ist, wird die Verbindungs-URL erstellt: Protokollprofil + :// + Host:Port +URL
MID Server verwenden	Option, um anzugeben, dass OAuth-Token-Anforderungen über einen MID-Server gesendet werden sollen. **Wichtig:** Bestätigen Sie, dass die Option ausgewählt ist.
Verbindungszeitüberschreitung	Anzahl der Millisekunden, die das System auf eine erfolgreiche Hostverbindung wartet. Wenn während dieser Zeit keine erfolgreiche Verbindung hergestellt wird, läuft die Verbindungsanforderung ab. Lassen Sie dieses Feld leer, um den Standard-Zeitüberschreitungswert für Verbindungen zu verwenden.
MID-Auswahl	Option zum Angeben einer der folgenden Optionen. ▪ MID-Server automatisch auswählen: Wählt aus MID-Servern basierend auf MID-Server-Kriterien aus, unabhängig davon, ob sie Mitglieder eines Clusters sind. ▪ Spezifischer MID-Server: Wählen Sie manuell einen MID-Server aus. ▪ Spezifischer MID-Server-Cluster: Bei der automatischen Neuzuweisung zu

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	einem anderen MID-Server werden nur Mitglieder des angegebenen Clusters ausgewählt. **Wichtig:** Stellen Sie sicher, dass sich der von Ihnen ausgewählte MID-Server auf demselben Computer befindet wie der CyberArk-AIM-Client, der für den Zugriff auf den CyberArk-Tresor konfiguriert ist. Weitere Informationen finden Sie unter CyberArk-Tresor konfigurieren und die AIM-API installieren.
MID-Server	Wählen Sie manuell einen MID-Server aus. Diese Option wird angezeigt, wenn Sie Spezifischer MID-Server im Feld „MID-Auswahl“ auswählen.
MID-Cluster	Wählen Sie manuell ein MID-Cluster aus. Diese Option wird angezeigt, wenn Sie Spezifischer MID-Server-Cluster im Feld „MID-Auswahl“ auswählen.
MID-Anwendung	Wählen Sie manuell eine MID-Anwendung aus.

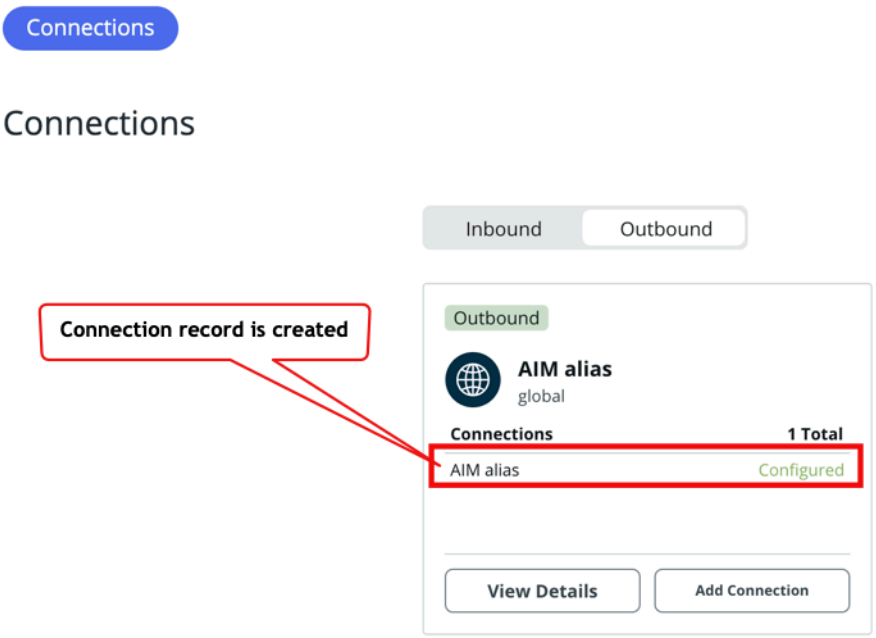
r. Wählen Sie **Absenden**.
Sie haben einen HTTP(s)-Verbindungsdatensatz erstellt.

s. Navigieren zu **Alle** > **Prozessautomatisierung** > **IntegrationHub** > **Verbindungs-Dashboard**an.

t. Geben Sie im Feld Alle Verbindungen durchsuchen den Namen des von Ihnen erstellten Verbindungsdatensatzes ein.
Der Verbindungsalias-Datensatz wird angezeigt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OAuth 2.0-Verbindungsdatensatz wird erstellt



Authentifizierungsalgorithmen

Verifizieren Sie die Identität des Absenders mithilfe von Authentifizierungsalgorithmen

Lassen Sie Integrationsschritte zur Authentifizierung bei Webservices zu, die komplexe oder nicht standardmäßige Verbindungs- oder Anmeldeinformationsmechanismen erfordern. Ordnen Sie Authentifizierungsalgorithmen Aliassen für Anmeldeinformationen und Verbindungen zu, um die Notwendigkeit einer manuellen Konfiguration von Integrationsschritten zu reduzieren oder zu beseitigen.

Sie können einen Authentifizierungsalgorithmus verwenden, um anwenderdefinierte Authentifizierungsdaten für Ihre Integrationsschritte zu generieren. Integrationsschritte können diese dynamischen Daten verwenden, um anwenderdefinierte Artefakte zu erstellen, die für die Authentifizierung beim Ziel-Webservice erforderlich sind. Beispielsweise kann ein REST-Schritt einen Authentifizierungsheader, Abfrageparameter oder ein Token erstellen.

Authentifizierungsalgorithmen unterstützen die folgenden Schritte:

- Schritt „Verbindungsinformationen abrufen“.
- REST-Schritt
- SOAP-Schritt

Weitere Informationen finden Sie unter Integrationsschritte

Typen des Authentifizierungsalgorithmus

- **Amazon-Signaturversion 4**: Dies ist ein vorgefertigter Authentifizierungsalgorithmus für die Verbindung mit Amazon Web Services.
- **Anwenderdefinierte Authentifizierung**: Dies ist eine Vorlage, mit der Entwickler ihre eigenen Authentifizierungsalgorithmen erstellen können.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zur Konfiguration des Authentifizierungsalgorithmus finden Sie unter Konfigurieren Sie einen Authentifizierungsalgorithmus.

Skripts

Instanzauthentifizierungsskripts befinden sich in Instanzskripts, die Teil der Tabelle *sys_script_include* sind.

Instanzauthentifizierungsskripts

RequestAuthInternal	Schreibgeschütztes Skript in Instanz, das die Generierung einer AWS V4-Signatur oder einer anwenderdefinierten Authentifizierung unterstützt, die mit einer ausgehenden Anforderung gesendet wird.
RequestAuthAWSV4Signer	Skript zur Erweiterung von „RequestAuthInternal“ zur Implementierung des Unterzeichners zum Generieren der AWS V4-Signatur.
RequestAuthTwitterSigner	Skript zur Erweiterung von „RequestAuthInternal“ zur Implementierung des Unterzeichners zum Generieren einer Twitter-Signatur mit OAuth 1.0a.
RequestAuthSampleCustomSigner	Beispielskript zur Erweiterung von RequestAuthInternal, um zu verstehen, wie ein anwenderdefinierter Unterzeichner in eine Instanz geschrieben wird.

MID-Authentifizierungsskripts befinden sich in MID-Skripts, die Teil der Tabelle *ecc_agent_script_include* sind.

MID-Authentifizierungsskripts

RequestAuthInternal	Schreibgeschütztes Skript auf MID, das die Generierung einer AWS V4-Signatur oder einer anwenderdefinierten Authentifizierung unterstützt, die mit einer ausgehenden Anforderung gesendet wird.
RequestAuthAWSV4MIDSigner	Skript zur Erweiterung von „RequestAuthInternal“ zur Implementierung des Unterzeichners zum Generieren der AWS V4-Signatur.
RequestAuthTwitterSigner	Skript zur Erweiterung von „RequestAuthInternal“ zur Implementierung des Unterzeichners zum Generieren einer Twitter-Signatur mit OAuth 1.0a.
RequestAuthSampleMidCustomSigner	Beispielskript zur Erweiterung von RequestAuthInternal, um zu verstehen, wie ein anwenderdefinierter Unterzeichner auf MID geschrieben wird.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

JavaScript-APIs

Im Folgenden finden Sie die JavaScript-APIs für den Authentifizierungsalgorithmus.

- Auth-Anmeldeinformationen
- HttpRequestAuthedData
- HTTPAnforderungsdaten
- RequestAuthAPI

Konfigurieren Sie einen Authentifizierungsalgorithmus

Konfigurieren Sie einen Authentifizierungsalgorithmus, damit Sie ausgehende HTTP-Anforderungen signieren können.

Vorbereitungen

Sie müssen eine Skripteinbindung konfigurieren, bevor Sie einen Authentifizierungsalgorithmus konfigurieren.
Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Anmeldeinformationen und Verbindungen** > **Authentifizierungsalgorithmen**und klicken Sie auf **Neu**.
2. Füllen Sie die Felder des Formulars aus.
   Anhand der Auswahl der Datenbank im Feld **Format** wird festgelegt, welche Felder verfügbar sind.

Authentifizierungsformular

Feld	Beschreibung
Name	Eindeutiger Name dieses Algorithmus.
Algorithmus	Typ der ausgehenden Anforderung.
Beschreibung	Beschreibung der Funktionsweise Ihres Algorithmus.
Anwendung	Umfang, in dem Ihre Anwendung ausgeführt wird.
Instanzauthentifizierungsskript	Skript, das Sie in der Tabelle „Skripteinbindungen“ auswählen.
MID-Authentifizierungsskript	Skript, das Sie in der Tabelle „MID-Server-Skripteinbindungen“ [Discovery-Ansicht] auswählen.

3. Klicken Sie auf **Absenden**.

Konfigurieren Sie einen anwenderdefinierten Algorithmus, der auf der Signatur Amazon basiert

Generieren Sie die Amazon signaturbasierten Daten, die für die Authentifizierung bei einem Webservice erforderlich sind, indem Sie ein Skript ausführen.

Vorbereitungen

- JavaScript-Wissen
- REST-Wissen
- Ziel-Webservice-API-Wissen

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Verbindungs-, Anmeldeinformations- und Alias-Wissen
- Erforderliche Rolle: Entwickler

Warum und wann dieser Vorgang ausgeführt wird

Verwenden Sie für die Authentifizierung einen Alias für Verbindungen und Anmeldeinformationen sowie einen auf Amazon Signaturversion 4 basierenden Algorithmus.

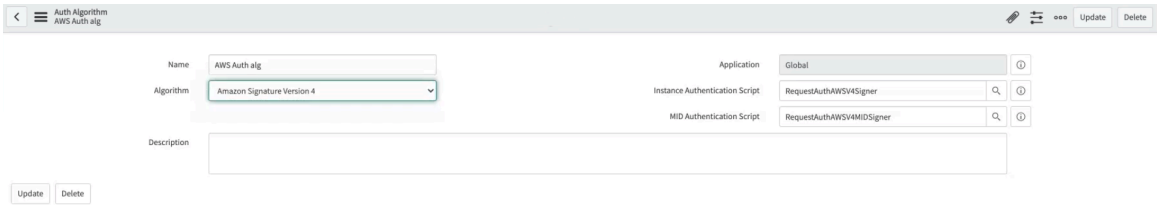
Prozedur

1. Navigieren zu **Alle** > **Anmeldeinformationen und Verbindungen** > **Authentifizierungsalgorithmen**und klicken Sie auf **Neu**.
2. Füllen Sie die Felder des Formulars aus.
   Anhand der Auswahl der Datenbank im Feld **Format** wird festgelegt, welche Felder verfügbar sind.

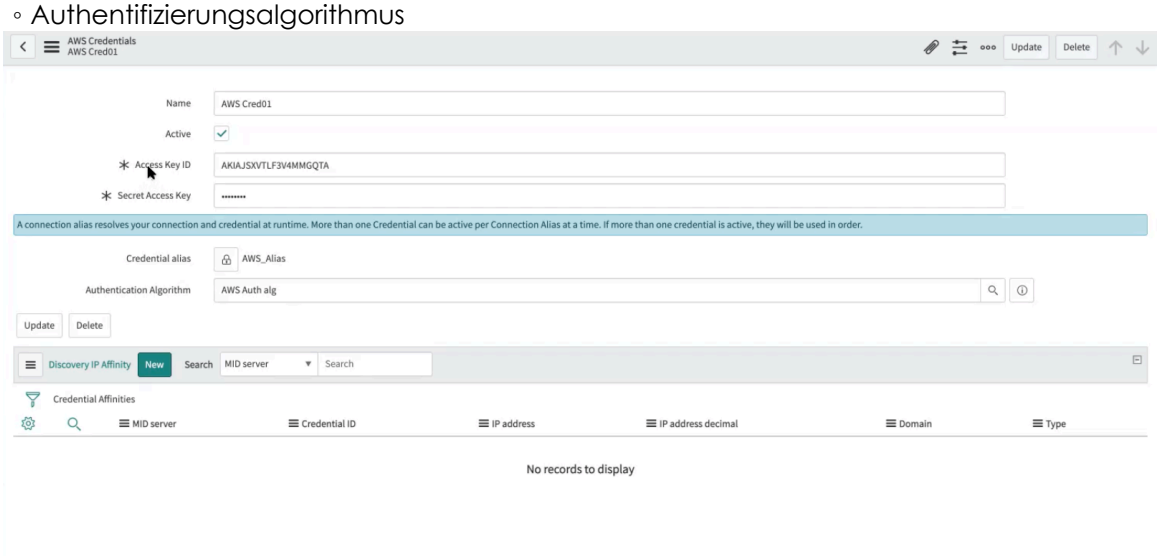
Authentifizierungsformular

Feld	Beschreibung
Name	Eindeutiger Name dieses Algorithmus.
Algorithmus	Typ der ausgehenden Anforderung. Wählen Sie **Amazon-Signaturversion 4 aus**.
Beschreibung	Beschreibung der Funktionsweise Ihres Algorithmus.
Anwendung	Umfang, in dem Ihre Anwendung ausgeführt wird.
Instanzauthentifizierungsskript	Skript, das Sie in der Tabelle „Skripteinbindungen“ auswählen. Im Falle des **Amazon Signature Version 4** -Algorithmus wählen **Sie RequestAuthAWSV4Signer aus**. Folgende Skripts sind verfügbar: ◦ RequestAuthAWSV4Signer ◦ RequestAuthInternal ◦ RequestAuthSampleCustomSigner ◦ RequestAuthTwitterSigner **Hinweis:** Um mehr über das Skript zu erfahren, klicken Sie auf das Informationssymbol neben dem Feld. Die Details des Skripts, z. B. Name, API-Name, Anwendung, Zugänglich von, Skript usw. werden angezeigt.
MID-Authentifizierungsskript	Skript, das Sie in der Tabelle „MID-Server-Skripteinbindungen“ [Discovery-Ansicht] auswählen. Folgende Skripts sind verfügbar: ◦ RequestAuthAWSV4Signer ◦ RequestAuthInternal ◦ RequestAuthSampleCustomSigner ◦ RequestAuthTwitterSigner

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Klicken Sie auf **Aktualisieren**.
4. Navigieren zu **Alle** > **Verbindungen und Anmeldeinformationen** > **Anmeldeinformationen**an.
5. Klicken Sie auf **Neu**.
6. Erstellen Sie AWS Anmeldeinformationen mit dem Authentifizierungsalgorithmus. In diesem Fall **AWS-Auth-Alg**.
7. Geben Sie Folgendes an:
   - Name
   - Aktiv
   - Zugangsschlüssel-ID
   - Geheimer Zugangsschlüssel
   - Anmeldeinformationsalias
   - Authentifizierungsalgorithmus



8. Klicken Sie auf **Aktualisieren**.

Ergebnisse

Basierend auf den ausgewählten Skripts und dem Authentifizierungsalgorithmus generieren die konfigurierten Anmeldeinformationen (**Zugriffsschlüssel-ID** und **geheimer Zugriffsschlüssel**) oder die Anmeldeinformationen des Anwenders (**Zugriffsschlüssel-ID**, **geheimer Zugriffsschlüssel**und **Sitzungstoken**) eine Amazon V4-Signatur, die als ausgehende Anforderung von gesendet wird ServiceNow an den Anbieter (in diesem Fall AWS).

Example: REST-Schritt mit AWS

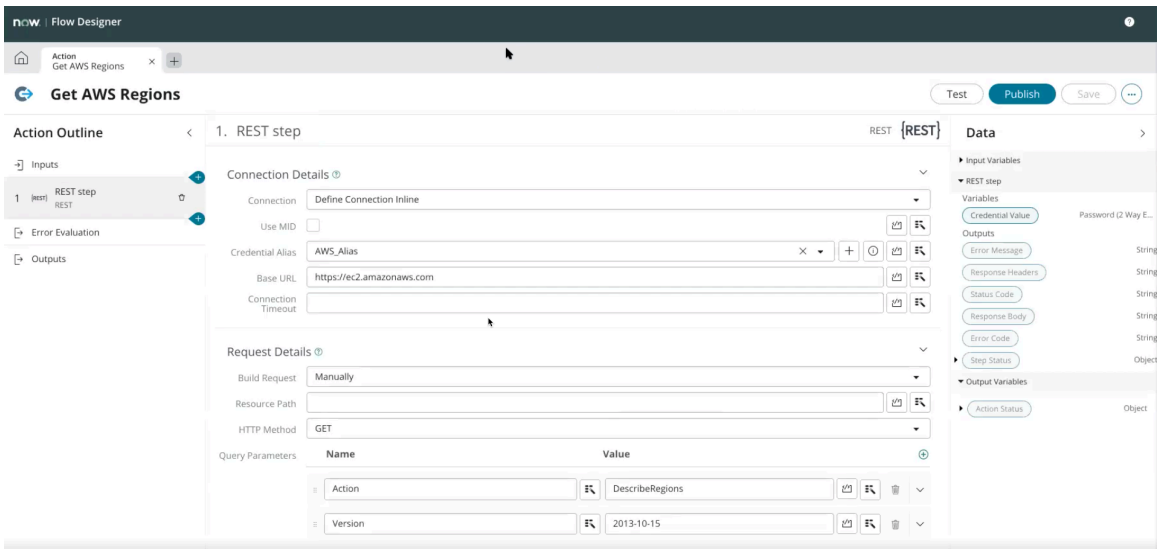
Hinweis: Amazon Die Authentifizierung auf Basis der V4-Signatur kann auch im Skripthintergrund verwendet werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktion: Rufen Sie AWS Regionen ab

Geben Sie den REST-Schritt mit AWS wie folgt ein:

- **Anmeldeinformationsalias**: Der Alias, der für AWSerstellt wird.
- **Basis-URL**: Basis-URL-Details von AWS.
- **HTTPS-Methode**: In diesem Fall die GET-Methode.
- **Abfrageparameter**: **Aktion** als **DescribeRegions**.



Sie können die Aktion testen, die zugehörigen Regionen werden angezeigt. Der Antworttext lautet wie folgt:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Automatische Übersetzung

Amazon V4 ist mit einem Standardsatz von Algorithmen definiert, der Authentifizierungsmechanismen unterstützt. Wenn dieser Algorithmus verwendet wird, fügt er die Signatur als Autorisierungsheader für die Authentifizierung (HTTP-Anforderung) mithilfe des REST-Schritts hinzu.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie einen anwenderdefinierten Authentifizierungsalgorithmus

Generieren Sie die anwenderdefinierten Daten, die für die Authentifizierung bei einem Webservice erforderlich sind, indem Sie ein Skript ausführen.

Vorbereitungen

- JavaScript-Wissen
- REST-Wissen
- Ziel-Webservice-API-Wissen
- Verbindungs-, Anmeldeinformations- und Alias-Wissen
- Erforderliche Rolle: Entwickler

Warum und wann dieser Vorgang ausgeführt wird

Verwenden Sie für die Authentifizierung einen Alias für Verbindungen und Anmeldeinformationen sowie einen anwenderdefinierten authentifizierungsbasierten Algorithmus.

Prozedur

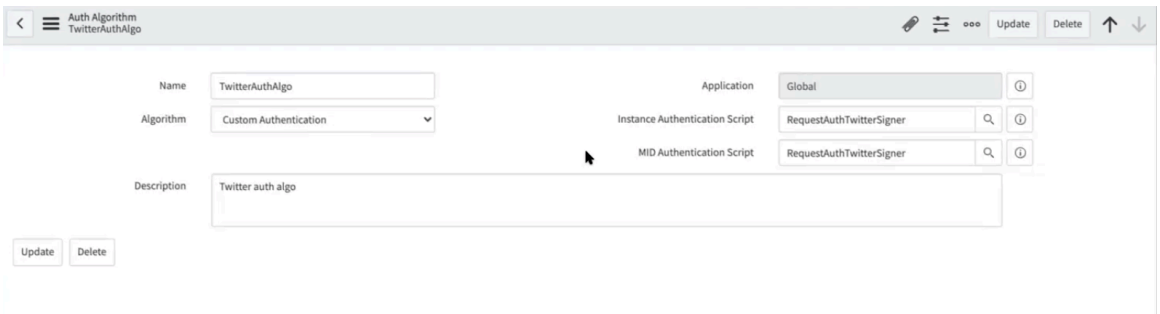
1. Navigieren zu **Alle** > **Anmeldeinformationen und Verbindungen** > **Authentifizierungsalgorithmen**und klicken Sie auf **Neu**.
2. Füllen Sie die Felder des Formulars aus.
   Anhand der Auswahl der Datenbank im Feld **Format** wird festgelegt, welche Felder verfügbar sind.

Authentifizierungsformular

Feld	Beschreibung
Name	Eindeutiger Name dieses Algorithmus.
Algorithmus	Typ der ausgehenden Anforderung. Wählen Sie **Anwenderdefinierte Authentifizierung aus**.
Beschreibung	Beschreibung der Funktionsweise Ihres Algorithmus.
Anwendung	Umfang, in dem Ihre Anwendung ausgeführt wird.
Instanzauthentifizierungsskript	das Sie in der Tabelle „Skripteinbindungen“ auswählen. Folgende Skripts sind verfügbar: ◦ RequestAuthAWSV4Signer ◦ RequestAuthInternal ◦ RequestAuthSampleCustomSigner ◦ RequestAuthTwitterSigner

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: ◦ Um mehr über das Skript zu erfahren, klicken Sie auf das Informationssymbol neben dem Feld. Die Details des Skripts, z. B. Name, API-Name, Anwendung, Zugänglich von, Skript usw. werden angezeigt. ◦ Im Falle einer anwenderdefinierten Authentifizierung mit Twitter können Sie **RequestAuthTwitterSigner**wählen, da eine OAuth 1.0a-Authentifizierungsmethode verwendet wird. Dies erfordert Informationen wie **API-Schlüssel und Geheimnis** sowie **Zugriffstoken und Geheimnis**, die zum Erstellen von Signaturen verwendet werden können, um einen Autorisierungsheader zu übergeben. Weitere Informationen finden Sie unter Authentifizierung in Twitter .
MID-Authentifizierungsskript	Skript, das Sie in der Tabelle „MID-Server-Skripteinbindungen“ [Discovery-Ansicht] auswählen. Folgende Skripts sind verfügbar: ◦ RequestAuthAWSV4Signer ◦ RequestAuthInternal ◦ RequestAuthSampleCustomSigner ◦ RequestAuthTwitterSigner

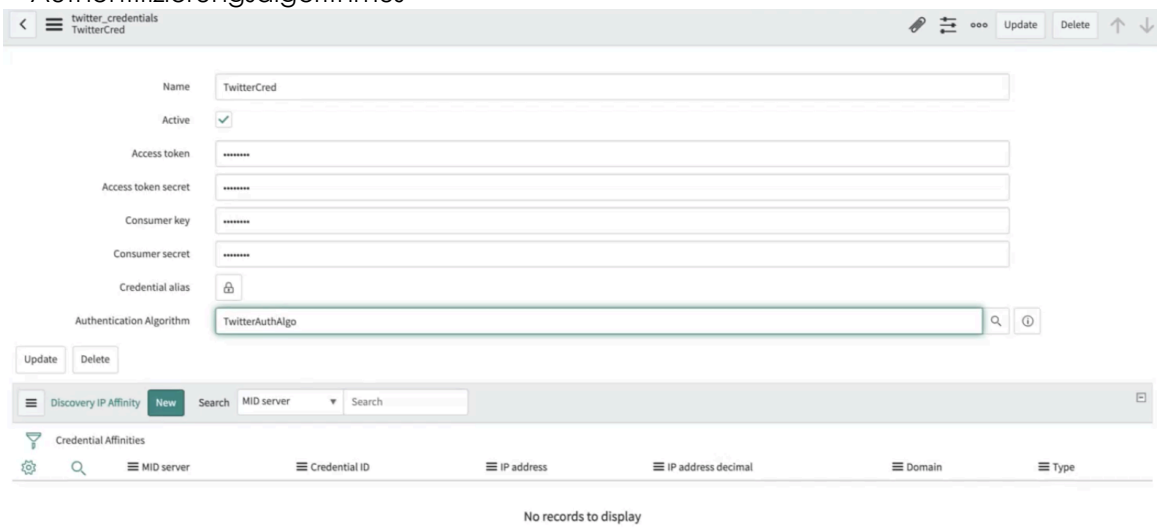


Basierend auf den ausgewählten Skripts und dem Authentifizierungsalgorithmus werden die konfigurierten Anmeldeinformationen als ausgehende Anforderung von ServiceNow an den Anbieter gesendet.

3. Klicken Sie auf **Aktualisieren**.
4. Navigieren zu **Alle** > **Verbindungen und Anmeldeinformationen** > **Anmeldeinformationen**an.
5. Klicken Sie auf **Neu**.
6. Erstellen Sie Twitter Anmeldeinformationen mit dem Authentifizierungsalgorithmus. In diesem Fall **TwitterAuthAlgo**.
7. Geben Sie die Felder an:
   - Name
   - Aktiv
   - Zugriffstoken

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zugriffstokengeheimnis
- Verbraucherschlüssel
- Verbrauchergeheimnis
- Anmeldeinformationsalias
- Authentifizierungsalgorithmus



8. Klicken Sie auf **Aktualisieren**.

Example: REST-Schritt mit Twitter

Im Fall von Twittermüssen Sie sicherstellen, dass die folgenden Spokes oder Anmeldeinformationen verfügbar sind:

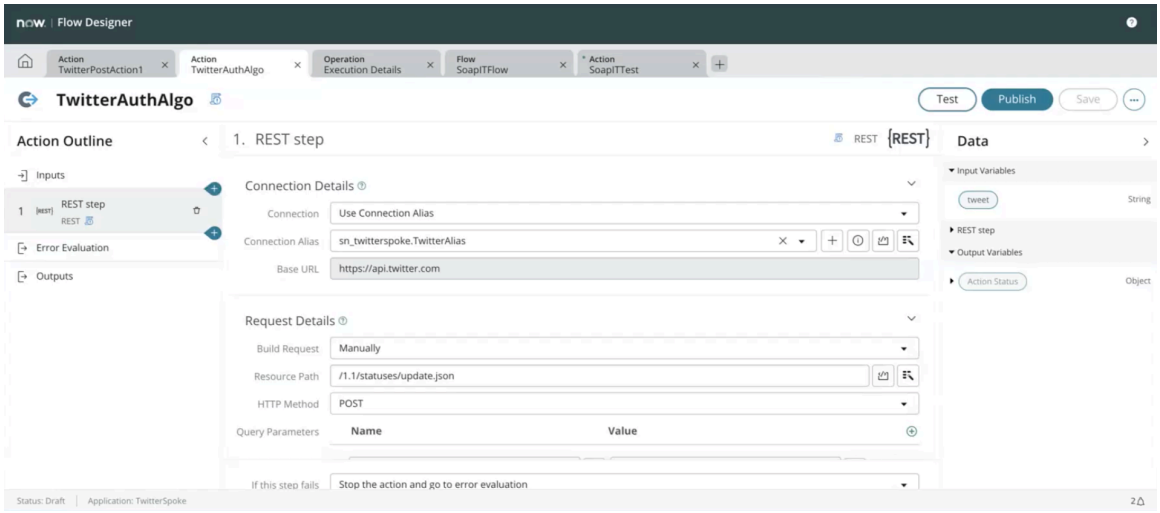
- Zugriffstoken
- Zugriffstokengeheimnis
- Verbraucherschlüssel
- Verbrauchergeheimnis
- Authentifizierungsalgorithmus

Aktion: TwitterAuthAlgo

Geben Sie den REST-Schritt mit Twitter wie folgt ein:

- **Anmeldeinformationsalias**: Der Alias, der für Twittererstellt wird.
- **Basis-URL**: Basis-URL-Details von Twitter.
- **HTTPS-Methode**: In diesem Fall die POST-Methode. Posten eines Tweets.
- **Abfrageparameter**: **Aktion** als **Tweet**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Sie können die Aktion testen. Der Tweet wird auf der Seite Twitter veröffentlicht.

IP-Service-Affinität für Discovery und Orchestration prüfen

Sie können in der Tabelle „IP-Services“ nach einer Liste von IP-Adressen suchen, die einem Protokoll zugeordnet sind.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Die Tabelle „IP-Services“ ordnet einen Port einem Protokoll zu. Für häufig verwendete Port-Protokoll-Kombinationen werden standardmäßig Zuordnungen bereitgestellt, z. B. Port 80 für HTTP, Port 22 für SSH und Port 161 für SNMP.
Mithilfe der Systemeigenschaft *glide.discovery.ip_service_affinity* kann sich Discovery den letzten Port der erkannten IP-Adresse merken. Diese Eigenschaft ist standardmäßig auf **false** festgelegt.

Wichtig: Sie sollten IP-Services nur dann ändern, wenn Ihre Organisation benutzerdefinierte Ports verwendet.

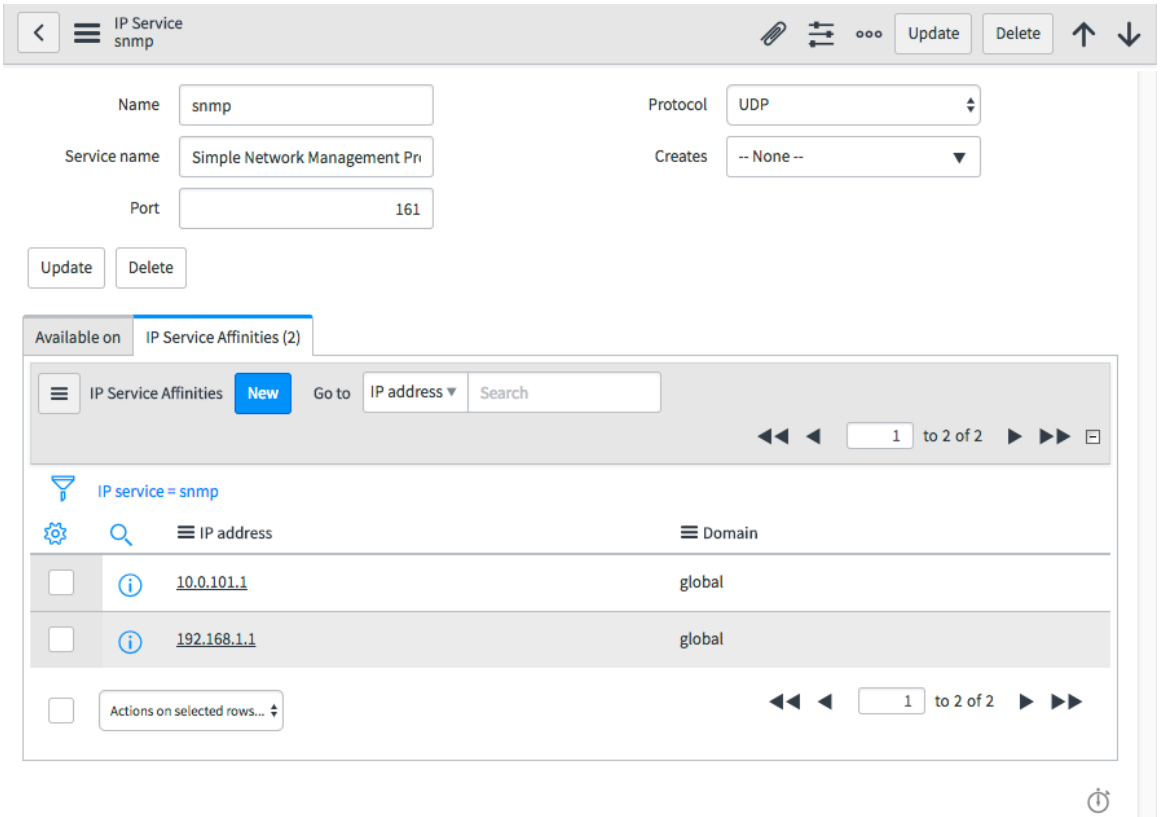
Prozedur

1. Navigieren zu **Alle** > **Discovery-Definition** > **IP-Services**an.
2. Filtern Sie die Liste, um den entsprechenden IP-Service zu finden.
3. Klicken Sie auf den Namen des Service, um zu dieser IP-Serviceseite zu gelangen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf die Registerkarte **IP-Serviceaffinitäten**, um die Liste der IP-Adressen anzuzeigen, die diesem Service zugeordnet sind.

IP-Serviceaffinitäten



ServiceNow®-Zugriffssteuerung

Mit dem Plugin „SNC Access Control“ (com.snc.snc_access_control) können Sie steuern, welche Kundenservice und Support Mitarbeiter wann auf Ihre Instanz zugreifen können.

Machen Sie sich mit der Zugriffssteuerung von ServiceNow vertraut



Aktivieren Sie die ServiceNow-Zugriffssteuerung



© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erfahren Sie mehr über die Funktionen der Zugriffssteuerung ServiceNow®.

Aktive ServiceNow® Zugriffssteuerung.

Konfigurieren Sie die ServiceNow-Zugriffssteuerung



Erfahren Sie, wie die Zugriffssteuerung für ServiceNow® konfiguriert wird.

Audit-Protokollierung



Lernen und überprüfen Sie die Audit-Protokollierung der Zugriffssteuerung ServiceNow®.

Automatische Übersetzung

Zugriffssteuerung ServiceNow® erkunden

Mit dem Plugin „SNC Access Control“ (com.snc.snc_access_control) können Sie steuern, welche Kundenservice und Support Mitarbeiter wann auf Ihre Instanz zugreifen können.

Wenn Sie das Plugin zum ersten Mal aktivieren, können sich die Mitarbeiter Kundenservice und Support nicht bei der Instanz anmelden. Alle derzeit angemeldeten Kundenservice und Support Mitarbeiter bleiben angemeldet. In der Tabelle „SNC-Zugriffssteuerung“ erstellen Sie Datensätze, die bestimmten SNC-Mitarbeitern oder allen Mitarbeitern Zugriff gewähren.

Das Plugin verhindert, dass Mitarbeiter von Kundenservice und Support ohne Ihre ausdrückliche Genehmigung auf die Instanzen zugreifen. Allerdings sind andere autorisierte ServiceNow Operations-Mitarbeiter in ihrer Kapazität für Support und Verwaltung des Produkts sowie für die Überprüfung der Nutzung erforderlich, um administrative Aktionen an der zugrunde liegenden Infrastruktur durchzuführen. Diese Infrastruktur umfasst neben anderen Infrastrukturkomponenten, aus denen die SaaS-Lösung besteht, Server und Datenbanken. Diese Zugriffsmethode ist vollständig überprüfbar und wird nachverfolgt.

Mit diesem Plugin können Sie den Zugriff auf Ihre Instanz ohne Ihre ausdrückliche Genehmigung einschränken. Dies kann sich auf die Servicelevel des Supports und das

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verfügbarkeits-SLA auswirken. Das Verfügbarkeits-SLA wird dann ab dem Zeitpunkt gemessen, zu dem Support-Mitarbeitern Zugriff auf Ihre Instanz gewährt wird.

Anmeldesicherheit

Zur Sicherheit werden für die Anmeldung autorisierter Kundenservice und Support -Mitarbeiter bei Instanzen verschlüsselte Token verwendet, die von einem sicheren Server generiert werden. Nur ordnungsgemäß authentifizierte Mitarbeiter Kundenservice und Support erhalten Zugriff auf eine Instanz. Ohne das Plugin „SNC Access Control“ stellt der Sicherheitsserver sicher, dass Zugriffsrechte auf hi.service-now.com erzwungen werden. Wenn das Plugin aktiviert ist, müssen die verschlüsselten Anmeldetoken mit den Namen in der vom Plugin bereitgestellten Zugriffsliste übereinstimmen und die in diesen Datensätzen definierten Kriterien verwenden. Mit dieser Authentifizierungsmethode können Sie genau bestimmen, welche Kundenservice und Support -Mitarbeiter wann auf ihre Instanzen zugreifen dürfen.

Die für dieses System ausgewählte Architektur weist mehrere Funktionen auf, um die Sicherheit für Ihre Instanzen zu erhöhen:

Sicherheitsserver

Der Sicherheitsserver ist ein gesperrter Linux-Host, auf den nur das -Sicherheitspersonal von ServiceNow zugreifen kann. Dieser Server ist das einzige System, das Zugriff auf den kritischen privaten Verschlüsselungsschlüssel hat, der zur Erstellung der Anmeldetoken erforderlich ist. Durch diese Aufteilung (eine standardmäßige Sicherheitsmethode) wird der private Schlüssel geschützt, selbst in dem unwahrscheinlichen Fall, dass ein Angreifer die HI-Instanz kompromittiert.

Synthetic-Benutzer

Für die Einrichtung in Instanzen, mit der sich autorisierte Mitarbeiter Kundenservice und Support bei ihrer Instanz anmelden können, muss in dieser Instanz kein Account bereitgestellt werden. Es ist kein Benutzerdatensatz bereitgestellt und keine permanenten oder persistenten Anmeldeinformationen vorhanden. Stattdessen wird für jede Kundenservice und Support -Mitarbeiteranmeldung ein Synthetic User erstellt. Dieser Anwender ist nur im Arbeitsspeicher vorhanden und bietet keine laufenden Berechtigungen. Wenn das Plugin „SNC Access Control“ aktiviert ist, können Sie jedem Kundenservice und Support -Mitarbeiter jederzeit die Autorisierung aufheben.

Token

Die Sicherheitstoken sind spezifisch für eine Instanz und einen bestimmten Mitarbeiter Kundenservice und Support. Darüber hinaus funktioniert der Mechanismus, der die Token generiert, nur mit tatsächlichen Kundenservice und Support -Mitarbeiteranmeldungen bei HI, nicht mit Benutzern, die die Identität von angenommen haben. Sobald ein Sicherheitstoken generiert wurde, kann sich nur ein bestimmter Kundenservice und Support -Mitarbeiter damit bei einer Instanz anmelden.

Zeitbegrenzung

Sicherheitstoken laufen vier Stunden nach ihrer Generierung ab. Dieser Ablauf schränkt die Nützlichkeit der gekaperten Token ein, die nur während dieses kurzen Zeitfensters verwendet werden können.

Protokollierung

Anmeldungen von Kundenservice und Support Mitarbeitern bei Instanzen werden als Anmeldeereignis aufgezeichnet.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Jede Aktion des angemeldeten Mitarbeiters Kundenservice und Support wird dem Transaktionsprotokoll in der Datenbank hinzugefügt.
- Es wird auch dem Instanzprotokoll im Dateisystem hinzugefügt, auf das die meisten Mitarbeiter von ServiceNow nicht zugreifen können.
- Kundenservice und Support Anmeldungen und Aktionen von Mitarbeitern sind leicht erkennbar, da die Anwendernamen alle auf @snc enden (z. B. frodo.beutlins@snc).

Diese Aktionen bieten Ihnen eine einfach zu verwendende, robuste und zuverlässige Sicherheitsprotokollierung für den Zugriff durch Nicht-Mitarbeiter.

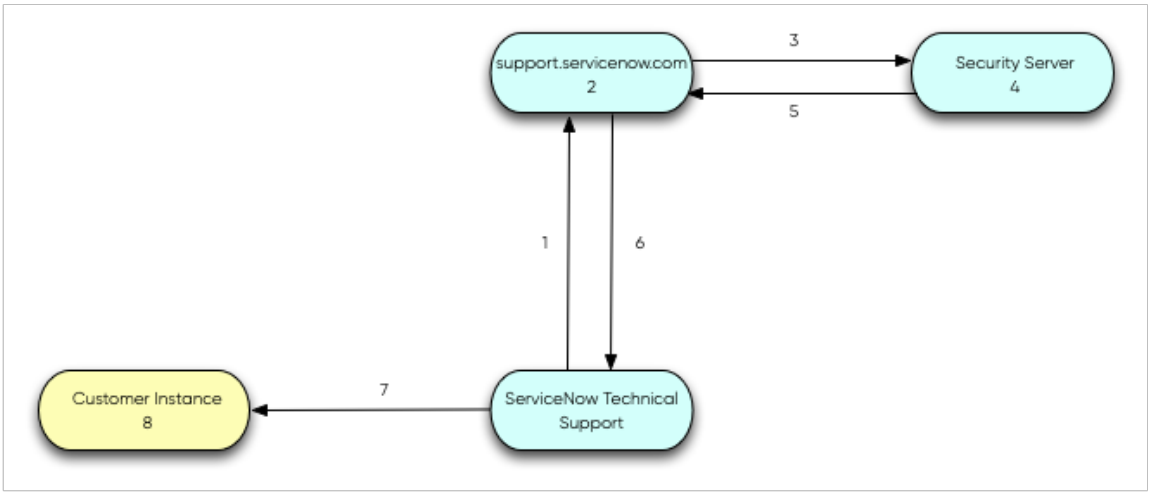
Sicherheitsverarbeitungs-Flow

Wenn sich ein -Mitarbeiter Kundenservice und Support bei einer Instanz anmelden möchte, sieht der Sicherheitsverarbeitungs-Flow wie folgt aus:

1. Ein Kundenservice und Support -Techniker fordert über hi.service-now.com eine Anmeldung für die Instanz an.
2. HI prüft, ob der Techniker über die richtige Rolle verfügt, um den Zugriff auf Instanzen zu autorisieren.
3. Wenn der Benutzer über die richtige Rolle verfügt, sendet HI die Zugriffsanforderung an den Sicherheitsserver.
4. Der Sicherheitsserver verifiziert, ob die Anforderung von der HI-IP-Adresse stammt, und wertet die Anforderung aus (Benutzer, Rolle und IP-Adresse der anfordernden Person). Wenn die Anforderung gültig ist, genehmigt der Sicherheitsserver sie und erstellt ein Token. Dieses Token enthält den Anwendernamen, die Rollen, die Instanz-ID und die Zeit (Beginn der viertägigen Token-Lebensdauer). Abschließend verschlüsselt der Sicherheitsserver das Token mit dem privaten Verschlüsselungsschlüssel.
5. Der Sicherheitsserver sendet das verschlüsselte Token an HI.
6. Hi sendet das Token an den Browser des Support-Technikers.
7. Der Browser des Support-Technikers initiiert eine Anmeldung bei der Instanz unter Verwendung des speziellen Anwendernamens, der mit `@snc`endet.
8. Die Instanz von verwendet den öffentlichen Schlüssel, um das Token zu entschlüsseln. Um das Token zu überprüfen, gleicht die Instanz es mit dem im vorherigen Schritt angegebenen Anwendernamen, der Instanz-ID und dem autorisierten Zeitfenster ab. Wenn das Plugin „SNC Access Control“ aktiviert ist, überprüft die Instanz, ob der Benutzer:
   - Aufgeführt
   - Aktiv
   - Konfiguriert, um auf die Instanz im aktuellen Zeitfenster zuzugreifen
9. Wenn der Benutzer authentifiziert ist, erstellt die Instanz im Arbeitsspeicher einen Synthetic-Benutzer mit den angegebenen Rollen. Dieser Anwender wird nicht beibehalten, nachdem die Zeitbegrenzung abgelaufen ist, er sich abmeldet oder die Instanz neu gestartet wurde.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ServiceNow Prozess-Flow für Sicherheitszugriff



Audit-Protokollierung

Die folgende Protokollierung verfolgt Anmeldungen und Aktivitäten von Kundenservice und Support Mitarbeitern:

- Ereignisprotokolle: Die Ereignisprotokolle zeigen alle Kundenservice und Support Anmeldungen bei einer Instanz an.
- Transaktionsprotokolle: Die Transaktionsprotokolle zeigen alle Aktivitäten in der Instanz, einschließlich aller Versuche, Protokolle zu löschen.

Hinweis: Weitere Informationen zu diesem Plugin finden Sie unter SNC Access Control-Plugin in Härtungseinstellungen für Instanzsicherheit.

Die Zugriffssteuerung ServiceNow® wird aktiviert

Sie fordern die Aktivierung des Plugins „SNC Access Control“ (com.snc.snc_access_control) an.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

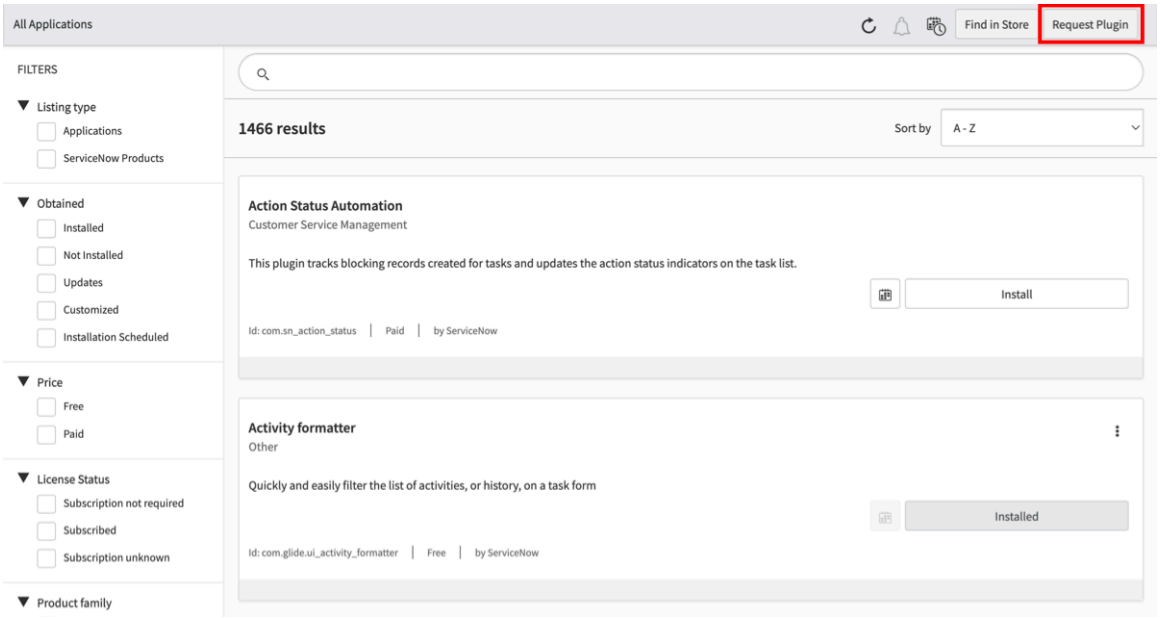
Es gibt zwei Möglichkeiten, ein Plugin anzufordern:

- Greifen Sie direkt auf den Now Support-Servicekatalog zu, indem Sie in Now Support auf **Alle** > **Servicekatalog** > **Plugin aktivieren** klicken.
- Greifen Sie über die Seite „Alle Anwendungen“ in Ihrer Instanz auf den Now Support-Servicekatalog zu, indem Sie die folgenden Schritte ausführen.

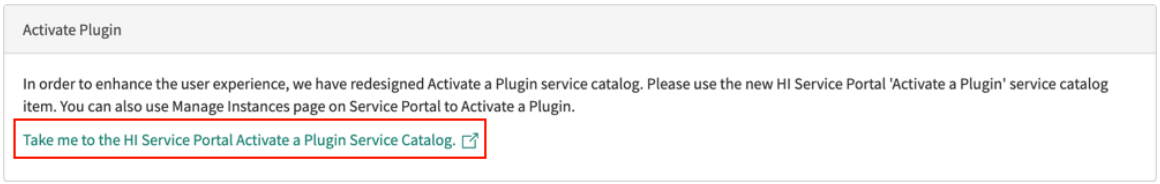
Prozedur

1. Navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Klicken Sie auf der Seite „Alle Anwendungen“ auf **Plugin anfordern**, um das Formular **Plugin aktivieren** auf Now Support zu öffnen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Wählen Sie unter Now Support den Link aus, um auf Now Support Serviceportal Servicekatalog zuzugreifen.



4. Wählen Sie Ihre Instanz aus.
5. Wählen Sie **Aktionen > Plugin aktivieren** aus.
6. Geben Sie im Formular **Plugin aktivieren** die folgenden Informationen an.

Formular „Plugin anfordern“

Feld	Beschreibung
What is your target instance (Ihre Zielinstanz)	Instanz, auf der das Plugin aktiviert werden soll.
Which plugin would you like to activate (Welches Plugin möchten Sie aktivieren?)	Name des zu aktivierenden Plugins **Hinweis:** Wenn das System das gewünschte Plugin nicht auflistet oder wenn Sie das Plugin auf einer OEM- oder lokalen Instanz aktivieren, aktivieren Sie das Kontrollkästchen **Plugin I'm looking for is not listed (Gesuchtes Plugin ist nicht aufgelistet)**, und geben Sie dann den Namen des Plugins ein.

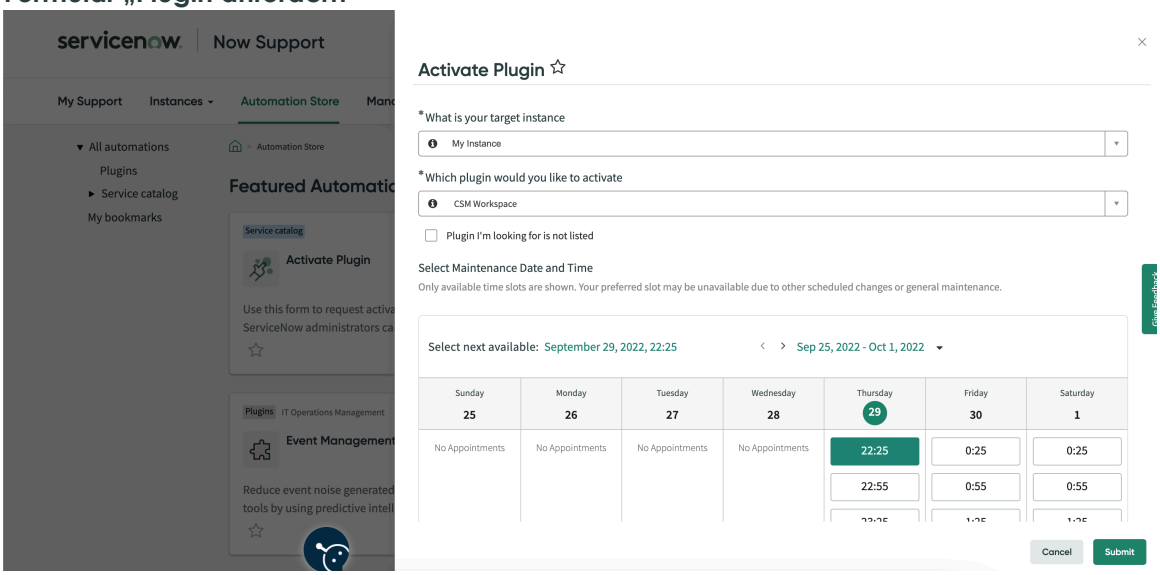
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Select Maintenance Date and Time (Datum und Uhrzeit der Wartung)	Datum und Uhrzeit zum Aktivieren des Plugins. **Hinweis:** Plugins werden in der pazifischen Zeitzone jeden Werktag in zwei Batches aktiviert, einmal am Morgen und einmal am Abend. Wenn das Plugin zu einem bestimmten Zeitpunkt aktiviert werden muss, geben Sie die Anforderung bei **Grund/ Kommentare** ein.

Example

Betrachten Sie beispielsweise das folgende Formular, um das Plugin „CSM Workspace“ in einer Instanz mit dem Namen „My Instance“ zu aktivieren.

Formular „Plugin anfordern“



7. Wählen Sie **Absenden**.
   Weitere Informationen zum Anfordern eines Plugins finden Sie im Artikel Plugin aus dem Servicekatalog anfordern [KB0751715] in der Now Support Knowledge Base.

Die Zugriffssteuerung für ServiceNow® wird konfiguriert

Konfigurieren Sie einen Zugriffssteuerungsdatensatz, um einen oder mehrere Kundenservice und Support Mitarbeiter anzugeben, die berechtigt sind, sich bei Ihrer -Instanz anzumelden.

Vorbereitungen
Erforderliche Rolle: admin

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Hinweis: Das Plugin „SNC Access Control“ (com.snc.snc_access_control) verhindert, dass -Mitarbeiter von Kundenservice und Support ohne Ihre ausdrückliche Genehmigung auf die Instanzen zugreifen. Andere autorisierte ServiceNow Operations-Mitarbeiter müssen jedoch aufgrund ihrer Kapazität für Support und Verwaltung des Produkts administrative Aktionen in der zugrunde liegenden Infrastruktur durchführen. Diese Infrastruktur umfasst neben anderen Infrastrukturkomponenten, aus denen die SaaS-Lösung besteht, Server und Datenbanken. Diese Zugriffsmethode ist vollständig überprüfbar und wird nachverfolgt.

Mit diesem Plugin können Sie den Zugriff auf Ihre Instanz ohne Ihre ausdrückliche Genehmigung einschränken. Dies kann sich auf die Servicelevel des Supports und das Verfügbarkeits-SLA auswirken. Das Verfügbarkeits-SLA wird dann ab dem Zeitpunkt gemessen, zu dem Support-Mitarbeitern Zugriff auf Ihre Instanz gewährt wird.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **SNC-Zugriffssteuerung**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Formularfelder aus (siehe Tabelle).
4. Klicken Sie auf **Absenden**.

SNC-Zugriffssteuerung

Formularfelder	Beschreibung
Name	Benennt jeden Mitarbeiter Kundenservice und Support, der berechtigt ist, sich bei dieser Instanz anzumelden. ◦ Drücken Sie die Namen als firstname.lastname in Kleinbuchstaben, getrennt durch einen Punkt (z. B. `john.smith`). Für jeden Namen muss ein entsprechender Anwenderdatensatz in *`support.servicenow.com`*vorhanden sein. ◦ Wenn mehr als ein Mitarbeiter Kundenservice und Support berechtigt ist, sich bei dieser Instanz anzumelden, geben Sie mehrere Namen ein, und trennen Sie sie durch Kommas. ◦ Um allen Kundenservice und Support -Mitarbeitern Anmelderechte für den Zugriff auf die Instanz zu gewähren, geben Sie ein Sternchen (*) anstelle des Namens ein. ◦ Wenn Sie den Zugriff des Mitarbeiters Kundenservice und Support auf die Instanz einschränken möchten, dürfen die Werte im Feld **Name** an keiner Stelle ein Sternchen (*****) im Feld enthalten.
Grund	Visuell lesbares Feld, das beschreibt, warum Sie die Zugriffsberechtigung gewähren. Dieses Feld ist optional.
Start	Gibt das Startdatum und die Startzeit des Zeitraums an, in dem die angegebenen Mitarbeiter Kundenservice und Support Anmeldezugriff haben. Dieses Feld ist ein Pflichtfeld.
Ende	Gibt das Enddatum und die Enduhrzeit des Zeitraums an, während dem die angegebenen Mitarbeiter vom Typ Kundenservice und Support Anmeldezugriff haben. Dieses Feld ist ein Pflichtfeld.
Aktiv	Steuert, ob dieser Berechtigungsdatensatz aktiv ist. Der Standardwert ist Aktiv.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Audit-Protokollierung

Die folgende Protokollierung verfolgt Anmeldungen und Aktivitäten von ServiceNow Mitarbeitern.

Ereignisprotokolle	Die Ereignisprotokolle zeigen alle ServiceNow Anmeldungen bei einer Kundeninstanz an.
Transaktionsprotokolle	Die Transaktionsprotokolle zeigen alle Aktivitäten in der Instanz, einschließlich aller Versuche, Protokolle zu löschen.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Identität

Erfahren Sie mehr über die Identitäten in der Instanz.

Zugriffsanalyse



Die Zugriffsanalyse ist ein ServiceNow® Store App, die eine Zugriffsdiagnose bietet. Dies hilft zu bestimmen, wer Zugriff auf eine Ressource hat.

Globale Identität



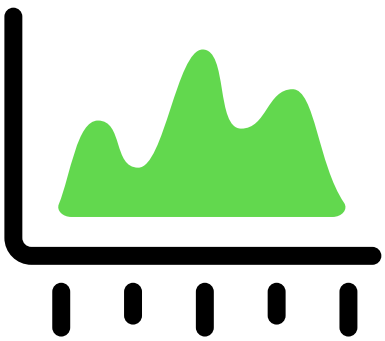
„Global Identity“ ist eine Store-App ServiceNow®, mit der Anwenderattribute von Instanz zu Instanz (mehrere Instanzen) aktualisiert werden können.

Identity Center



Mit Identity Center können Sie identitätsbasierte Risiken und Sicherheitslücken überwachen, verwalten und minimieren.

System für domänenübergreifendes Identitätsmanagement (SCIM)



Identitäts- und Zugriffsaudit



Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die System for Cross Domain Identity Management-API (SCIM) bietet Endpunkte zum Erstellen, Lesen, Aktualisieren und Löschen von Vorgängen für Benutzer und Gruppen mithilfe des SCIM-Protokolls.

Verwenden Sie das Identitäts- und Zugriffsaudit, um die an einem Anwender, einer Gruppe, einer Rolle und einer ACL vorgenommenen Änderungen nachzuvollziehen.

Zugriffsanalyse

ServiceNow® Die Zugriffsanalyse ist ein Zugriffsdiagnosetool, mit dem die Berechtigungen einer Identität für eine Ressource angezeigt werden können.

Untersuchen



Lernen Sie die Funktionen und den Geschäftsnutzen der Zugriffsanalyse kennen.

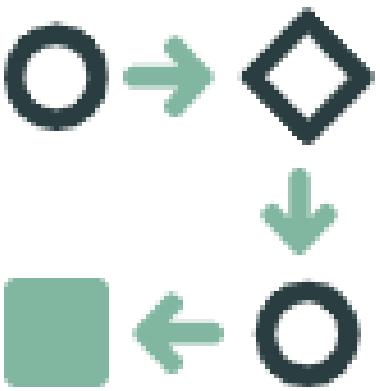
Verwenden



Erfahren Sie, wie die Zugriffsanalyse verwendet wird.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Berechtigungsauswertung



Wissen, wie die Berechtigungen ausgewertet werden.

Häufige Fragen



Rufen Sie Details zu häufig gestellten Fragen zur Zugriffsanalyse ab.

Zugriffsanalyse erkunden

Analysieren Sie Identitäten in der Instanz ServiceNow.

ServiceNow Die Zugriffsanalyse ist eine Anwendung, mit der Administratoren Berechtigungen für ausgewählte Anwender, Rollen oder Gruppen anzeigen können.

Hinweis:

- Die Zugriffsanalyse ist ein Produkt des ServiceNow Store. Besuchen Sie die Website ServiceNow Store , um sich alle verfügbaren Apps anzusehen und Informationen zum Senden von Anforderungen an den Store zu erhalten.
- Die Zugriffsanalyse nimmt die Identität des Identitätsdatensatzes an, um Details zu den Berechtigungen abzurufen, und liest oder speichert keine personenbezogenen oder vertraulichen Daten der Identität.
- Die Auswertungsergebnisse der Zugriffsanalyse sind unabhängig von für die Anwender definierten Zugriffsrichtlinien wie Zero Trust Access (ZTA) identisch. Die Richtlinien werden nur während der tatsächlichen Benutzeranmeldung ausgewertet und werden nicht während des Zugriffsanalyse-Flows ausgewertet.
- Die Zugriffsanalyse weist Einschränkungen bei der genauen Auswertung des Zugriffs auf die Ressourcen im Zusammenhang mit verwalteten Bereichsressourcen und delegierten Entwicklern auf.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugriff auswerten

„Zugriff auswerten“ ist eine Funktion der ServiceNow Zugriffsanalyse, mit der Administratoren Berechtigungen für den ausgewählten Anwender, die ausgewählte Rolle oder die ausgewählte Gruppe anzeigen können.

Damit können Sie die Berechtigungen von Benutzern, Gruppen, Rollen für eine Tabelle, vom Client aufrufbare Skripteinbindungen, UI-Seiten und REST-Endpunkte analysieren und anzeigen.

Mit der Zugriffsanalyse können Unternehmen ihren Sicherheitsstatus, ihre Identitäts-Governance und ihr Risikomanagement verbessern, ihre Compliance-Ziele erreichen und nachvollziehen, wer (Identität) Zugriff auf was (Ressourcen) hat.

Zugriff vergleichen

„Zugriffsvergleich“ ist eine Funktion der ServiceNow Zugriffsanalyse V2, mit der Administratoren den Benutzerzugriff vergleichen und die richtige Zugriffsebene für die Benutzer in Ihrer Instanz von ServiceNow bestimmen können.

Der Zugriffsvergleich kann zwischen den Anwendern für die Benutzerdatensätze und die Zugriffssteuerung durchgeführt werden.

Mit dem Zugriffsvergleich können Sie die folgenden Analysen durchführen:

- Ebene 1: Vergleichen Sie Anwenderdatensätze, um die Attribute, Rollen und Gruppen zu verstehen.
- Ebene 2: Vergleichen Sie die Zugriffssteuerungen, um die Ursachenanalyse auszuführen, indem Sie Zugriffsprobleme finden.

Vorteile

Im Folgenden sind einige der Vorteile der Verwendung der Zugriffsanalyse aufgeführt:

- Analysieren Sie den Zugriff auf Ressourcen (Tabellen).
- Vergleichen Sie den Zugriff von 2 Anwendern.
- Vergleichen Sie die Rollen und Gruppen von 2 Anwendern.
- Generieren Sie einen Bericht, der anzeigt, ob eine Identität Zugriff auf eine Ressource (Tabelle) hat.
- Nachvollziehen, wer Zugriff auf kritische Sicherheitshygiene hat.
- Hilft, eine übermäßige Bereitstellung von Berechtigungen zu verhindern.
- Bei der Implementierung von Zugriffssteuerungen die Prinzipale mit den niedrigsten Berechtigungen erreichen.
- Beschränken Sie den Zugriff auf bestimmte Daten, einschließlich Anwendungen, Tabellen, Zeilen oder Spalten und andere Ressourcen.
- Berichterstellungsfunktionen für die Analyseergebnisse bereitstellen.
- Vergleichen Sie den Zugriff zwischen Anwenderdatensätzen und Zugriffssteuerungen.
- Bestimmen Sie die richtige Zugriffsebene für Benutzer in Ihrer Instanz ServiceNow.

Mithilfe der Zugriffsanalyse

Analysieren Sie Identitäten und ihren Zugriff auf die Instanz ServiceNow®.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: admin

Im folgenden Verfahren werden die Schritte für den Zugriff auf die Zugriffsanalyse und die Verwendung der verschiedenen Funktionen der Zugriffsanalyse beschrieben.

Hinweis: Die Zugriffsanalyse ist ein Produkt des ServiceNow® Store.

Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Berechtigungen analysieren**an.
   Die Homepage „Zugriffe und Berechtigungen analysieren“ wird angezeigt.

   Die Zugriffsanalyse verfügt über die folgenden Funktionen:

   - Zugriff auswerten
   - Anwenderdatensätze vergleichen
   - Vergleichen Sie die Zugriffssteuerungen
2. Wählen Sie die entsprechende Registerkarte aus, um die Zugriffsanalyse basierend auf Ihren Anforderungen zu verwenden.

Mithilfe des Zugriffs „Auswerten“

Analysieren Sie Identitäten in der Instanz ServiceNow®.

Vorbereitungen
Erforderliche Rolle: admin

Im folgenden Verfahren werden die Schritte für den Zugriff auf Zugriff auswerten in der Zugriffsanalyse und die Verwendung der verschiedenen Funktionen beschrieben.

Hinweis: Die Zugriffsanalyse ist ein ServiceNow Store -Produkt.

Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Berechtigungen analysieren**an.
   Die Homepage „Zugriffe und Berechtigungen analysieren“ wird angezeigt.
2. Wählen Sie die Registerkarte **Zugriff** auswerten.
3. Wählen Sie Ihre Kriterien wie folgt aus:

Wählen Sie Ihre Kriterien für die Analyse von Zugriffen und Berechtigungen aus

Feld	Beschreibung
Analysieren nach *	Analysieren Sie den Zugriff für einen Anwender, eine Rolle oder eine Gruppe
Anwender auswählen *	Geben Sie einen Anwendernamen an, den Sie aus der Liste auswählen möchten.
Regeltyp *	Analysieren Sie den Zugriff für eine Tabelle, eine UI-Seite, einen REST-Endpunkt oder eine vom Client aufrufbare Skripteinbindung.
Tabelle auswählen *	Geben Sie einen Tabellennamen an, um ihn aus der Liste auszuwählen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

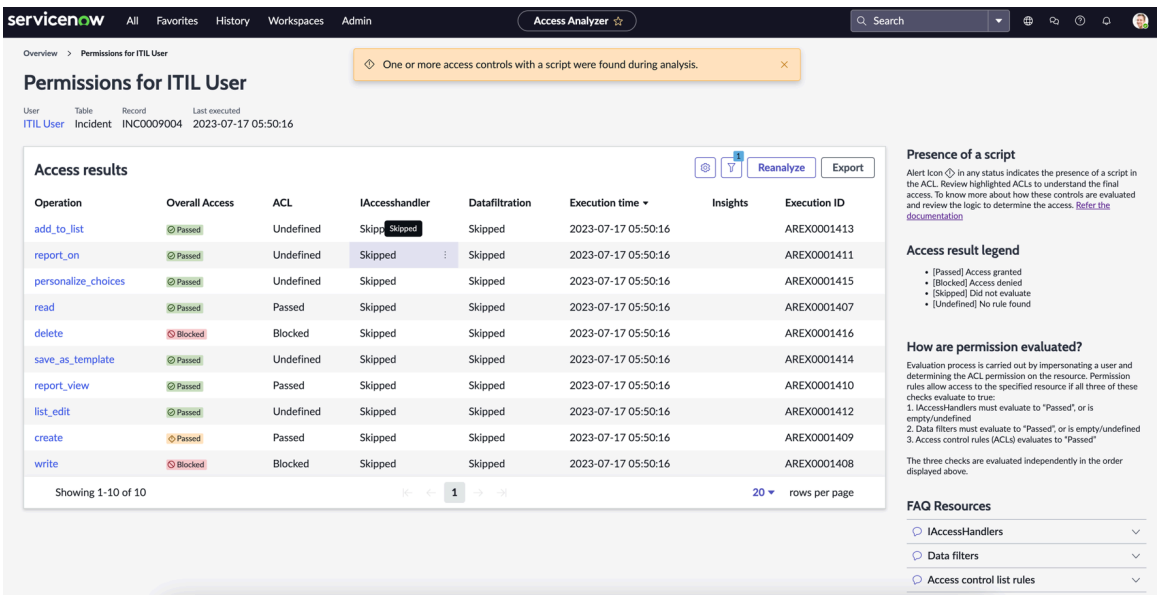
Feld	Beschreibung
Datensatz auswählen	Geben Sie einen Datensatznamen an, um ihn aus der Liste auszuwählen.
Feld auswählen	Geben Sie einen Feldnamen an, um ihn aus der Liste auszuwählen.

4. Geben Sie die Beschreibung im Feld **Beschreibung** an.
5. Wählen Sie **Berechtigungen analysieren aus**.

   Die Zugriffsergebnisse für den Anwender werden angezeigt. Auf ähnliche Weise können Sie die Berechtigungen einer Gruppe oder Rolle für die folgenden Regeltypen analysieren:

   - Tabelle (Datensatz)
   - Vom Client aufrufbare Skripts einschließen
   - REST-Endpunkte

   Die Zugriffsergebnisse werden angezeigt.



Die Tabelle „Zugriffsergebnisse“ enthält die folgenden Felder:

Auf Ergebnisse zugreifen

Felder	Beschreibung
Vorgang	Die Art des Vorgangs, den der Anwender, die Gruppe oder die Rolle für die ausgewählte Tabelle, den ausgewählten Datensatz oder das ausgewählte Feld ausführen kann.
Allgemeiner Zugriff	Ergebnis des Gesamtzugriffs. Die Ergebnisse lauten wie folgt: ◦ [Bestanden] Zugriff gewährt ◦ [Blockiert] Zugriff verweigert

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder	Beschreibung
	◦ [Übersprungen] Wurde nicht ausgewertet ◦ [Nicht definiert] Keine Regel gefunden
ACL	Gibt an, ob für den ausgewählten Vorgang eine ACL definiert ist.
IAccesshandler	Eine interne Systemprüfung mit ausgeblendetem Quellcode auf der Plattform. IAccessHandler kann den Zugriff auf eine Ressource gewähren oder verweigern, ohne ACLs auszuwerten. Wenn IAccessHandler ignoriert wird, werden die ACLs ausgewertet.
Datenfilterung	Ein Datenfilter ist eine Form der Zugriffssteuerung, die auf die vorhandenen Zugriffssteuerungsregeln (ACLs) in Ihrer Instanz abgestimmt ist.
Ausführungszeit	Der Zeitpunkt, zu dem die Zugriffsergebnisse ausgeführt wurden.
Einblicke	Weitere Informationen zum ausgewählten Vorgang.
Ausführungs-ID	Eine eindeutige ID für jede Ausführung des Zugriffsergebnisses.

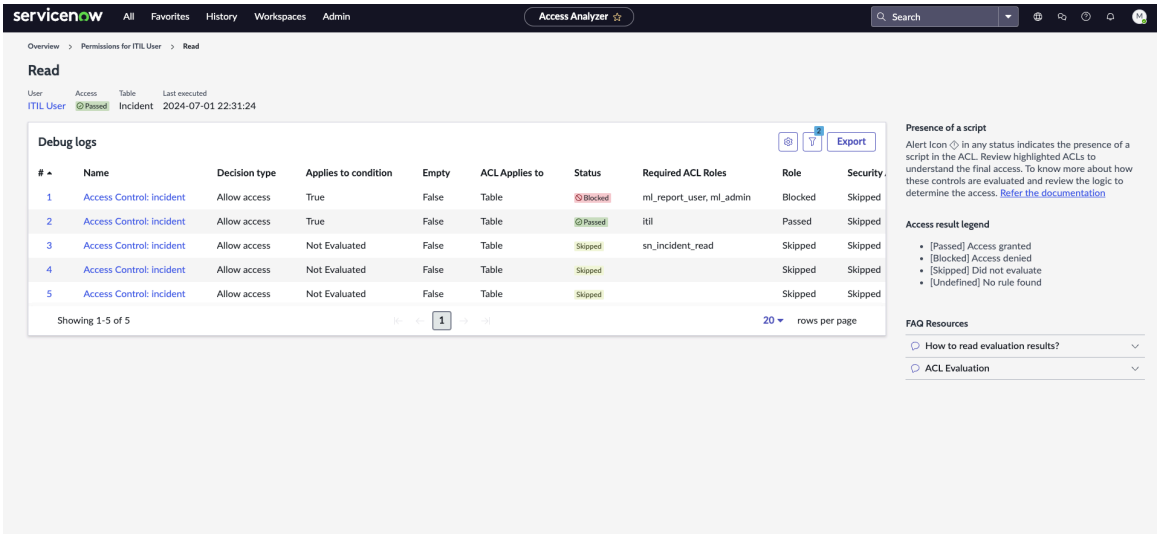
6. Wählen Sie den Vorgang aus, um weitere Informationen über die ACL zu erhalten. Wenn Sie beispielsweise **Lesen**auswählen, wird die mit dem Lesen verbundene Zugriffssteuerung angezeigt.

ACL-Details

Feld	Beschreibung
Name	Name der ACL.
Entscheidungstyp	Für die ACL konfigurierter Entscheidungstyp. **Zugriff zulassen oder Zugriffverweigern**.
Gilt für Bedingung	Gibt an, ob die ACL auf eine Bedingung angewendet wird.
ACL gilt für	Details zur Ressource, auf die die ACL angewendet wird.
Status	Status des ACL- oder Zugriffsergebnisses.
Erforderliche ACL-Rollen	Details der Rolle, die für den Zugriff auf die Ressource erforderlich ist.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Rolle	Status der Rolle. „Bestanden“, „Übersprungen“ oder „Blockiert“.



Zeigen Sie Berechtigungen für einen Anwender an

Verwenden Sie die Zugriffsanalyse, um Berechtigungen für einen ausgewählten Anwender anzuzeigen.

Vorbereitungen

Erforderliche Rolle: admin

Im folgenden Verfahren werden Beispielschritte zum Anzeigen von Berechtigungen für einen ausgewählten Benutzer (**ITIL-Benutzer**) beschrieben, um die Berechtigungen der **Incident** -Tabelle mithilfe des Bewertungszugriffs in der Zugriffsanalyse anzuzeigen.

Hinweis: Die Zugriffsanalyse ist ein Produkt des ServiceNow® Store.

Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Berechtigungen analysieren**an.
   Die Homepage „Zugriffe und Berechtigungen analysieren“ wird angezeigt.
2. Wählen Sie Ihre Kriterien wie folgt aus:

Wählen Sie Ihre Kriterien für die Analyse von Zugriffen und Berechtigungen aus

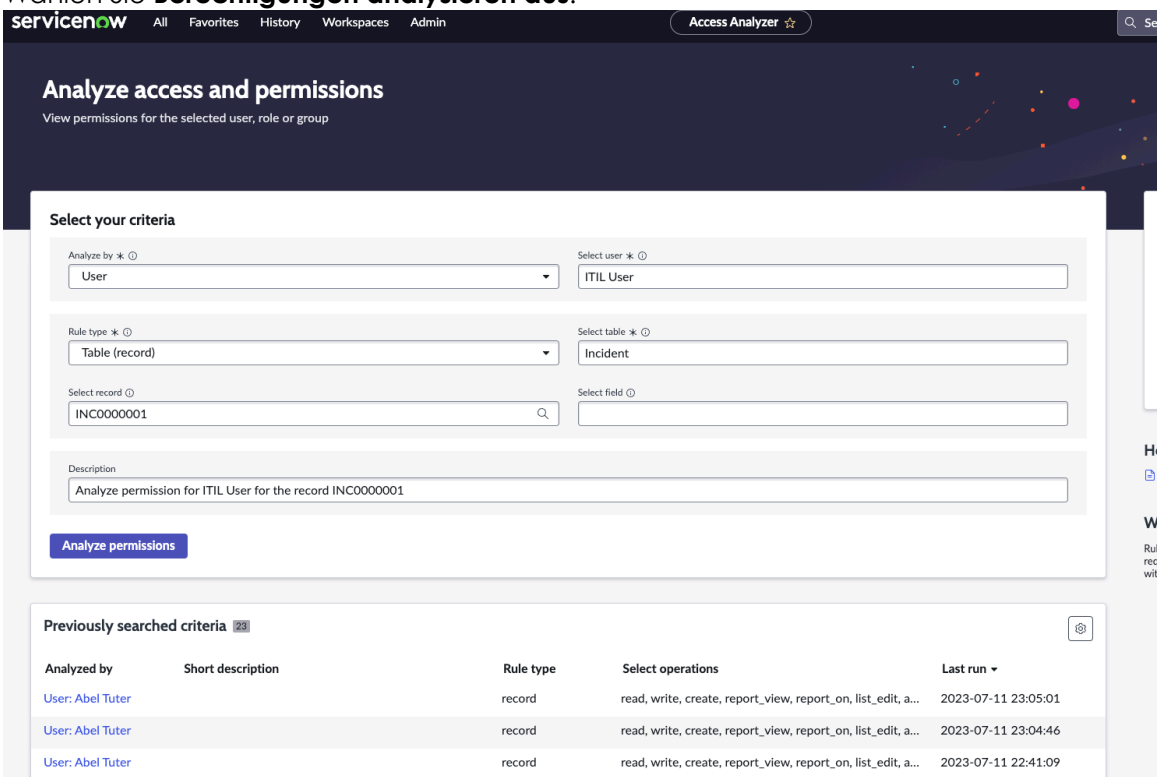
Feld	Beschreibung
Analysieren nach *	Wählen Sie **Benutzer** aus.
Anwender auswählen *	Geben Sie einen Anwendernamen an, den Sie aus der Liste auswählen möchten. In diesem Beispiel **ITIL-Benutzer**.
Regeltyp *	Analysieren Sie den Zugriff für eine **Tabelle**, eine **UI-Seite**, einen **REST-Endpunkt**oder eine vom **Client aufrufbare Skripteinbindung**. Im Beispiel `Tabelle`.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

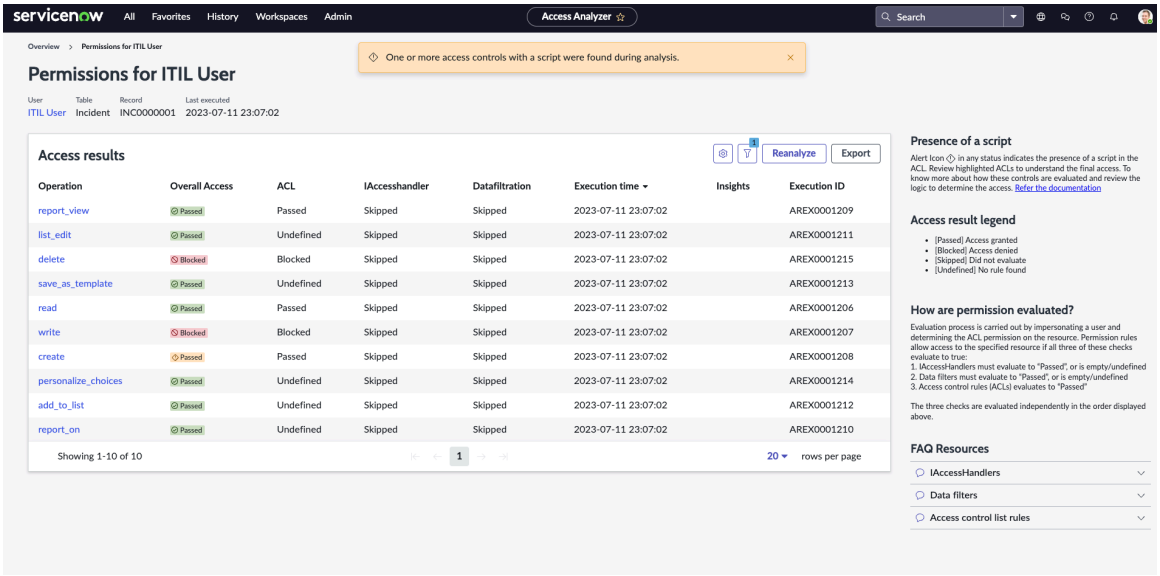
Feld	Beschreibung
Tabelle auswählen *	Geben Sie einen Tabellennamen an, um ihn aus der Liste auszuwählen. In diesem Beispiel **Incident**.
Datensatz auswählen	Geben Sie einen Datensatznamen an, um ihn aus der Liste auszuwählen. In diesem Beispiel **INC0000001**.
Feld auswählen	Geben Sie einen Feldnamen an, um ihn aus der Liste auszuwählen. Dieses Feld kann verwendet werden, um Berechtigungen auch auf Feldebene zu analysieren. Zum Beispiel „Aktiv“, „Erstellt von“ usw.

3. Geben Sie die Beschreibung im Feld **Beschreibung** an.
4. Wählen Sie **Berechtigungen analysieren aus**.



Die **Zugriffsergebnisse** für den **ITIL-Benutzer** werden angezeigt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



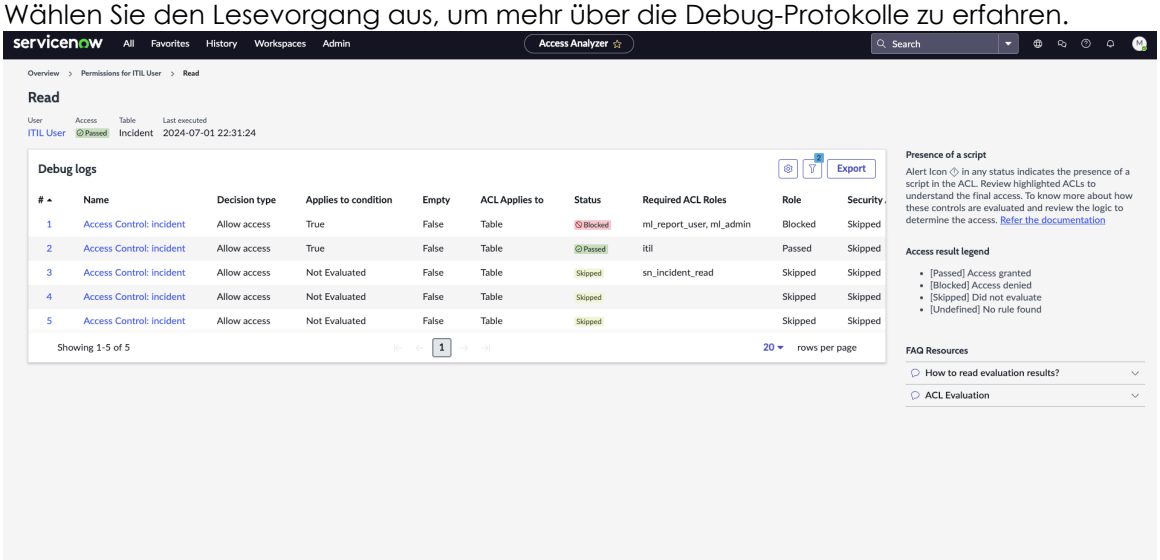
Die Ergebnisse können unter Verweis auf die Filter Legenden, Zugriffssteuerungsliste (ACL), IAccesshandler und Daten gelesen werden.

Nehmen wir das Beispiel eines **Lesevorgangs**. Für den **ITIL-Benutzer** ist der Gesamtzugriff Bestanden, was bedeutet, dass der Benutzer den Datensatz mit den richtigen Berechtigungen (ACL) lesen kann.

Ebenso wird für den **Erstellungsvorgang** der Gesamtzugriff mit einem Warnungssymbol übergeben, was bedeutet, dass ein Skript für die ACL-Bewertung vorhanden sein könnte.

Hinweis: Im Beispiel sind **Schreib-** und **Löschvorgänge** für den ausgewählten Anwender blockiert, und der Anwender kann den ausgewählten Datensatz nicht bearbeiten oder löschen (INC0000001).

5. Wählen Sie den Lesevorgang aus, um mehr über die Debug-Protokolle zu erfahren.



Auf der Seite „Protokolle debuggen“ wurden die Geschäftsregel und die zugehörigen ACLs angezeigt, die zum Ausführen des **Lesevorgangs** für den Datensatz erforderlich sind.

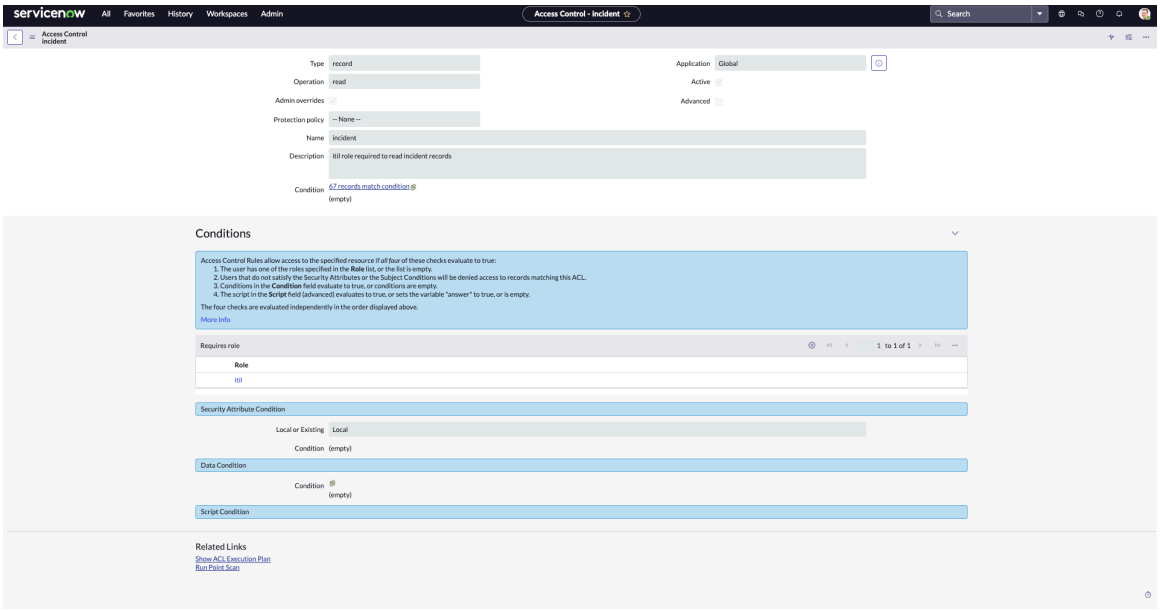
Aus den Debug-Protokollen geht hervor, dass für den Lesevorgang eine Geschäftsregel und vier ACLs zugeordnet sind.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

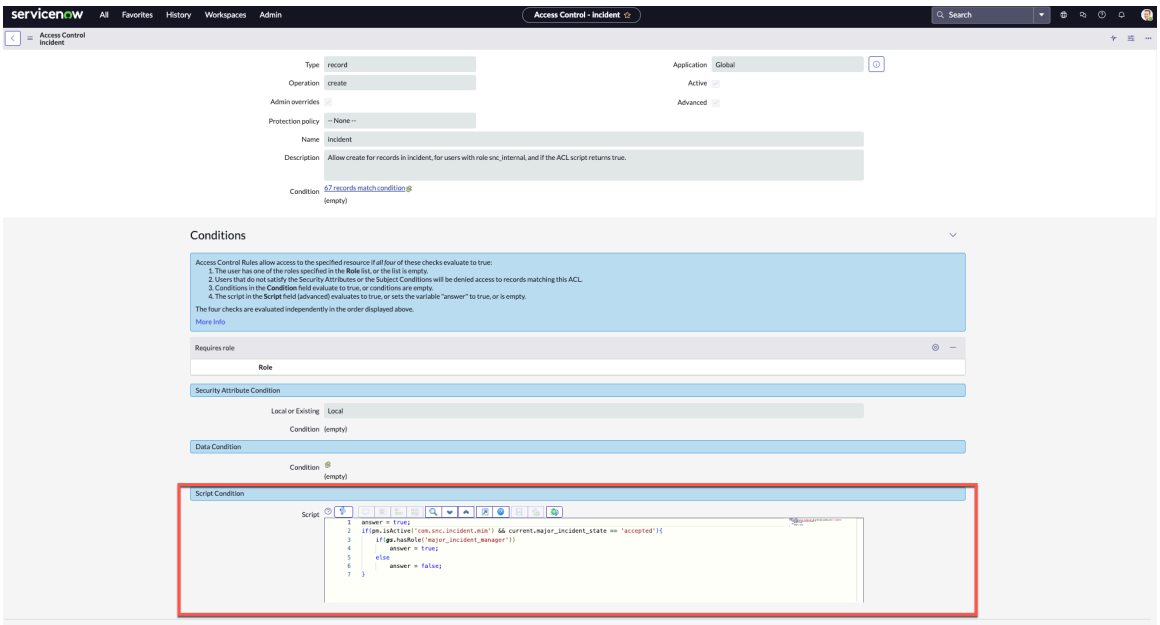
Für eine der ACLs gibt es den Status „ **Bestanden** “. Um den ausgewählten Datensatz zu lesen, muss der Anwender über die erforderliche ACL verfügen und den Datensatz lesen. Da eine der ACLs **Bestanden**ist, gelten die anderen ACL-Bewertungen als **Übersprungen**.

6. Wählen Sie die Zugriffssteuerung aus, die übergeben wird, um die Details der ACL zu erfahren.



Die Details der Zugriffssteuerung für die ausgewählte ACL werden angezeigt.

Für einen ausgewählten Vorgang mit **„Bestanden“** und Vorhandensein eines Skripts. Auf der Seite „Zugriffssteuerung“ wird das zugehörige Skript für den Datensatz angezeigt.



Zeigen Sie Berechtigungen für eine Rolle an

Verwenden Sie die Zugriffsanalyse, um Berechtigungen für eine ausgewählte Rolle anzuzeigen.

Vorbereitungen

Erforderliche Rolle: admin

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das folgende Verfahren beschreibt die Beispielschritte zum Anzeigen von Berechtigungen für eine ausgewählte Rolle (**user_admin**), um die Berechtigung für einen REST-API-Endpunkt mithilfe des Bewertungszugriffs in der Zugriffsanalyse anzuzeigen.

Hinweis: Die Zugriffsanalyse ist ein Produkt des ServiceNow® Store.

Prozedur

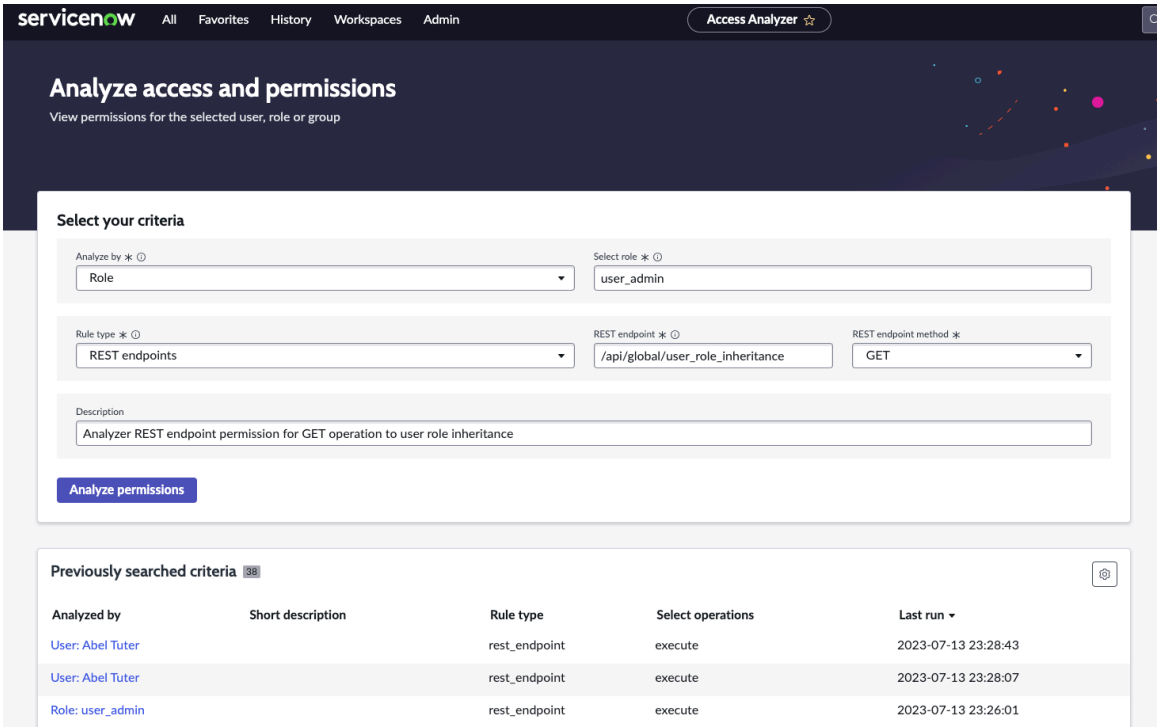
1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Berechtigungen analysieren**an.
   Die Homepage „Zugriffe und Berechtigungen analysieren“ wird angezeigt.
2. Wählen Sie Ihre Kriterien wie folgt aus:

Wählen Sie Ihre Kriterien für die Analyse von Zugriffen und Berechtigungen aus

Feld	Beschreibung
Analysieren nach *	Wählen Sie **Rolle aus**.
Anwender auswählen *	Geben Sie eine Rolle an, die aus der Liste ausgewählt werden soll. Beispiel: **user_admin**.
Regeltyp *	Analysieren Sie den Zugriff für eine Tabelle, eine UI-Seite, einen REST-Endpunkt oder eine vom Client aufrufbare Skripteinbindung. Beispiel: **REST-Endpunkt**.
REST-Endpunkt*	Geben Sie einen REST-Endpunkt an. Beispiel: `/api/global/user_role_inheritance`. **Hinweis:** Bei Verwendung des ausgewählten Felds muss der vollständige REST-Endpunkt verwendet werden.
REST-Endpunktmethode *	Geben Sie eine REST-Endpunktmethode an. Beispiel: GET.

3. Geben Sie die Beschreibung im Feld **Beschreibung** an.
4. Wählen Sie **Berechtigungen analysieren aus**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die **Zugriffsergebnisse** für die Rolle **user_admin** werden angezeigt.

Die Ergebnisse können unter Verweis auf die Filter Legenden, Zugriffssteuerungsliste (ACL), IAccesshandler und Daten gelesen werden.

Der Gesamtzugriff für die Rolle wird übergeben, was bedeutet, dass die Rolle (**user_admin**) auf den **REST-Endpunkt** für die ausgewählte **GET** -Methode zugreifen kann.

Zeigen Sie Berechtigungen für eine Gruppe an

Verwenden Sie die Zugriffsanalyse, um Berechtigungen für eine ausgewählte Gruppe anzuzeigen.

Vorbereitungen

Erforderliche Rolle: admin

Das folgende Verfahren beschreibt die Beispielschritte zum Anzeigen von Berechtigungen für eine ausgewählte Gruppe (**Incident-Management**), um die Berechtigungen einer **Incident-UI** -Seite mithilfe des Bewertungszugriffs in der Zugriffsanalyse anzuzeigen.

Hinweis: Die Zugriffsanalyse ist ein Produkt des ServiceNow® Store.

Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Berechtigungen analysieren**an.
   Die Homepage „Zugriffe und Berechtigungen analysieren“ wird angezeigt.
2. Wählen Sie Ihre Kriterien wie folgt aus:

Wählen Sie Ihre Kriterien für die Analyse von Zugriffen und Berechtigungen aus

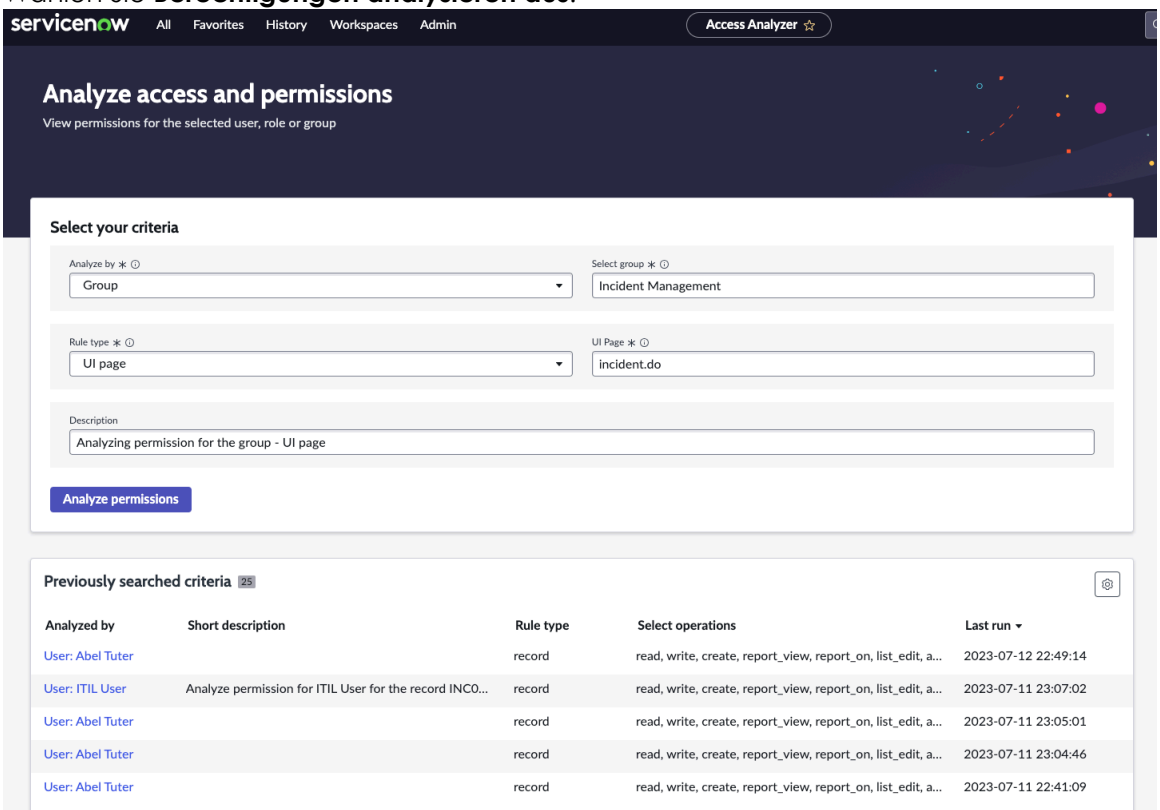
Feld	Beschreibung
Analysieren nach *	Wählen Sie **Gruppe**aus.

Automatische Übersetzung

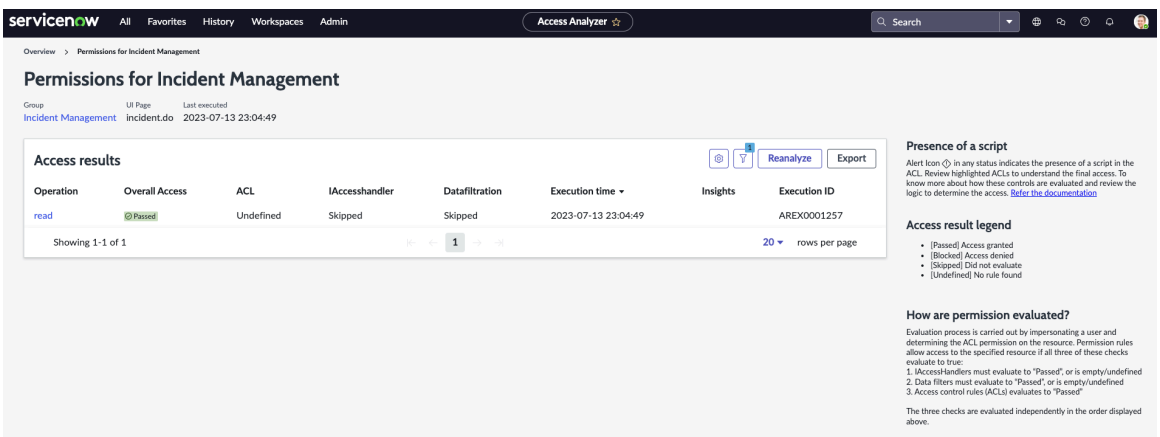
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Anwender auswählen *	Geben Sie einen Anwendernamen an, den Sie aus der Liste auswählen möchten. Beispiel: **Incident Management**.
Regeltyp *	Analysieren Sie den Zugriff für eine Tabelle, eine UI-Seite, einen REST-Endpunkt oder eine vom Client aufrufbare Skripteinbindung. Beispiel: **UI-Seite**.
UI-Seite *	Geben Sie die UI-Seite an. Beispiel: **incident.do**.

3. Geben Sie die Beschreibung im Feld **Beschreibung** an.
4. Wählen Sie **Berechtigungen analysieren aus**.



Die **Zugriffsergebnisse** für die **Incident-Management** -Gruppe werden angezeigt.



© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Ergebnisse können unter Verweis auf die Filter Legenden, Zugriffssteuerungsliste (ACL), IAccesshandler und Daten gelesen werden.

Der Gesamtzugriff für die Gruppe wird übergeben, was bedeutet, dass die Benutzer innerhalb der Gruppe (**Incident-Management**) auf den Incident-Datensatz zugreifen können.

Abfragen der Exportzugriffsanalyse

Exportieren Sie die mit der Zugriffsanalyse analysierten Abfragen.

Vorbereitungen

Erforderliche Rolle: admin

Im folgenden Verfahren werden die Schritte für den Zugriff auf die Zugriffsanalyse und die Verwendung der verschiedenen Funktionen der Zugriffsanalyse beschrieben.

Hinweis: Die Zugriffsanalyse ist ein Produkt des ServiceNow® Store.

Prozedur

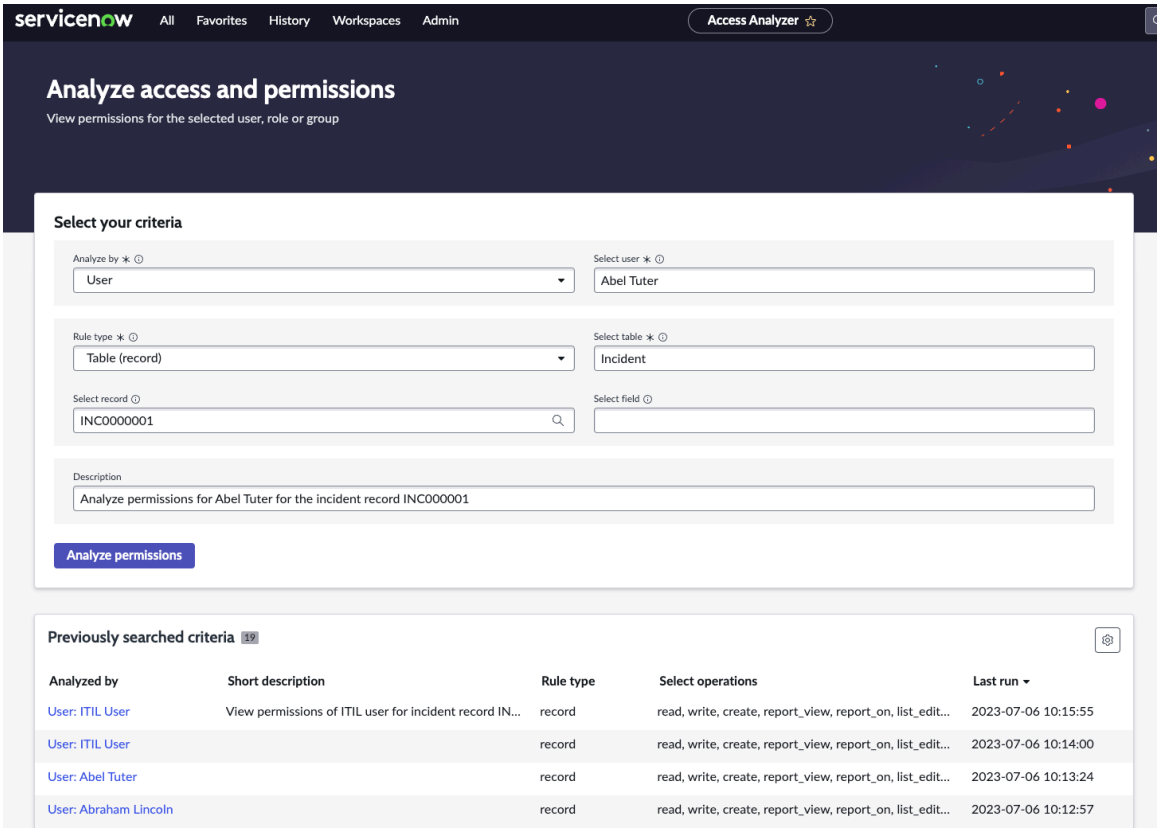
1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Berechtigungen analysieren**an.
   Die Homepage „Zugriffe und Berechtigungen analysieren“ wird angezeigt.
2. Wählen Sie Ihre Kriterien wie folgt aus:

Wählen Sie Ihre Kriterien für die Analyse von Zugriffen und Berechtigungen aus

Feld	Beschreibung
Analysieren nach *	Analysieren Sie den Zugriff für einen Anwender, eine Rolle oder eine Gruppe
Anwender auswählen *	Geben Sie einen Anwendernamen an, den Sie aus der Liste auswählen möchten.
Regeltyp *	Analysieren Sie den Zugriff für eine Tabelle, eine UI-Seite, einen REST-Endpunkt oder eine vom Client aufrufbare Skripteinbindung.
Tabelle auswählen *	Geben Sie einen Tabellennamen an, um ihn aus der Liste auszuwählen.
Datensatz auswählen	Geben Sie einen Datensatznamen an, um ihn aus der Liste auszuwählen.
Feld auswählen	Geben Sie einen Feldnamen an, um ihn aus der Liste auszuwählen.

3. Geben Sie die Beschreibung im Feld **Beschreibung** an.
4. Wählen Sie **Berechtigungen analysieren aus**.

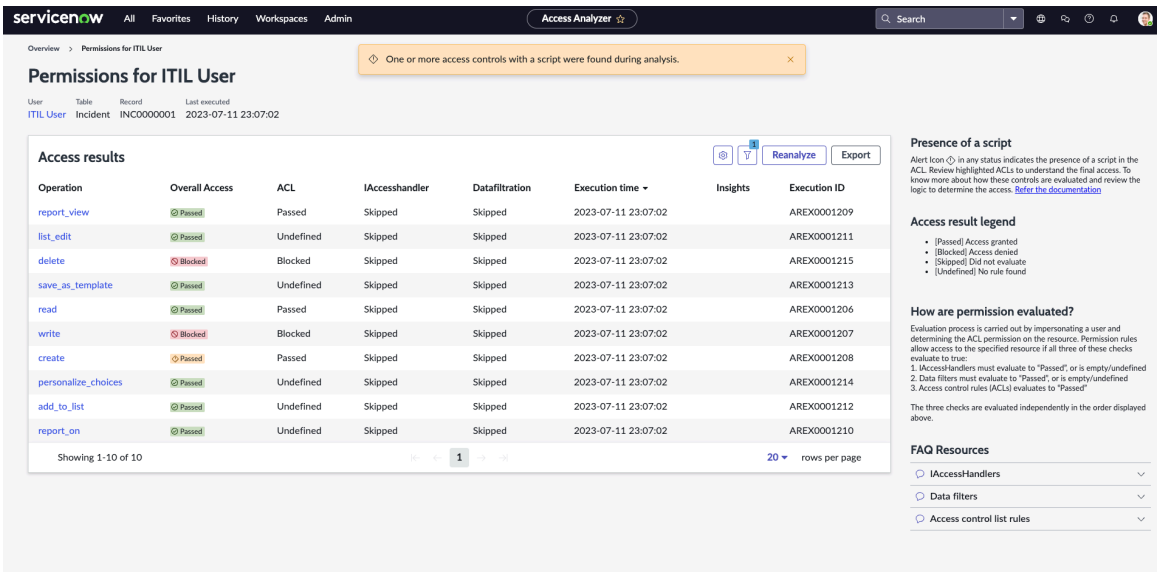
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die Zugriffsergebnisse für den Anwender werden angezeigt. Auf ähnliche Weise können Sie die Berechtigungen einer Gruppe bzw. Rolle für die folgenden Regeltypen analysieren:

- Tabelle (Datensatz)
- Vom Client aufrufbare Skripteinbindung
- REST-Endpunkte

Die **Zugriffsergebnisse** für den ausgewählten Regeltyp werden angezeigt.

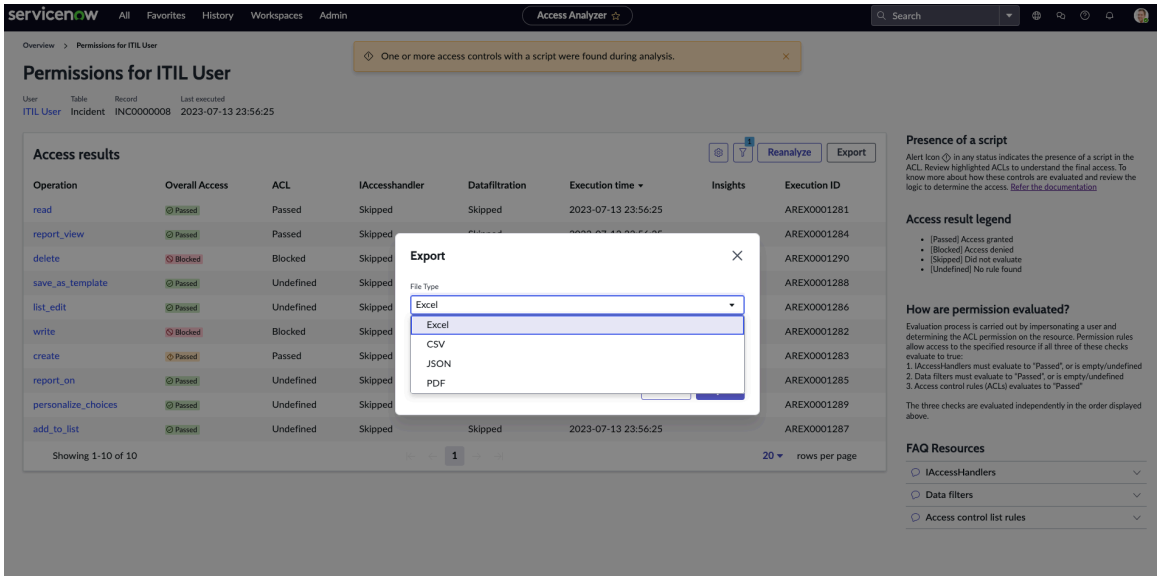


5. Klicken Sie auf **Exportieren**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

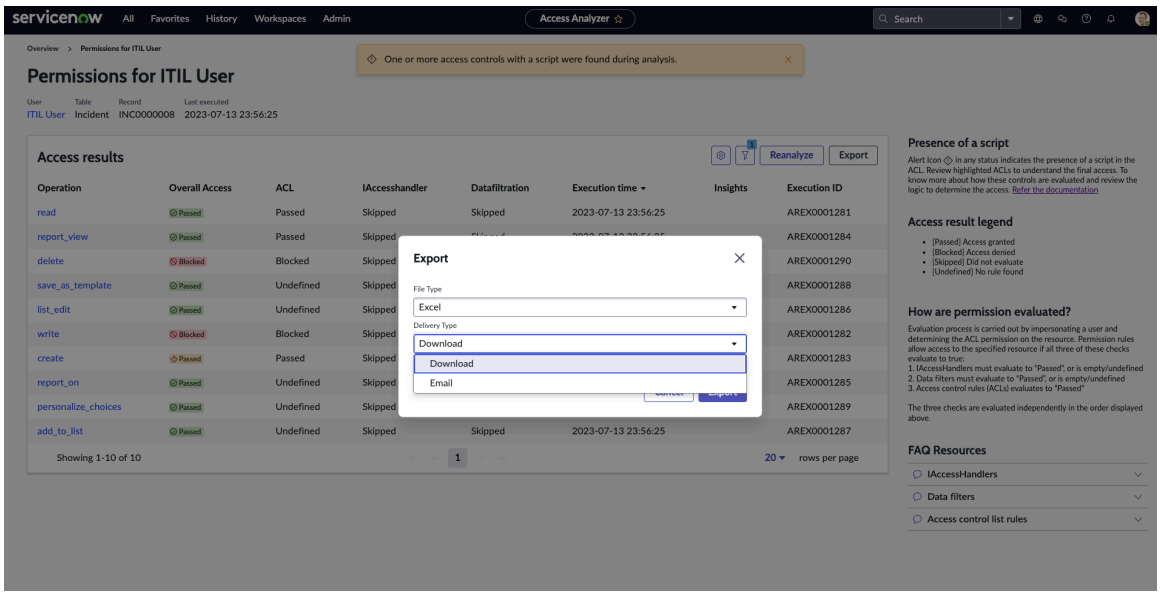
a. Wählen Sie den Dateityp aus.

Verfügbare Dateitypen: Excel, CSV, JSON, PDF.



b. Wählen Sie die Lieferart aus.

Verfügbare Bereitstellungstypen sind Download und E-Mail.



Vergleichen von Anwenderdatensätzen

Vergleichen Sie Benutzerdatensätze, um den Zugriff zwischen zwei Benutzern zu verstehen.

Vorbereitungen

Erforderliche Rolle: admin

Im folgenden Verfahren werden die Schritte zum Vergleichen von Benutzerdatensätzen mit der Zugriffsanalyse beschrieben.

Hinweis: Die Zugriffsanalyse ist ein ServiceNow® Store -Produkt.

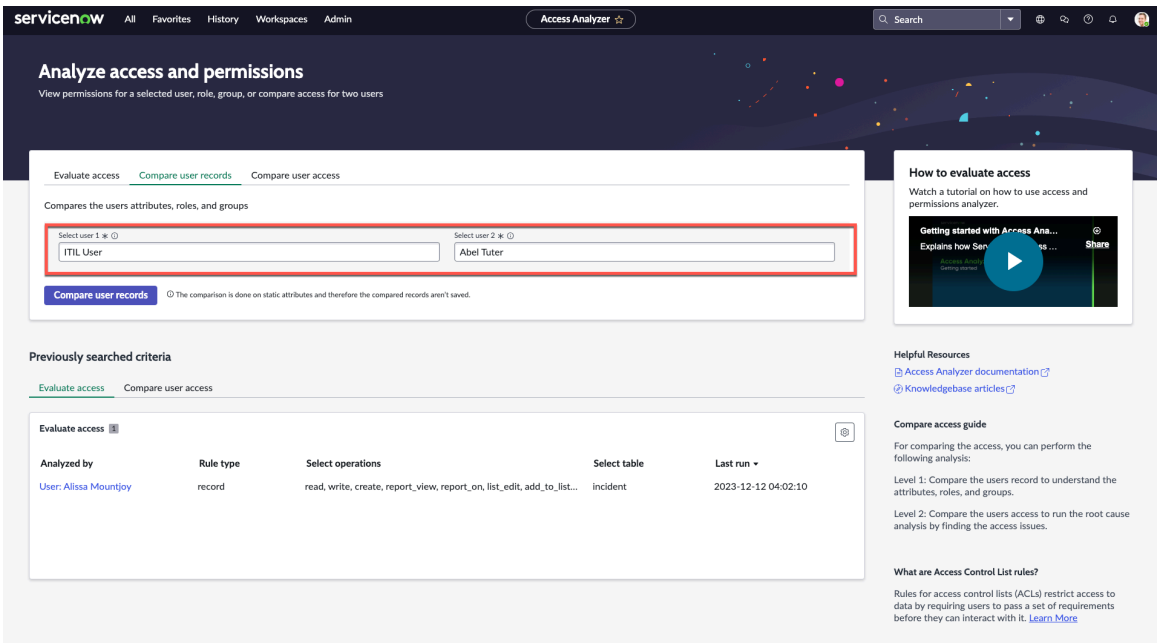
Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Berechtigungen analysieren**an.
   Die Homepage „Zugriffe und Berechtigungen analysieren“ wird angezeigt.
2. Wählen Sie die Registerkarte **Anwenderdatensätze vergleichen**.
3. Wählen Sie **Anwender 1** und **Anwender 2** zum Vergleich aus.

   Beispiel: `ITIL-Benutzer` als **Benutzer 1** und `Abel Tuter` als **Benutzer 2**.



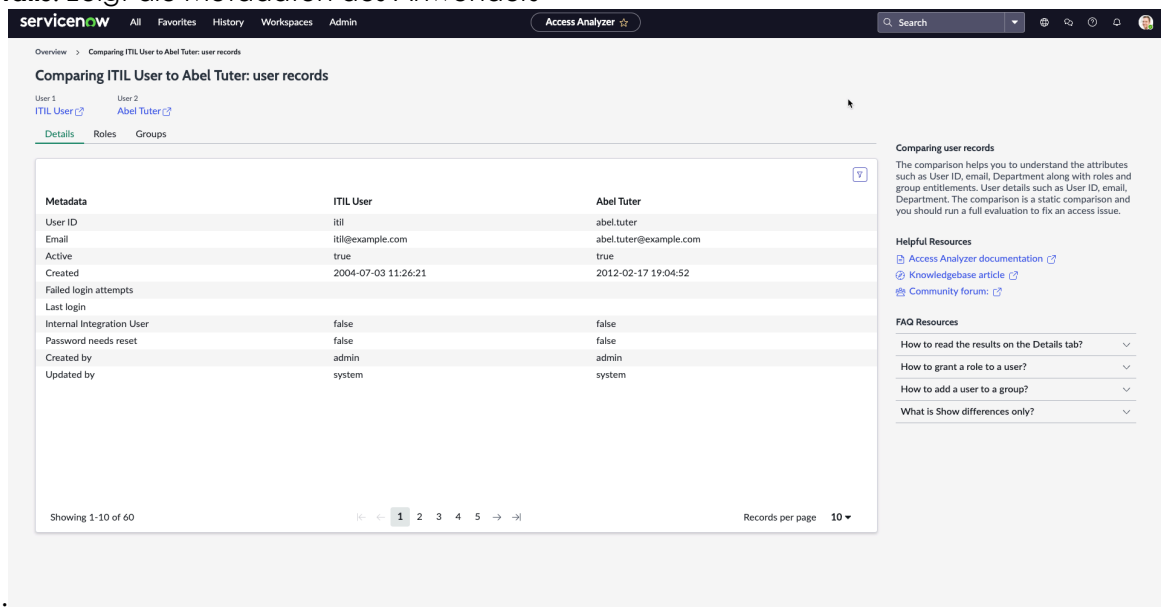
4. Wählen **Sie Anwenderdatensätze vergleichen**.

   Die Ergebnisse werden auf den folgenden Registerkarten angezeigt:

Automatische Übersetzung

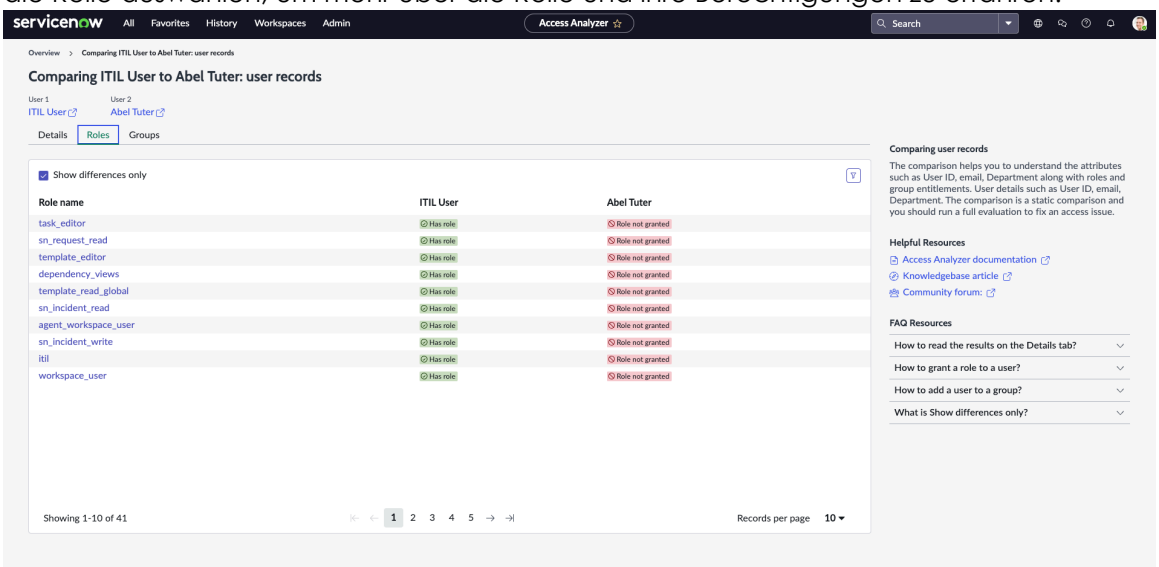
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Details**: Zeigt die Metadaten des Anwenders



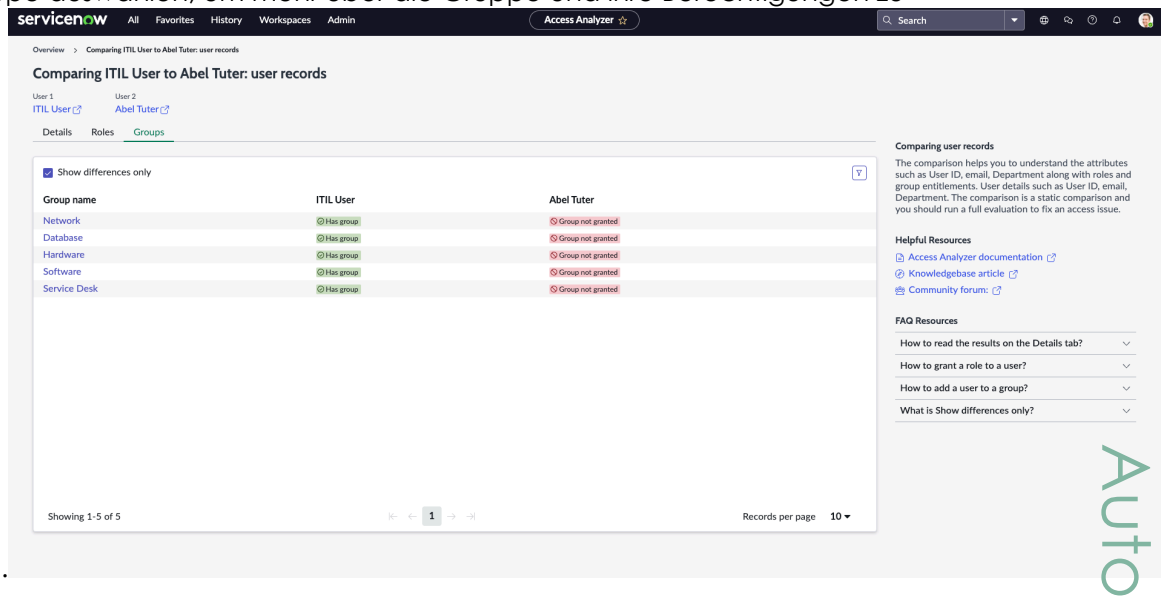
an.

- **Rollen**: Zeigen Sie die Rollen an, die dem Anwender zugewiesen sind. Sie können die Rolle auswählen, um mehr über die Rolle und ihre Berechtigungen zu erfahren.



© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Gruppen**: Zeigen Sie die Gruppen an, die dem Anwender zugewiesen sind. Sie können die Gruppe auswählen, um mehr über die Gruppe und ihre Berechtigungen zu erfahren.



Auf ähnliche Weise können Sie verschiedene Benutzer in der Instanz ServiceNow vergleichen, um zu verstehen, welcher Zugriff ihnen zugewiesen ist.

Vergleich des Anwenderzugriffs

Vergleichen Sie die Zugriffssteuerung des -Benutzers mit der Zugriffsanalyse.

Vorbereitungen

Erforderliche Rolle: admin

Das folgende Verfahren beschreibt die Schritte zum Vergleichen der Zugriffssteuerung zwischen den Anwendern mithilfe der Zugriffsanalyse.

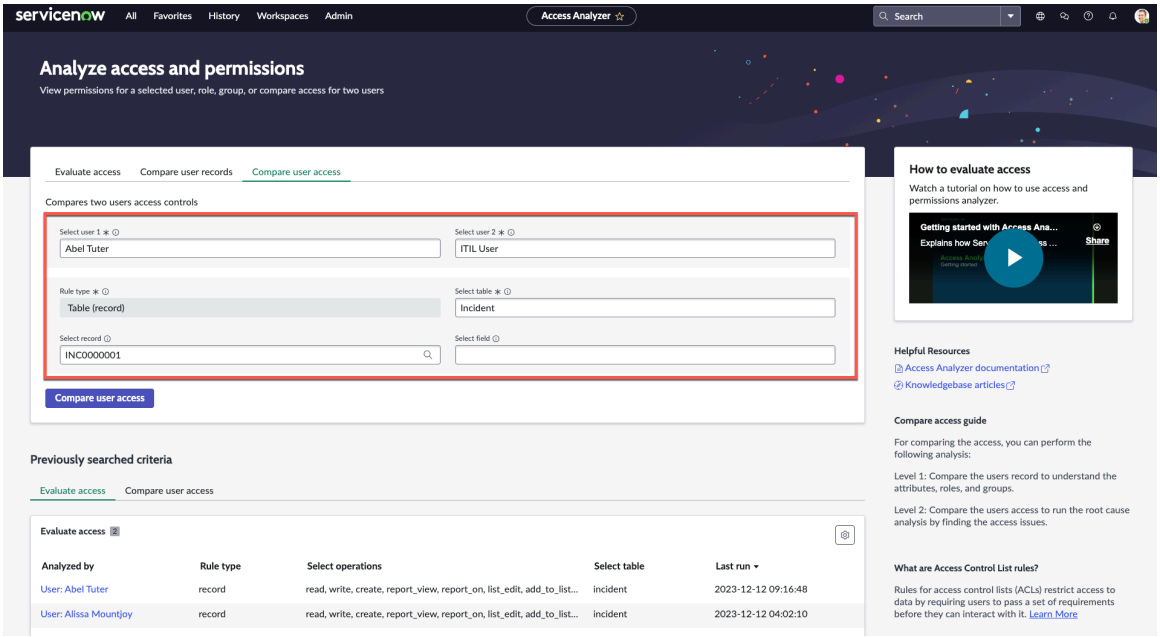
Hinweis: Die Zugriffsanalyse ist ein ServiceNow® Store -Produkt.

Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Berechtigungen analysieren**an.
   Die Homepage „Zugriffe und Berechtigungen analysieren“ wird angezeigt.
2. Wählen Sie die Registerkarte **Anwenderzugriff vergleichen**.
3. Füllen Sie folgende Felder aus:

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Benutzerzugriff vergleichen

Feld	Beschreibung
Anwender auswählen 1*	Geben Sie einen Anwendernamen an, den Sie in der Liste für den Vergleich auswählen möchten.
Anwender auswählen 2*	Geben Sie einen Anwendernamen an, der aus der Liste ausgewählt und mit Anwender 1 verglichen werden soll.
Regeltyp*	Analysieren Sie die Zugriffsberechtigungen für eine Tabelle. **Hinweis:** Für den **Vergleich des Anwenderzugriffs**können nur Zugriffsberechtigungen für eine Tabelle verwendet werden.
Tabelle auswählen*	Geben Sie einen Tabellennamen an, um ihn aus der Liste auszuwählen.
Datensatz auswählen	Geben Sie einen Datensatznamen an, um ihn aus der Liste auszuwählen.
Feld auswählen	Geben Sie einen Feldnamen an, um ihn aus der Liste auszuwählen.

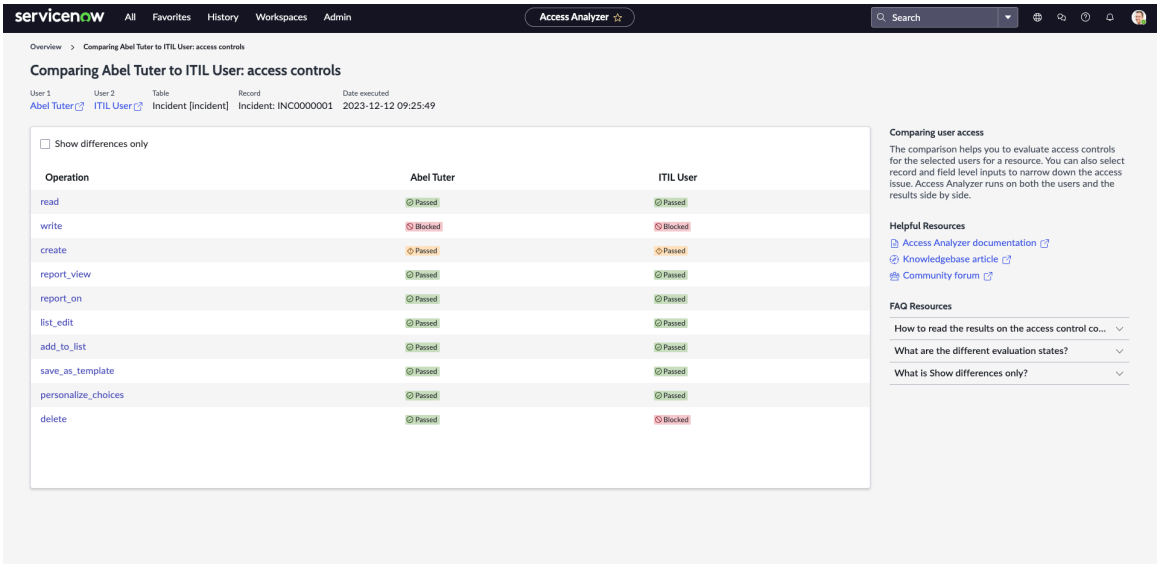
4. Wählen **Sie Anwenderzugriff vergleichen aus**.

   Die Ergebnisse des **Anwenderzugriffsvergleichs** für die ausgewählten Anwender werden angezeigt.

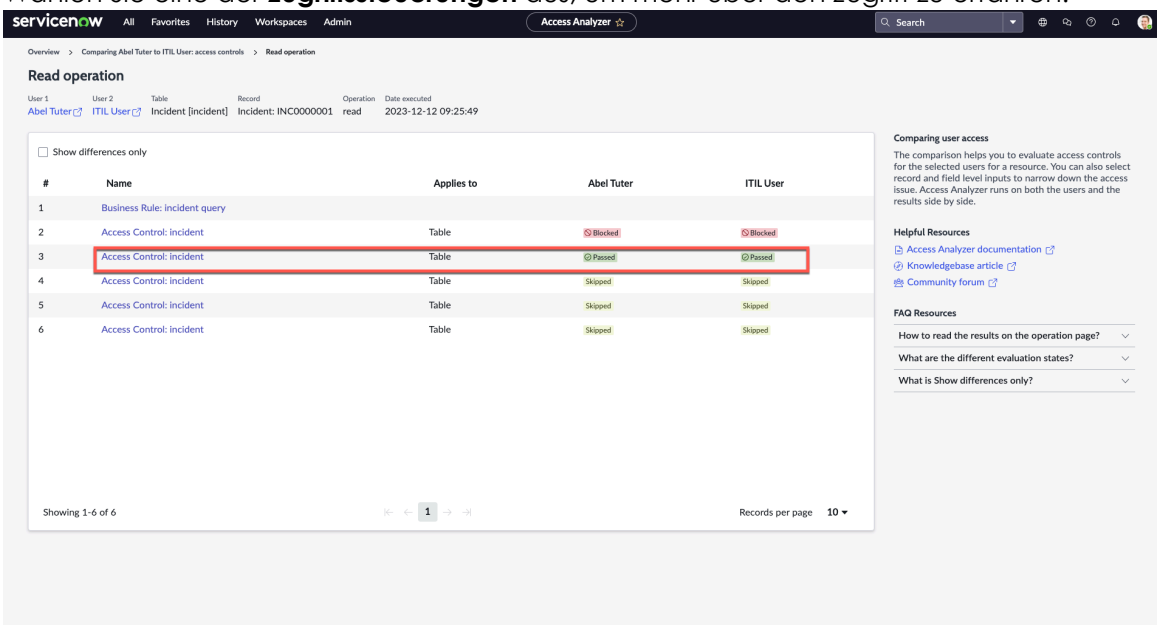
   Die Ergebnisse des Anwenderzugriffsvergleichs zeigen den Vorgang und den Zugriffsauswertungsstatus für die Anwender an. Beispiel: Abel Tuter und ITIL User.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

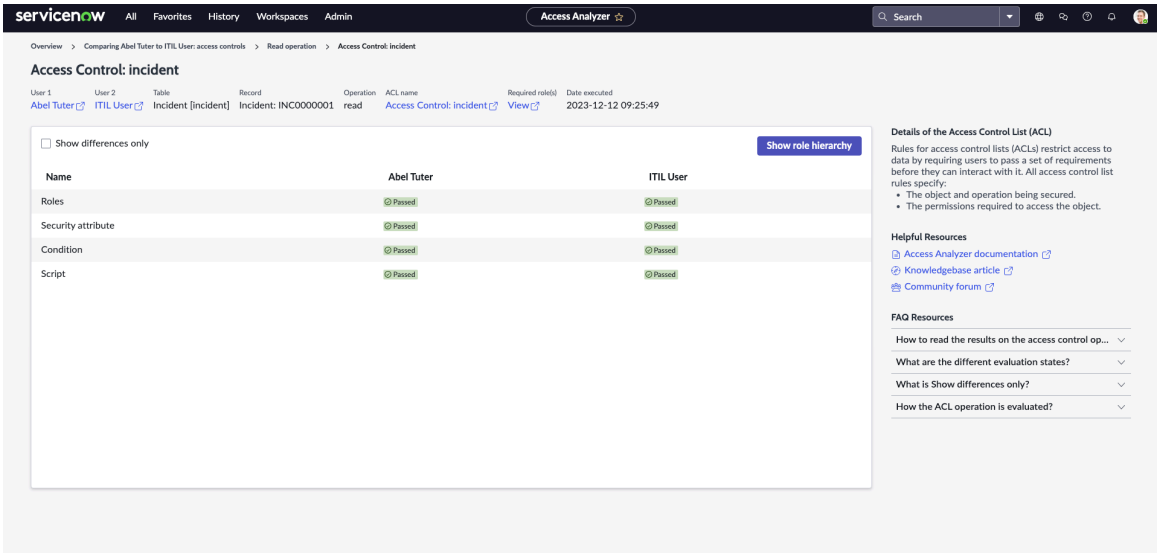


5. Wählen Sie den Vorgang aus, um mehr über die Berechtigungsauswertung und die Rollen zu erfahren, denen die Benutzer zugewiesen sind.
   Beispiel: **Lesevorgang**.
6. Wählen Sie eine der **Zugriffssteuerungen** aus, um mehr über den Zugriff zu erfahren.



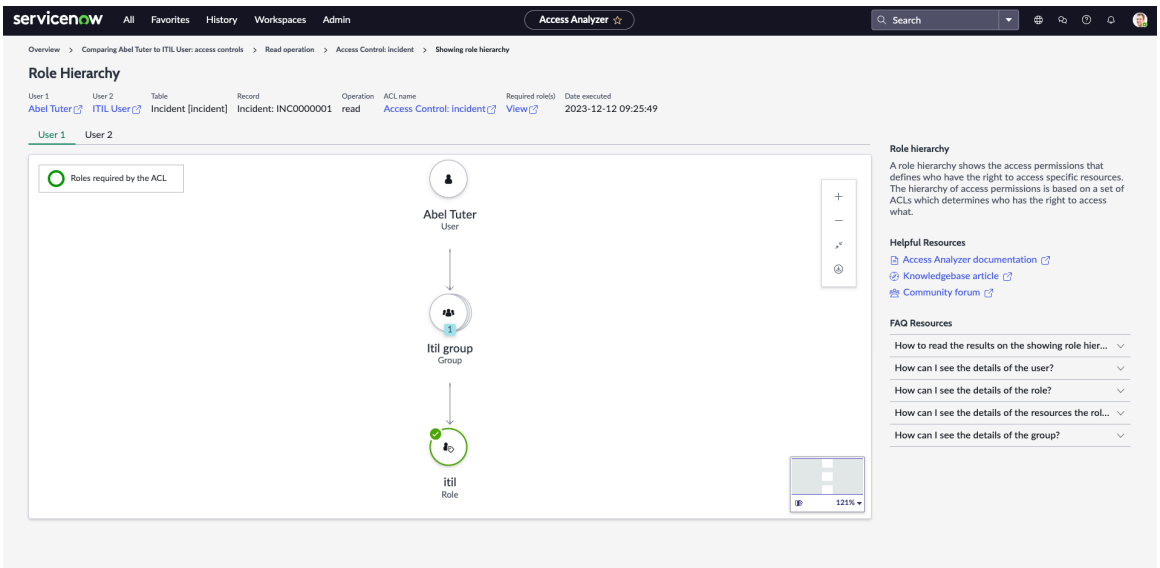
Die Details der Zugriffssteuerung wie Rollen, Sicherheitsattribut, Bedingung und Skriptauswertungsstatus werden angezeigt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Wählen Sie **Rollenhierarchie anzeigen** aus, um mehr über die Rollen und Gruppen zu erfahren, die dem Anwender zugewiesen sind, und vergleichen Sie die beiden Anwender.

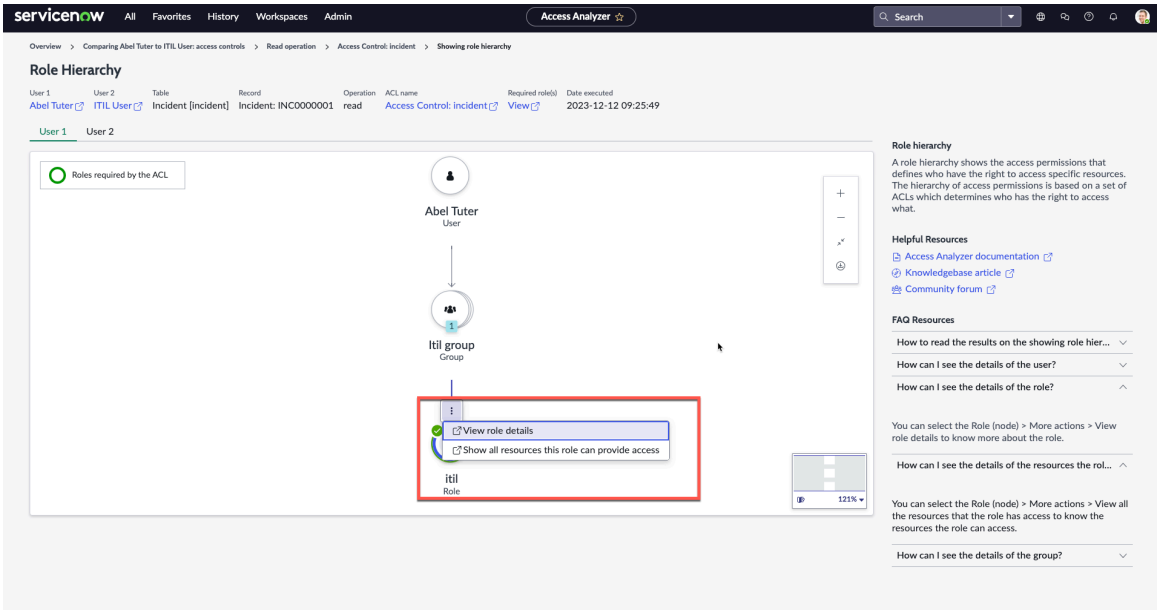
   Basierend auf der Rollenhierarchie können Sie dem Benutzer die erforderlichen Rollen- und Gruppenzuweisungen zuweisen, um Zugriff auf die Ressourcen (Tabelle) zu erhalten.



Im Beispiel ist **Abel Tuter** und **ITIL** -Benutzer der Benutzer `itil` zugewiesen. Beide Zugriffssteuerungen wurden also bestanden. Sie können die erforderliche Rollen- und Gruppenzuweisung für den Benutzer ermitteln, indem Sie sich die Rollenhierarchie ansehen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können den Knoten auswählen, um mehr über die Rolle, Ressourcen, auf die sie zugreifen kann, oder Gruppe zu erfahren.



Abfragen der Zugriffsanalyse anzeigen – Zuvor gesuchte Kriterien

Zeigen Sie zuvor gesuchte Kriterien für die Zugriffsanalyse an.

Vorbereitungen

Erforderliche Rolle: admin

Hinweis: Die Zugriffsanalyse ist ein ServiceNow® Store -Produkt.

Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Abfragen der Zugriffsanalyse**an.

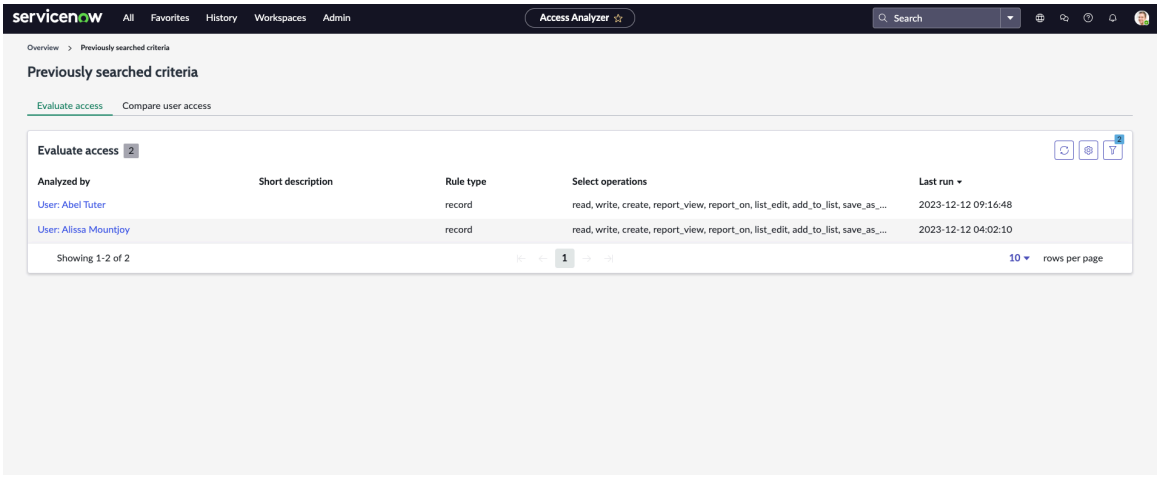
   Zuvor gesuchte Kriterien haben die folgenden Abschnitte:

   - **Zugriff auswerten**: Zeigt Ergebnisse basierend auf Abfragen an, die über die Funktionen zum **Auswerten des Zugriffs** gestellt wurden.
   - **Anwenderzugriff vergleichen**: Zeigt Ergebnisse basierend auf Abfragen an, die über die Funktionen zum **Vergleichen des Anwenderzugriffs** gestellt wurden.

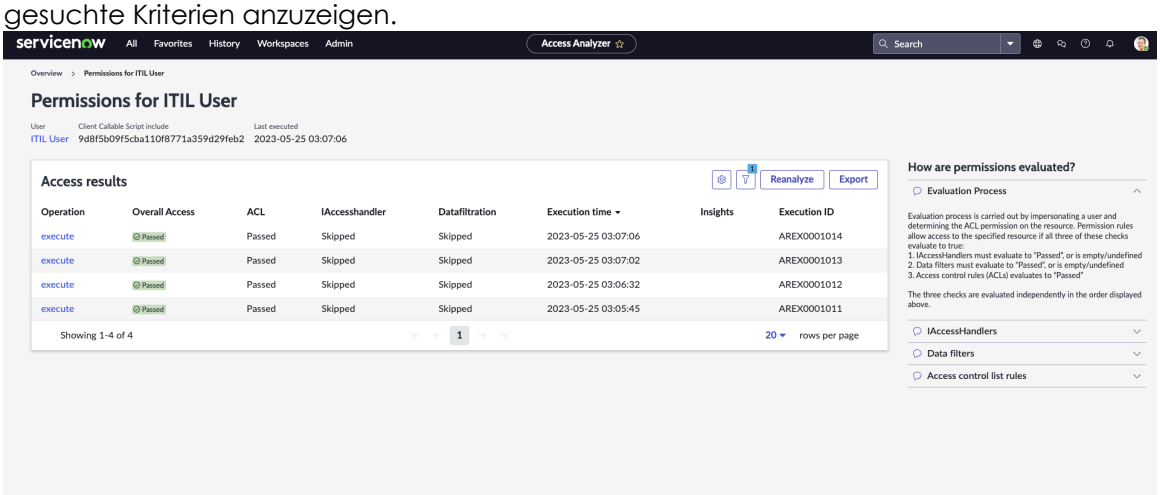
   Hinweis: Die zuvor gesuchten Kriterien werden nicht gespeichert, wenn Sie die Funktion zum Vergleichen von Anwenderdatensätzen verwenden.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

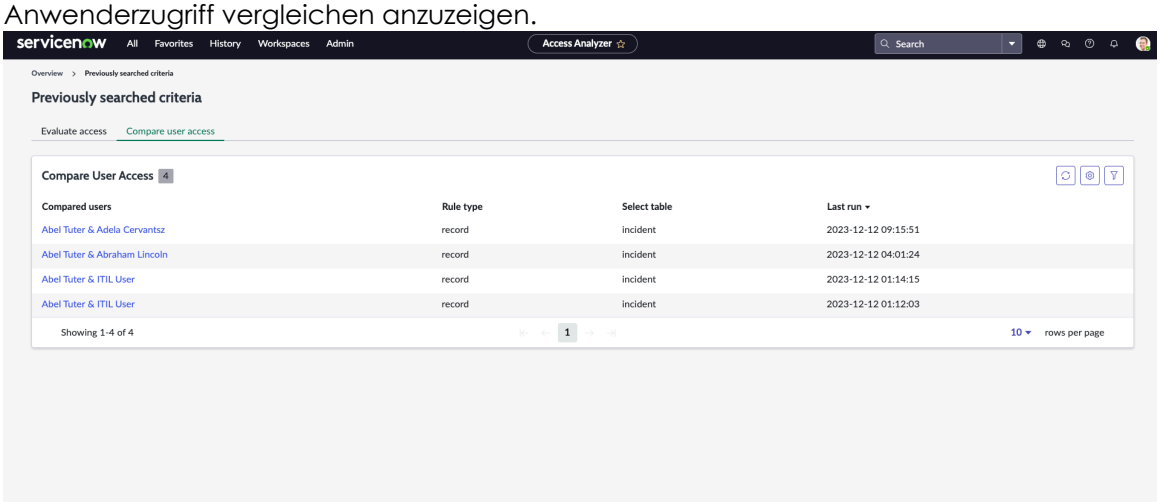


2. Wählen Sie im Abschnitt Zugriff auswerten die **Option Analysiert nach** Links, um zuvor gesuchte Kriterien anzuzeigen.



Sie können Zugriff für Benutzer **neu analysieren** auswählen. Exportieren Sie die Details mit der Option **Exportieren**.

3. Wählen Sie die Links **Vergleichte Anwender**, um die zuvor gesuchten Kriterien im Abschnitt Anwenderzugriff vergleichen anzuzeigen.



Berechtigungsauswertung

Kriterien für Berechtigungsauswertung bei Verwendung der Zugriffsanalyse.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auswertungshierarchie

Die Berechtigung für den ausgewählten Anwender, die ausgewählte Gruppe oder die ausgewählte Rolle wird in der folgenden Hierarchie ausgewertet:

- Geschäftsregel: Eine Geschäftsregel ist ein serverseitiges Skript, das ausgeführt wird, wenn ein Datensatz angezeigt, eingefügt, aktualisiert oder gelöscht wird oder wenn eine Tabelle abgefragt wird.
- Zugriffshandler: Eine interne Systemprüfung mit ausgeblendetem Quellcode auf der Plattform.
- Datenfilterung: Der Datenfilter ist eine Form der Zugriffssteuerung, die auf die vorhandenen Zugriffssteuerungsregeln (ACLs) in Ihrer Instanz abgestimmt ist. Datenfilter unterstützen nur Lesevorgänge.
- Zugriffssteuerungsliste (ACL): Regeln für Zugriffssteuerungslisten (ACLs) schränken den Zugriff auf Daten ein, indem sie von Anwendern die Erfüllung einer Reihe von Anforderungen verlangen, bevor sie mit der Interaktion beginnen können. Innerhalb einer ACL wird die folgende Hierarchie ausgewertet:
  - Rolle
  - Sicherheitsattribut
  - Bedingung
  - Skript

Sie können den Zugriff und die Berechtigungen für den ausgewählten Anwender, die ausgewählte Rolle oder die ausgewählte Gruppe mit der Zugriffsanalyse analysieren. Die Berechtigungen werden basierend auf den folgenden Regeltypen ausgewertet:

- **Auswertung auf Tabellenebene**: Rollen- und Sicherheitsattribut-ACLs werden für die Auswertung auf Tabellenebene verwendet.
- Auswertung auf**Datensatz- oder Feldebene**: Für die Auswertung auf Datensatz- oder Feldebene werden ACLs für Rollen, Sicherheitsattribute, Bedingungen und Skriptebenen verwendet.
- **UI-Seite**: Unterstützt nur betriebsbereite Vorgänge. Nur ACLs auf Leseebene werden ausgewertet.
- **REST-Endpunkt**: Unterstützt nur Ausführungsvorgänge. Nur ACLs der Ausführungsebene werden ausgewertet.

Details zu den wichtigen Feldern in den Zugriffsergebnissen:

- Vorhandensein eines Skripts
- Auf die Ergebnislegende zugreifen
- Auswertungsvorgang
- IAccessHandlers
- Datenfilter
- Regeln der Zugriffssteuerungsliste

Vorhandensein eines Skripts

Das Warnungssymbol in jedem Status zeigt an, dass ein Skript in der ACL vorhanden ist. Überprüfen Sie die markierten ACLs, um den endgültigen Zugriff zu verstehen. Weitere

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen darüber, wie diese Steuerungen ausgewertet werden und wie die Logik zur Bestimmung des Zugriffs überprüft wird, finden Sie unter Debug-Protokolle der Zugriffsanalyse.

Legende in der Zugriffsanalyse

Bei der Analyse des Zugriffs und der Berechtigungen werden Legenden als Teil des Bewertungsprozesses angezeigt. Es folgen die Legenden:

- [Bestanden] Zugriff gewährt
- [Blockiert] Zugriff verweigert
- [Übersprungen] Wurde nicht ausgewertet
- [Nicht definiert] Keine Regel gefunden

Auswertungsvorgang

Der Bewertungsprozess wird durchgeführt, indem die Identität eines Benutzers angenommen und die Berechtigung der Zugriffssteuerungsliste (ACL) für die Ressource ermittelt wird. Berechtigungsregeln ermöglichen den Zugriff auf die angegebene Ressource, wenn die folgenden Prüfungen als „true“ ausgewertet werden:

- IAccessHandlers müssen als „Bestanden“ ausgewertet werden oder sind leer oder nicht definiert
- Datenfilter müssen als „Bestanden“ ausgewertet werden oder sind leer oder nicht definiert
- Zugriffssteuerungsregeln (ACLs) werden als „Bestanden“ ausgewertet.

IAccessHandlers

Eine interne Systemprüfung mit ausgeblendetem Quellcode auf der Plattform. IAccessHandler kann den Zugriff auf eine Ressource gewähren oder verweigern, ohne ACLs auszuwerten. Wenn IAccessHandler ignoriert wird, werden die ACLs ausgewertet.

Sie können die IAccessHandler-Prüfungen nicht ändern. Beispielsweise wird eine IAccessHandler-Implementierung für Zugriffsprüfungen auf Anwendungsressourcen wie Lesezugriff verwendet.

Datenfilter

Der Datenfilter ist eine Form der Zugriffssteuerung, die auf die vorhandenen Zugriffssteuerungsregeln (ACLs) in Ihrer Instanz abgestimmt ist.

Regeln der Zugriffssteuerungsliste

Regeln für Zugriffssteuerungslisten (ACLs) schränken den Zugriff auf Daten ein, indem sie von Anwendern die Erfüllung einer Reihe von Anforderungen verlangen, bevor sie mit der Interaktion beginnen können.

Häufige Fragen

Häufig gestellte Fragen bei der Verwendung der Zugriffsanalyse.

Zugriff auswerten

Im Folgenden finden Sie einige Fragen, die bei Verwendung der Funktion „Zugriff auswerten“ in der Zugriffsanalyse häufig gestellt werden:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Häufige Fragen

Fragen	Erklärung
Wie werden die von der Zugriffsanalyse angezeigten Bewertungsergebnisse gelesen?	Jede Zeile stellt eine einzelne Zugriffssteuerungsliste (ACL) dar. Die Reihenfolge (#) in den Ergebnissen gibt die Reihenfolge an, in der ACLs ausgewertet werden. Der Status zeigt an, ob der Gesamtzugriff gewährt (bestanden) oder verweigert (blockiert) ist.
Wie werden ACLs ausgewertet?	Auf Tabellenebene werden ACLs nur für Rollen und Sicherheitsattribute ausgewertet, Bedingungen und Skripts werden nicht ausgewertet. Rollen werden zuerst ausgewertet. Wenn Rollen blockiert sind, werden Bedingungen und Skripts übersprungen. Weitere Informationen finden Sie unter Konfigurieren einer ACL-Regel.
Wie lauten die Legenden in der Zugriffsanalyse?	Bei der Analyse des Zugriffs und der Berechtigungen werden Legenden als Teil des Bewertungsprozesses angezeigt. Die Legenden lauten wie folgt: • [Bestanden] Zugriff gewährt • [Blockiert] Zugriff verweigert • [Übersprungen] Wurde nicht ausgewertet • [Nicht definiert] Keine Regel gefunden
Was bedeutet das Warnungssymbol in den Zugriffsergebnissen?	Das Warnungssymbol in jedem Status zeigt an, dass ein Skript in der ACL vorhanden ist. Überprüfen Sie die markierten ACLs, um den endgültigen Zugriff zu verstehen. Weitere Informationen darüber, wie diese Steuerungen ausgewertet werden und wie die Logik zur Bestimmung des Zugriffs überprüft wird, finden Sie unter Debug-Protokolle der Zugriffsanalyse.
Was ist **IAccesshandler**?	Eine interne Systemprüfung mit ausgeblendetem Quellcode auf der Plattform. Es handelt sich um eine Systemsicherheitsprüfung, die Sie nicht ändern können. **IAccessHandler** kann den Zugriff auf eine Ressource gewähren oder verweigern, ohne ACLs auszuwerten.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Häufige Fragen (Fortsetzung)

Fragen	Erklärung
	Wenn dieser **IAccessHandler** ignoriert wird, werden die ACLs ausgewertet. Sie können die **IAccessHandler-** Prüfungen in keiner Weise ändern. Beispielsweise wird eine **IAccessHandler** -Implementierung für Zugriffsprüfungen auf Anwendungsressourcen wie den Lesezugriff verwendet.
Was sind Datenfilter?	Datenfilter sind eine Form der Zugriffssteuerung, die auf die vorhandenen Zugriffssteuerungsregeln (ACLs) in Ihrer Instanz abgestimmt ist.
Was ist eine ACL-Regel?	Regeln für Zugriffssteuerungslisten (ACLs) schränken den Zugriff auf Daten ein, indem sie von Anwendern die Erfüllung einer Reihe von Anforderungen verlangen, bevor sie mit der Interaktion beginnen können.

Zeitlich begrenzte Rollenzuweisungen für den Anwender gefunden, aufgrund derer die Ergebnisse betroffen sein können. Sie können die dem Anwender zugewiesenen zeitlich begrenzten Rollen hier überprüfen.

Anwenderdatensätze vergleichen

Im Folgenden finden Sie einige Fragen, die bei der Verwendung der Funktion „Benutzerdatensatz vergleichen“ in der Zugriffsanalyse häufig gestellt werden:

Häufige Fragen

Fragen	Erklärung
Wie werden die Ergebnisse auf der Registerkarte „Details“ gelesen?	Auf der Registerkarte Details werden die Metadaten angezeigt, die Anwender 1 und Anwender 2 zugeordnet sind
Wie erteile ich einem Anwender eine Rolle?	Auf der Registerkarte Anwender können Sie die Rolle überprüfen, die dem Anwender gewährt werden muss, und diese Rolle zuweisen.
Wie füge ich einer Gruppe einen Anwender hinzu?	Auf der Registerkarte Gruppen können Sie die Gruppe überprüfen, der der Anwender hinzugefügt werden muss, und den Anwender der Gruppe hinzufügen.
Was ist „Nur Unterschiede anzeigen“?	Wenn Sie das Kontrollkästchen „Nur Unterschiede anzeigen“ aktivieren, werden nur die Rollen oder Gruppen angezeigt, die sich zwischen Anwender 1 und Anwender 2 unterscheiden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benutzerzugriff vergleichen

Im Folgenden finden Sie einige Fragen, die bei Verwendung der Funktion „Benutzerzugriff vergleichen“ in der Zugriffsanalyse häufig gestellt werden:

Häufige Fragen

Fragen	Erklärung
Wie werden die Ergebnisse auf der Seite für Zugriffsvergleichsvorgänge gelesen?	Auf der Vergleichsseite der Zugriffssteuerung werden die Bewertungsstatus für verschiedene ACL-Vorgänge angezeigt.
Was sind die verschiedenen Auswertungsstatus?	Beim Vergleich der Zugriffssteuerungen zwischen den Anwendern ergaben sich die folgenden verschiedenen Bewertungsstatus: • Bestanden • Blockiert
Was ist „Nur Unterschiede anzeigen“?	Wenn Sie das Kontrollkästchen „Nur Unterschiede anzeigen“ aktivieren, wird nur der Betriebsauswertungsstatus angezeigt, der sich zwischen Anwender 1 und Anwender 2 unterscheidet.
Wie wird der ACL-Vorgang ausgewertet?	Die Zugriffssteuerungsliste (Access Control List, ACL) ist die Regel für Zugriffssteuerungslisten (ACLs), die den Zugriff auf Daten einschränken, indem sie von Anwendern die Erfüllung einer Reihe von Anforderungen verlangen, bevor sie mit der Interaktion beginnen können. Innerhalb einer ACL wird die folgende Hierarchie ausgewertet: • Rolle • Sicherheitsattribut • Bedingung • Skript
Wie werden die Ergebnisse auf der Seite mit der angezeigten Rollenhierarchie gelesen?	Auf der Seite mit der Rollenhierarchie wird die Rolle angezeigt, die Anwender 1 und Anwender 2 zugewiesen ist. Sie können die Rolle verstehen, die für den Anwender für einen bestimmten ACL-Vorgang erforderlich ist.
Wie kann ich die Details des Anwenders anzeigen?	Sie können auswählen **Anwender (Knoten)** > **Weitere Aktionen** > **Zeigen Sie Benutzer an** Details, um mehr über den Anwender zu erfahren.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Häufige Fragen (Fortsetzung)

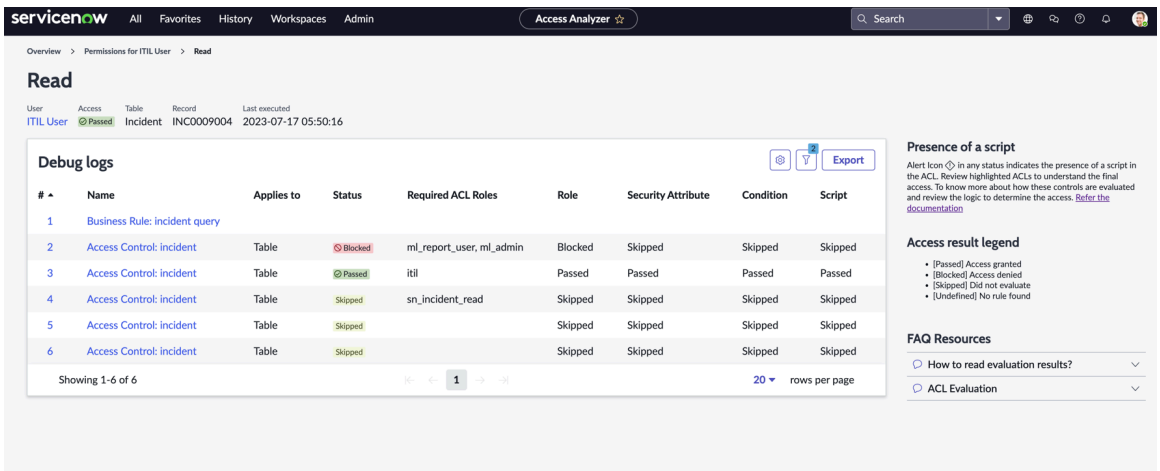
Fragen	Erklärung
Wie kann ich die Details der Rolle anzeigen?	Sie können auswählen **Rolle (Knoten)** > **Weitere Aktionen** > **Zeigen Sie die Rolle an** Details, um mehr über die Rolle zu erfahren.
Wie kann ich die Details der Ressourcen anzeigen, auf die die Rolle zugreifen kann?	Sie können auswählen **Rolle (Knoten)** > **Weitere Aktionen** > **Zeigen Sie alle Ressourcen an, auf die die Rolle Zugriff hat** um zu erfahren, auf welche Ressourcen die Rolle zugreifen kann.
Wie kann ich die Details der Gruppe anzeigen?	Sie können auswählen **Gruppe (Knoten)** > **Weitere Aktionen** > **Gruppe anzeigen** Details, um mehr über die Gruppe zu erfahren.

Debug-Protokolle der Zugriffsanalyse

Debug-Protokolle zeigen die Details des Vorgangs „Auswählen des Zugriffsergebnisses“ an.

Felder in Debug-Protokollen

Die Debug-Protokolle in der Zugriffsanalyse zeigen Informationen zum ausgewählten Vorgang an, um die Berechtigungen, Business-Regeln und ACLs zu verstehen, die dem Vorgang zugeordnet sind.



Im Folgenden finden Sie die Felder und ihre Beschreibung in den Debug-Protokollen:

Protokolle debuggen

Felder	Beschreibung
Name	Die Details zur Geschäftsregel oder ACL. Sie können die Business-Regel der ACL auswählen, um weitere Informationen zu erhalten.
Betrifft	Die Details zur Anwendung der ACL auf Feld-, Datensatz- oder Tabellenebene.
Status	Status der ACL für die zugeordnete Rolle und Berechtigung.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Protokolle debuggen (Fortsetzung)

Felder	Beschreibung
Erfordert ACL	Die für den Zugriff auf das Feld, den Datensatz oder die Tabelle erforderliche Rolle
Rolle	Die Details zu den Rollen, die für die Zugriffssteuerung blockiert, bestanden und übersprungen sind.
Sicherheitsattribut	Die Details zum Sicherheitsattribut, das für die Zugriffssteuerung blockiert, bestanden und übersprungen ist.
Bedingung	Die Details zur Bedingung „Blockiert“, „Bestanden“, „Übersprungen“ für die Zugriffssteuerung.
Skript	Die Details zum Skript, das für die Zugriffssteuerung blockiert, übergeben oder übersprungen wird.
Angepasst	Die Details zur angepassten ACL, falls vorhanden, für die Zugriffssteuerung.
Anwendung	Status der Anwendung. Global oder Store.

Auswertungshierarchie

Die Berechtigung für den ausgewählten Anwender, die ausgewählte Gruppe oder die ausgewählte Rolle wird in der folgenden Hierarchie ausgewertet:

- Geschäftsregel: Eine Geschäftsregel ist ein serverseitiges Skript, das ausgeführt wird, wenn ein Datensatz angezeigt, eingefügt, aktualisiert oder gelöscht wird oder wenn eine Tabelle abgefragt wird.
- Zugriffshandler: Eine interne Systemprüfung mit ausgeblendetem Quellcode auf der Plattform.
- Datenfilterung: Ein Datenfilter ist eine Form der Zugriffssteuerung, die auf die vorhandenen Zugriffssteuerungsregeln (ACLs) in Ihrer Instanz abgestimmt ist. Datenfilter unterstützen nur Lesevorgänge.
- Zugriffssteuerungsliste (ACL): Regeln für Zugriffssteuerungslisten (ACLs) schränken den Zugriff auf Daten ein, indem sie von Anwendern die Erfüllung einer Reihe von Anforderungen verlangen, bevor sie mit der Interaktion beginnen können. Innerhalb einer ACL wird die folgende Hierarchie ausgewertet:
  - Rolle
  - Sicherheitsattribut
  - Bedingung
  - Skript

Auswertung der Zugriffssteuerungsliste

ACLs für die Vorgänge werden in der folgenden Reihenfolge ausgewertet:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Rolle
- Sicherheitsattribut
- Bedingung
- Skript

Vorhandensein eines Skripts

Das Warnungssymbol in jedem Status zeigt an, dass ein Skript in der ACL vorhanden ist. Überprüfen Sie die markierten ACLs, um den endgültigen Zugriff zu verstehen.

Hinweis: Bei einer Abfrage durch die Zugriffsanalyse werden zuerst Business-Regeln und dann die Zugriffssteuerungsliste ausgeführt.

Reihenfolge der Ausführung

Die Ausführung der Zugriffsergebnisse wird in verschiedenen Szenarien wie folgt ausgeführt:

- **Vorhandensein einer geerbten ACL oder einer Platzhalter-ACL**: Während der Ausführungssequenz werden zuerst die geerbten ACLs und dann die Platzhalter-ACL ausgewertet.
- **Eine ACL wird übergeben, die anderen werden übersprungen**: Während der Ausführung und Auswertung der Berechtigung wird die Ausführung und Auswertung der anderen ACL übersprungen, wenn eine ACL übergeben wird. Weil die allgemeine Berechtigung für den ausgewählten Vorgang eine ACL erfordert, um auf ein Feld, einen Datensatz oder eine Tabelle für eine Identität zuzugreifen.
- Ausführung von ACLs auf Feldebene**und Tabellenebene**: Während der Ausführung werden zuerst ACLs auf Feldebene ausgeführt, gefolgt von der ACL auf Tabellenebene, um bei der Analyse des Zugriffs für eine Identität präzisere Ergebnisse zu liefern.
- **Auswertung des Vorhandenseins einer geskripteten ACL**: Wenn ein Skript vorhanden ist, wird der Gesamtzugriff für den Vorgang mit einem Warnungssymbol übergeben, um das Skript in der ACL anzuzeigen.

Zugriffssimulator

Mit dem Zugriffssimulator können Sie simulieren, wie sich der Zugriff auf die angegebene Tabelle ändern würde, nachdem eine Rolle oder Gruppe dem Anwender zugewiesen oder von ihm entfernt wurde.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Untersuchen



Lernen Sie die Funktionen und den Geschäftsnutzen des Zugriffssimulators kennen.

Verwenden



Erfahren Sie, wie der Zugriffssimulator verwendet wird.

Konfigurieren



Erfahren Sie, wie der Zugriffssimulator konfiguriert wird.

Häufige Fragen



Rufen Sie Details zu häufig gestellten Fragen zum Zugriffssimulator ab.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugriffssimulator erkunden

Mit dem Zugriffssimulator können Sie simulieren, wie sich der Zugriff auf die angegebene Tabelle ändern würde, nachdem eine Rolle oder Gruppe dem Anwender zugewiesen oder von ihm entfernt wurde.

Administratoren können mit dem Zugriffssimulator die Zugriffsanforderungen ihrer Benutzer auf eine bestimmte Tabelle simulieren und nachvollziehen, wie sich die Zugriffssteuerungen für einen Benutzer ändern. Dies hilft, den aktuellen Zugriff der Benutzer schnell zu erfassen und die Auswirkungen des Bereitstellens oder Entfernens von Rollen für Benutzer zu verstehen.

https://player.vimeo.com/video/988627830?badge=0&autopause=0&player_id=0&app_id=58479

Der Zugriffssimulator kann für die Simulation des Zugriffs auf einen Anwender in den folgenden Szenarien verwendet werden:

- Dem Anwender wird eine Rolle hinzugefügt
- Eine Rolle wird vom Anwender entfernt
- Der Anwender wird einer Gruppe hinzugefügt
- Der Anwender wird aus einer Gruppe entfernt

Weitere Informationen zu den Einstellungen für den Zugriffssimulator und zur Aktivierung von Aktionen finden Sie unter Zugriffssimulator konfigurieren (Aktionen durchführen).

Zugriffssimulator konfigurieren (Aktionen durchführen)

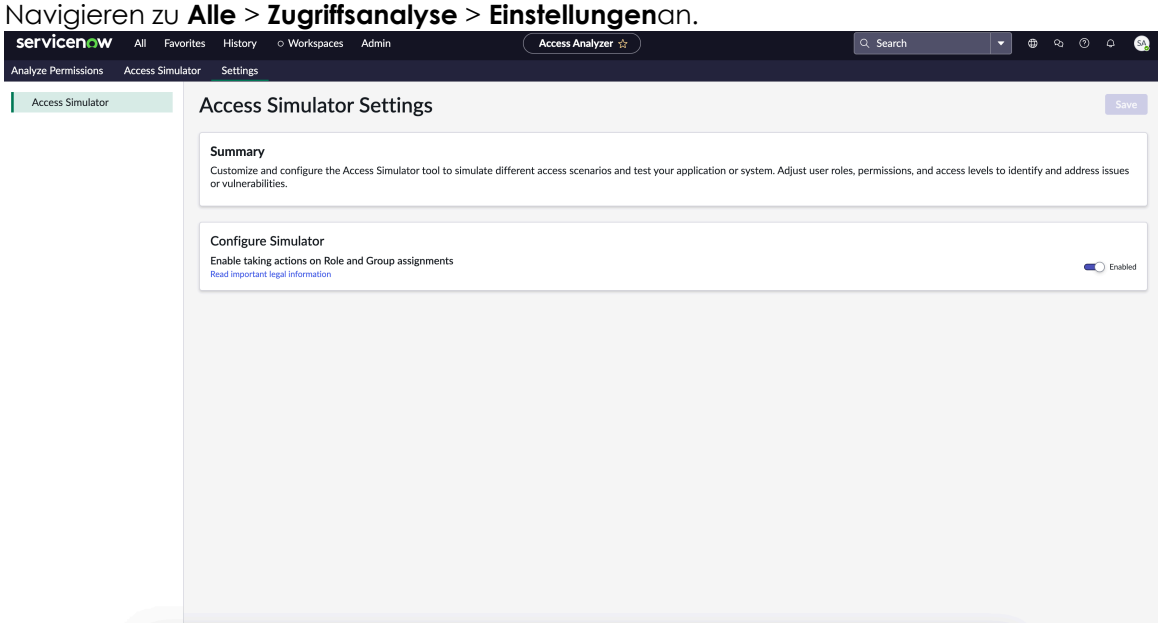
Konfigurieren Sie die Optionen zum Durchführen von Aktionen, um die Rollen- und Gruppenzuweisungen abzuschließen, die Sie nach der Simulation hinzufügen möchten.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Einstellungen**an.



2. Wählen Sie zum Aktivieren den Umschalter.
   Lesen Sie sich die rechtlichen Informationen durch, bevor Sie den Zugriffssimulator aktivieren (Aktionen durchführen).

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie **Akzeptieren** aus.
4. Wählen **Sie Speichern** aus, um die Konfiguration zu speichern.

Mithilfe des Zugriffssimulators

Verwenden Sie den Zugriffssimulator, um zu simulieren, dass sich der Zugriff des Anwenders auf die angegebene Tabelle ändert, sobald eine Rolle oder Gruppe zugewiesen oder entfernt wird.

Vorbereitungen

Erforderliche Rolle: admin

Aktivieren Sie die Aktionen durchführen. Weitere Informationen finden Sie unter Zugriffssimulator konfigurieren (Aktionen durchführen).

Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Zugriffssimulator**an.
2. Wählen Sie die Option **Simulieren** unter jedem Abschnitt basierend auf den folgenden Szenarien aus:
   - Dem Anwender wird eine Rolle hinzugefügt
   - Eine Rolle wird vom Anwender entfernt
   - Der Anwender wird einer Gruppe hinzugefügt
   - Der Anwender wird aus einer Gruppe entfernt

Dem Anwender wird eine Rolle hinzugefügt

Verwenden Sie die **Rolle „Simulieren und Hinzufügen** “, um die Zugriffsänderungen des Anwenders für eine Ressource (Tabellen) zu simulieren.

Vorbereitungen

Erforderliche Rolle: admin

Aktivieren Sie die Aktionen durchführen. Weitere Informationen finden Sie unter Zugriffssimulator konfigurieren (Aktionen durchführen).

Prozedur

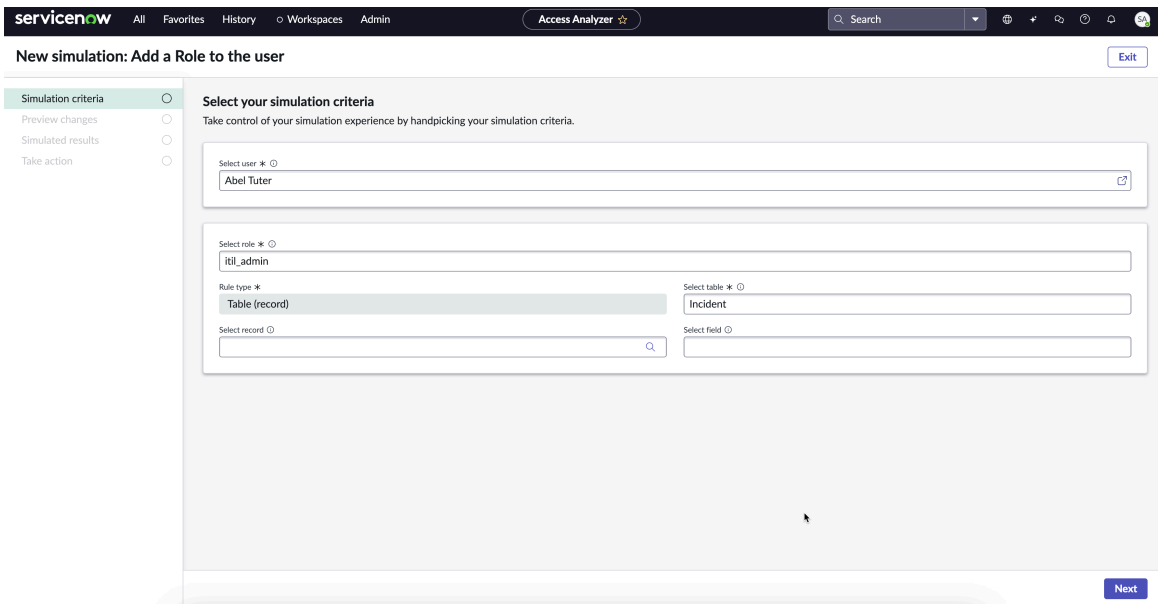
1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Zugriffssimulator**an.
2. Wählen Sie im Abschnitt „Dem Benutzer eine Rolle hinzufügen“ die Option **Simulieren** aus.
3. Geben Sie die folgenden Felder für Ihre Simulationskriterien an:

Dem Anwender eine Rolle hinzufügen

Feld	Beschreibung
Anwender auswählen *	Geben Sie einen Anwendernamen an, den Sie aus der Liste auswählen möchten. In diesem Beispiel **Abel Tuter**.
Rolle auswählen *	Geben Sie eine Rolle an, die aus der Liste ausgewählt werden soll. In diesem Beispiel **itil_admin**.

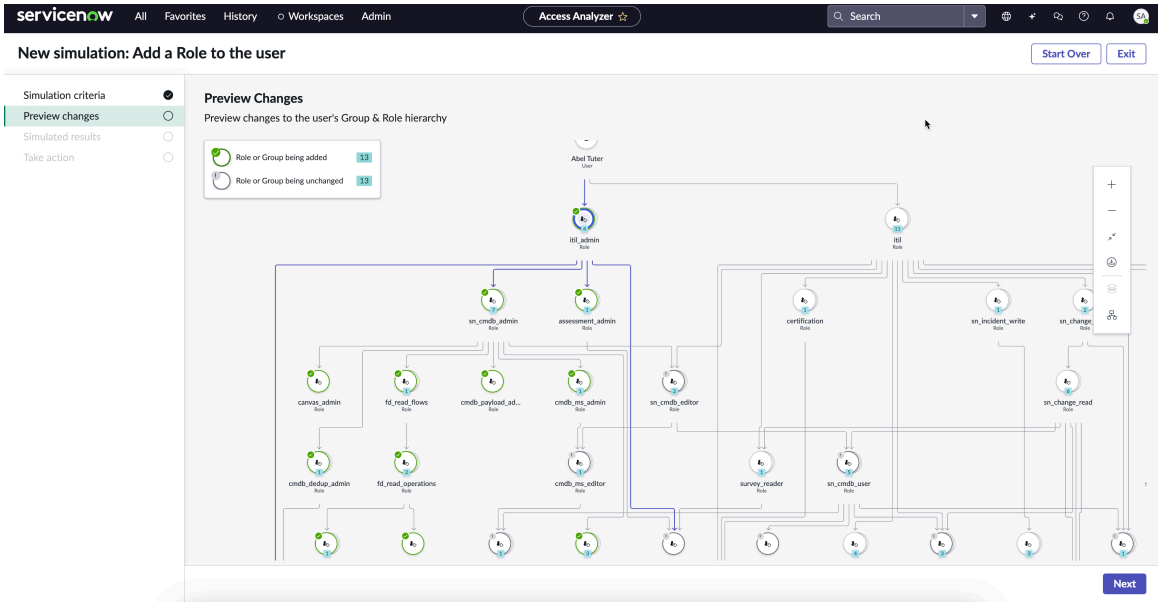
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Regeltyp *	Regeltyp wird automatisch ausgefüllt und kann nicht geändert werden.
Tabelle auswählen *	Geben Sie einen Tabellennamen an, um ihn aus der Liste auszuwählen. In diesem Beispiel **Incident**.
Datensatz auswählen	Geben Sie einen Datensatznamen an, um ihn aus der Liste auszuwählen (optional).
Feld auswählen	Geben Sie einen Feldnamen an, um ihn aus der Liste auszuwählen. Dieses Feld kann verwendet werden, um Berechtigungen auch auf Feldebene zu analysieren. Zum Beispiel „Aktiv“, „Erstellt von“ usw.



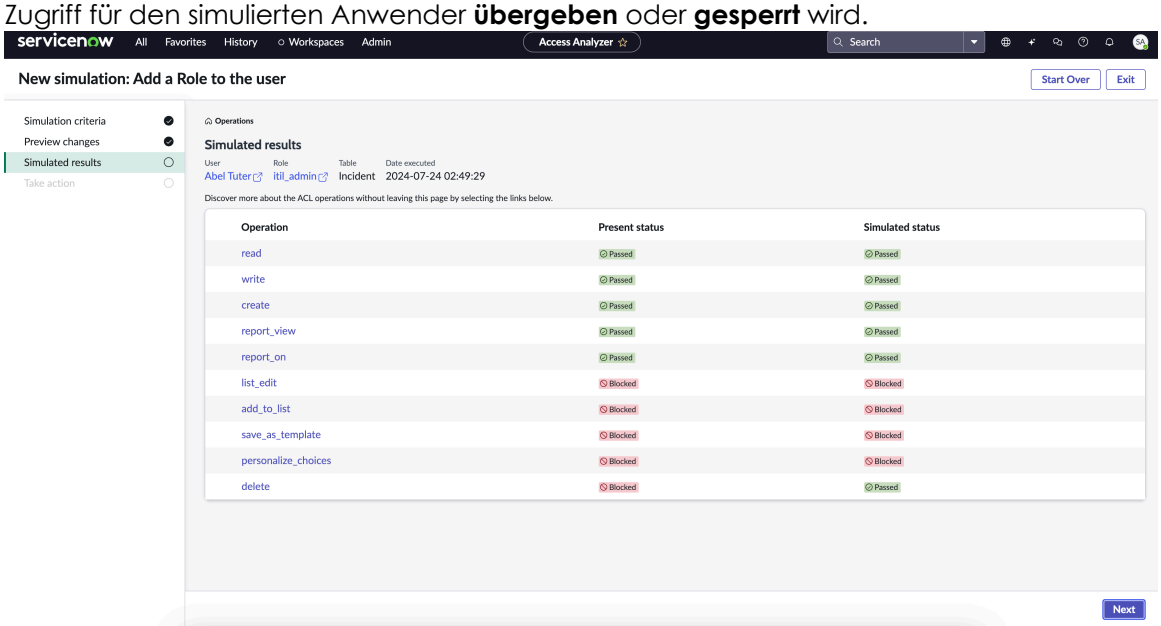
4. Wählen Sie **Weiter**.
5. Zeigen Sie eine Vorschau der Änderungen an.
   Die neu zugewiesenen Rollen werden in der Vorschau auf die Änderungen simuliert. Sie können die Rollen und untergeordneten Rollen validieren, die dem Benutzer hinzugefügt werden, bevor Sie mit dem nächsten Schritt fortfahren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Sie können sehen, dass die neuen Rollen, die als Teil der Rolle **itil_admin** hinzugefügt werden, zusammen mit den vorhandenen Rollen des Benutzers angezeigt werden.

6. Wählen Sie **Weiter**.
7. Validieren Sie den Status „ **Anwesend“ und den Status „Simuliert“**, um zu überprüfen, ob der Zugriff für den simulierten Anwender **übergeben** oder **gesperrt** wird.



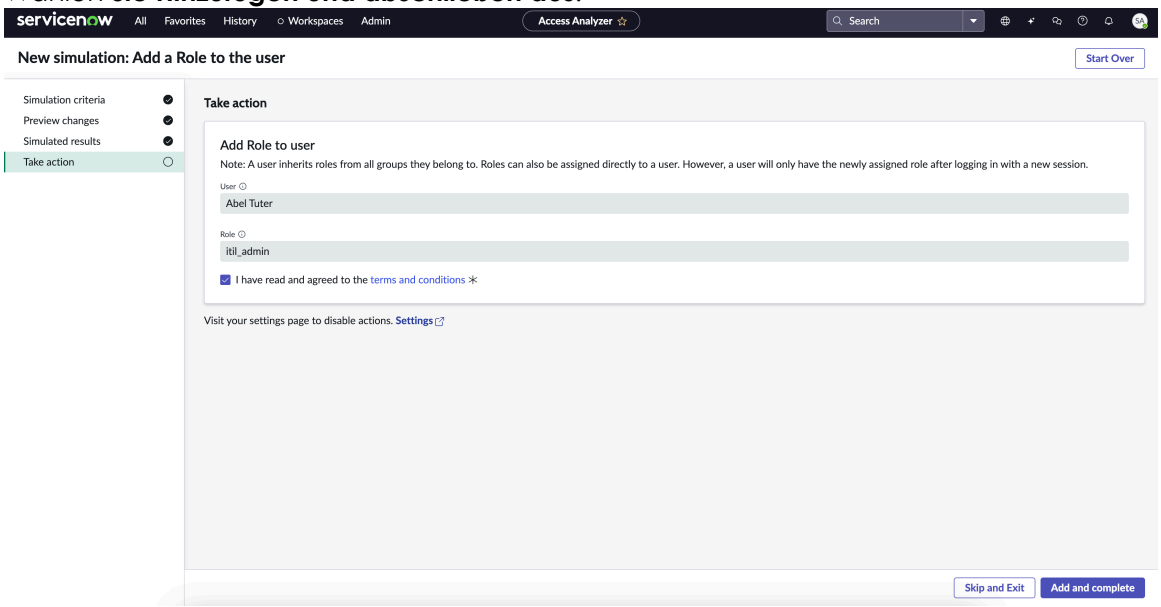
Durch Hinzufügen von **itil_admin** kann der Benutzer einen Löschvorgang für die Tabelle (Incident) ausführen.

Hinweis:

- Wenn Sie mehr über die ACL (Vorgänge) erfahren möchten, wählen Sie die Links zu Vorgängen für jeden Datensatz aus.
- Wenn Sie die Simulation für eine andere Rolle erneut starten möchten, wählen Sie Neu **starten aus**.
- Wenn Sie die Simulation beenden möchten, wählen Sie **Beenden**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Wählen Sie **Weiter**.
9. Wählen **Sie Hinzufügen und abschließen aus**.



Hinweis:

- Wenn der Zugriffssimulator nicht aktiviert ist, können Sie die Simulation nicht abschließen. Wählen Sie zum Aktivieren **Aktionen** aktivieren, und akzeptieren Sie die rechtlichen Informationen.
- Wenn Sie die Simulation ausblenden möchten, wählen Sie **Aktionen ausblenden**aus. Um Aktionen einzublenden und zu aktivieren, wechseln Sie zu den Einstellungen. Weitere Informationen finden Sie unter Zugriffssimulator konfigurieren (Aktionen durchführen).
- Wenn Sie die Simulation beenden möchten, wählen Sie **Überspringen und Beenden**aus.

Die Rollen wurden dem Anwender erfolgreich hinzugefügt. Sie können den Zugriff mit der Zugriffsanalyse überprüfen. Weitere Informationen zum Überprüfen des Zugriffs eines -Benutzers finden Sie unter Zugriffsanalyse.

Eine Rolle wird vom Anwender entfernt

Verwenden Sie die **Rolle „Entfernen** simulieren“, um die Zugriffsänderungen des Anwenders für eine Ressource (Tabellen) zu simulieren.

Vorbereitungen

Erforderliche Rolle: admin

Aktivieren Sie die Aktionen durchführen. Weitere Informationen finden Sie unter Zugriffssimulator konfigurieren (Aktionen durchführen).

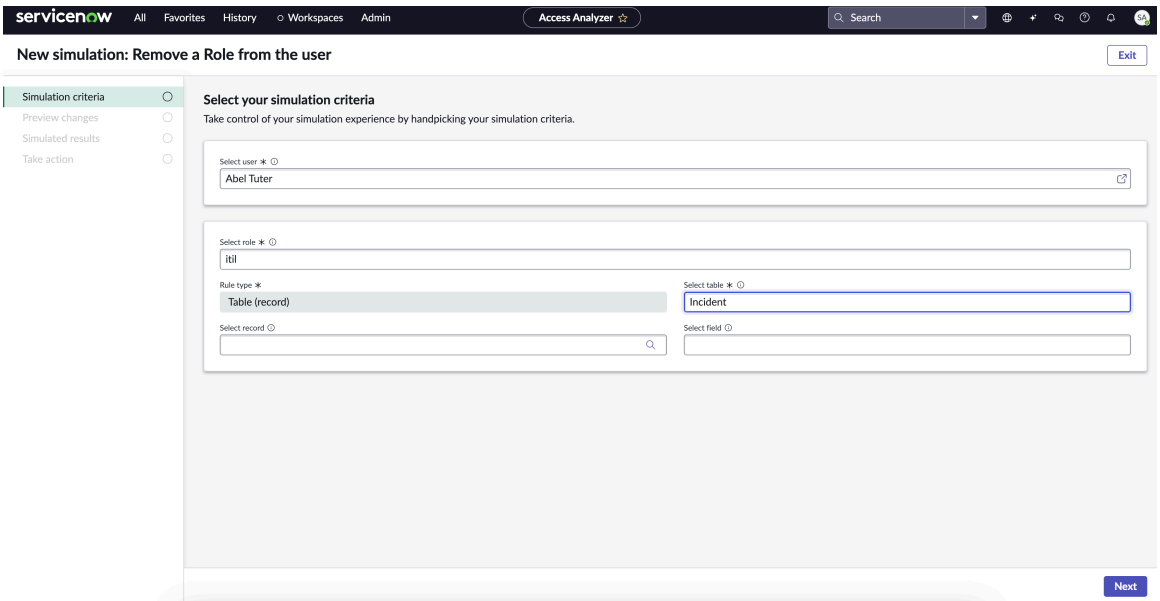
Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Zugriffssimulator**an.
2. Wählen Sie im Abschnitt Eine Rolle vom Benutzer entfernen die Option **Simulieren** aus.
3. Geben Sie die folgenden Felder für Ihre Simulationskriterien an:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

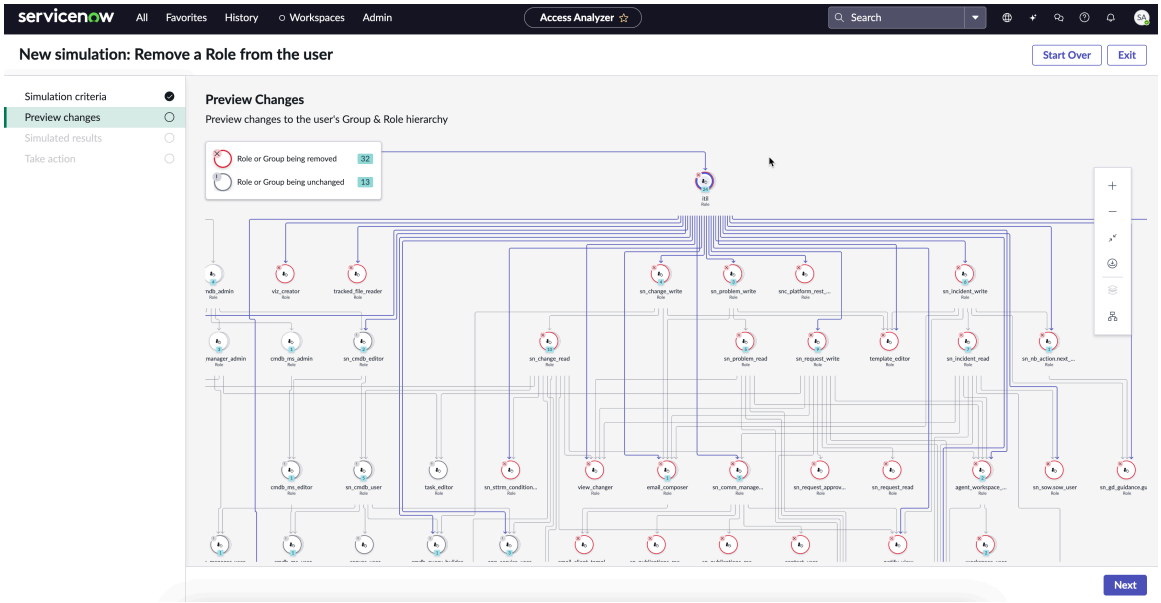
Eine Rolle vom Anwender entfernen

Feld	Beschreibung
Anwender auswählen *	Geben Sie einen Anwendernamen an, den Sie aus der Liste auswählen möchten. In diesem Beispiel **Abel Tuter**.
Rolle auswählen *	Geben Sie eine Rolle an, die aus der Liste ausgewählt werden soll. In diesem Beispiel **itil**.
Regeltyp *	Regeltyp wird automatisch ausgefüllt und kann nicht geändert werden.
Tabelle auswählen *	Geben Sie einen Tabellennamen an, um ihn aus der Liste auszuwählen. In diesem Beispiel **Incident**.
Datensatz auswählen	Geben Sie einen Datensatznamen an, um ihn aus der Liste auszuwählen.
Feld auswählen	Geben Sie einen Feldnamen an, um ihn aus der Liste auszuwählen. Dieses Feld kann verwendet werden, um Berechtigungen auch auf Feldebene zu analysieren. Zum Beispiel „Aktiv“, „Erstellt von“ usw.

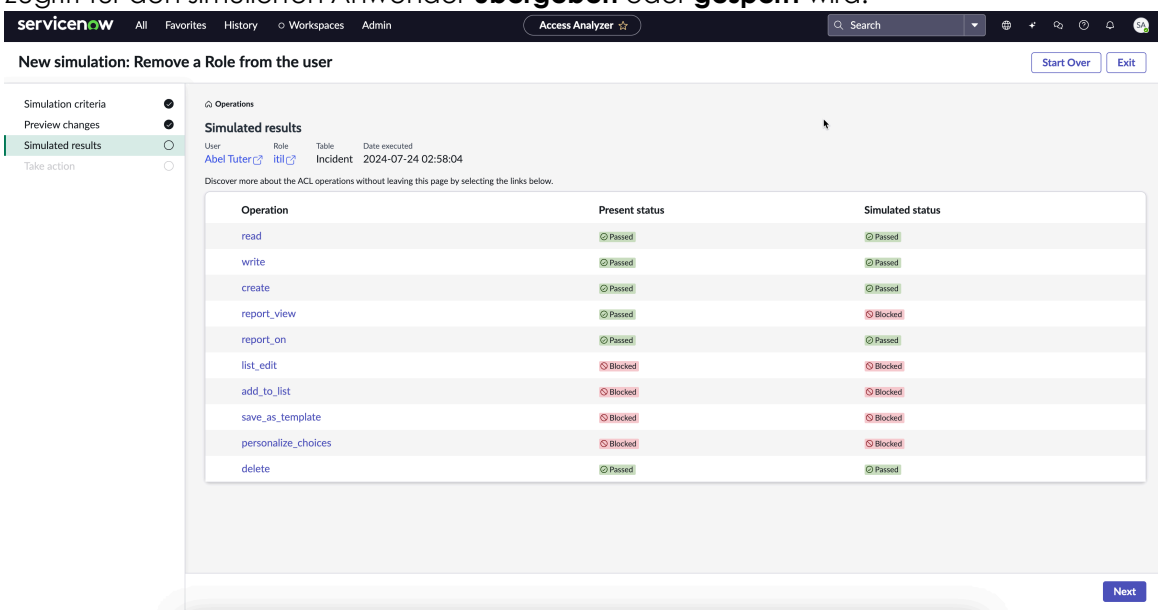


4. Wählen Sie **Weiter**.
5. Zeigen Sie eine Vorschau der Änderungen an.
   Die entfernten Rollen werden in der Vorschau auf die Changes simuliert. Sie können die Rollen und untergeordneten Rollen validieren, die für den Anwender entfernt werden, bevor Sie mit dem nächsten Schritt fortfahren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Wählen Sie **Weiter**.
7. Validieren Sie den Status „ **Anwesend“ und den Status „Simuliert“**, um zu überprüfen, ob der Zugriff für den simulierten Anwender **übergeben** oder **gesperrt** wird.



Hinweis:

- Wenn Sie mehr über die ACL (Vorgänge) erfahren möchten, wählen Sie die Links zu Vorgängen für jeden Datensatz aus.
- Wenn Sie die Simulation für eine andere Rolle erneut starten möchten, wählen Sie Neu **starten aus**.
- Wenn Sie die Simulation beenden möchten, wählen Sie **Beenden**.

8. Wählen Sie **Weiter**.
9. Wählen **Sie Entfernen und abschließen aus**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Wenn der Zugriffssimulator nicht aktiviert ist, können Sie die Simulation nicht abschließen. Wählen Sie zum Aktivieren **Aktionen** aktivieren, und akzeptieren Sie die rechtlichen Informationen.
- Wenn Sie die Simulation ausblenden möchten, wählen Sie **Aktionen ausblenden**aus. Um Aktionen einzublenden und zu aktivieren, wechseln Sie zu den Einstellungen. Weitere Informationen finden Sie unter Zugriffssimulator konfigurieren (Aktionen durchführen).
- Wenn Sie die Simulation beenden möchten, wählen Sie **Überspringen und Beenden**aus.

Die Rollen wurden erfolgreich vom Anwender entfernt. Sie können den Zugriff mit der Zugriffsanalyse überprüfen. Weitere Informationen zum Überprüfen des Zugriffs eines -Benutzers finden Sie unter Zugriffsanalyse.

Der Anwender wird einer Gruppe hinzugefügt

Verwenden **Sie „Zu Gruppe hinzufügen“ simulieren,** um die Zugriffsänderungen des Benutzers für eine Ressource (Tabellen) zu simulieren, wenn der Benutzer zu einer Gruppe hinzugefügt wird.

Vorbereitungen

Erforderliche Rolle: admin

Aktivieren Sie die Aktionen durchführen. Weitere Informationen finden Sie unter Zugriffssimulator konfigurieren (Aktionen durchführen).

Prozedur

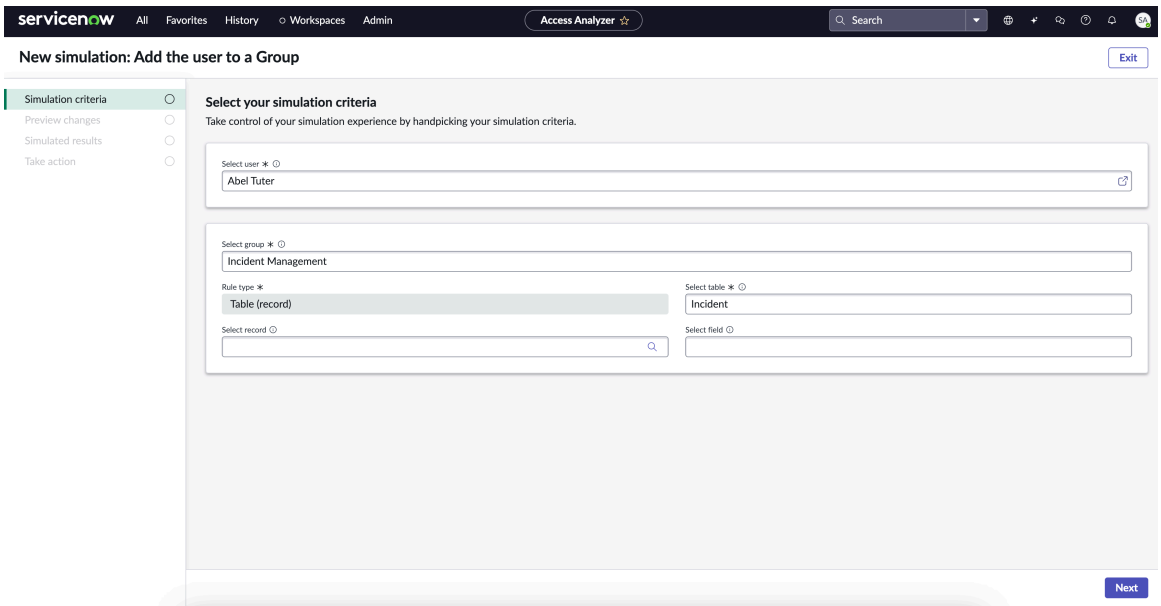
1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Zugriffssimulator**an.
2. Wählen Sie im Abschnitt Anwender zu Gruppe hinzufügen die Option **Simulieren** aus.
3. Geben Sie die folgenden Felder für Ihre Simulationskriterien an:

Fügen Sie den Anwender einer Gruppe hinzu

Feld	Beschreibung
Anwender auswählen *	Geben Sie einen Anwendernamen an, den Sie aus der Liste auswählen möchten. In diesem Beispiel **Abel Tuter**.
Gruppe auswählen *	Geben Sie eine Gruppe an, die aus der Liste ausgewählt werden soll. In diesem Beispiel **Incident Management**.
Regeltyp *	Regeltyp wird automatisch ausgefüllt und kann nicht geändert werden.
Tabelle auswählen *	Geben Sie einen Tabellennamen an, um ihn aus der Liste auszuwählen. In diesem Beispiel **Incident**.
Datensatz auswählen	Geben Sie einen Datensatznamen an, um ihn aus der Liste auszuwählen.
Feld auswählen	Geben Sie einen Feldnamen an, um ihn aus der Liste auszuwählen. Dieses Feld kann

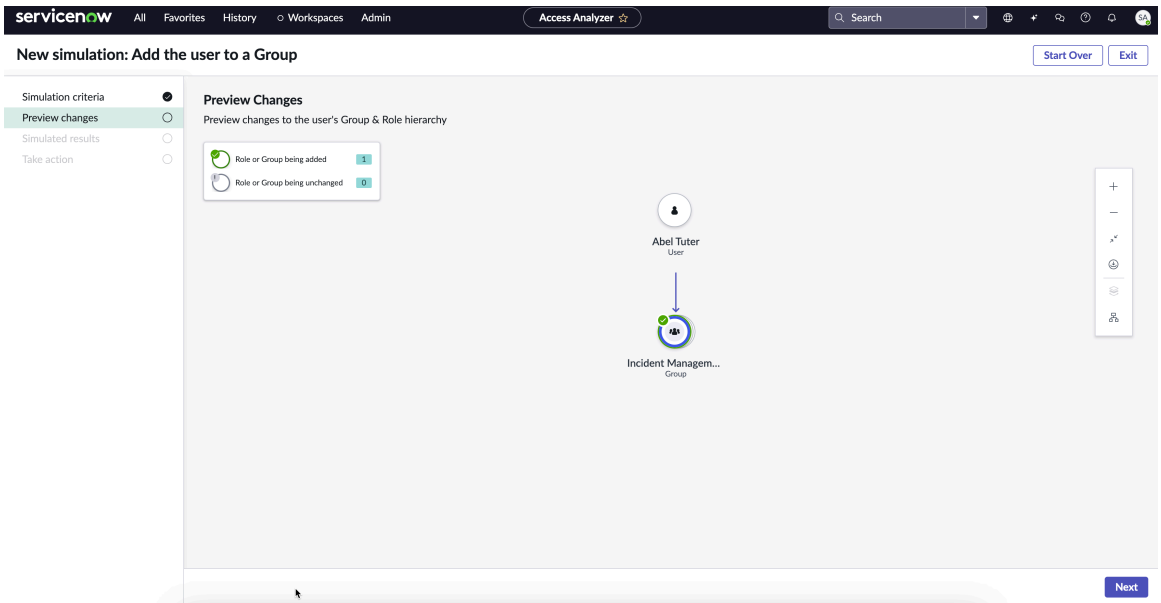
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	verwendet werden, um Berechtigungen auch auf Feldebene zu analysieren. Zum Beispiel „Aktiv“, „Erstellt von“ usw.



4. Wählen Sie **Weiter**.
5. Zeigen Sie eine Vorschau der Änderungen an.

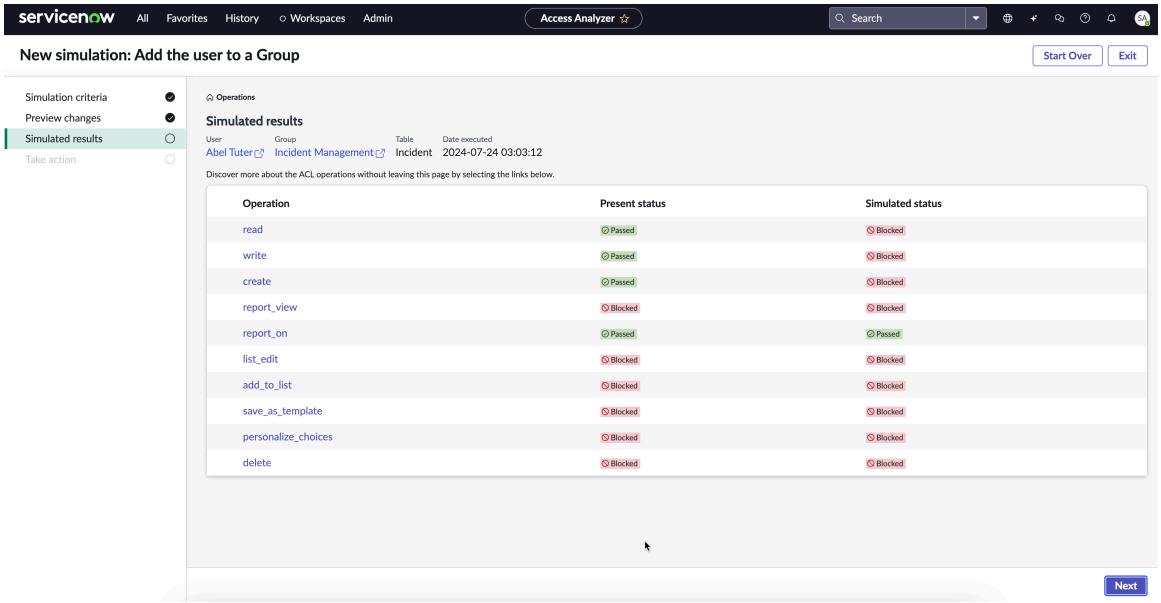
   Die Gruppe, der der Benutzer zugewiesen ist, wird in der Vorschau auf die Änderungen simuliert. Sie können die Änderungen validieren, bevor Sie mit dem nächsten Schritt fortfahren.



6. Wählen Sie **Weiter**.
7. Validieren Sie den Status „ **Anwesend“ und den Status „Simuliert“**, um zu überprüfen, ob der Zugriff für den simulierten Anwender **übergeben** oder **gesperrt** wird.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:

- Wenn Sie mehr über die ACL (Vorgänge) erfahren möchten, wählen Sie die Links zu Vorgängen für jeden Datensatz aus.
- Wenn Sie die Simulation für eine andere Rolle erneut starten möchten, wählen Sie Neu **starten aus**.
- Wenn Sie die Simulation beenden möchten, wählen Sie **Beenden**.

8. Wählen Sie **Weiter**.
9. Wählen **Sie Hinzufügen und abschließen aus**.

Hinweis:

- Wenn der Zugriffssimulator nicht aktiviert ist, können Sie die Simulation nicht abschließen. Wählen Sie zum Aktivieren **Aktionen** aktivieren, und akzeptieren Sie die rechtlichen Informationen.
- Wenn Sie die Simulation ausblenden möchten, wählen Sie **Aktionen ausblenden**aus. Um Aktionen einzublenden und zu aktivieren, wechseln Sie zu den Einstellungen. Weitere Informationen finden Sie unter Zugriffssimulator konfigurieren (Aktionen durchführen).
- Wenn Sie die Simulation beenden möchten, wählen Sie **Überspringen und Beenden**aus.

Der Anwender wurde erfolgreich der Gruppe hinzugefügt.

Der Anwender wird aus einer Gruppe entfernt

Verwenden **Sie Entfernen aus Gruppe** simulieren, um die Zugriffsänderungen des Anwenders für eine Ressource (Tabellen) zu simulieren, wenn der Anwender aus einer Gruppe entfernt wird.

Vorbereitungen

Erforderliche Rolle: admin

Aktivieren Sie die Aktionen durchführen. Weitere Informationen finden Sie unter Zugriffssimulator konfigurieren (Aktionen durchführen).

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

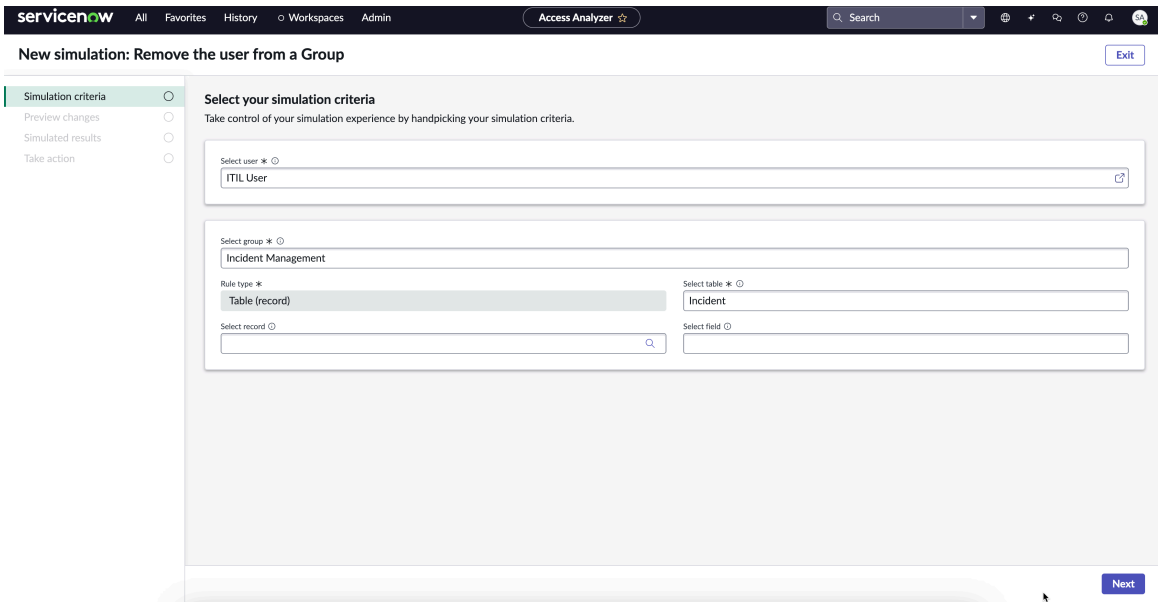
Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Zugriffssimulator**an.
2. Wählen Sie **Simulieren** im Abschnitt Benutzer aus Gruppe entfernen aus.
3. Geben Sie die folgenden Felder für Ihre Simulationskriterien an:

Entfernen Sie den Anwender aus einer Gruppe

Feld	Beschreibung
Anwender auswählen *	Geben Sie einen Anwendernamen an, den Sie aus der Liste auswählen möchten. In diesem Beispiel **ITIL-Benutzer**.
Gruppe auswählen *	Geben Sie eine Gruppe an, die aus der Liste ausgewählt werden soll. In diesem Beispiel **Incident Management**.
Regeltyp *	Regeltyp wird automatisch ausgefüllt und kann nicht geändert werden.
Tabelle auswählen *	Geben Sie einen Tabellennamen an, um ihn aus der Liste auszuwählen. In diesem Beispiel **Incident**.
Datensatz auswählen	Geben Sie einen Datensatznamen an, um ihn aus der Liste auszuwählen.
Feld auswählen	Geben Sie einen Feldnamen an, um ihn aus der Liste auszuwählen. Dieses Feld kann verwendet werden, um Berechtigungen auch auf Feldebene zu analysieren. Zum Beispiel „Aktiv“, „Erstellt von“ usw.

d

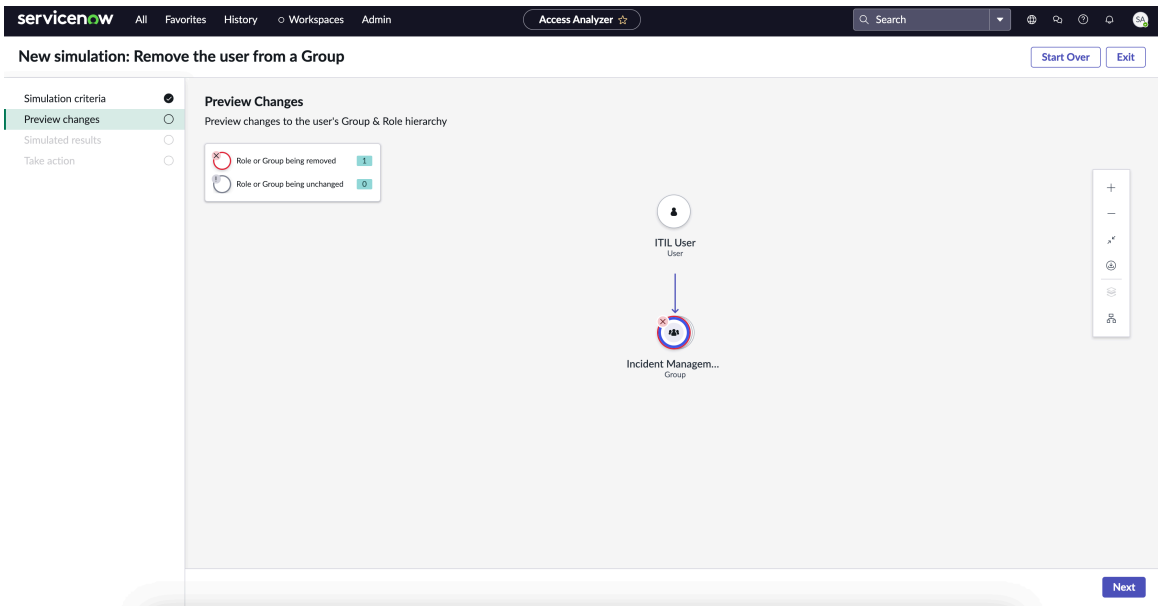


4. Wählen Sie **Weiter**.
5. Zeigen Sie eine Vorschau der Änderungen an.

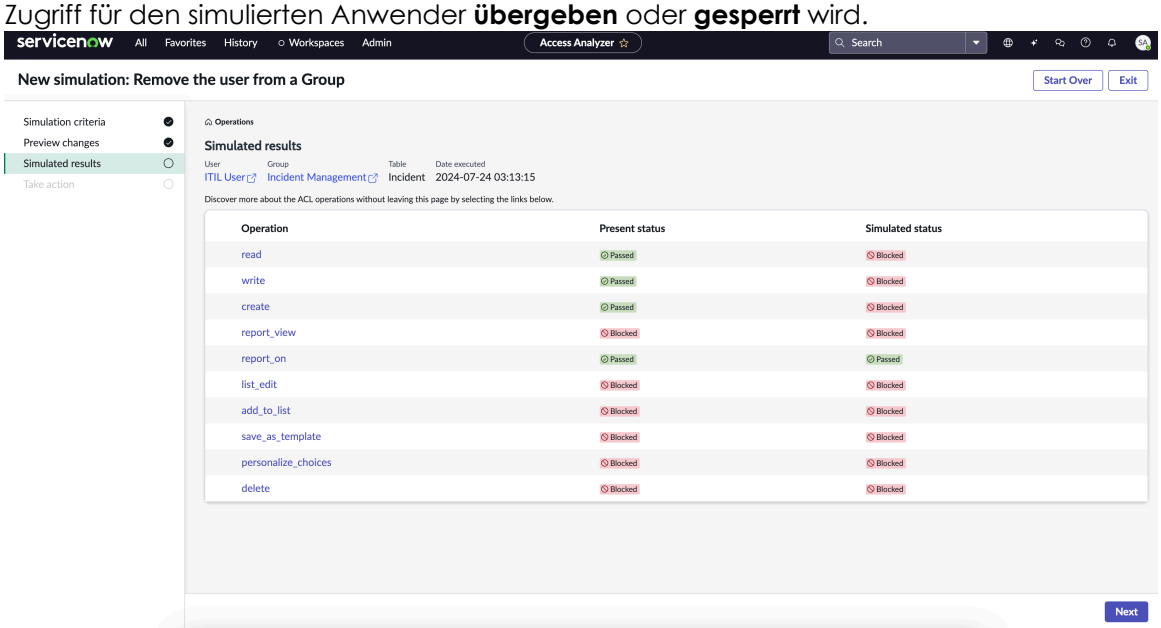
Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Gruppe, aus der der Benutzer entfernt wird, wird in der Vorschau auf die Änderungen simuliert. Sie können die Änderungen validieren, bevor Sie mit dem nächsten Schritt fortfahren.



6. Wählen Sie **Weiter**.
7. Validieren Sie den Status „ **Anwesend“ und den Status „Simuliert“**, um zu überprüfen, ob der Zugriff für den simulierten Anwender **übergeben** oder **gesperrt** wird.



Hinweis:

- Wenn Sie mehr über die ACL (Vorgänge) erfahren möchten, wählen Sie die Links zu Vorgängen für jeden Datensatz aus.
- Wenn Sie die Simulation für eine andere Rolle erneut starten möchten, wählen Sie Neu **starten aus**.
- Wenn Sie die Simulation beenden möchten, wählen Sie **Beenden**.

8. Wählen Sie **Weiter**.
9. Wählen **Sie Entfernen und abschließen aus**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Wenn der Zugriffssimulator nicht aktiviert ist, können Sie die Simulation nicht abschließen. Wählen Sie zum Aktivieren **Aktionen** aktivieren, und akzeptieren Sie die rechtlichen Informationen.
- Wenn Sie die Simulation ausblenden möchten, wählen Sie **Aktionen ausblenden**aus. Um Aktionen einzublenden und zu aktivieren, wechseln Sie zu den Einstellungen. Weitere Informationen finden Sie unter Zugriffssimulator konfigurieren (Aktionen durchführen).
- Wenn Sie die Simulation beenden möchten, wählen Sie **Überspringen und Beenden**aus.

Der Anwender wurde erfolgreich aus dem Anwender entfernt.

Häufige Fragen

Häufig gestellte Fragen zur Verwendung des Zugriffssimulators.

Häufige Fragen

Fragen	Erklärung
Wie beginne ich mit dem Simulator?	Sie können die Option „Simulieren“ für das andere Szenario auswählen, das Sie für die Anwender simulieren möchten, und die Schritte ausführen.
Wie funktioniert der Simulator?	Der Zugriffssimulator simuliert den Zugriff auf die angegebene Tabelle für den ausgewählten Anwender und zeigt eine Vorschau der Zugriffsänderungen an, um Entscheidungen über die Zugriffsbereitstellung zu treffen.
Wie aktiviere oder deaktiviere ich Aktionen im Simulator?	Sie können Aktionen im Zugriffssimulator aktivieren oder deaktivieren, indem Sie zu den Einstellungen navigieren, oder während der Schritte von „Aktionen ausführen“ im Simulationsprozess.

Globale Identität

Global Identity ist ein Produkt von ServiceNow®, mit dem eindeutige Benutzer über mehrere Instanzen hinweg identifiziert werden können.

Global Identity hilft bei mehreren ServiceNow® -Instanzen, Benutzer, ihre Attribute und andere grundlegende Daten über mehrere ServiceNow® -Instanzen hinweg zu verwalten.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkunden Sie die Föderierte ID



Lernen Sie die wichtigsten Funktionen und den Geschäftsnutzen von Föderierte ID kennen.

Zugriff auf Verbund-ID



Greifen Sie auf die Verbund-ID zu.

ID-Felder werden aktualisiert



Aktualisieren und richten Sie die Verbund-ID ein.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Föderierte ID erkunden

Bestimmen Sie die Anwender in mehreren Instanzen basierend auf Anwendername und E-Mail-Adresse, und stellen Sie dem Anwender in allen Instanzen eine eindeutige ID (Verbund-ID) bereit.

Die Föderierte ID wird verwendet, um Benutzer in mehreren Instanzen ServiceNow® zu identifizieren. Basierend auf der Verbund-ID kann der Benutzer identifiziert und die genaue Anzahl der Benutzer über mehrere Instanzen hinweg ermittelt werden. Weitere Informationen finden Sie unter Föderierte ID.

Hinweis: Zum Generieren von Verbund-IDs ist ein Anwendername erforderlich.

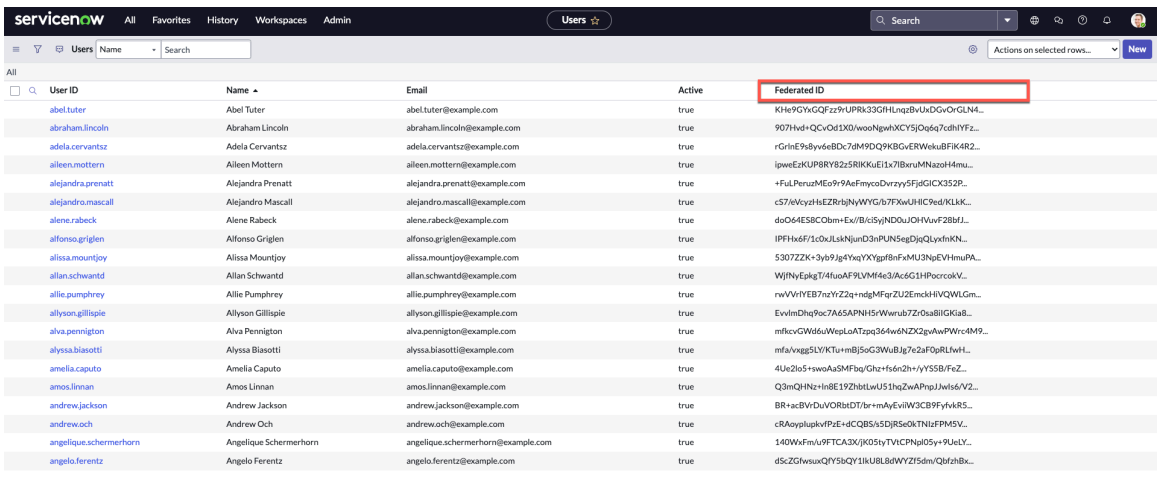
Die Verbund-ID ist ein eindeutiger Bezeichner für eine Identität, die eine Hashing-Funktion für die Instanzen ServiceNow® verwendet.

Unter Verwendung der **Anwender-ID** und der E- **Mail** -Adresse des Anwenders in allen Instanzen wird die Verbund-ID erstellt und in der Tabelle „sys_user“ angezeigt.

Nach dem Upgrade auf Release Xanadu wird das Plugin „Federated ID Generation“ (`com.glide.identity.globalid`) automatisch in allen Instanzen installiert.

Hinweis:

- Zum Generieren von Verbund-IDs ist ein Anwendername erforderlich.
- Anwendername und E-Mail-Adresse werden standardmäßig zum Generieren von Verbund-IDs verwendet. Informationen zum Aktualisieren der Felder zum Generieren von Verbund-IDs basierend auf Ihren Anforderungen finden Sie unter ID-Felder werden aktualisiert.
- Die Rolle**„iamsync_admin“** ist zum Aktualisieren der Konfiguration erforderlich.
- Wenn es Anwender mit doppelten Anwendernamen und E-Mail-Adressen gibt, wird die Verbund-ID nur für einen Anwender generiert. Wenn der Anwendername NULL oder leer ist, ist die Verbund-ID NULL.



Nach der Installation des Plugins ändert sich wie folgt das Schema:

- Die neue Spalte „federated_id“ in der Tabelle `„sys_user“` wird erstellt.
- Neue Tabelle – `„iamsync_type“` wird automatisch mit der Standardkonfiguration für die Tabelle `„sys_user“ ausgefüllt`.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Föderierte ID wird nur für die Tabelle `„sys_user“` und alle Tabellen unterstützt, die die Tabelle „sys_user“ erweitern.

Nach dem Upgrade auf Release Xanadu wird das Plugin „Federated ID Generation“ (`com.glide.identity.globalid`) automatisch in allen Instanzen installiert.

Zugriff auf föderierte ID-Kriterien

Greifen Sie auf die Kriterien für Föderierte ID zu, um mehr über die ID-Felder zu erfahren, die für die generierte Föderierte ID verwendet werden.

Vorbereitungen

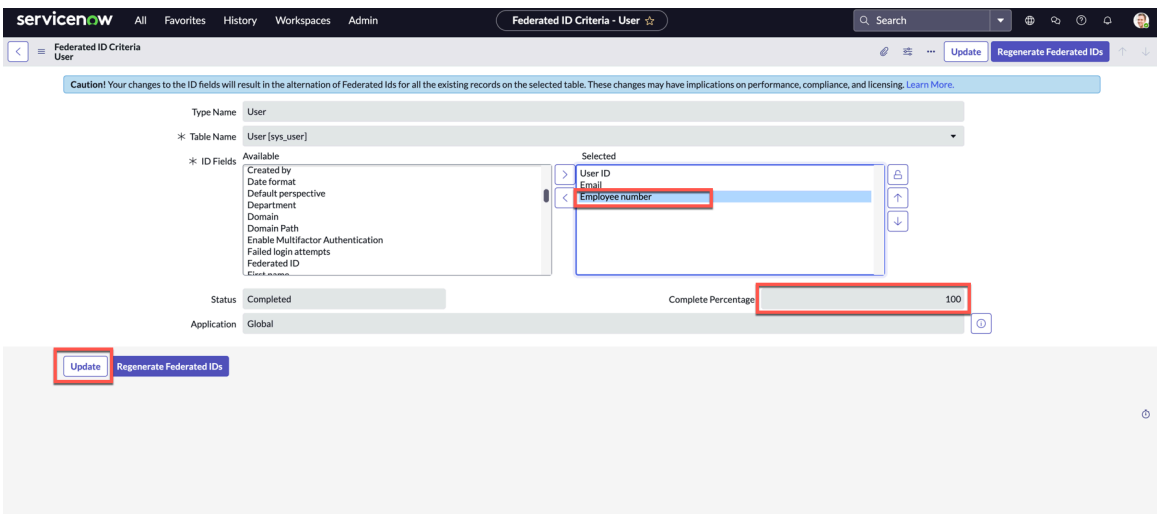
Erforderliche Rolle: iamsync_admin

Prozedur

1. Navigieren zu **Alle** > **Verbund-ID verwalten** > **Kriterien für Verbund-ID**an.
2. Auf der Seite „Kriterien für föderierte ID“ wird der Datensatz mit den folgenden Details angezeigt:
   - Typname: **Anwender**
   - Tabellenname: **Benutzer [sys_user]**
   - ID-Felder: **user_name (Anwender-ID), email** (Standardfelder, die für die Generierung der föderierten ID verwendet werden).
   - Status: **Abgeschlossen** (Status der föderierten ID-Generierung). Verfügbarer Status: **Bereit**, **Wird ausgeführt**, **Abgeschlossen**, **Fehler**.

Hinweis:

- Zum Generieren von Verbund-IDs ist ein Anwendername erforderlich.
- Anwendername und E-Mail-Adresse werden standardmäßig zum Generieren von Verbund-IDs verwendet.



Hinweis: Nur die ID-Felder können aktualisiert werden, um eine neue föderierte ID für die vorhandenen Datensätze zu generieren. Weitere Informationen finden Sie unter ID-Felder werden aktualisiert.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ID-Felder werden aktualisiert

Aktualisieren Sie die ID-Felder, um die Verbund-IDs basierend auf den aktualisierten Feldern neu zu generieren.

Vorbereitungen

Erforderliche Rolle: iamsync_admin

Hinweis: Alle Änderungen an den ID-Feldern führen zur Änderung der Verbund-IDs für alle vorhandenen Datensätze in der ausgewählten Tabelle. Diese Änderungen können sich auf Leistung, Compliance und Lizenzierung auswirken.

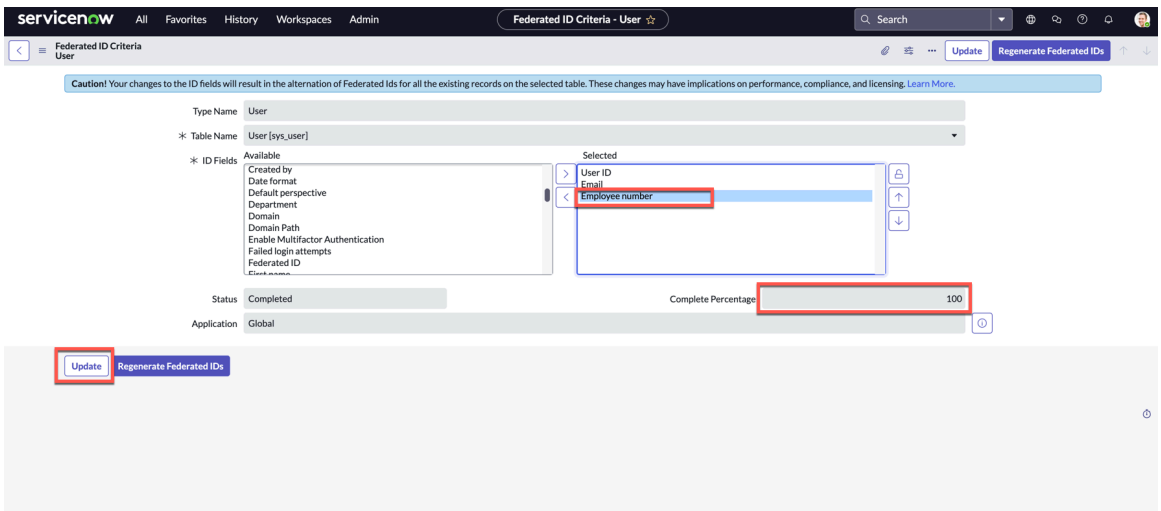
Prozedur

1. Navigieren zu **Alle** > **Verbund-ID verwalten** > **Kriterien für Verbund-ID**an.
2. Wählen Sie den Typnamen (**Anwender**) aus.
3. Wählen Sie auf der Seite Föderierte ID-Kriterien für Anwender, die Sie hinzufügen möchten, von Verfügbar zu Ausgewählt, indem Sie die Pfeiltasten verwenden.

   Beispiel: **Personalnummer**.

   Hinweis:

   - Zum Generieren von Verbund-IDs ist ein Anwendername erforderlich.
   - Anwendername und E-Mail-Adresse werden standardmäßig zum Generieren von Verbund-IDs verwendet.
   - Wenn es Anwender mit doppelten Anwendernamen und E-Mail-Adressen gibt, wird die Verbund-ID nur für einen Anwender generiert. Wenn der Anwendername NULL oder leer ist, ist die Verbund-ID NULL.



   Jetzt wird die ausgewählte **Mitarbeiternummer** zu einem weiteren Attribut zum Generieren der Verbund-ID.

4. Wählen Sie **Aktualisieren** aus, um Föderierte IDs zu generieren.

   Hinweis: Wählen Sie zuerst **Aktualisieren** aus, und überprüfen Sie dann den Prozentsatz der Fertigstellung (100), bevor Sie ein weiteres Update initiieren.

   Der Statusprozentsatz gibt die Generierung der Verbund-ID für alle Identitäten in allen Instanzen an.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Ändern Sie das Feld nicht, bis der vorherige Aktualisierungsauftrag abgeschlossen ist.
- Felder, die aktualisiert werden, müssen vom Typ „Zeichenfolge“ sein.
- Folgende Felder können nicht als ID-Felder ausgewählt werden:
  - Felder auf Systemebene
  - Edge Encryption-Felder
  - Passwortfelder.

5. Navigieren Sie zur Tabelle „sys_user“, um die neuen föderierten IDs anzuzeigen, die aufgrund der Aktualisierung der ID-Felder generiert werden.

Hinweis: Wählen Sie **Föderierte IDs erneut generieren** aus, wenn ein Anwender über XML-Importe oder Datenbankaktualisierungen auf niedriger Ebene erstellt oder aktualisiert wird oder die Instanz nicht ordnungsgemäß funktioniert. Wenn **Sie Föderierte IDs**erneut generieren auswählen, werden die IDs für alle Anwender unter Verwendung der aktuellen ID-Feldkriterien neu generiert.

Identity Center

Ermöglicht die Überwachung, Verwaltung und Minimierung von identitätsbasierten Risiken und Sicherheitslücken.

Untersuchen



Lernen Sie die Funktionen und den Geschäftsnutzen von Identity Center kennen.

Aktivieren



© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erfahren Sie, wie Sie Identity Center aktivieren.

Identitätsmetriken für Administratoren



Wissen, wie die Berechtigungen ausgewertet werden.

Identity Center für Benutzer



Rufen Sie Details zu den häufig gestellten Fragen zur Zugriffsanalyse ab.

Identity Center erkunden

Identity Center ist eine Sammlung von Anwenderattributen, Zugriff, Geräten, Anmeldeverlauf, Sicherheitsaktivität und vielem mehr.

Identity Center bietet Funktionen zum Überwachen, Verwalten und Minimieren von identitätsbasierten Risiken und Sicherheitslücken.

Identity Center bietet eine einzige Anlaufstelle für die Überwachung, Verwaltung und Minimierung von identitätsbasierten Risiken und Sicherheitslücken in ServiceNow.

Um das Identity Center zu aktivieren, installieren Sie das Plugin „Identity Center“ (`com.snc.identity_center`). Identity Center ist für Endanwender verfügbar, um die Details zu aktiven Sitzungen, dem Anmeldeverlauf und vertrauenswürdigen Geräten mit Identity Center anzuzeigen. Weitere Informationen finden Sie unter Identity Center für Benutzer.

Identity Center wird aktiviert

Installieren Sie für Identity Center das Plugin „Identity Center“ (`com.snc.identity_center`).

Vorbereitungen
Erforderliche Rolle: admin

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie das Plugin „Identity Center“ (`com.snc.identity_center`) mithilfe der Filterkriterien und der Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: `Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.`

   Nach Abschluss der Installation wird eine Meldung angezeigt.

Identity Center für Benutzer

Zeigen Sie mit dem Identity Center Details zu Ihren aktiven Sitzungen, dem Anmeldeverlauf und den vertrauenswürdigen Geräten an.

Identity Center ist eine Sammlung von Anwenderattributen, Geräten, Anmeldeverlauf, Sicherheitsaktivität und vielem mehr. Sie bietet eine Einzelansicht aller Daten mit zusätzlichen Sicherheitskontrollen und Benachrichtigungsfunktionen.

Mit Identity Center können Sie Details zu Ihren aktiven Sitzungen, dem Anmeldeverlauf und den vertrauenswürdigen Geräten anzeigen.

Um auf das Identity Center für Benutzer zuzugreifen, navigieren Sie zu einem der folgenden Elemente:

- Navigieren Sie auf Now Platformzu **Alle** > **Self-Service** > **Mein Profil** und wählen Sie im Abschnitt „Zugehörige Links“ die **Option Identity Center** anzeigen aus.

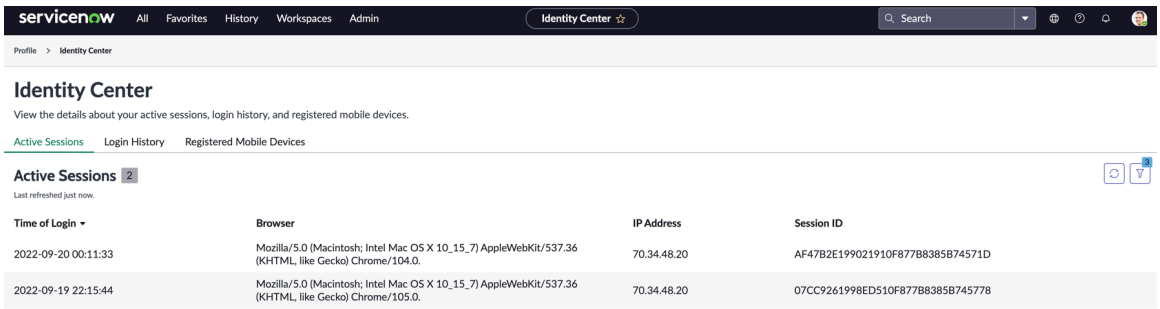
  Hinweis: Sie können auch auf Ihr Profil zugreifen, indem Sie Ihren Benutzernamen im Instanzheader auswählen.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



- Wählen Sie unter Now Supportdas Profil aus, und wählen Sie **Identity Center anzeigen** unten auf der Seite aus.

Die Seite „Identity Center“ wird wie folgt angezeigt:



Identity Center besitzt die folgenden Registerkarten:

- Aktive Sitzungen
- Anmeldungsverlauf
- Registrierte Mobilgeräte

Sie können diese Registerkarten auswählen, um Details wie Browser, IP-Adressen, Informationen zur Sitzungsbeziehung, Anmeldeinformationen und Ihre registrierten Mobilgeräte anzuzeigen.

Zeigen Sie aktive Sitzungen an

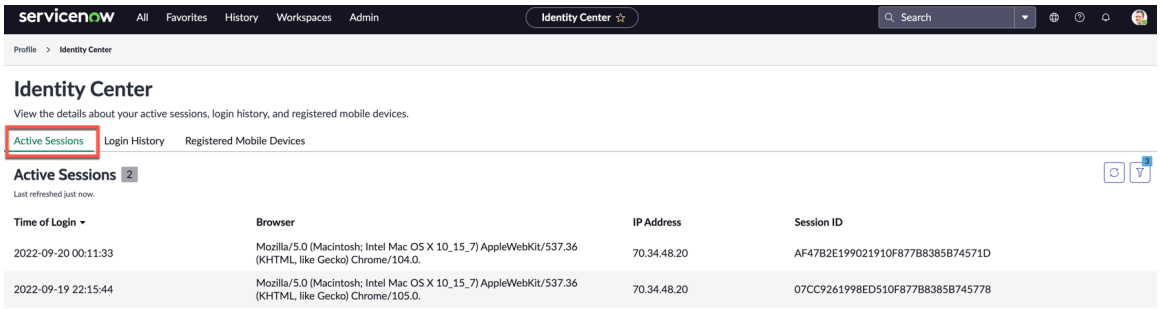
Zeigt die Informationen zu den Anwendersitzungen an.

Aktive Sitzungen sind die Sitzungen, die in der aktuellen Instanz ServiceNow® mit verschiedenen Browsern oder Geräten geöffnet sind.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auf der Registerkarte Aktive Sitzungen im Identity Center können Sie Ihre Sitzungen anhand des Browsers, der IP-Adresse und der Sitzungs-ID identifizieren. Mit diesen Informationen können Sie die erforderlichen Aktionen ausführen, z. B. Verlängern oder Beenden der Sitzung.

Mithilfe dieser Informationen können Sie feststellen, ob die Sitzungen real sind und kein Sicherheitsproblem darstellen.



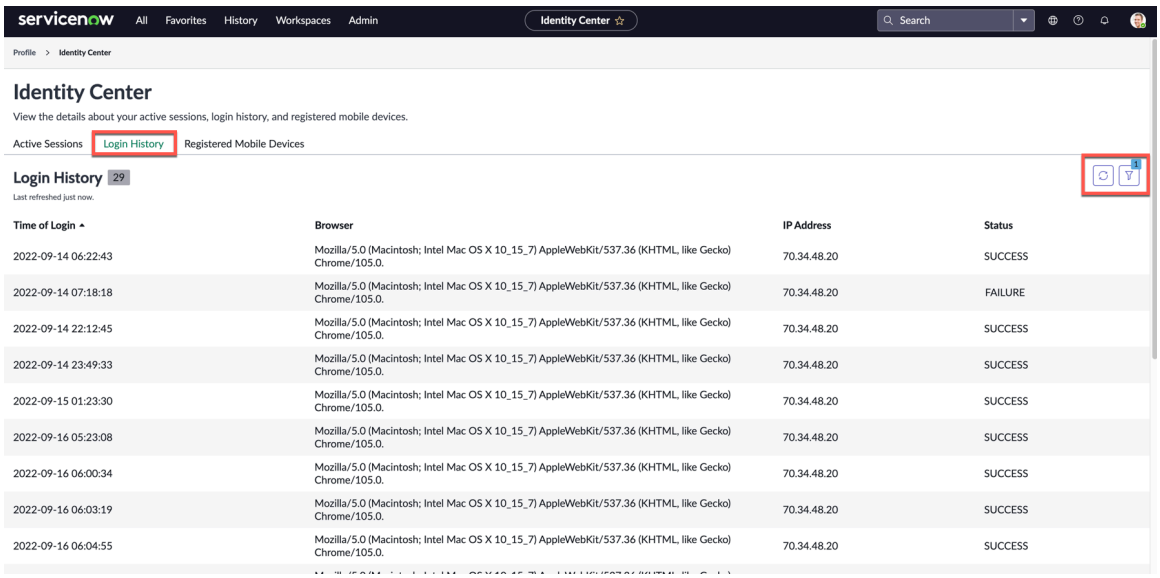
Anmeldeverlauf anzeigen

Stellt Details zu Ihrem Anmeldeverlauf bereit.

Die Registerkarte Anmeldeverlauf im Identity Center hilft Ihnen mit Ihren Anmeldeinformationen und dem Status Ihrer Anmeldung.

Sie können die Filter verwenden, um Anmeldeaktionen zur Unterstützung von Sicherheitsuntersuchungen anzugeben. Mithilfe von Filtern können Sie feststellen, ob die Aktivität real oder verdächtig war, und die Informationen an Ihren Administrator melden.

Die Paginierung im Anmeldeverlauf beträgt standardmäßig 20 und kann auf maximal 100 festgelegt werden.



Im Folgenden finden Sie einige weitere Details aus dem Anmeldeverlauf:

- Die Anmeldungszeit ist die aktualisierte Zeit, zu der die Mobilgeräte für den Zugriff auf die Instanz verwendet werden.
- Die Datensätze werden 30 Tage lang im Identity Center gespeichert.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registrierte Mobilgeräte anzeigen

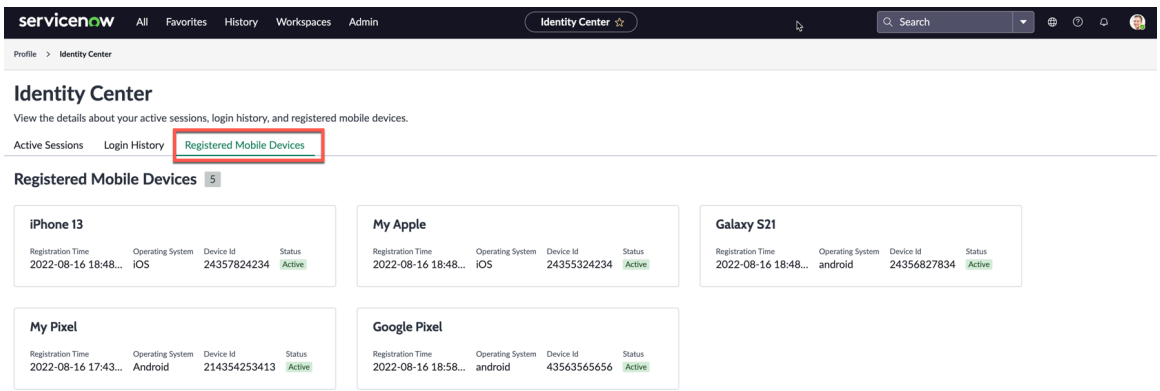
Geben Sie Details zu Ihrem registrierten Mobiltelefon in der Instanz ServiceNow an.

Auf der Registerkarte Registrierte Mobilgeräte im Identity Center werden die Details der registrierten Geräte angezeigt, die für den Zugriff auf die Instanz ServiceNow verwendet wurden.

Wenn das Modul Adaptive Authentifizierung aktiviert und ein registriertes Mobilgerät registriert ist, zeigt Identity Center die Details zu Ihren registrierten Geräten an.

Darüber hinaus werden Details zu den Geräten angezeigt, z. B. Betriebssystem, Geräte-ID und Status des Geräts sowie die Registrierungszeit des Geräts.

Um Ihr Mobilgerät zu registrieren, müssen Sie sicherstellen, dass das Plugin „Adaptive Authentifizierung“ (*com.snc.adaptive_authentication*) installiert ist und Sie Ihre Funktion „Trusted Mobile App“ aktiviert haben. Weitere Informationen finden Sie unter Aktivieren Sie die Trusted Mobile App.



Identitätsmetriken für Administratoren

Zeigen Sie Trends der -Benutzer, privilegierter Benutzer, aktiver Sitzungen und des integrierten Accounts in Ihrer Instanz ServiceNow an.

Identitätsmetriken für Administratoren weisen die Trends für Folgendes auf:

- Anwender
- Privilegierte Benutzer
- Integration oder nicht menschliche Konten
- Aktive Sitzungen
- Inaktive Sitzungen

Weitere Informationen finden Sie unter Security Center-Metriken.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

System für domänenübergreifendes Identitätsmanagement (SCIM)

Die System for Cross Domain Identity Management-API (SCIM) bietet Endpunkte zum Erstellen, Lesen, Aktualisieren und Löschen von Vorgängen für Benutzer und Gruppen mithilfe des SCIM-Protokolls.

SCIM-Anbieter



Der SCIM-Anbieter synchronisiert die an den Identitäten im IdP vorgenommenen Änderungen, einschließlich des Erstellens, Aktualisierens oder Löschens von Datensätzen.

SCIM-Client



Der SCIM-Client wird zum Erstellen, Aktualisieren und Löschen von Identitätsressourcen in einem System verwendet, das SCIM-konforme REST-Anforderungen unterstützt.

Automatische Übersetzung

Das SCIM-Protokoll ist ein HTTP-basiertes Protokoll auf Anwendungsebene, das auf dem HTTP-Standard (RFC7230) basiert. Verwenden Sie diese API für die Bereitstellung und Verwaltung von Identitätsdaten, z. B. Anwender und Gruppen. Verwenden Sie die API im Web und in domänenübergreifenden Umgebungen, z. B. in Szenarien von Enterprise-to-Cloud-Service Providern oder Inter-Cloud-Szenarien.

Um auf diese API zuzugreifen, müssen Sie das Plugin „SCIM v2 - ServiceNow® Cross-domain Identity Management“ (com.snc.integration.scim2) aktivieren.

Weitere Informationen zur SCIM-API finden Sie unter System for Cross-Domain Identity Management (SCIM) API .

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SCIM-Anbieter

Der Service Provider stellt Benutzer und Gruppen mithilfe der SCIM-API bereit.

Untersuchen



Erfahren Sie mehr über den SCIM-Anbieter.

Aktivieren



Aktivieren Sie SCIM.

SCIM-Anpassung



Quelldefinition



Erfahren Sie mehr über die Quelldefinition für SCIM.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rufen Sie Details zur Anpassung von SCIM ab.

SCIM-Anbieter erkunden

Der Service Provider stellt Benutzer und Gruppen mithilfe der SCIM-API bereit.

Als SCIM-Anbieter unterstützen die Schemata ServiceNow SCIM-APIs zur Bereitstellung von Benutzern und Gruppen.

Der SCIM-Anbieter synchronisiert die an den Identitäten im IdP vorgenommenen Änderungen, einschließlich des Erstellens, Aktualisierens oder Löschens von Datensätzen. Diese Änderungen werden gemäß dem SCIM-Protokoll automatisch mit dem Anbieter synchronisiert. Außerdem kann der IdP Identitäten vom Provider lesen und dem IdP-Verzeichnis hinzufügen. Der IdP kann dann falsche Werte beim Provider erkennen, die zu Sicherheitsschwachstellen führen könnten. Die Synchronisierung ermöglicht Endanwendern einen nahtlosen Zugriff auf Anwendungen, für die sie zugewiesen sind, mit aktuellen Profilen und Berechtigungen.

Konfigurationen für SCIM-Provider

Führen Sie die folgenden Aufgaben aus, um den SCIM-Anbieter zu konfigurieren:

- Aktivieren Sie das Plugin **„SCIM v2 - ServiceNow Cross-domain Identity Management“**. Weitere Informationen finden Sie unter SCIM-Plugin aktivieren.
- Aktivieren Sie die anderen Plugins, die für SCIM erforderlich sind:
  - OAuth 2.0
  - REST API-Anbieter
  - REST API-Zugriffsrichtlinie
- Fügen Sie die Rolle scim_admin als Teil des SCIM-Service hinzu.

⚠ **Warnung:** Gewähren Sie diese Rolle mit Bedacht. Die Rolle scim_admin entspricht der Gewährung der Rolle admin, wobei scmin_admin personenbezogene Daten hinzufügen oder aktualisieren kann.

Tabellen

Die beiden Tabellen „sys_user“ und „sys_group“ enthalten die SCIM-Attribute, die keinen vorhandenen ServiceNow -Tabellen zugeordnet sind. Weitere Informationen zu den Tabellen finden Sie unter SCIM-spezifische Tabellen .

SCIM-Plugin aktivieren

Installieren Sie zur Aktivierung von SCIM das Plugin „SCIM v2 - ServiceNow Cross-domain Identity Management (com.snc.integration.scim2).

Vorbereitungen

Erforderliche Rolle: admin

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie das Plugin „SCIM v2 - ServiceNow Cross-domain Identity Management“ (com.snc.integration.scim2) mithilfe der Filterkriterien und der Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: `Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.`

   Nach Abschluss der Installation wird eine Meldung angezeigt.

Lernprogramm: Konfigurieren Sie SCIM für die Anwenderbereitstellung mit einem Anbieter

Durch die Konfiguration von SCIM werden Benutzer und Gruppen automatisch über den Bereitstellungsservice des Anbieters für ServiceNow bereitgestellt bzw. aufgehoben.

Vorbereitungen

Installieren Sie das SCIM-Plugin.

Erforderliche Rolle: scim_admin

Warnung: Gewähren Sie diese Rolle mit Bedacht. Die Rolle scim_admin entspricht der Gewährung der Rolle admin, wobei scmin_admin personenbezogene Daten hinzufügen oder aktualisieren kann.

Warum und wann dieser Vorgang ausgeführt wird

Sie können Benutzer mit SCIM mithilfe der folgenden Authentifizierungsmethoden bereitstellen:

- Bereitstellen des Anwenders mit Standardauthentifizierung
- Bereitstellung des Anwenders mit OAuth

Bereitstellen des Anwenders mit Standardauthentifizierung

Durch die Konfiguration von SCIM werden Benutzer und Gruppen automatisch für ServiceNow bereitgestellt bzw. deren Bereitstellung aufgehoben, indem der Bereitstellungsservice des Anbieters mit Standardauthentifizierung verwendet wird.

Vorbereitungen

Erforderliche Rolle: scim_admin

Warnung: Gewähren Sie diese Rolle mit Bedacht. Die Rolle scim_admin entspricht der Gewährung der Rolle admin, wobei scmin_admin personenbezogene Daten hinzufügen oder aktualisieren kann.

Sie müssen das SCIM-Plugin aktivieren.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **REST API-Zugriffsrichtlinien** um die Details der REST API-Zugriffsrichtlinien zu überprüfen.
2. Klicken Sie auf der Seite „API-Zugriffsrichtlinie“ auf den Datensatz **SCIM-API-Richtlinie**.
3. Stellen Sie sicher, dass der Datensatz „ **SCIM-API-Basisauth**.“ in den Abschnitten „Authentifizierungsprofile“ verfügbar ist.
4. Überprüfen Sie, ob das Feld „Standardauthentifizierung“ mit dem **SCIM** - **API** -Datensatz angegeben ist, der zuvor als Anwendungsregistrierung konfiguriert oder verifiziert wurde.
5. Erstellen Sie die erforderlichen Konfigurationen auf Seiten des Anbieters.
6. Testen Sie die Verbindung, um sicherzustellen, dass der Anbieter eine Verbindung zu ServiceNowherstellen kann.

Hinweis: Wenn die Verbindung fehlschlägt, vergewissern Sie sich, dass Ihr Konto ServiceNow über Administratorrechte verfügt, und versuchen Sie es erneut.

Bereitstellung des Anwenders mit OAuth

Konfigurieren Sie den Anbieter für die automatische SCIM-Bereitstellung und die Aufhebung der Bereitstellung von Anwendern und Gruppen für ServiceNow, indem Sie den Bereitstellungsservice des Anbieters mit OAuth verwenden.

Vorbereitungen

Erforderliche Rolle: scim_admin

Warnung: Gewähren Sie diese Rolle mit Bedacht. Die Rolle scim_admin entspricht der Gewährung der Rolle admin, wobei scmin_admin personenbezogene Daten hinzufügen oder aktualisieren kann.

Sie müssen das SCIM-Plugin aktivieren.

Prozedur

1. Navigieren zu **Alle** > **System-OAuth** > **Applikationsregistrierung**an.
2. Klicken Sie auf der Seite „Anwendungsregistrierungen“ auf den **SCIM-API** -Datensatz.
3. Verifizieren Sie die **SCIM-API** -Datensatzdetails.

   Diese Details sollten bei der Konfiguration der Anwendung ServiceNow in Azure AD angegeben werden.
4. Navigieren zu **Alle** > **System-Webservices** > **REST API-Zugriffsrichtlinien** um die Details der REST API-Zugriffsrichtlinien zu überprüfen.
5. Klicken Sie auf der Seite „API-Zugriffsrichtlinie“ auf den Datensatz **SCIM-API-Richtlinie**.
6. Stellen Sie sicher, dass der Datensatz **„SCIMAPIOAuthOnly“** in den Abschnitten „Authentifizierungsprofile“ verfügbar ist.
7. Überprüfen Sie, ob das Feld „ **OAuth-Entität** “ mit dem **SCIM-API** -Datensatz angegeben ist, der zuvor als Anwendungsregistrierung konfiguriert oder verifiziert wurde.
8. Erstellen Sie die erforderlichen Konfigurationen auf Seiten des Anbieters.
9. Testen Sie die Verbindung, um sicherzustellen, dass der Anbieter eine Verbindung zu ServiceNowherstellen kann.

Hinweis: Wenn die Verbindung fehlschlägt, vergewissern Sie sich, dass Ihr Konto ServiceNow über Administratorrechte verfügt, und versuchen Sie es erneut.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SCIM-Fehlerbehebung

Häufige Fehlerszenarien bei der Integration mit SCIM.

Ungültige REST-API-URL

Aktion: Geben Sie eine gültige API-URL ein. Könnte die REST-API-URL im **REST-API-Explorer gegenprüfen**.

In der Instanz ServiceNow ist keine Umleitungs-URL festgelegt

Aktion: Geben Sie eine gültige Umleitungs-URL für die SCIM-OAuth-Entität in ServiceNowein. Geben Sie die Umleitungs-URL ein, während Sie die OAuth-Entität in ServiceNowkonfigurieren.

Wenn sich die Umleitungs-URL von der Anforderung unterscheidet

Aktion: „**redirect_url**“ unter „**Autorisierungsendpunkt“** muss mit der in ServiceNowkonfigurierten OAuth-Entität übereinstimmen.

Hinweis:

Dieser Fehler tritt auf, wenn eine Diskrepanz zwischen Azure „Autorisierungsendpunkt“ und ServiceNow „Umleitungs-URL“ besteht

Wenn ein ungültiger geheimer Clientschlüssel übergeben wird

Aktion: Der unter „Client-Geheimnis“ eingegebene Wert muss mit der in ServiceNowkonfigurierten OAuth-Entität übereinstimmen.

Wenn in Azure „Autorisierungsendpunkt“ eine ungültige „ClientId“ übergeben wurde

Aktion: Der für den Parameter „client_id“ in „Autorisierungsendpunkt“ eingegebene Wert muss mit der in ServiceNowkonfigurierten OAuth-Entität übereinstimmen.

SCIM-Anpassung

Passen Sie SCIM-Protokolle für Ihr Identitätsmanagement an.

Mit der SCIM-Anpassung können Sie:

- Unterstützen Sie anwenderdefinierte Felder in den Tabellen „sys_user“ und „sys_user_group“ durch die Generierung dynamischer Erweiterungsschemata.
- Möglichkeit zum Überschreiben der standardmäßigen SCIM-Zuordnungen bereitstellen

Ein SCIM-Administrator kann anwenderdefinierte Erweiterungsschemata für Benutzer- und Gruppenressourcen definieren. Die im anwenderdefinierten Erweiterungsschema definierten Attribute können Feldern in den Tabellen „sys_user“ oder „sys_user_group“ zugeordnet werden.

Konfigurationen für die SCIM-Anpassung

Zur SCIM-Anpassung sollten Sie die folgenden Aufgaben ausführen:

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Definieren Sie ein anwenderdefiniertes Erweiterungsschema für Benutzer und Gruppen in der SCIM-Erweiterungsschematabelle. Weitere Informationen finden Sie unter Erstellen Sie ein SCIM-Erweiterungsschema.
- Erstellen Sie Entitäten in einer -ETL-Definition für anwenderdefinierte Schemaattribute. Die Entitäten werden für die Zieltabelle erstellt, die entweder dem Attribut „sys_user“ oder „sys_user_group“ zugeordnet ist. Weitere Informationen finden Sie unter Erstellen Sie eine SCIM ETL-Definition.
- Erstellen Sie eine RTE-Zuordnung zwischen diesen beiden Entitäten. Weitere Informationen finden Sie unter Schritt 5 in Erstellen Sie eine SCIM ETL-Definition.
- Anwenderdefinierte Schemaattribute mit Daten in der Nutzlast der SCIM-API-Anforderung senden.

Die SCIM-API ruft die RTE-Engine mit der definierten Zuordnung auf. Die Daten werden in den entsprechenden Feldern in der Zieltabelle gespeichert, wie in der Zuordnung definiert.

SCIM-Anpassungseigenschaften und -schemas

Die SCIM-Anpassung umfasst die folgenden Eigenschaften, unterstützten und nicht unterstützten Schemas.

Eigenschaften

Durch die SCIM-Anpassung werden die folgenden Systemeigenschaften hinzugefügt.

Eigenschaften

Name	Beschreibung
com.snc.integration.scim2.max.member.count	Die maximale SCIM-Mitgliederanzahl.
com.snc.integration.scim2.resolve.external.id.filter	Lösen Sie SCIM-Ressourcen basierend auf der Quelldefinition des anfordernden Clients auf, wenn mehrere Ressourcen mit einem externen ID-SCIM-Filter gefunden werden. **Hinweis:** Wenn die Bereitstellung aus mehreren Quellen erfolgt, müssen die Quellen in der SCIM-Quelldefinitionstabelle definiert sein. Wenn keine Quellen definiert sind oder diese Eigenschaft inaktiv ist, werden alle übereinstimmenden Ressourcen mit einer externen ID-Filterantwort zurückgegeben.
com.snc.integration.scim2.user.etl.definition	ID der ETL-Definition für SCIM-Anwender.
com.snc.integration.scim2.group.etl.definition	Die ETL-Definitions-ID für die SCIM-Gruppe.
com.snc.integration.scim2.rte.verbose.logging.enabled	Aktiviert die ausführliche Protokollierung für RTE-Definitionen von SCIM-Anwendern und -Gruppen.
com.snc.integration.scim2.string.field.length.validation.enabled	Die Längenvalidierung für Felder. Diese Eigenschaft ermöglicht die Validierung, anstatt das Feld zu kürzen und zu speichern.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften (Fortsetzung)

Name	Beschreibung
com.snc.integration.scim2.provider.customizer.script.sys_id	Die ID der Skripteinbindung zum Anpassen der SCIM-Antworten.

Unterstützte Schemas

Die SCIM-Anpassung fügt die folgenden unterstützten Schemas hinzu.

Unterstützte Schemas

Schemen	Beschreibung	Präfix	Beispiel
urn:ietf:params:scim:schemas:core:2.0:User	Enthält Kernattribute für die Ressourcen.	Keine	name.mittelname
urn:ietf:params:scim:schemas:servicenow:2.0:User	Enthält Attribute, die sich auf ServiceNowbeziehen.	servicenow	servicenow.manager.value
urn:ietf:params:scim:schemas:extension:customer:2.0:User	Enthält anwenderdefinierte Attribute, die nicht als Teil der Core-Erweiterung oder des Erweiterungsschemas ServiceNow zugeordnet sind.	anwenderdefiniert	custom.socialId

Nicht unterstütztes Schema

urn:ietf:params:scim:schemas:extension:enterprise:2.0:User: Enthält Attribute, die häufig zur Darstellung von Anwendern verwendet werden, die zu einem Unternehmen gehören oder in dessen Namen handeln.

Hinweis: Das Enterprise-Schema ist ein gültiges Schema, seine Attribute werden jedoch einer beliebigen Tabelle zugeordnet. Da Datenbankpersistenz nicht unterstützt wird, wird kein Fehler angezeigt, wenn ein Enterprise-Schema im Anforderungstext enthalten ist.

Erstellen Sie ein SCIM-Erweiterungsschema

Erstellen Sie anwenderdefinierte Attribute für die Zuordnung zu Feldern, die nicht als Teil des Kernschemas oder des Erweiterungsschemas ServiceNow zugeordnet sind.

Vorbereitungen

Erforderliche Rolle: scim_admin

Warnung: Gewähren Sie diese Rolle mit Bedacht. Die Rolle „scim_admin“ entspricht dem Gewähren der Rolle „admin“, wobei die Rolle „scmin_admin“ neue Datensätze in die Tabellen einfügen kann, die Geschäftslogik oder ACL-Schutz umgehen können.

Prozedur

1. Navigieren zu **Alle** > **SCIM** > **SCIM-Erweiterungsschemas**an.
2. Klicken Sie auf **Neu**.

Automatische Übersetzung

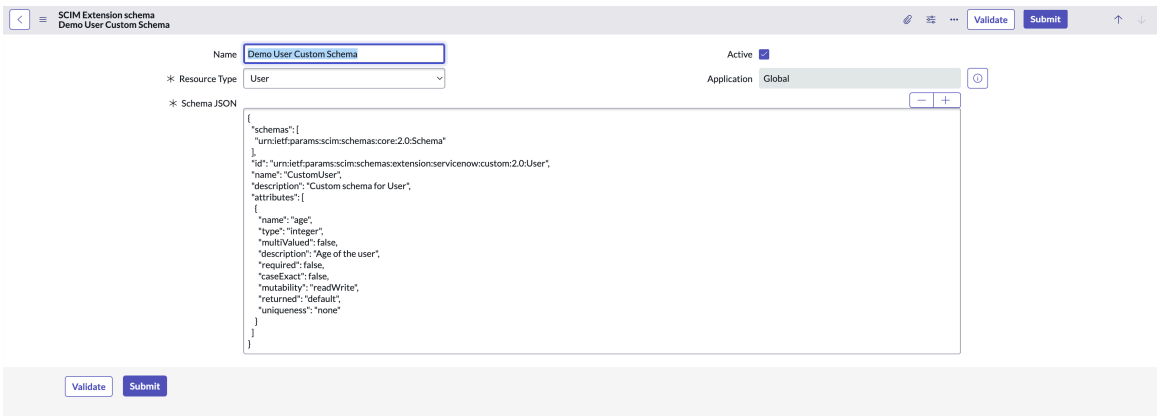
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Füllen Sie die Felder des Formulars aus.

Hinweis: Dem Feld „ **Ressourcentyp** “ kann nur ein Erweiterungsschema zugeordnet werden. Beispielsweise kann Benutzer als Ressourcentyp einem Benutzererweiterungsschema zugeordnet werden.

SCIM-Erweiterungsschema

Feld	Beschreibung
Name	Name des Erweiterungsschemas.
Aktiv	Option zum Aktivieren des Schemas. Wählen Sie dieses Feld aus, wenn der Datensatz als anwenderdefiniertes Erweiterungsschema betrachtet werden muss. Für einen bestimmten Ressourcentyp (Benutzer- oder Gruppentyp) kann jeweils nur ein Datensatz eines anwenderdefinierten Erweiterungsschemas aktiv sein.
Ressourcentyp	Ressourcentyp, der dem Erweiterungsschema zugeordnet werden muss. Die folgenden Optionen stehen zur Verfügung: ◦ **Benutzer** ◦ **Gruppe**
Anwendung	Anwendungsbereich für diesen Datensatz
Schema-JSON	Details innerhalb der JSON-Schemata. Weitere Informationen zum Definieren des Erweiterungsschemas mit Attributen finden Sie unter Datentracker .



4. Validieren Sie die Attribute, indem Sie auf **Validieren**klicken.
5. Klicken Sie auf **Absenden**.

Ergebnisse

Das Erweiterungsschema mit anwenderdefinierten Attributen, die sich auf den Ressourcentyp „Anwender“ oder „Gruppe“ beziehen, wird erstellt. Verwenden Sie die SCIM-ETL-Definitionen, um die Ressourcen basierend auf dem Erweiterungsschema in den Tabellen „sys_user“ und

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

„sys_user_group“ zuzuordnen. Weitere Informationen finden Sie unter Erstellen Sie eine SCIM ETL-Definition.

Erstellen Sie eine SCIM ETL-Definition

Verwenden Sie die SCIM-ETL-Definitionen, um die anwenderdefinierten Attribute den Tabellen „sys_user“ oder „sys_user_group“ zuzuordnen.

Vorbereitungen

Erforderliche Rolle: scim_admin

Warnung: Gewähren Sie diese Rolle mit Bedacht. Die Rolle „scim_admin“ entspricht dem Gewähren der Rolle „admin“, wobei die Rolle „scmin_admin“ neue Datensätze in die Tabellen einfügen kann, die Geschäftslogik oder ACL-Schutz umgehen können.

Hinweis:

- SCIM-Gruppen- und SCIM-Anwender-ETL-Definitionen sind Teil des Basissystems für die Ressourcenzuordnung. Sie können dieselben Ressourcenzuordnungen verwenden und die Kriterien nach Bedarf ändern oder neue Ressourcenzuordnungen erstellen.
- Es gibt keine Unterstützung für [*]-Felder über RTE in der SCIM-Zuordnung.

Prozedur

1. Befolgen Sie die Anweisungen unter ETL-Definitionen (Extract Transform Load) erstellen .
2. Öffnen Sie den neu erstellten Datensatz, und zeigen Sie die Details an.
3. Erstellen Sie im Abschnitt ETL-Entitäten eine Entität, indem Sie auf **Neu**klicken.
   Sie müssen Entitäten für die folgenden Anwender erstellen:
   - scim-user: Für die Felder, die aus SCIM stammen.
   - Tabelle „user“ (sys_user) oder „group“ (sys_user_group): Für die Felder, die Sie aus der Datenbanktabelle mit SCIM zuordnen möchten. Beispielsweise können Sie zur Anpassung von Benutzerdetails über SCIM die Tabelle sys_user verwenden.

   a. Füllen Sie die Felder des Formulars aus.

Formular „ETL-Entität“.

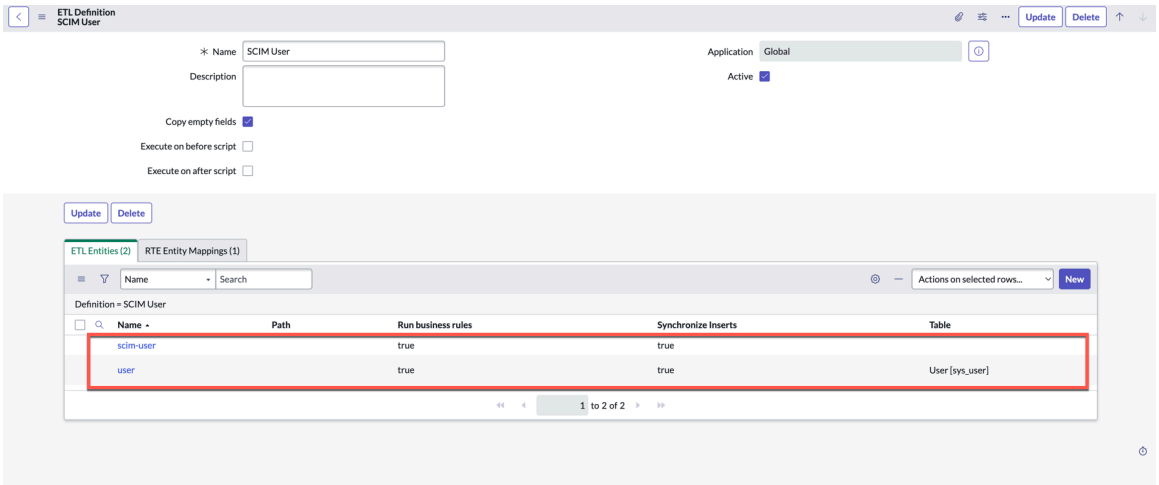
Feld	Beschreibung
Name	Name der ETL-Entität.
Anwendung	Anwendungsbereich für diesen Datensatz
Tabelle	Zieltabelle für die ETL-Entität.
Definition	Ausgewählte ETL-Entität.
Pfad	Eindeutiger Pfad für diese Entität. Geben Sie keinen Pfad für die Entität an, die die Importsatztabelle darstellt. Wenn eine Entität eine Sammlung darstellt, muss der Pfad mit einem Sternchen [*] enden. Diese Anforderung gilt für Zwischeneinträge und die Zieltabellenentität.
Einfügungen synchronisieren	Option, um durch Synchronisierung von Datensatzeinfügungen zu garantieren, dass nur ein Datensatz mit eindeutigen

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	zusammengefügten Feldwerten vorhanden ist.
Business-Regeln ausführen	Option zum Ausführen von Business-Regeln.

b. Klicken Sie auf **Absenden**.

Die ETL-Entitäten werden für die Tabellen scim-user und user erstellt. Sie müssen ETL-Entitätsfelder innerhalb dieser ETL-Entitäten erstellen und beide Entitäten zuordnen, indem Sie eine RTE-Entitätszuordnung erstellen.



4. Erstellen Sie die Entitäten, und ordnen Sie sie zu.

a. Öffnen Sie den übermittelten Datensatz (scim-user und user).

b. Fügen Sie in den Feldern ETL-Entität die Felder hinzu, indem Sie auf **Neu**klicken.

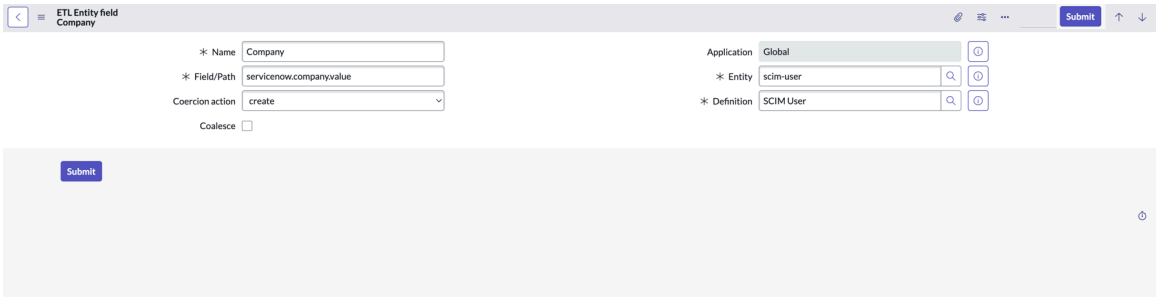
c. Füllen Sie die Felder des Formulars aus.

Formular „ETL-Entität“.

Feld	Beschreibung
Name	Name der ETL-Entitätsfelddefinition.
Anwendung	Ausgewählte ETL-Entität, zu der diese Felddefinition gehört.
Feld/Pfad	Dieses Feld ist entweder eine Spalte oder ein Pfad. ▪ Das Feld ist ein Spaltenname, wenn die Entität die Import- oder Zieltabelle ist. ▪ Das Feld ist ein Pfad, wenn das Feld geschachtelte Strukturen aufweist.
Entität	Entität, für die dieser Vorgang gilt. Wählen Sie die Entität mithilfe des Suchsymbols aus.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

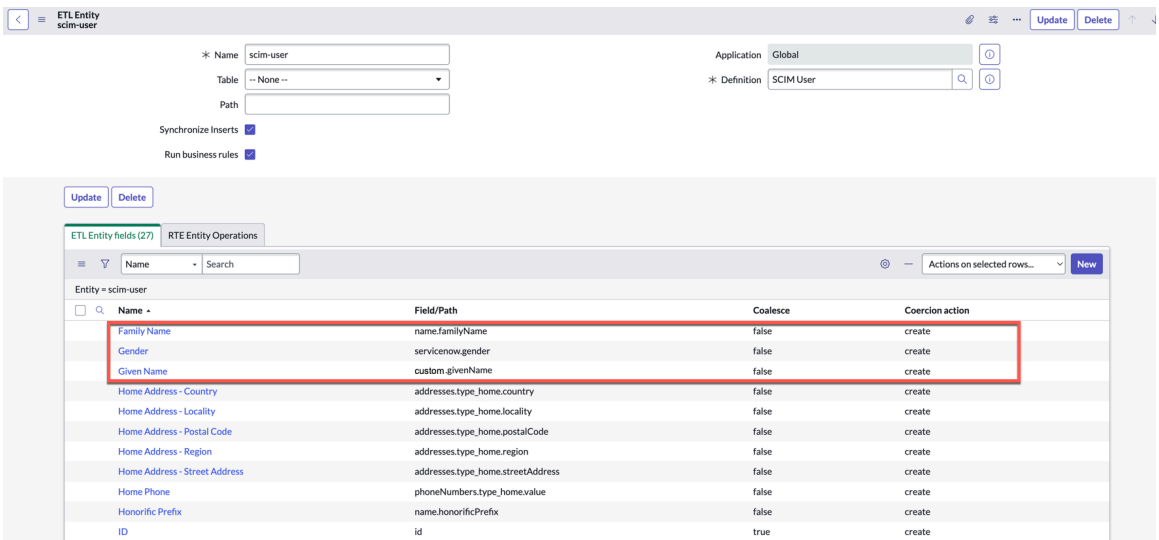
Feld	Beschreibung
Zwangsaktion	Was das System tun soll, wenn eine Referenz oder Auswahl nicht gefunden werden kann. Die Optionen sind wie folgt: ▪ **Erstellen**: Erstellt eine neue Referenz oder Auswahl. Weisen Sie die Referenz oder Auswahl dem aktuellen Datensatz zu. ▪ **Ablehnen**: Der gesamte Datensatz wird nicht in der Datenbank gespeichert. ▪ **Ignorieren**: Legen Sie den aktuellen Wert als leer fest.
Definition	Ausgewählte ETL-Entität, zu der diese Felddefinition gehört.
Zusammenfügen	Option zum Abfragen der vorhandenen Datensätze.



d. Senden Sie die Einträge, indem Sie auf **Absenden**klicken.

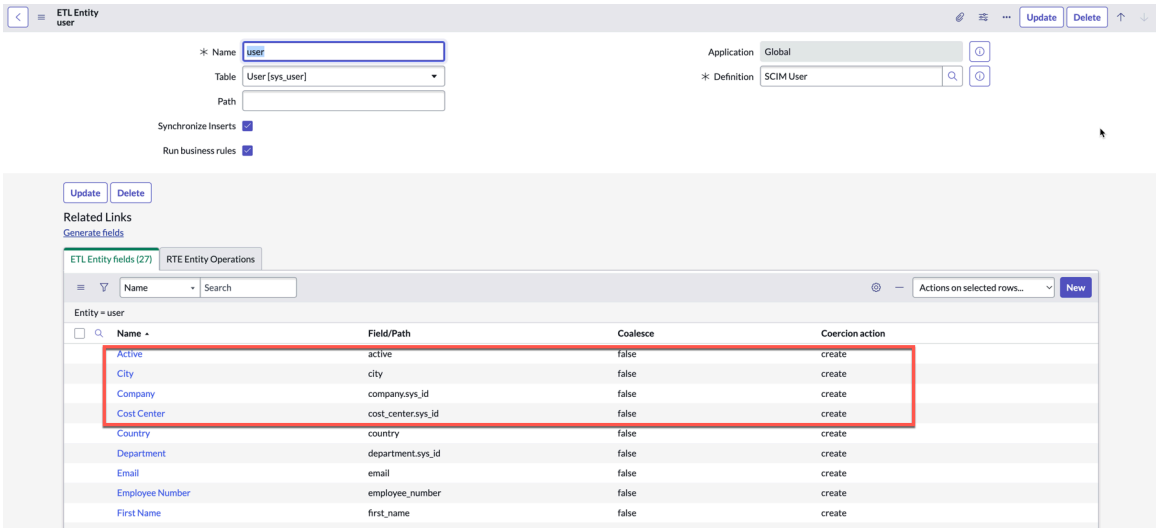
Sie können basierend auf Ihren Anforderungen mehrere Einträge als ETL-Entitätsfeld hinzufügen.

Die ETL-Entität „scim-user“ kann Entitäten mit der Core-Erweiterung (Benutzer), der Erweiterung ServiceNow oder der anwenderdefinierten Erweiterung aufweisen.



Die ETL-Anwenderentität kann Entitäten aus der Datenbanktabelle haben. Beispiel: Tabelle sys_user.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



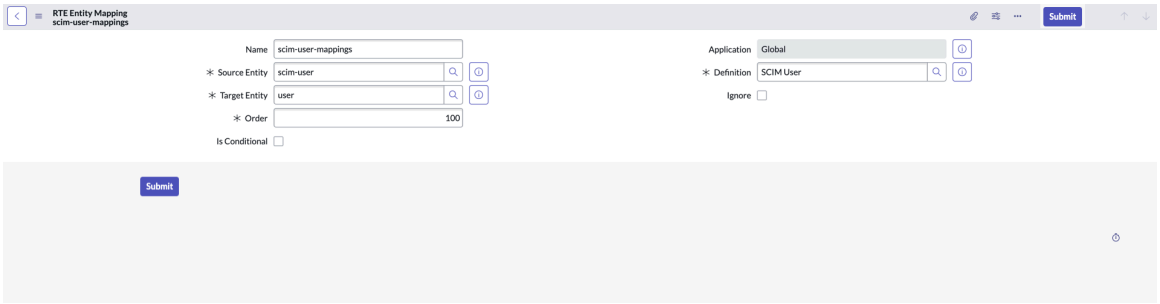
Hinweis: Verwenden Sie einen Unterstrich (_), um einen Filter in den eingehenden SCIM-Feldern hinzuzufügen. Dieser Unterstrich wird in einen EQ-Filter übersetzt. Zum Beispiel wendet das Attribut *email.type_work.value* den SCIM-Filter der E-Mail *[type eq "work"].value*an.

Nachdem die Felder in den ETL-Entitätsdatensätzen „scim-user“ und „user“ erstellt wurden, müssen Sie einen RTE-Entitätszuordnungsdatensatz erstellen. Anschließend müssen Sie die Quell- und Zieldefinition angeben, um beide Felder zuzuordnen.

5. Erstellen Sie im Abschnitt RTE-Entitätszuordnungen eine Entitätszuordnung, indem Sie auf **Neu**klicken
6. Füllen Sie die Felder im Formular aus.

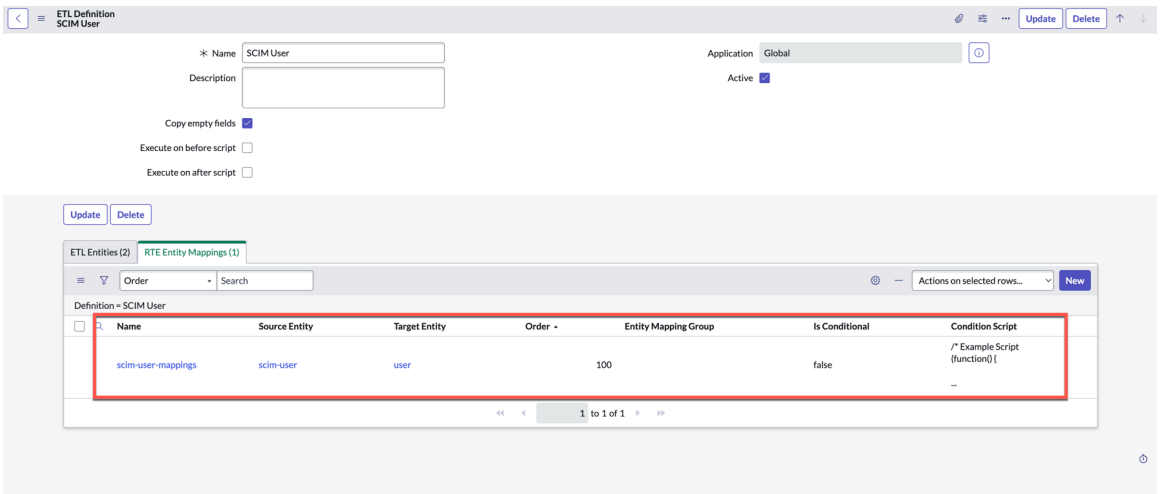
Feld	Beschreibung
Name	Name der Feldzuordnung.
Quellentität	Quellenentität für die Zuordnung.
Zielentität	Zielentität für die Zuordnung.
Bestellung	Reihenfolge, in der die Zuordnung verarbeitet werden soll.
Ist bedingt	Option zum Festlegen der Zuordnung als bedingt.
Bedingungsskript	Skript, das die Bedingungen definiert, die für die Zuordnung erfüllt werden müssen.
Anwendung	Anwendungsbereich für diesen Datensatz
Definition	Ausgewählte ETL-Entität, zu der diese Zuordnung gehört.
Ignorieren	Option zum Festlegen, ob diese ETL-Entitätszuordnung bei Datenintegrationen mit Robust Import Set Transformation (RTE) ignoriert werden soll.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Klicken Sie auf **Absenden**.

Das folgende Beispiel zeigt einen Datensatz, der für die Zuordnung der ETL-Entitätsdatensätze „scim-user“ und „user“ erstellt wurde.



8. Öffnen Sie den übermittelten Datensatz (scim-user-mappings), und erstellen Sie eine Zuordnung zwischen den Datensätzen „scim-user“ und „ETL-Entität des Anwenders“.

a. Klicken Sie im Abschnitt „RTE-Feldzuordnungen“ auf **Neu**.

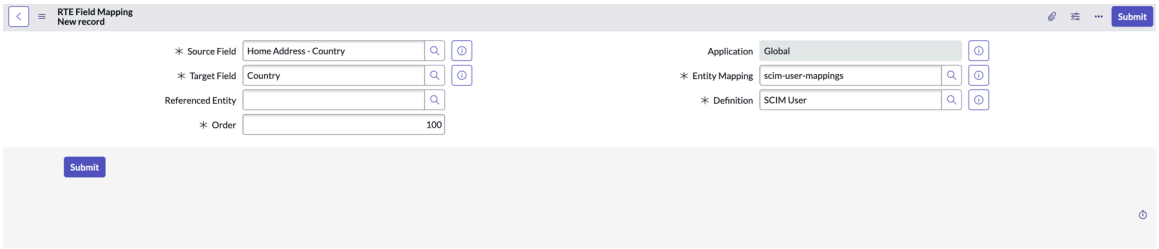
b. Füllen Sie die Felder des Formulars aus.

ETL-Entitätsfelder

Feld	Beschreibung
Quellfeld	Anwendungsbereich für diesen Datensatz
Anwendung	Ausgewählte ETL-Entität, zu der diese Felddefinition gehört.
Zielfeld	ETL-Ausgabefeld für den Vorgang, wenn der Vorgang eine einzelne Ausgabe erfordert.
Entitätszuordnung	Entitätszuordnung, für die dieser Vorgang gilt.
Referenzierte Entität	Entität, auf die verwiesen wird, und der Vorgang, auf den sie sich bezieht.
Definition	Ausgewählte ETL-Entität, zu der diese Felddefinition gehört.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

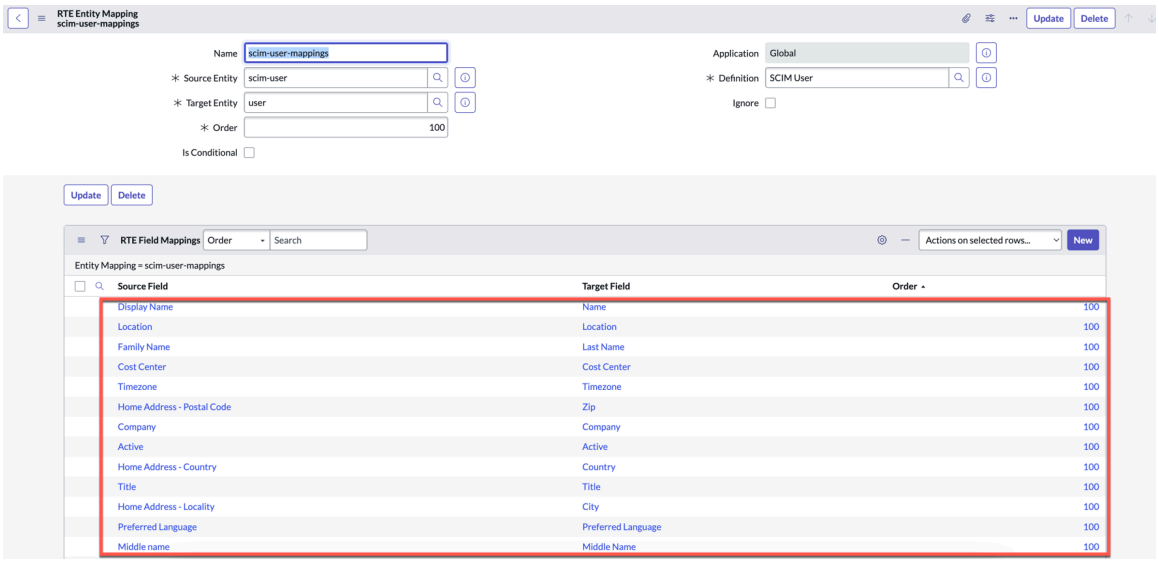
Feld	Beschreibung
Bestellung	Reihenfolge, in der der Vorgang für die Entität ausgeführt wird.



Das Quellfeld Privatadresse **– Land** (scim-user ETL Entity) ordnet das Zielfeld als **Land** (user ETL Entity) zu.

c. Senden Sie die Einträge, indem Sie auf **Absenden**klicken.

Sie können basierend auf Ihren Anforderungen mehrere Einträge als RTE-Entitätszuordnungen hinzufügen.



Die Quell- und Zielfelder werden wie konfiguriert zugeordnet. Wenn Sie CRUD-Vorgänge mit SCIM ausführen, werden die angepassten Werte in der entsprechenden Tabelle aktualisiert.

Ergebnisse

Mit diesen ETL-Definitionen und -Zuordnungen können Sie Daten aus einer Quelltabelle extrahieren, die Daten nach Bedarf umwandeln und in eine Zieltabelle laden.

Zugehörige Informationen

Erstellen Sie ETL-Definitionen (Extract Transform Load).

Behandelt nicht zugeordnete Felder

Sie können nicht zugeordnete Felder in der SCIM-Anpassung auf unterschiedliche Weise behandeln.

Während der SCIM-Anpassung können die Felder, die nicht Teil der Tabellen „sys_user“ und „sys_user_group“ sind, durch Ausführen der folgenden Funktionen zugeordnet werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SCIM anpassen (Erstellen oder aktualisieren)

Sie können den SCIM-Client erstellen oder aktualisieren.

- Der SCIM-Administrator kann anwenderdefinierte Skripts in den Skripten *onBefore* und *onAfter* für Felder hinzufügen, die nicht in der ETL-Definition oder RTE zugeordnet sind.
- Der SCIM-Administrator kann RTE-Zuordnungen überschreiben, indem er anwenderdefinierte Skripts in den Skripten *onBefore* und *onAfter* hinzufügt.
- Sie können eine skriptfähige API in den RTE-Skripts *onBefore* oder *onAfter* aufrufen, um auf eingehende Anforderungen zuzugreifen und Transformationen für andere Tabellen, Listen und nicht zugeordnete Attribute durchzuführen.
- Mit der Methode *sn_auth.SCIM2Util.getScimProviderCustomizationContext()* können Sie den SCIM-Anforderungskontext angeben, der das Objekt *scimResource* enthält. *scimResource* im Kontext steht bei jedem Vorgang für Folgendes:
  - **POST**: Die SCIM-Ressource, die in der Anforderungsnutzlast gesendet wird.
  - **PUT**: Die aktuelle SCIM-Ressource aus der Datenbank, die durch die in der Anforderungsnutzlast gesendete SCIM-Ressource ersetzt wird.
  - **PATCH**: Die aktuelle SCIM-Ressource aus der Datenbank nach der Durchführung der Patch-Vorgänge.

Im Folgenden finden Sie ein Beispiel für ein *onAfter*-Skript.

```
(function onAfter(source, target, importLog) {

    var ctx = sn_auth.SCIM2Util.getScimProviderCustomizationContext();
    gs.info("scim context ee: " + JSON.stringify(ctx.scimResource));

    var roles = ctx.scimResource.roles;
    if(roles) {
        var removingRolesGR = new GlideRecord("sys_user_has_role");
        removingRolesGR.addQuery("user", target.sys_user[0].sys_id);
        removingRolesGR.query();
        removingRolesGR.deleteMultiple();

    for (var i = 0; i < roles.length; i++) {
        var addingRolesGR = new GlideRecord("sys_user_has_role");
        addingRolesGR.setValue("user", target.sys_user[0].sys_id);
        addingRolesGR.setValue("role", roles[i].value);
        addingRolesGR.setValue("state", "active");
        addingRolesGR.insert();
        }
        }
        var customUserExtn = new
 global.SCIMProviderCustomization().getCustomExtensionUrn('User');
        var salary = ctx.scimResource[customUserExtn].salary;
        if (salary) {
            var gr = new GlideRecord("u_user_salary");
            gr.addQuery("user", target.sys_user[0].sys_id);
            gr.query();
            if (gr.next()) {
                gr.setValue("salary", salary);
                gs.info("scim update: " + gr.update());
            } else {
            gr.setValue("salary", salary);
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
            gr.setValue("user", target.sys_user[0].sys_id);
            gr.insert();
            }
           }

})(source, target, importLog);
```

Passen Sie die SCIM-Antwort an

Bei den GET-API-Aufrufen kann jede Antwort an den SCIM-Client mithilfe des Skripts angepasst werden, indem das Skript *SCIMProviderCustomization* erweitert wird.

Beim Erweitern des Skripts kann der Autor die Methoden *customizeUserResponse* und *customizeGroupResponse* überschreiben, um die Antworten für Benutzer- und Gruppenressourcen zu ändern.

Mit der Eigenschaft *com.snc.integration.scim2.provider.customization.script.id* kann das SCIM-Plugin das Skript verwenden, das für die Anpassung der Antwort verwendet werden soll.

Im Folgenden finden Sie ein Beispiel für die Erweiterung des Basisskripts.

```
var SCIMCustomizationScript = Class.create();
SCIMCustomizationScript.prototype =
 Object.extendsObject(SCIMProviderCustomization, {
    initialize: function() {
        SCIMProviderCustomization.prototype.initialize.call(this);
    },
    customizeUserResponse: function(context) {
        try {
            var rolesGR = new GlideRecord("sys_user_has_role");
            rolesGR.addQuery("user", context.scimResource.id);
            rolesGR.query();
            var i = 0;
            context.scimResource.roles = [];
            while (rolesGR.next()) {
                context.scimResource.roles[i] = {
                    display: rolesGR.getElement('role.name').getValue(),
                    value: rolesGR.getElement('role.sys_id').getValue()
                };
                i++;
            }
            var userGR = new GlideRecord("u_user_salary");
            userGR.addQuery("user", context.scimResource.id);
            userGR.query();
            if (userGR.next()) {
                var salary = userGR.getValue("salary");
                if (salary) {
                    var customExtensionValue =
 SCIMProviderCustomization.prototype.getCustomExtensionNodeValue.call(th
is, "User", context);
                    customExtensionValue.salary = salary;

 SCIMProviderCustomization.prototype.setCustomExtensionNodeValue.call(th
is, "User", context, customExtensionValue);
                }
            }
        } catch (ex) {
```


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
            gs.error("err: " + ex);
        }
        return context;
    },
    customizeGroupResponse: function(context) {
        return context;
    },
    type: 'SCIMCustomizationScript'
});
```

Hinweis:

- Der Parameter, den die Methoden *customizeUserResponse* und *customizeGroupResponse* enthalten, ist ein Kontextobjekt mit einem Attribut namens *scimResource*. Dieses Attribut weist alle Attribute eines Anwender- oder Gruppenressourcenobjekts auf.
- Eine anwenderdefinierte Skripteinbindung kann nur vom Administrator erstellt und angezeigt werden.
- Wenn eine Benutzer- oder Gruppenressource geändert wird, müssen Sie den Kontext wiederherstellen.
- Wenn kein Attribut im Ressourcenobjekt geändert wird, legen Sie *com.snc.integration.scim2.provider.customization.script.id* auf leer fest, oder geben Sie es als NULL zurück.
- Wenn bestimmte Attribute über das Skript *onAfter* beibehalten werden, müssen sie mit Datenbankwerten im Objekt *scimResource* im angepassten Skript gefüllt werden. Diese Aktion ist erforderlich, damit das System Folgendes ausführen kann:
  - Zum Abrufen des richtigen *scimResource*-Objekts in *onAfter*-Skripts während des PUT- und PATCH-Vorgangs.
  - Um die Attribute, die durch das Skript *onAfter* beibehalten wurden, in die Antwort an den Client aufzunehmen.

Hilfsfunktionen

Im Folgenden sind einige der Hilfsfunktionen für die SCIM-Anpassung aufgeführt. Mit diesen Funktionen können Sie verschiedene Arten von Informationen abrufen oder festlegen.

Hilfsfunktionen

Funktion	Zweck
SCIMProviderCustomization.prototype.getUserExtensionSchema(); "User");	Rufen Sie den Wert des anwenderdefinierten Erweiterungsschemas ab.
SCIMProviderCustomization.prototype.getUserExtensionSchema(); "User");	Rufen Sie den Wert des Erweiterungsschemas ServiceNow ab.
SCIMProviderCustomization.prototype.getUserExtensionSchemaNode.call(this, "User", context);	Rufen Sie den anwenderdefinierten Schemaknoten aus der Antwort ab.
SCIMProviderCustomization.prototype.getServiceNowExtensionSchemaNode.call(this, "User", context);	Rufen Sie den Schemaknoten ServiceNow aus der Antwort ab
SCIMProviderCustomization.prototype.setUserExtensionSchemaNode.call(this, "User", context, customExtensionValue);	Legen Sie den anwenderdefinierten Schemaknoten in der Antwort fest.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Im Folgenden finden Sie ein Beispiel für die Verwendung der Hilfsfunktion:

```
var customExtensionUrn =
SCIMProviderCustomization.prototype.getCustomExtensionUrn.call(this,
 "User");
var customExtensionValue =
SCIMProviderCustomization.prototype.getCustomExtensionNodeValue.call(th
is, "User", context);
customExtensionValue.age = "18";
SCIMProviderCustomization.prototype.setCustomExtensionNodeValue
 call(this, "User", context, customExtensionValue);
```

Hinweis: RTE unterstützt das Festlegen von Daten in anderen Tabellen als den Tabellen „sys_user“ und „sys_user_group“.

Eine Quelldefinition wird erstellt

Erstellen Sie eine Quelldefinition, um Informationen darüber zu erfassen, aus welcher Identitätsquelle eine Ressource bereitgestellt wird.

Vorbereitungen

Erforderliche Rolle: scim_admin

Warnung: Gewähren Sie diese Rolle mit Bedacht. Die Rolle scim_admin entspricht der Gewährung der Rolle admin, wobei scmin_admin personenbezogene Daten hinzufügen oder aktualisieren kann.

Warum und wann dieser Vorgang ausgeführt wird

Mithilfe einer Quelldefinition kann die Identitätsquelle der Bereitstellung einer OAuth-Entität zugeordnet werden, mit der sie sich während der Bereitstellung authentifiziert.

Nachdem eine Quelldefinition erstellt wurde, werden alle Ressourcen, die von dieser Identitätsquelle bereitgestellt werden, der entsprechenden Quelldefinitions-ID zugeordnet.

Die Quelldefinition erfasst die erforderlichen Quellinformationen, z. B. durch:

- Gibt den SCIM-Client an, von dem die Ressource bereitgestellt wird.
- Löst doppelte Informationen auf, die von der externen ID bereitgestellt werden:
  - Wenn mehrere Identitätsquellen Ressourcen bereitstellen, können zwei oder mehr Ressourcen denselben externen ID-Wert haben, da die externe ID nur für die Identitätsquelle eindeutig ist.
  - Wenn mehrere Ressourcen mit einem SCIM-Filter für die externe ID zurückgegeben werden, können die Ressourcen basierend auf der Quelldefinition der anfordernden Identitätsquelle aufgelöst werden.

Hinweis: Eine Quelldefinition kann nur für die Identitätsquelle erstellt werden, die eine OAuth-Authentifizierungsmethode verwendet.

Prozedur

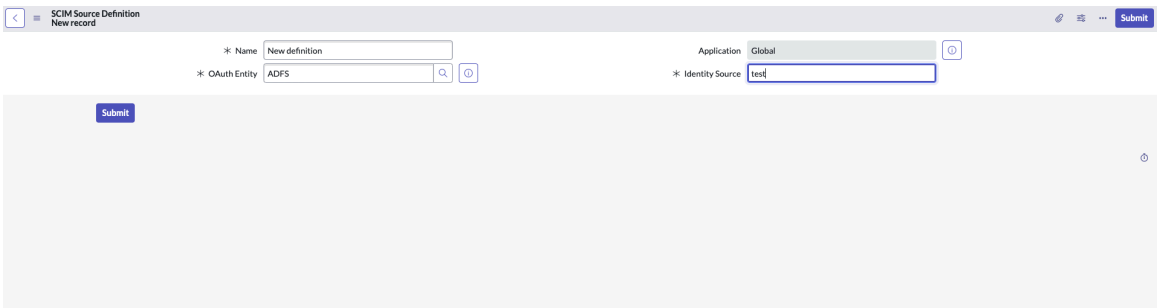
1. Navigieren zu **Alle** > **SCIM** > **Quellendefinition**an.
2. Klicken Sie auf der Seite „SCIM-Quellendefinitionen“ auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SCIM-Quellendefinition

Feld	Beschreibung
Name	Name der Quelldefinition.
Anwendung	Anwendungsbereich für diesen Datensatz
OAuth-Entität	Die OAuth-Entität des Integrationsanwenders. Die Entität wird für die Bereitstellung des Benutzers durch den Identitätsquellenanbieter verwendet.
Identitätsquelle	Der Name des Identitätsquellanbieters. Zum Beispiel Azure AD, Okta usw

Hinweis: Aktivieren Sie die Eigenschaft *com.snc.integration.scim2.resolve.externalid.conflict*, um nur SCIM-Ressourcen zurückzugeben, die von der anfordernden Identitätsquelle erstellt wurden. Standardmäßig werden alle übereinstimmenden Ressourcen mit einem externen ID-Filter zurückgegeben.



4. Klicken Sie auf **Absenden**.

Ergebnisse

Die Definition der SCIM-Quelle wird erstellt. Verwenden Sie die SCIM-ETL-Definitionen, um die Ressourcen basierend auf dem Erweiterungsschema in den Tabellen „sys_user“ und „sys_user_group“ zuzuordnen. Weitere Informationen finden Sie unter Erstellen Sie eine SCIM ETL-Definition.

SCIM-Client

Der SCIM-Client erleichtert die Bereitstellung und Aktualisierung von Identitätsressourcen durch CRUD-Vorgänge, die vom SCIM-Endpunkt in einem externen System verfügbar gemacht werden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Untersuchen



Erfahren Sie mehr über den SCIM-Client.

Aktivieren



Aktivieren Sie den SCIM-Client.

Eigenschaften des SCIM-Clients



Rufen Sie Details zur Anpassung von SCIM ab.

Problembehandlung



Erfahren Sie mehr über die Quelldefinition für SCIM.

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SCIM-Client erkunden

Der SCIM-Client erleichtert die Bereitstellung und Aktualisierung von Identitätsressourcen durch CRUD-Vorgänge, die vom SCIM-Endpunkt in einem externen System verfügbar gemacht werden.

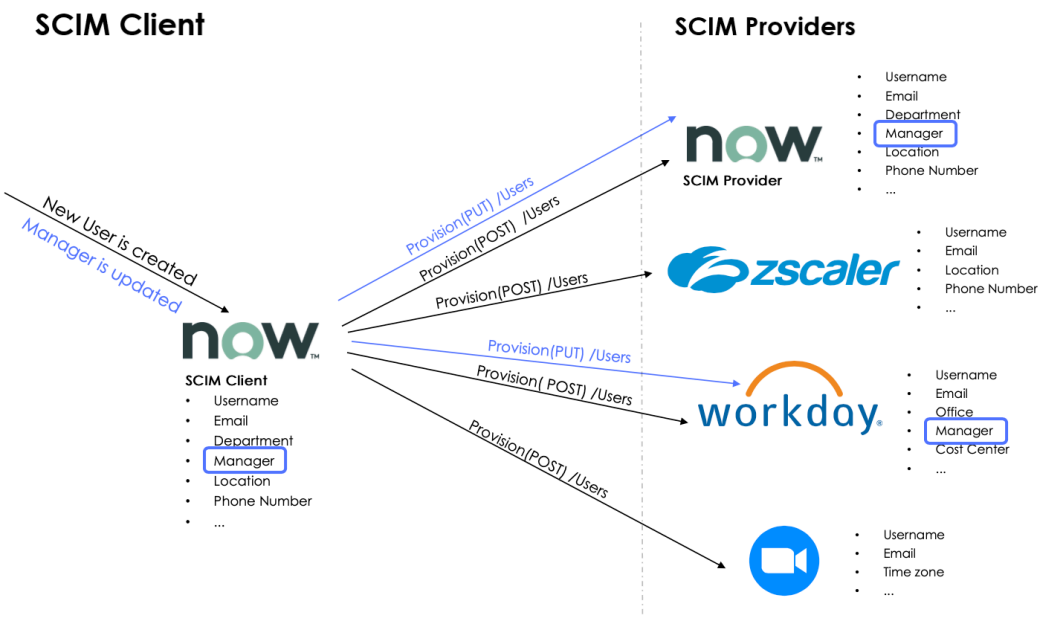
Der SCIM-Client wird zum Erstellen, Aktualisieren und Löschen von Identitätsressourcen in einem System verwendet, das SCIM-konforme REST-Anforderungen unterstützt. Der Client wird für das Management des Identitätslebenszyklus und für die Synchronisierung von Identitätsattributen zwischen [ServiceNow -Instanzen oder zwischen ServiceNow und anderen SCIM-Anbietern verwendet.

Da die APIs vom Client verfügbar gemacht werden, können Sie den Prozess des Erstellens, Aktualisierens oder Löschens von Ressourcen bei einem einzelnen oder mehreren SCIM-Anbietern automatisieren. Wenn beispielsweise ein Entwickler der Organisation beitritt, müssen Sie Zugriff auf Git, Arbeitsplatz usw. gewähren.

Mit dem SCIM-Client können Sie die folgenden Aktionen ausführen:

- Stellen Sie Identitäten und Zugriff für Benutzer oder Gruppenmitgliedschaften bereit.
- Identität und zugehörige Ressourcen mit SCIM-konformen Systemen synchronisieren
- Integrieren Sie einen beliebigen SCIM-Anbieter unter ServiceNow®.
- Heben Sie die Bereitstellung von Identitäten und Zugriff auf.

Der SCIM-Client stellt skriptfähige APIs bereit, mit denen Integrationsentwickler Workflows oder Automatisierungen für bestimmte Aufgaben erstellen kann. Weitere Informationen zur skriptfähigen API finden Sie unter SCIM2Client-API .



Konfigurationen für SCIM-Client

Führen Sie zum Konfigurieren des SCIM-Clients die folgenden Aufgaben aus:

- Erstellt eine REST-Nachricht für alle ausgehenden Anrufe für einen bestimmten SCIM-Anbieter. Weitere Informationen finden Sie unter REST-Nachrichten erstellen.
- Erstellen Sie einen SCIM-Anbieter, um Ressourcentypen und Schemainformationen mit der REST-Nachricht vom SCIM-Anbieter abzurufen. Aktivieren Sie die Konfiguration der HTTP-

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Methode (PUT oder PATCH), um eine Ressource im SCIM-Anbieter zu aktualisieren. Weitere Informationen finden Sie unter Erstellen Sie einen SCIM-Provider.

- Erstellt die Zuordnungen von SCIM-Attributen zu ServiceNow -Attributen für einen bestimmten Ressourcentyp und SCIM-Provider. Weitere Informationen finden Sie unter Erstellt eine Ressourcenzuordnung für den SCIM-Anbieter.
- Zuordnung des SCIM-Felds zur Datenbanktabelle und zum Feldnamen durchführen. Übergeben Sie den Standardwert, oder schreiben Sie ein Skript, um den Wert abzurufen. Weitere Informationen finden Sie unter Erstellen Sie eine SCIM-Attributzuordnung.

Aktivieren Sie das SCIM-Client-Plugin

Installieren Sie zur Aktivierung des SCIM-Clients das Plugin „SCIM v2 - ServiceNow Cross-domain Identity Management Client (com.snc.integration.scim2.client).

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie das Plugin „SCIM v2 - ServiceNow Cross-domain Identity Management Client“ (com.snc.integration.scim2.client) mithilfe der Filterkriterien und der Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: `Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.`

   Nach Abschluss der Installation wird eine Meldung angezeigt.

Eigenschaften, Tabellen, skriptfähige APIs und Protokolle des SCIM-Clients

Das Plugin „SCIM v2 - ServiceNow Cross-domain Identity Management Client“ (com.snc.integration.scim2.client) enthält die folgenden Systemeigenschaften, Tabellen, skriptfähigen APIs und Protokolle.

Eigenschaften

Der SCIM-Client fügt die folgenden Systemeigenschaften hinzu.

Eigenschaften

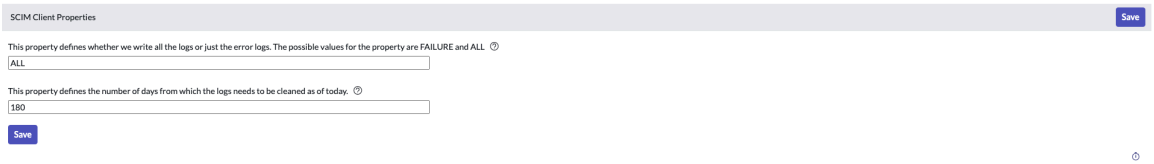
Name	Beschreibung
com.snc.integration.scim2.client.log.level	Diese Eigenschaft bestimmt, ob alle Protokolldatensätze oder nur die Fehlerprotokolldatensätze geschrieben werden sollen. Die möglichen Werte sind **FEHLER** oder **ALLE**.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften (Fortsetzung)

Name	Beschreibung
	Standardwert: **ALL**
com.snc.integration.scim2.client.log.days_to_clean	Diese Eigenschaft bestimmt die Anzahl der Tage zum Löschen der Protokolle. Standardwert: **180**

Um die Eigenschaften festzulegen, navigieren Sie zu **Alle** > **SCIM** > **Eigenschaften des SCIM-Clients**an.



Tabellen

Der SCIM-Client fügt die folgenden Tabellen hinzu.

Tabellen

Name	Beschreibung
SCIM-Anbieter (sys_scim_provider)	Speichert Daten für jeden SCIM-Anbieter, z. B. den Namen, Definitionen der REST-Nachrichtenressourcen usw.
Ressourcenzuordnung für SCIM-Anbieter (sys_scim_provider_resource_mapping)	Speichert die primären Tabelleninformationen für jeden Anbieter und jeden Ressourcennamen.
SCIM-Attributzuordnung (sys_scim_attribute_mapping)	Speichert die Quelldetails, aus denen jeder SCIM-Attributwert stammen sollte, z. B. Tabellenfeld, Skript usw.
SCIM-Clientprotokoll (sys_scim_client_logs)	Speichert den Status jedes Anrufs, der beim SCIM-Anbieter ausgelöst wurde.

Skriptfähige API

Die SCIM2Client-API ruft den Anbieter des System for Cross-Domain Identity Management (SCIM) (Serverrolle) auf, um Daten in einem Service Provider (SP) zu erstellen, zu aktualisieren oder zu löschen. Die skriptfähige API des SCIM-Clients sollte in den Skripts verwendet werden, die im Systemkontext oder von einem Systemadministrator ausgeführt werden.

Beispielsweise können Sie das Skript verwenden, während Sie den Integrations-Hub-Workflow als Systembenutzer ausführen, während Sie die geplanten Aufgaben ausführen usw.

Im Folgenden finden Sie einige Anwendungsfälle für die Verwendung der skriptfähigen APIs:

Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Als Administrator stellen Sie Identitätsinformationen aus Hintergrundskripts, Business-Regeln, Skripteinbindungsaufrufen, Workflows usw. bereit.
- Führen Sie als Administrator eine regelmäßige oder eine bedarfsgesteuerte Aufgabe für die Identitätsbereitstellung aus.
- Führen Sie mit dem Schritt Skript einen Workflow oder Sub-Workflow aus, indem Sie den skriptfähigen API-Aufruf für die Bereitstellung verwenden.
- Fügen Sie das Bereitstellungsskript direkt in einer Geschäftsregel oder Skripteinbindung hinzu. Das Skript kann von Nicht-Administratoren ausgelöst werden. Dieser Anwendungsfall funktioniert in den folgenden Situationen:
  - Der Benutzer hat Zugriff auf das Token, was bedeutet, dass der Benutzer über die Rolle verfügt, um das Token aus der REST-Vorlage zu generieren.
  - Der Benutzer hat Zugriffsrechte, um die SCIM-Attributwerte aus den zugeordneten Tabellen abzurufen.

Weitere Informationen zur skriptfähigen API finden Sie unter SCIM2Client-API .

SCIM-Clientprotokolle

Die SCIM-Client-Protokolle zeigen den Bereitstellungsstatus der SCIM-APIs an. Um den Bereitstellungsstatus anzuzeigen, navigieren Sie zu **Alle** > **SCIM** > **SCIM-Clientprotokolle**an.

REST-Nachrichten erstellen

Konfigurieren Sie eine REST-Nachricht für alle ausgehenden Anrufe für einen bestimmten SCIM-Anbieter.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **Ausgehend** > **REST-Nachricht**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

SCIM-Anbieter

Feld	Beschreibung
Name	Beschreibender Name für diese Nachricht.
Endpunkt	Basis-URL des SCIM-Anbieters. Beispiel: `https://beispiel.service-now.com/api/now/scim`.
Authentifizierungstyp	Typ der Authentifizierung, die zum Herstellen einer Verbindung mit dem externen SCIM-Anbieter verwendet werden soll. Weitere Informationen finden Sie unter Ausgehende REST-Authentifizierung .
REST-Nachrichtenheader	Der Inhaltstyp, der vom externen SCIM-Anbieter erwartet wird.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Beispiel: Headername ist der Inhaltstyp im folgenden API `-Anforderungstext: Inhaltstyp: application/scim+json`

4. Klicken Sie in der zugehörigen Liste „HTTP-Methoden“ auf **Neu**.
5. Konfigurieren Sie die folgenden HTTP-Methoden.

Hinweis: Die URLs enthalten Variablen, die Sie ersetzen müssen.

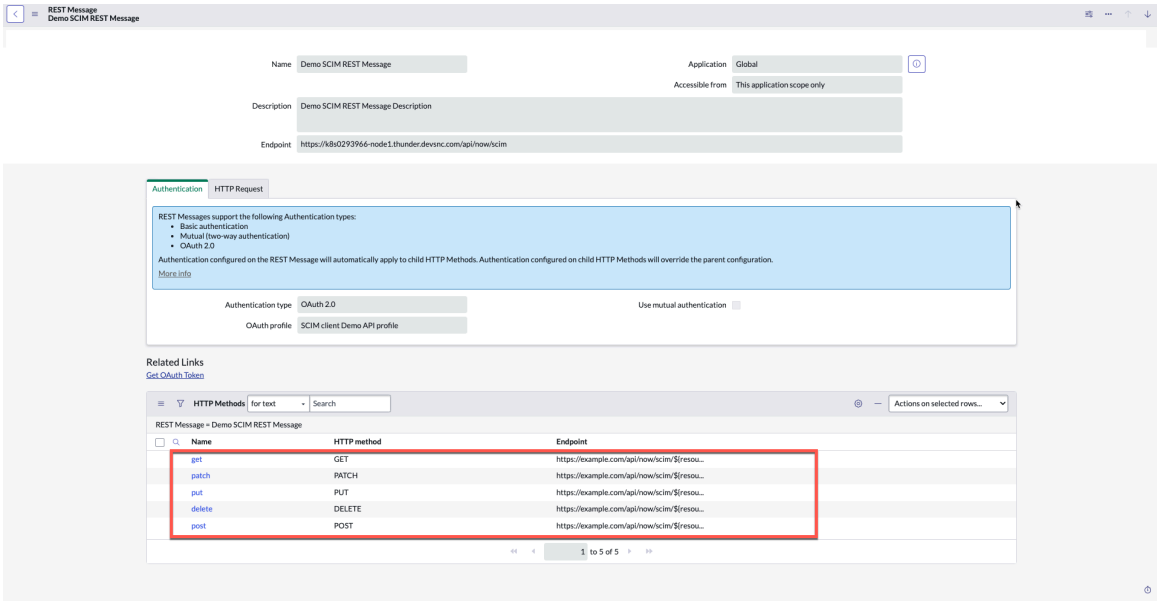
REST-Nachrichtenfunktionen

Methoden	Beispiel-URL
GET	`https://beispiel.com/api/now/scim/${resourceName}`
PATCH	`https://beispiel.com/api/now/scim/${resourceName}/${resourceId}`
PUT	`https://beispiel.com/api/now/scim/${resourceName}/${resourceId}`
LÖSCHEN	`https://beispiel.com/api/now/scim/${resourceName}/${resourceId}`
POST	`https://beispiel.com/api/now/scim/${resourceName}/${resourceId}`

Hinweis:

- Sie müssen alle HTTP-Methoden für den Betrieb des SCIM-Clients erstellen.
- Eine REST-Beispielnachricht wird vom Basissystem bereitgestellt.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Klicken Sie auf **Absenden**.

Ergebnisse
Der REST-Nachrichtendatensatz wird erstellt.

Nächste Maßnahme
Verwenden Sie die REST-Nachricht, um einen SCIM-Provider zu erstellen. Weitere Informationen finden Sie unter Erstellen Sie einen SCIM-Provider.

Weitere Informationen zum Erstellen einer REST-Nachricht finden Sie unter REST- Nachricht erstellen .

Erstellen Sie einen SCIM-Provider

Erstellen Sie einen SCIM-Anbieter, um Ressourcentypen und Schemainformationen mit der REST-Nachricht vom SCIM-Anbieter abzurufen. Aktivieren Sie die Konfiguration der HTTP-Methode (PUT oder PATCH), um eine Ressource im SCIM-Anbieter zu aktualisieren.

Vorbereitungen
Hinweis: Ein Beispiel-SCIM-Provider ist Teil des Basissystems. Sie können basierend auf Ihren Anforderungen konfigurieren oder einen neuen Datensatz erstellen.

Erforderliche Rolle: admin

Prozedur
1. Navigieren zu **Alle** > **SCIM-Client** > **SCIM-Anbieter**an.
2. Klicken Sie auf der Seite „SCIM-Anbieter“ auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular „SCIM-Provider“.

Feld	Beschreibung
Name	Name des SCIM-Anbieters
Ausgehende REST-Nachricht	Nachricht, die zum Aufrufen der API des SCIM-Anbieters verwendet wird. Weitere

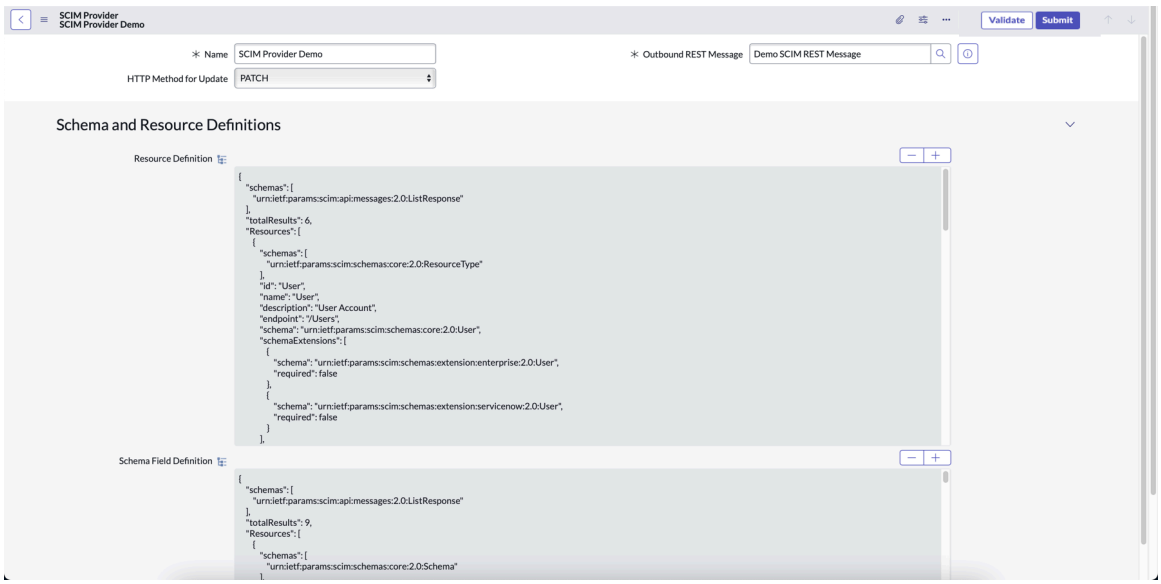
Automatische Übersetzung

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Informationen finden Sie unter REST-Nachrichten erstellen.
HTTP-Methode für Aktualisierung	Typ der HTTPS-Methode, die zum Aktualisieren der Ressourcenzuordnung verwendet wird. Die PATCH- oder PUT-Methode kann vom Client während der Aktualisierung der Identitätsressource während der Bereitstellung einer bereits vorhandenen Ressource verwendet werden.

Hinweis:

- Die Felder „ **Ressourcendefinition** “ und „ **Schemafelddefinition** “ werden von den öffentlichen Endpunkten */ResourceTypes* und */Schemas* des SCIM-Anbieters abgerufen. Diese Felder werden automatisch ausgefüllt, nachdem die REST-Nachricht ausgewählt wurde.
- Wenn die REST-Nachricht, Schemas oder Ressourcentypen im SCIM-Provider aktualisiert werden, klicken Sie auf Aktualisieren und dann auf **Aktualisieren**, um die **FelderRessourcendefinition** und **Schemafelddefinition** zu aktualisieren.



4. Klicken Sie auf **Absenden**.

Ergebnisse

Die SCIM-Providerdetails wurden erfolgreich erstellt. Verwenden Sie die Ressourcenzuordnung des SCIM-Anbieters, um die SCIM-Anbieterdetails den Ressourcen wie Benutzern oder Gruppen zuzuordnen. Weitere Informationen finden Sie unter Erstellt eine Ressourcenzuordnung für den SCIM-Anbieter.

Erstellt eine Ressourcenzuordnung für den SCIM-Anbieter

Definieren Sie die Zuordnungen von SCIM-Attributen zu ServiceNow -Attributen für einen bestimmten Ressourcentyp und SCIM-Provider.

Vorbereitungen

Erforderliche Rolle: admin

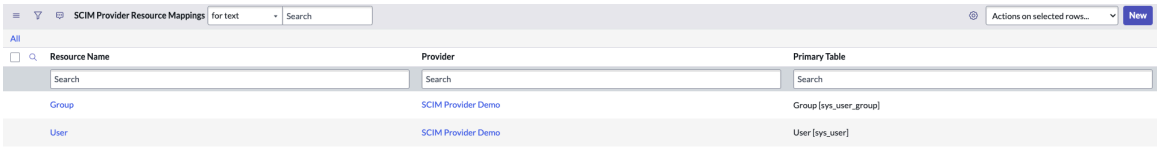
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **SCIM-Client** > **Ressourcenzuordnung des SCIM-Anbieters**an.

   Die Ressourcenzuordnung des SCIM-Anbieters wird standardmäßig mit der Anwender- und Gruppenzuordnung geliefert.

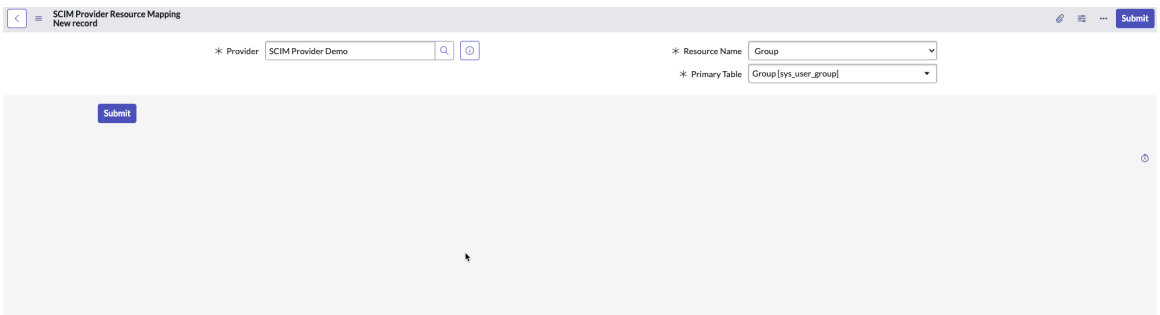
   Hinweis: Die Benutzer- oder Gruppenzuordnungen enthalten Beispielzuordnungen, die Sie als Referenz verwenden können. Sie können Zuordnungen auch basierend auf Benutzer- oder Gruppenressourcen erstellen.



2. Erstellen Sie eine Ressourcenzuordnung, indem Sie auf **Neu**klicken.
3. Füllen Sie die Felder des Formulars aus.

Ressourcenzuordnung

Felder	Beschreibung
Anbieter	Name des SCIM-Anbieters. Verweisen Sie beim Erstellen eines SCIM-Anbieters auf den konfigurierten Anbieternamen.
Ressourcenname	Ressource, für die die Zuordnung definiert werden muss.
Primäre Tabelle	Die Tabelle, die die sys_id der zugeordneten Ressource enthält.



4. Klicken Sie auf **Absenden**.

Ergebnisse

Der Datensatz wird erstellt und auf der Seite „Ressourcenzuordnung des SCIM-Anbieters“ angezeigt. Verwenden Sie die SCIM-Attributzuordnungen, um die Attribute aus Schemas weiter zuzuordnen. Weitere Informationen finden Sie unter Erstellen Sie eine SCIM-Attributzuordnung.

Erstellen Sie eine SCIM-Attributzuordnung

Erstellen Sie eine SCIM-Attributzuordnung, und verwenden Sie sie als einzelne Ressourcenquelle für die Felder der Tabelle ServiceNow.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Im Folgenden finden Sie die Attributzuordnungstypen und ihre Beschreibungen.

Attributzuordnungstypen

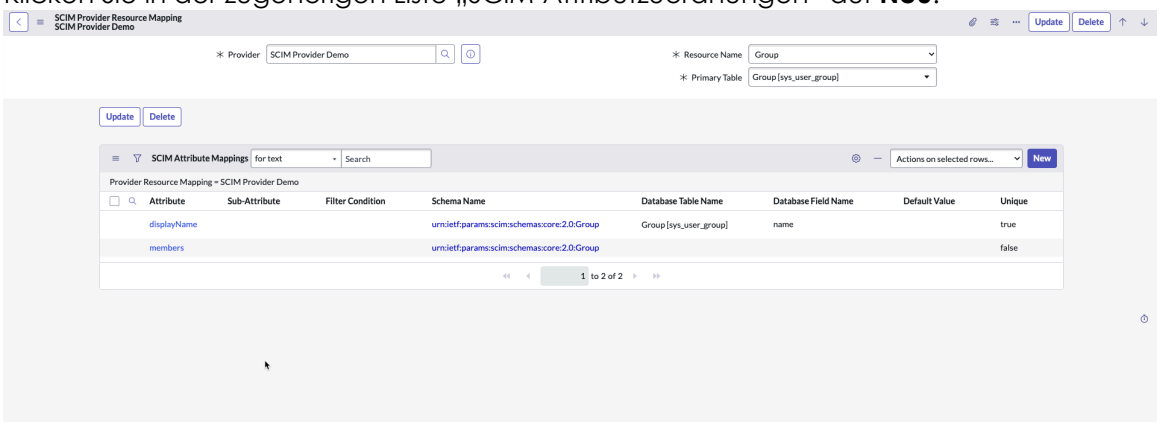
Attributzuordnungstyp	Beschreibung
Direkt	Das SCIM-Attribut wird mit Hilfe der Felder **Datenbanktabellenname** und **Datenbankfeldname ausgefüllt**.
Konstante	Das SCIM-Attribut wird mit Hilfe eines angegebenen Standardwerts ausgefüllt.
Skript/Anwenderdefiniert	Das SCIM-Attribut wird mit Hilfe des Rückgabewerts eines Skripts ausgefüllt. Dieses Attribut erfordert die Aktivierung der Option „Skript ausführen“.

Hinweis:

- Das Passwortattribut wird nicht unterstützt
- Eine Beispielattributzuordnung für die Ressourcen Anwender und Gruppe ist Teil des Basissystems. Sie können die Zuordnungen basierend auf Ihren Anforderungen verwenden und konfigurieren oder einen neuen Datensatz erstellen.

Prozedur

1. Navigieren zu **Alle** > **SCIM-Client** > **Ressourcenzuordnung des SCIM-Anbieters**an.
2. SCIM-Ressourcenzuordnung ausgewählt, die für die Konfiguration erstellt wird.
3. Klicken Sie in der zugehörigen Liste „SCIM-Attributzuordnungen“ auf **Neu**.



4. Füllen Sie die Felder des Formulars aus.

Formular „SCIM-Attributzuordnungen“.

Felder	Beschreibung
Ressourcenzuordnung des Anbieters	Attributzuordnung für eine Kombination aus Anbieter und Ressource

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder	Beschreibung
	Wenn dieses Feld nicht automatisch ausgefüllt wird, verwenden Sie die Suchoption. Wählen Sie den Datensatz „Ressourcenzuordnung des Anbieters“ aus.
Schemaname	Schemaname des SCIM-Attributs, für das die Zuordnung definiert werden muss. Zum Beispiel *urn:ietf:params:scim:schemas:core:2.0:User*.
Attribut	Attribut, für das die Zuordnung definiert werden muss. Zum Beispiel *userName*.
Unterattribut	Unterattribut (falls vorhanden), für das die Zuordnung definiert werden muss. Wenn beispielsweise ein komplexes Attribut wie *name.familyName*vorhanden ist, lautet das Attribut „ **name** “ und das **Unterattribut „familyName“**(Familienname).
Feldtyp	Datentyp des SCIM-Attributs. Dieses Feld wird automatisch mit den vom SCIM-Anbieter definierten Schemas gefüllt. Beispiel: **boolean**.
Mehrwertig	Mehrere Werte, die dem Attribut zugewiesen sind. Ein Attribut kann mehrere Werte haben, z. B. geschäftliche E-Mail-Adresse, private E-Mail-Adresse oder eine andere E-Mail-Adresse. Zum Beispiel *emails*. Dieses Feld wird mit den vom SCIM-Anbieter definierten Schemas ausgefüllt.
Filterbedingung	Einige Attribute mit mehreren Werten können zusätzliche Informationen enthalten, die mithilfe einer Filterbedingungangegeben werden können. Die Auswahlmöglichkeiten für Filterbedingungen werden mit den vom SCIM-Anbieter definierten Schemas gefüllt. Zum Beispiel hat das Attribut *phoneNumbers* mehrere Typen wie Arbeit, Mobil, Privat usw

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder	Beschreibung
Eindeutig	Option zur eindeutigen Identifizierung einer Ressource zwischen den Systemen des SCIM-Clients und des SCIM-Anbieters. Attribute mit mehreren Werten können nicht als eindeutig markiert werden. Beispielsweise kann für eine Benutzerressource das Attribut *username* eindeutig festgelegt werden.
Name der Datenbanktabelle	Verwenden Sie dieses Feld, um den Attributtabellennamen dem ServiceNow -Tabellennamen zuzuordnen. Wenn Sie die direkte Attributzuordnung wählen, müssen Sie dieses Feld definieren. Beispielsweise kann das SCIM-Attribut *username* dem Feld **Benutzer** im Feld **Name der Datenbanktabelle** zugeordnet werden.
Name des Datenbankfelds	DasFeld „Datenbankfeldname “ordnet das SCIM-Attribut dem Feldnamen ServiceNow zu, der dem SCIM-Attribut zugeordnet werden soll. Wenn Sie die direkte Attributzuordnung wählen, müssen Sie dieses Feld definieren. Beispielsweise kann das SCIM-Attribut *username* dem Feld **Anwender-ID** im Feld **Datenbankfeldname** zugeordnet werden.
Standardwert	Details zum Standardwert , der an den SCIM-Anbieter übergeben wird. Kann verwendet werden if Die direkte Attributzuordnung des Felds gibt [] null zurück, oder wenn der Standardwert verwendet werden kann, kann ein hartcodierter Wert zurückgegeben werden. Im Falle eines hartcodierten Werts müssen der Name der Datenbanktabelle und der Feldname „ **Keine**“ lauten. Beispielsweise kann der Wert des primären Unterattributs einer geschäftlichen E-Mail-Adresse als **true**hartcodiert werden.
Skript ausführen	Option zum Abrufen des Attributwerts per Skript. Diese Option ist für die Attribute mit mehreren Werten erforderlich, die keine

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder	Beschreibung
	Filterbedingung enthalten. Bei einem komplexen Attributtyp kann ein Skript den Wert auf Attribut- oder Unterattributebene bereitstellen. Beispielsweise hat das Attribut „ **Mitglieder** “ der Gruppenressource keine Filterbedingung. Daher sollte die Skriptoption auf der übergeordneten Attributebene des **Mitgliederattributs** definiert werden.
Skript	Skript, das zum Abrufen des Attributwerts verwendet wird. Der Rückgabetyp des Skripts muss eine Zeichenfolge oder ein als Zeichenfolge konvertiertes JSON-Objekt sein. Die Ausgabe des Skripts muss im richtigen Format vorliegen, wie vom Anbieter für dieses Attribut erwartet.

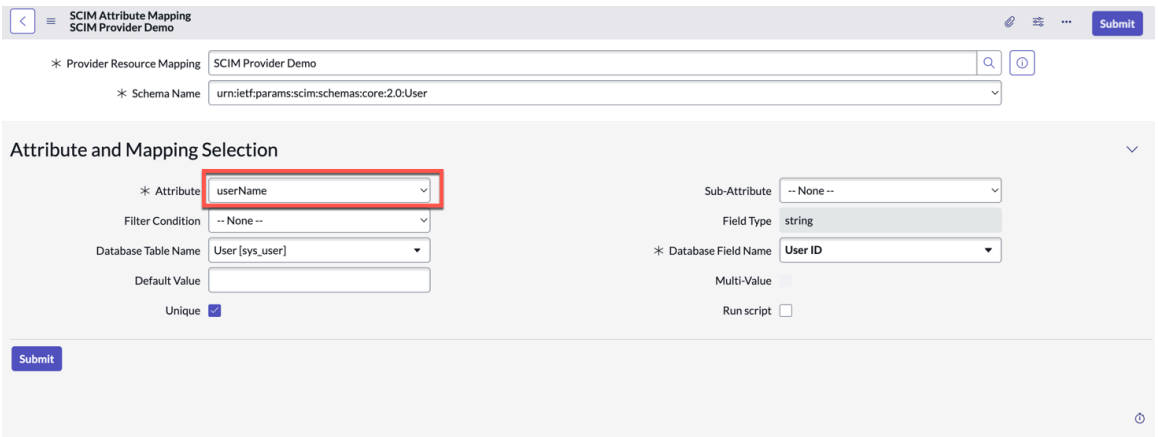
5. Klicken Sie auf **Absenden**.

Attributzuordnungsreferenzen

Mit Attributzuordnungen können Sie Attribute als einzelne Ressourcenquelle für die Felder der Tabelle ServiceNow verwenden.

Attribut

Das Attribut, für das die Zuordnung definiert werden muss. Zum Beispiel *userName*.



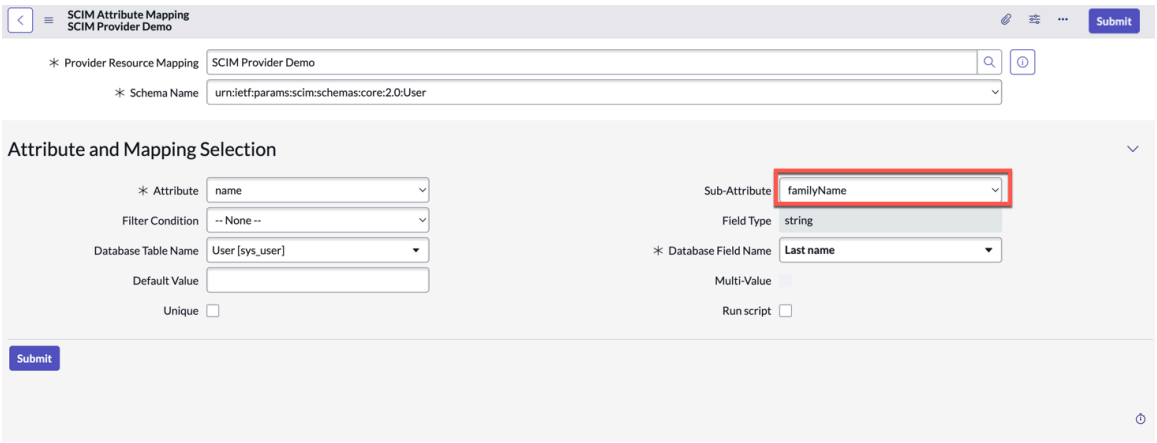
Unterattribut

Wählen Sie das Unterattribut aus, für das eine Zuordnung definiert werden muss, falls vorhanden.

Wenn beispielsweise ein komplexes Attribut wie *name.familyName*vorhanden ist, ist das Attribut *name* und das Unterattribut *familyName*.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für einfache Attribute wie den Anwendernamen wäre der **Unterattributwert „ Keine**“.

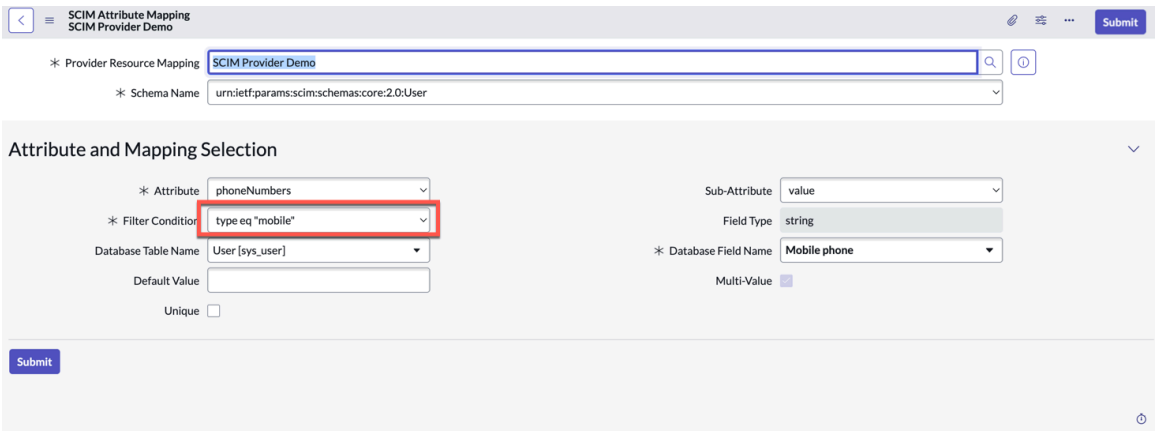


Filterbedingung

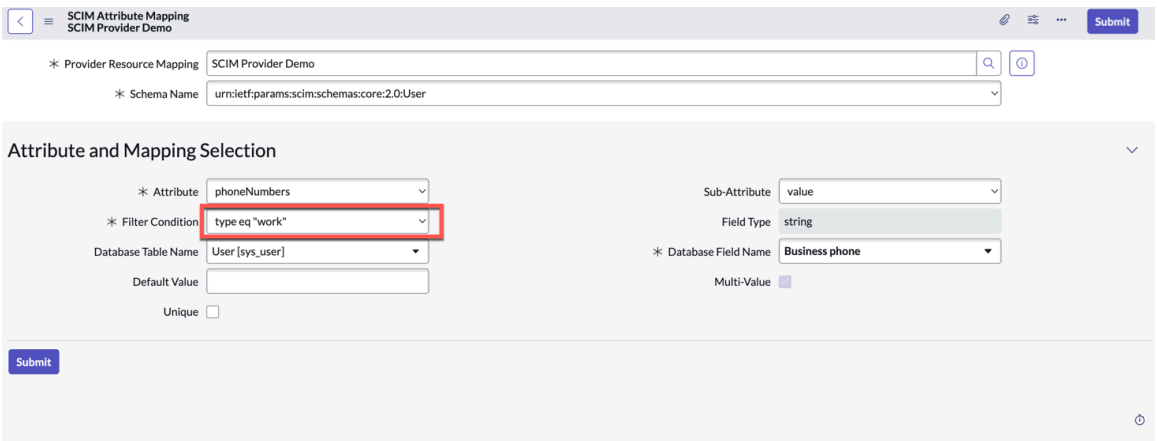
Ein Attribut mit mehreren Werten kann zusätzliche Informationen enthalten, die mithilfe einer Filterbedingung angegeben werden können. Die Auswahlmöglichkeiten für die Filterbedingung werden mit den vom SCIM-Anbieter definierten Schemas gefüllt.

Zum Beispiel hat das Attribut *phoneNumbers* mehrere Typen wie Arbeit, Mobil, Privat usw.

Sie können eine Filterbedingung aus einem Satz möglicher Werte angeben. Beispielsweise kann das Attribut *phoneNumber* die Filterbedingung als **Typ-EQ "mobile"**haben.



Das Attribut *phoneNumber* kann stattdessen eine Filterbedingung als **Typ-EQ „work“**haben.

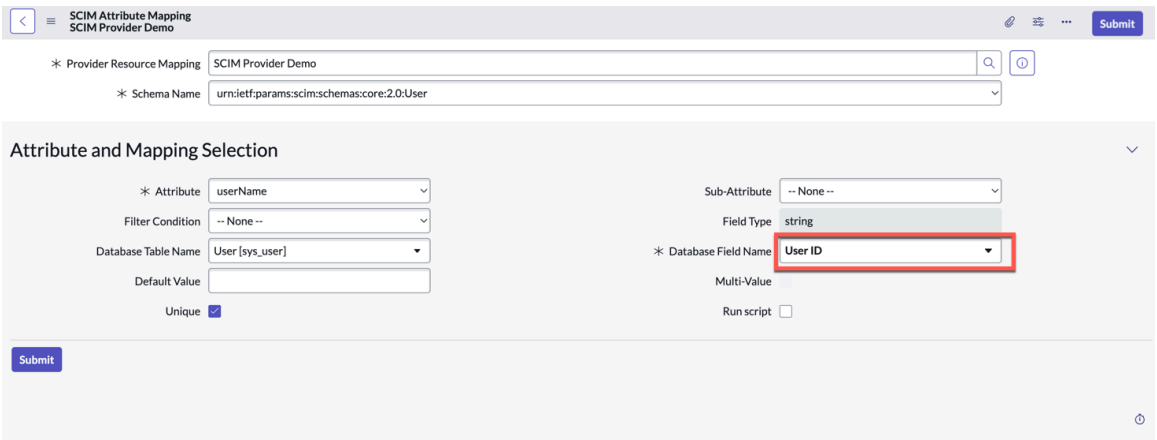


© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

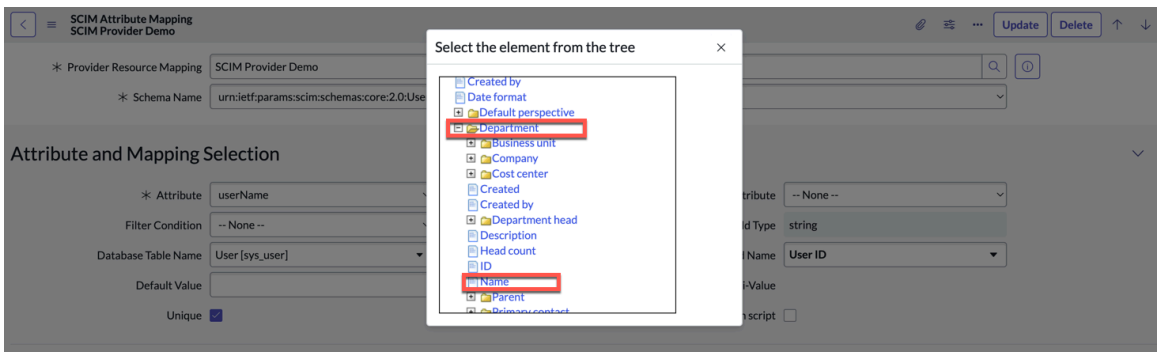
Name des Datenbankfelds

Wenn die Option für die direkte Attributzuordnung ausgewählt ist, muss dieses Attribut definiert werden. Das **Feld Datenbankfeldname** stellt den Feldnamen ServiceNow dar, der dem SCIM-Attribut zugeordnet ist.

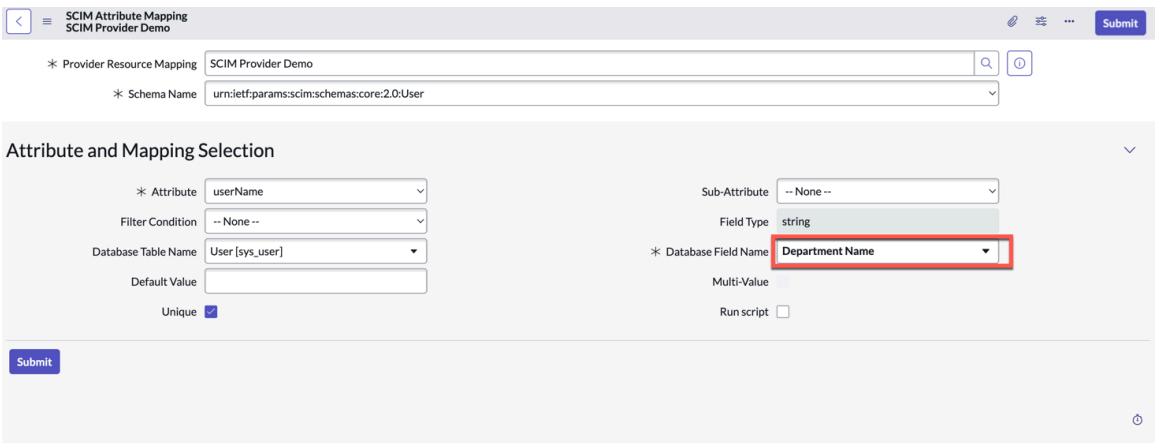
Beispielsweise kann das SCIM-Attribut *`username`* einem Benutzer als Feld **Datenbanktabellenname** und dem Feld Benutzer-ID als Feld **Datenbankfeldname** zugeordnet werden.



Sie können auch mit dem **Datenbankfeldnamen einen Dot-Walking durchführen**. Beispielsweise kann das SCIM-Attribut der **Abteilung** dem Feld „ **Abteilungsname** “ zugeordnet werden.



Hier lautet die Datenbanktabelle „ **Anwender**“ und das Feld „Datenbankname“ lautet „ **Abteilungsname**“.



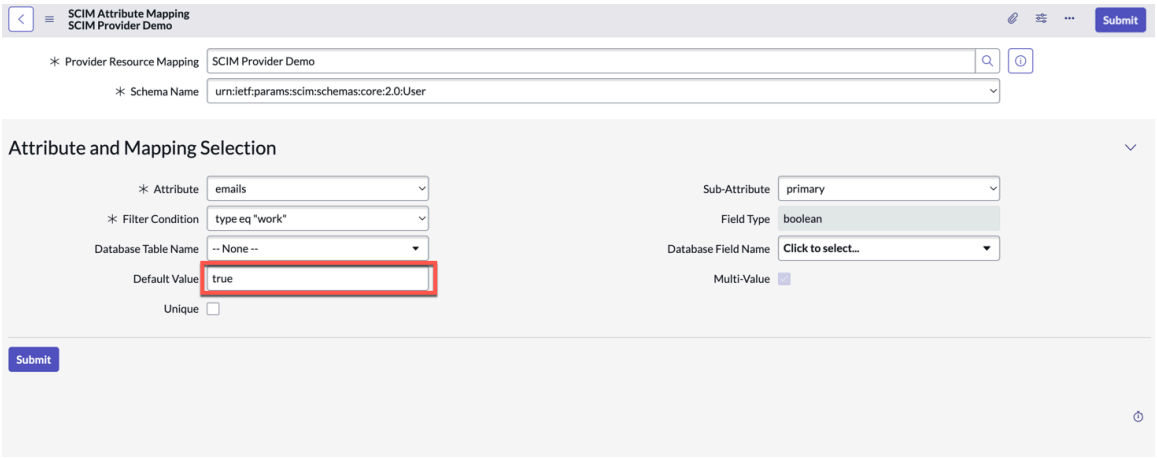
© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardwert

Der Standardwert wird an den SCIM-Provider übergeben, wenn die direkte Attributzuordnung dieses Felds NULL zurückgibt. Der Standardwert kann auch verwendet werden, um einen hartcodierten Wert zurückzugeben.

Im Falle eines hartcodierten Werts müssen der Name der Datenbanktabelle und der Feldname „ **Keine**“ lauten.

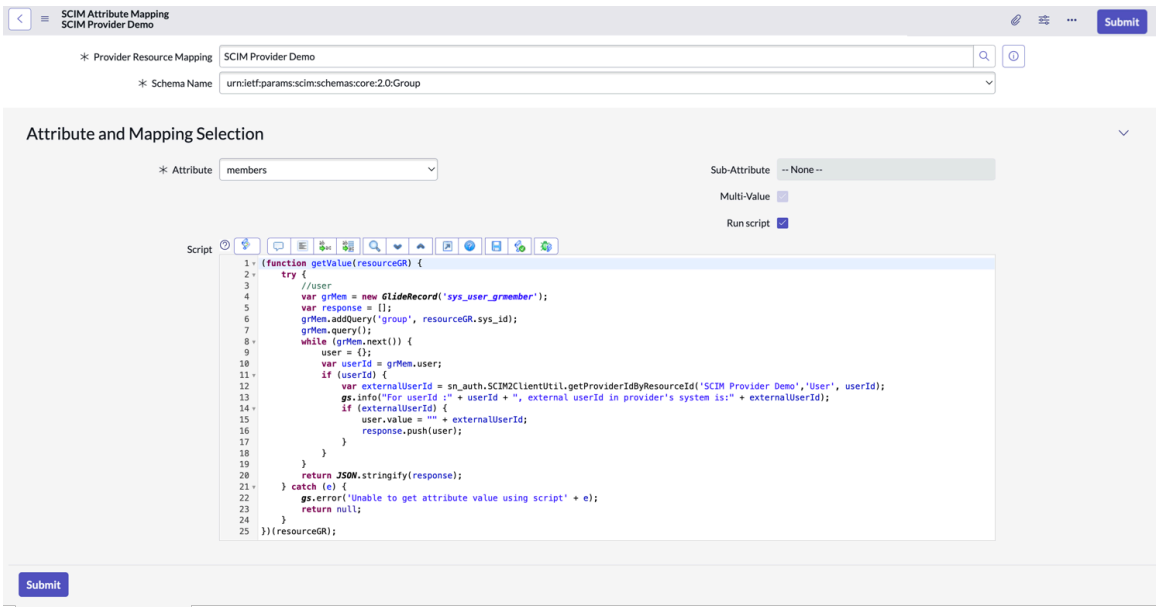
Beispielsweise kann der primäre Unterattributwert der geschäftlichen E-Mail-Adresse als hartcodiert werden **true**.



Skript

Das Skript wird zum Abrufen des Attributwerts verwendet. Der Rückgabetyp des Skripts muss immer eine Zeichenfolge oder ein als Zeichenfolge konvertiertes JSON-Objekt sein. Die Ausgabe des Skripts muss im richtigen Format vorliegen, wie vom Anbieter für dieses Attribut erwartet.

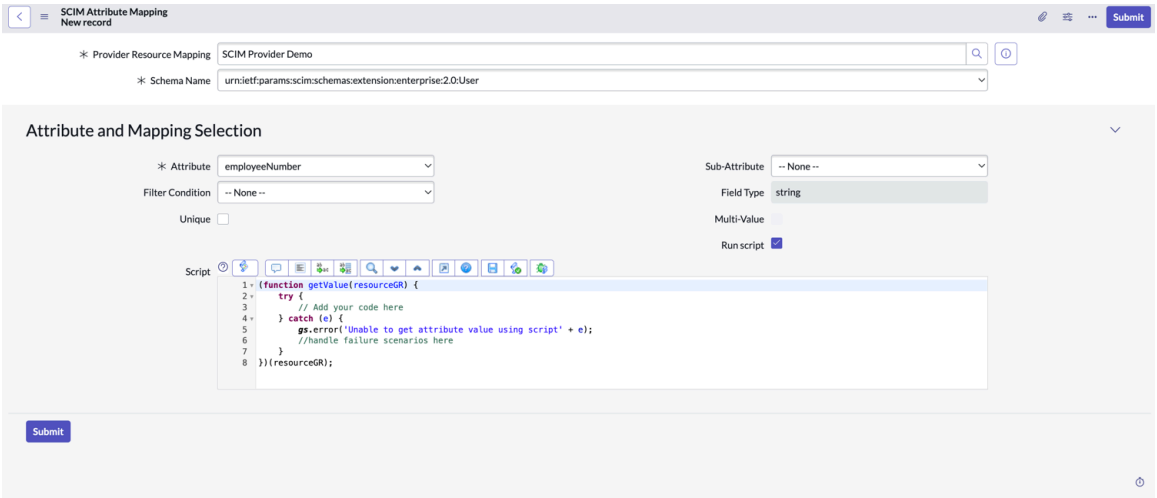
Im Folgenden finden Sie ein Beispielskript für ein Attribut mit mehreren Werten.



Die Ausgabe des Skripts muss ein JSON-Array in Zeichenfolgenform enthalten.

Im Folgenden finden Sie ein Beispielskript für ein Attribut mit einfachem Wert.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die Ausgabe des Skripts muss eine Zeichenfolge sein.

Problembehandlung für SCIM-Client

Aktionen zur Fehlerbehebung können zur Behebung allgemeiner Probleme beim Einrichten oder Ausführen des SCIM-Clients beitragen.

Problembehandlung

Problem	Aktion
Antwort enthält folgende Nachricht: `"message":"Unable to access the table core_company with id: 0c441abbc6112275000025157c651c89, Please cross check the Access control rules"`	Die Nachricht wird angezeigt, wenn die API in einem Benutzerkontext aufgerufen wird und der Benutzer keinen Zugriff auf die Tabelle hat. Sie müssen sicherstellen, dass die skriptfähige API im Systemkontext aufgerufen wird.
Antwort enthält folgende Nachricht: `{"message":"User Not Authenticated","detail":"Required to provide Auth information"}`	• Stellen Sie sicher, dass das Token durch die entsprechende REST-Nachricht generiert wird und gültig ist. • Stellen Sie sicher, dass die skriptfähige API im Systemkontext aufgerufen wird.
Antwort enthält folgende Nachricht: `Script execution failed, the reason is: Cannot cast java.lang.Integer to java.lang.String`	Wenn das Feld in der SCIM-Attributzuordnung zum Abrufen von einem Skript mit diesem Problem definiert ist, stellen Sie sicher, dass der Rückgabetyp immer eine Zeichenfolge sein muss.
Antwort enthält folgende Nachricht: `"status": "400", "scimType": "invalidValue",`	Für jedes SCIM-Attribut, das die ID erwartet, ist diese ID immer die des Anbietersystems. Stellen Sie sicher, dass die in der Nutzlast übergebene ID im Anbietersystem gültig ist.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problembehandlung (Fortsetzung)

Problem	Aktion
`"detail": "Manager id : 02826bf03710200044e0bfc8bcbe5ds8 doesn't exist"`	

Bereiche, die bei der Problembehandlung überprüft werden sollen

Im Folgenden sind einige der Bereiche aufgeführt, die bei Verwendung des SCIM-Clients auf Behebungsfehler überprüft werden können:

- Wenn beim Ausführen einer der skriptfähigen APIs ein Problem auftritt, lesen Sie den Abschnitt „SCIM-Client-Protokolle“.

Protokollfelder

Feld	Beschreibung
Anforderungs-ID	Eindeutige ID, die eine skriptfähige API namens darstellt.
SCIM-Anbieter	Anbietername, für den die API aufgerufen wird.
Ressource	Name der Ressource, für die die API aufgerufen wird.
Ressourcen-ID	Die ID, für die die API aufgerufen wird. Beim Löschen stellt die ID die Ressourcen-ID im Anbietersystem dar, und die ID im Client-System.
Aktion	API, die aufgerufen wird
Status	Status des Protokolls als Erfolg oder Fehler
Nachricht	Erfolgs- oder Fehlermeldung. Die Fehlermeldung kann vom SCIM-Anbieter oder aufgrund von Konfigurationsproblemen im SCIM-Client stammen.

- Überprüfen Sie den Anforderungstext, indem Sie ausgehende Anrufe konfigurieren und anzeigen. Weitere Informationen finden Sie unter Protokollierung ausgehender Webservices .
- Aktualisieren Sie die Protokollebenen, indem Sie den Inhaltstyp hinzufügen, das Beispiel testen und zum entsprechenden Formular „HTTP-Methode“ in der REST-Nachricht des entsprechenden Anbieters navigieren.
- Wenn der Anforderungstext gekürzt ist, erhöhen Sie den Grenzwert mithilfe der Systemeigenschaft *glide.outbound_http.content.max_limit*.

Identitäts- und Zugriffsaudit

Verwenden Sie das Identitäts- und Zugriffsaudit, um Änderungen zu verstehen, die für Anwender, Gruppen, Rollen und ACLs vorgenommen wurden.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

Untersuchen



Erfahren Sie mehr über die Funktionen und den Geschäftsnutzen von Identity and Access Audit.

Konfigurieren



Erfahren Sie, wie Sie Identitäts- und Zugriffsaudits konfigurieren.

Audit-Ergebnisse



Zeigen Sie die Ergebnisse des Identitäts- und Zugriffsaudits an.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Identitäts- und Zugriffsaudit erkunden

Verwenden Sie das Identitäts- und Zugriffsaudit, um Änderungen zu verstehen, die für Anwender, Gruppen, Rollen und ACLs vorgenommen wurden.

Das Identitäts- und Zugriffsaudit hilft, die kritischen Informationen darüber zu verstehen, wer was, wo und wann an Anwenderaccounts, Gruppen und Rollen geändert hat.

Hilft dabei, böswillige Benutzer zu erkennen und ungewöhnliche Aktivitäten in der Instanz ServiceNow® zu verfolgen und Compliance-Standards für die Nachverfolgung von Zugriffsänderungen einzuhalten.

Das Identitäts- und Zugriffsaudit (Identitätssicherheitsaudit) ist ein Plugin (`com.glide.security.audit`), das automatisch installiert wird.

Die Audit-Funktion kann durch Umschalten der Systemeigenschaft „`glide.identity.security.audit.enabled` “ aktiviert oder deaktiviert werden. Standardmäßig ist diese Eigenschaft auf `true`festgelegt.

Mit dem Identitäts- und Zugriffsaudit können Sie:

- Zeigen Sie die Changes an, die in den letzten 30 Tagen an Anwendern, Gruppen, Rollen-ACL-Attributen, Rollenmitgliedschaften, Gruppenmitgliedschaften und ACL-Rollen vorgenommen wurden.
- Verfolgen Sie die Changes in Ihrer Instanz von ServiceNow.
- Tragen Sie zur Minimierung potenzieller Sicherheitsrisiken und regulatorischer Risiken bei.
- Demonstrieren Sie die Compliance mit Auditoren für verschiedene Gruppen innerhalb der Organisation.
- Zeigen Sie, dass die Organisation nicht angreifbar für Bedrohungen ist, die mit fehlender Transparenz in Bezug auf Benutzergruppen- und Rollenänderungen zusammenhängen.

Benutzerpersonas in Identitätszugriff und Audit

Im Folgenden sind die verschiedenen Benutzerpersonas im Identitäts- und Zugriffsaudit aufgeführt:

- **Administrator**: Zeigen Sie die Audit-Datensätze und die Konfiguration an.
- **Sicherheitsadministrator**: Zeigen Sie diese Audit-Trails an. Ändern Sie die Konfiguration, um Auditing für eine bestimmte Tabelle zu aktivieren oder zu deaktivieren, oder ändern Sie die Felder, die geprüft werden.

Audit-Tabellen

Die folgenden Tabellen können mit dem Identitäts- und Zugriffsaudit geprüft werden:

- Gruppe [sys_user_group]
- Rolle [sys_user_role]
- Zugriffssteuerung [sys_security_acl]
- Benutzer [sys_user]
- Gruppenrolle [sys_group_has_role]
- Benutzerrolle [sys_user_has_role]
- Zugriffsrollen [sys_security_acl_role]

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Enthaltene Rolle [sys_user_role_contains]
- Gruppenmitglied [sys_user_grmember]

Module im Identitäts- und Zugriffsaudit

Das Identitäts- und Zugriffsaudit weist die folgenden Module in der Instanz ServiceNow auf:

Modul	Beschreibung
Audit-Ergebnisse	Zeigt die Audits an, die in der Instanz ServiceNow aufgetreten sind.
Konfigurieren Sie Tabelle und Felder	Konfigurieren Sie die Systemtabellen und -felder mit den verfügbaren Feldern aus dem Identitäts- und Zugriffsaudit.
Aufbewahrungszeitraum konfigurieren	Konfigurieren Sie den Aufbewahrungszeitraum der geprüften Daten. Der maximale Zeitraum, der festgelegt werden kann, beträgt 30 Tage.
Anwenderpfade	Zeigt Audits von Anwendern an.
Gruppenpfade	Zeigt Audits von Gruppen an.
Rollenpfade	Zeigt Audits von Rollen an.
ACL-Pfade	Zeigt Audits von ACLs an.

Ergebnisse des Identitätsaudits

Zeigt Audits an, die in der Instanz ServiceNow® aufgetreten sind.

Audit-Ergebnisse zeigen Änderungen an, die für Anwender, Gruppen, Rollen und ACLs in der Instanz ServiceNow vorgenommen wurden.

Um auf die Audit-Ergebnisse zuzugreifen, navigieren Sie **Alle** > **Systemsicherheit** > **Identitäts- und Zugriffsaudit** > **Audit-Ergebnisse**an. Die Seite „Audits Sicherheitstabelle“ wird mit den folgenden Informationen angezeigt.

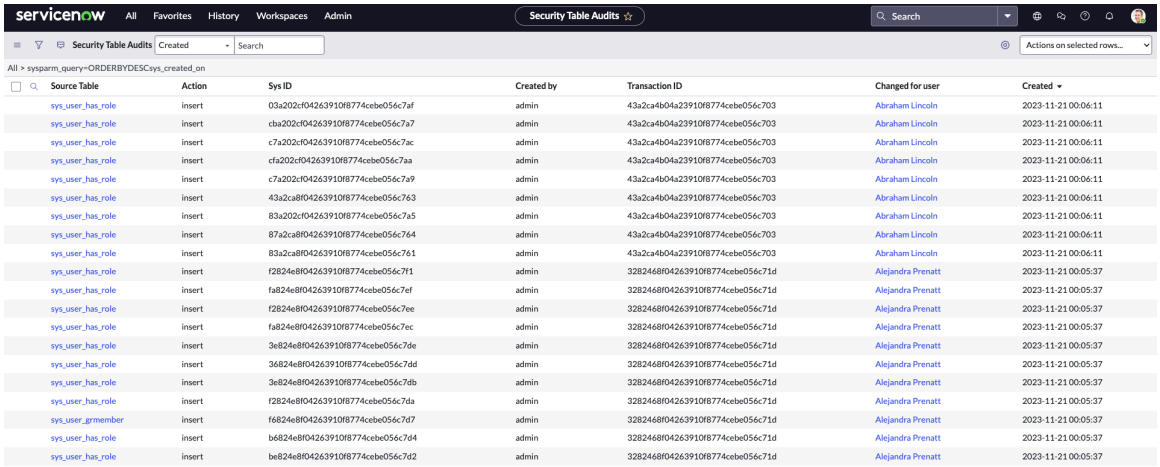
Sicherheitstabellen-Audits

Spaltenname	Beschreibung
Quelltabelle	Details der Quelltabelle, in der das Audit aufgetreten ist.
Aktion	Beschreibt die Audit-Aktion.
Sys_id	Details zur sys_id für den geprüften Datensatz.
Erstellt von	Details des Audits, das von erstellt wurde.
Transaktion-ID	Eine eindeutige ID, die jede Aktion für den jeweiligen durchgeführten Audit darstellt.
Für Anwender geändert	Name des Anwenders, wenn das Audit durchgeführt wurde.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitstabellen-Audits (Fortsetzung)

Spaltenname	Beschreibung
Erstellt	Uhrzeit und Datum der Durchführung des Audits.



Anwenderpfade

Zeigt Audits von Benutzern in der Instanz ServiceNow® an.

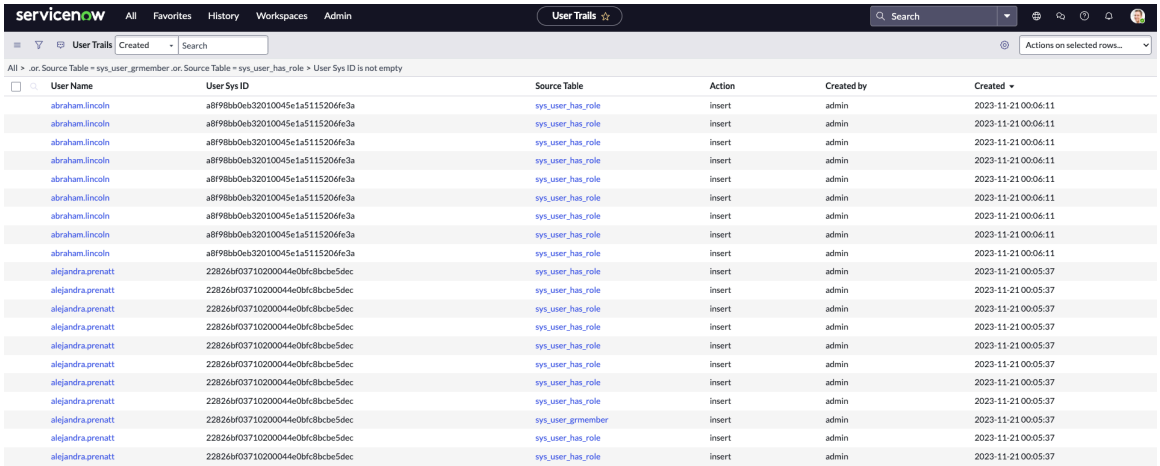
Anwenderpfade zeigen Identitätsattribut-Änderungen, Rollenmitgliedschaftsänderungen und Gruppenmitgliedschaftsänderungen für einen Anwender an.

Um auf Benutzerpfade zuzugreifen, navigieren Sie zu **Alle** > **Systemsicherheit** > **Identitäts- und Zugriffsaudit** > **Anwenderpfade**an. Die Seite „Anwenderpfade“ wird mit den folgenden Informationen angezeigt.

Anwenderpfade

Anwendernamen	Der Name des Benutzers.
Anwender-Sys-ID	Details zur sys_id des Anwenders für den geprüften Datensatz.
Quelltabelle	Details zur Quelltabelle, in der das Audit durchgeführt wurde.
Aktion	Beschreibt die Audit-Aktion.
Erstellt von	Der Anwender, der die Änderung vorgenommen hat.
Erstellt	Uhrzeit und Datum der Durchführung des Audits.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Gruppenpfade

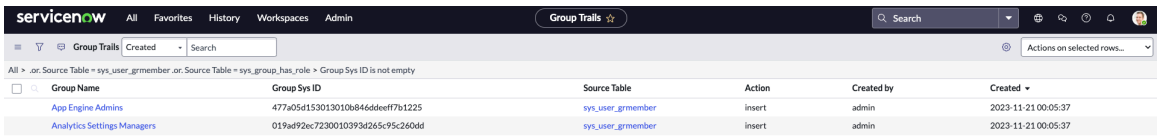
Zeigt Audits von Gruppen in der Instanz ServiceNow® an.

Gruppenpfade zeigen Attributänderungen, Mitgliedschaftsänderungen und Rollenänderungen für eine Gruppe an.

Um auf Gruppenpfade zuzugreifen, navigieren Sie zu **Alle** > **Systemsicherheit** > **Identitäts- und Zugriffsaudit** > **Gruppenpfade**an. Die Seite „Gruppenpfade“ wird mit den folgenden Informationen angezeigt.

Gruppenpfade

Gruppenname	Name der Gruppe.
Gruppen-Sys-ID	Details zur Gruppen-sys_id für den geprüften Datensatz.
Quelltabelle	Details zur Quelltabelle, in der das Audit durchgeführt wurde.
Aktion	Beschreibt die Audit-Aktion.
Erstellt von	Der Anwender, der die Änderung vorgenommen hat.
Erstellt	Uhrzeit und Datum der Durchführung des Audits.



© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollenpfade

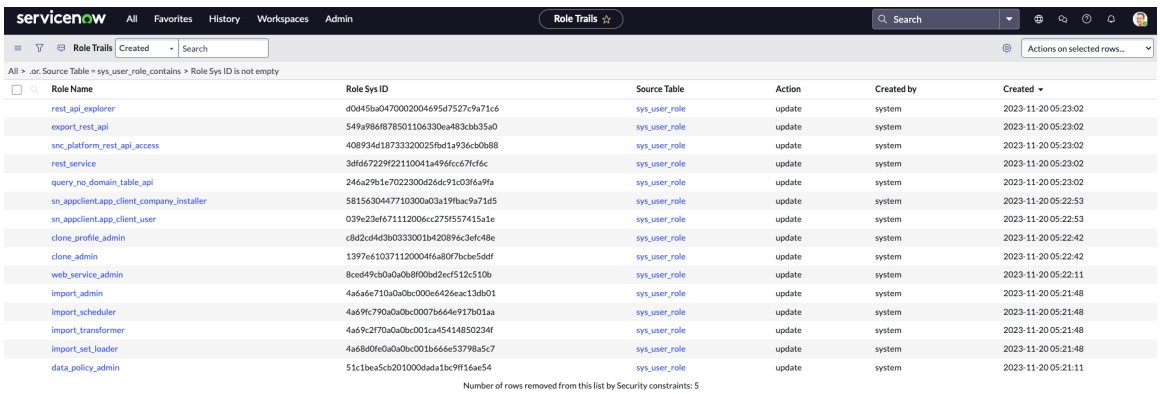
Zeigt Audits von Rollen in der Instanz ServiceNow® an.

Rollenpfade zeigen Attributänderungen und Änderungen der über- und untergeordneten Beziehung für eine Rolle an.

Um auf Rollenpfade zuzugreifen, navigieren Sie zu **Alle** > **Systemsicherheit** > **Identitäts- und Zugriffsaudit** > **Rollenpfade**an. Die Seite „Rollenpfade“ wird mit den folgenden Informationen angezeigt.

Rollenpfade

Rollenname	Name der Rolle.
Rollen-Sys-ID	Details zur sys_id der Rolle für den geprüften Datensatz.
Quelltabelle	Details zur Quelltabelle, in der das Audit durchgeführt wurde.
Aktion	Beschreibt die Audit-Aktion.
Erstellt von	Der Anwender, der die Änderung vorgenommen hat.
Erstellt	Uhrzeit und Datum der Durchführung des Audits.



ACL-Pfade

Zeigt Audits von ACLs in der Instanz ServiceNow® an.

ACL-Pfade zeigen Attributänderungen und erforderliche Rollenbeziehungsänderungen für eine ACL an.

Um auf die ACL-Pfade zuzugreifen, navigieren Sie zu **Alle** > **Systemsicherheit** > **Identitäts- und Zugriffsaudit** > **ACL-Pfade**an. Die Seite „ACL-Pfade“ wird mit den folgenden Informationen angezeigt.

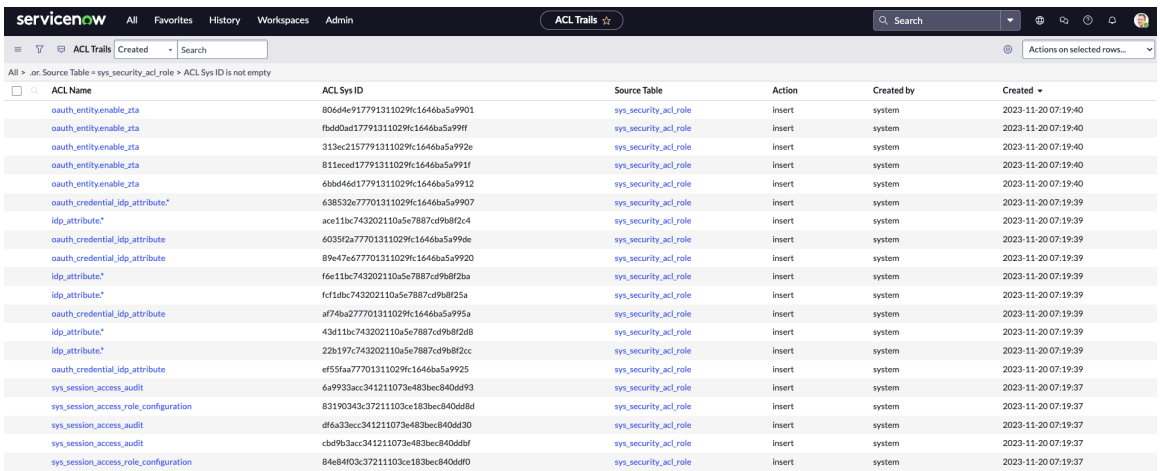
ACL-Pfade

ACL-Name	Name der ACL.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ACL-Pfade (Fortsetzung)

ACL-Sys-ID	Details zur sys_id der ACL für den geprüften Datensatz.
Quelltabelle	Details zur Quelltabelle, in der das Audit durchgeführt wurde.
Aktion	Beschreibt die Audit-Aktion.
Erstellt von	Der Anwender, der die Änderung vorgenommen hat.
Erstellt	Uhrzeit und Datum der Durchführung des Audits.



Prüfbare Felder für Sicherheit

Zeigt Details auf Tabellen- und Feldebene an, die in der Instanz ServiceNow® geprüft werden.

Prüfbare Felder für Sicherheit zeigt die Details von Tabellen und Feldern an, die in der Instanz ServiceNow geprüft werden.

Um auf die Seite „Prüfbare Felder für Sicherheit“ zuzugreifen, navigieren Sie zu **Alle** > **Systemsicherheit** > **Identitäts- und Zugriffsaudit** > **Tabellen und Felder konfigurieren**an. Die Seite „Prüfbare Felder für Sicherheit“ wird mit den folgenden Informationen angezeigt.

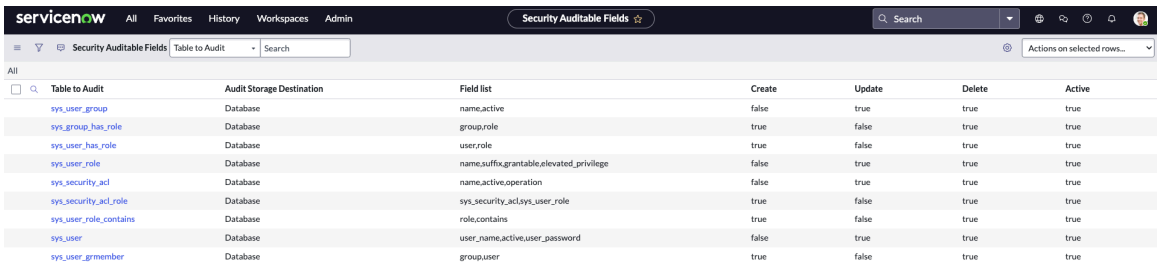
Prüfbare Felder für Sicherheit

Spaltenname	Beschreibung
Zu prüfende Tabelle	Details der geprüften Tabelle.
Audit-Speicherziel	Details des Ziels, in dem die Audit-Details gespeichert werden.
Feldliste	Auditing wird für Felder durchgeführt, die in der Liste angegeben sind.
Erstellen	Überprüft die Changes im Zusammenhang mit dem Vorgang „Erstellen“.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfbare Felder für Sicherheit (Fortsetzung)

Spaltenname	Beschreibung
Aktualisierung	Überprüft die Changes im Zusammenhang mit dem Aktualisierungsvorgang.
Löschen	Überprüft die Changes im Zusammenhang mit dem Löschvorgang.
Aktiv	Führen Sie nur eine Audit durch, wenn die Konfiguration für die Tabelle aktiv ist.



Die folgenden Tabellen können mit dem Identitäts- und Zugriffsaudit geprüft werden:

- Gruppe [sys_user_group]
- Rolle [sys_user_role]
- Zugriffssteuerung [sys_security_acl]
- Benutzer [sys_user]
- Gruppenrolle [sys_group_has_role]
- Benutzerrolle [sys_user_has_role]
- Zugriffsrollen [sys_security_acl_role]
- Enthaltene Rolle [sys_user_role_contains]
- Gruppenmitglied [sys_user_grmember]

Tabellen und Felder konfigurieren

Identitäts- und Zugriffsaudit, um die für Anwender, Gruppen, Rollen und ACLs vorgenommenen Änderungen zu verstehen.

Vorbereitungen

Erforderliche Rolle: security_admin

Sie müssen Ihre Rolle auf Sicherheitsadministrator erhöhen, um Tabellen und Felder für das Identitäts- und Zugriffsaudit zu konfigurieren.

Die folgenden Tabellen können für Audits konfiguriert werden:

- Gruppe [sys_user_group]
- Rolle [sys_user_role]
- Zugriffssteuerung [sys_security_acl]
- Benutzer [sys_user]

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

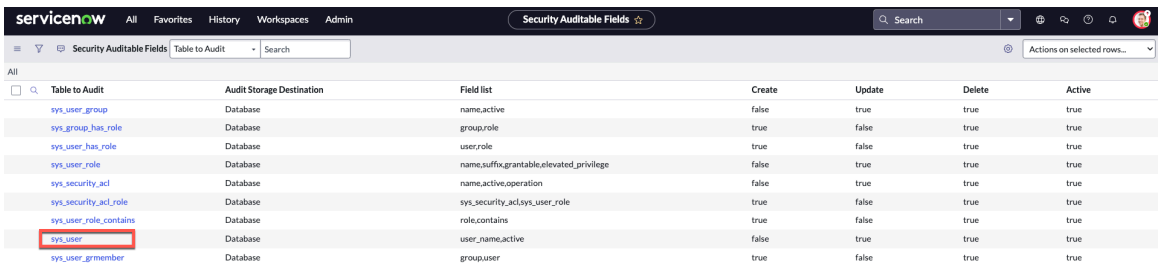
- Gruppenrolle [sys_group_has_role]
- Benutzerrolle [sys_user_has_role]
- Zugriffsrollen [sys_security_acl_role]
- Enthaltene Rolle [sys_user_role_contains]
- Gruppenmitglied [sys_user_grmember]

Hinweis: Informationen dazu, welche Felder für die Tabellen konfiguriert werden können, finden Sie unter Für Identitätszugriff und Audit unterstützte und nicht unterstützte Felder.

Prozedur

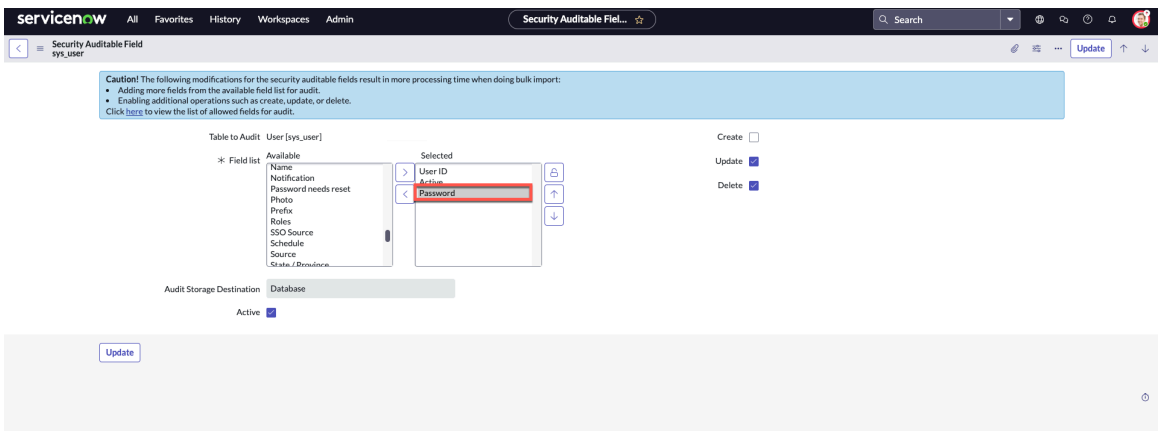
1. Navigieren zu **Alle** > **Systemsicherheit** > **Identitäts- und Zugriffsaudit** > **Tabellen und Felder konfigurieren**an.
2. Wählen Sie die Tabelle aus, aus der Sie ein Feld prüfen möchten.

   Beispiel: **sys_user**.



3. Fügen Sie das zu überwachende Feld hinzu.

   Beispiel: **Passwort**.



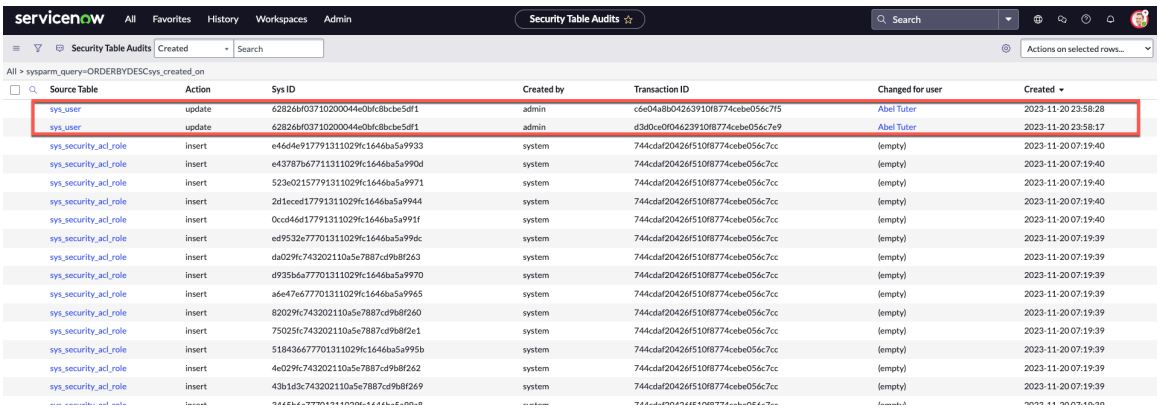
Hinweis: Die folgenden Änderungen für die auditierbaren Sicherheitsfelder führen zu mehr Verarbeitungszeit beim Massenimport:

- Hinzufügen weiterer Felder aus der Liste der verfügbaren Felder für Audit.
- Aktivieren zusätzlicher Vorgänge wie Erstellen, Aktualisieren oder Löschen.

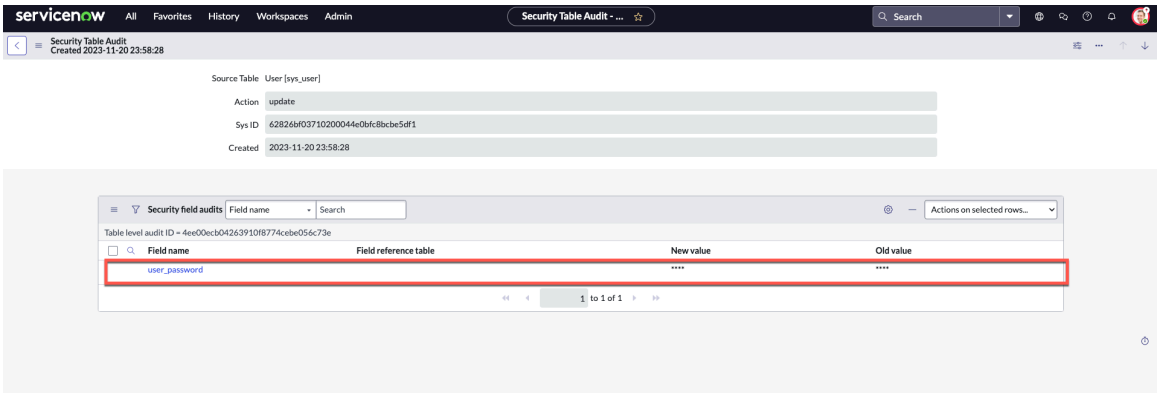
4. Aktualisieren Sie den Datensatz.

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Alle Änderungen am Passwortfeld fügen einen neuen Datensatz zu den Sicherheitstabellen-Audits hinzu. In diesem Beispiel zeigt der Audit ein geändertes Passwortfeld für den Benutzer **Abel Tuter**.



Wenn Sie den erstellten Datensatz auswählen, werden die Details der Änderungen angezeigt.



Aufbewahrungszeitraum konfigurieren

Konfigurieren Sie den Aufbewahrungszeitraum für das Identitäts- und Zugriffsaudit.

Vorbereitungen

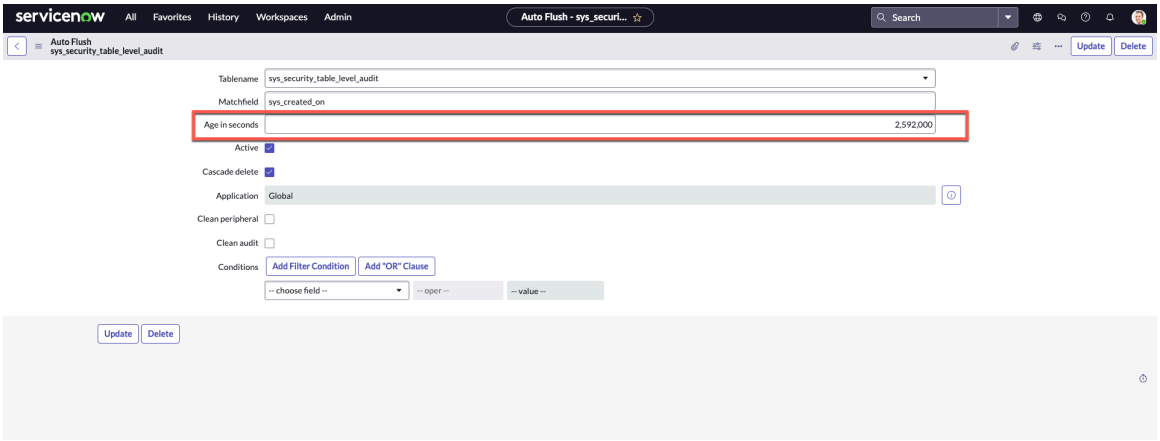
Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Identitäts- und Zugriffsaudit** > **Aufbewahrungszeitraum konfigurieren**an.
2. Im Formular können Sie das Alter in Sekunden ändern.

> **Hinweis:** Die maximale Anzahl von Tagen für das Identitäts- und Zugriffsaudit beträgt 30 Tage (2.592.000 Sekunden).

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Speichern oder aktualisieren Sie den Datensatz.

Für Identitätszugriff und Audit unterstützte und nicht unterstützte Felder

Liste der Felder, die für Audits unterstützt werden und für die es nicht gilt.

Die Validierung der Audit-Felder verhindert, dass einige Felder in „field_list“ in der Tabelle „Sicherheitsfeld-Audit-Konfiguration“ (sys_sec_field_audit_config) ausgewählt werden.

Feld, das für Audit unterstützt oder nicht unterstützt wird

Tabelle	Felder unterstützt oder nicht unterstützt
Alle Tabellen	Felder, die nicht unterstützt werden: • Erstellt am (sys_created_on) • Erstellt von (sys_created_by) • Aktualisiert von (sys_updated_by) • Aktualisiert am (sys_updated_on)
Anwender hat Rolle (sys_user_has_role)	Unterstützte Felder: • Anwender • Rolle • Geerbt • Anzahl
Benutzer (sys_user)	Felder, die nicht unterstützt werden: • Letzte Anmeldung (last_login) • Zeitpunkt der letzten Anmeldung (last_login_time) • Gerät der letzten Anmeldung (last_login_device) • Multifaktor-Authentifizierung aktivieren (enable_multifactor_authn)

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld, das für Audit unterstützt oder nicht unterstützt wird (Fortsetzung)

Tabelle	Felder unterstützt oder nicht unterstützt
	• Standardperspektive (default_perparente) • Kalenderintegration (calendar_integration) • Föderierte ID (federated_id) • Passwort muss zurückgesetzt werden (password_needs_reset) • Fehlgeschlagene Versuche (failed_attempts) • Letztes Passwort (last_password) • LDAP-Server (ldap_server) • Ausgesperrt (locked_out) • Benachrichtigung (Benachrichtigung) • Rollen (Rollen) • Domäne (sys_domain) • Domänenpfad (sys_domain_path) • Zeitformat (time_format) • Anwender-ID mit Hash (hasht_user_id) • Klassenname (sys_class_name) • Mod.-Anzahl (sys_mod_count)

© 2024 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.