



Yokohama Operational Technology Management

Zuletzt aktualisiert: 17.12.2025

Automatische Übersetzung

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. Eine 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

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

Inhaltsverzeichnis

Operational Technology.....	5
Operational Technology-Management-Lizenzierung und -Abonnements.....	7
Abonnements für OTM.....	8
Installieren Sie ITOM SU-Lizenzierung.....	8
Abonnementstatistiken für OTM anzeigen.....	10
Überprüfen Sie die Ressourcennutzung OTM anhand der zugewiesenen Abbonementseinheiten.....	10
Für OTM-Abonnements verwendete CI-Anzahl prüfen.....	11
OTM-Abbonementseinheiten verbrauchende CIs anzeigen.....	13
OTM SU-Lizenzierungsreferenzen.....	14
Now Assist für Operational Technology Service Management (OTSM).....	18
[store-future: BEGIN review]	
Now Assist für Operational Technology Service Management erkunden (OTSM).....	20
[store-future: BEGIN review]	
[End]	
Verwenden von Anwendungsfällen von KI-Agenten für Now Assist für Operational Technology Service Management (OTSM).....	21
[store-future: BEGIN review]	
[End]	
Now Assist für Operational Technology Service Management (OTSM) konfigurieren.....	24
[store-future: BEGIN review]	
[End]	
Now Assist für Operational Technology Service Management (OTSM) verwenden.....	28
[store-future: BEGIN review]	
[End]	
[End]	
Empfohlene Aktionen für Operational Technology Service Management (OTSM).....	30
[store-future: BEGIN review]	
Empfohlene Aktionen für Operational Technology Service Management erkunden.....	31
[store-future: BEGIN review]	
[End]	
Empfohlene Aktionen für Operational Technology Service Management in der konfigurieren Industrial Workspace.....	33
[store-future: BEGIN review]	
[End]	
Empfohlene Aktionen für Operational Technology Service Management verwenden.....	34
[store-future: BEGIN review]	
[End]	
[End]	
Operational Technology Manager.....	35
Operational Technology Manager erkunden.....	37
Operational Technology Manager konfigurieren.....	40
Operational Technology Manager Integrationen.....	57
Operational Technology Manager verwenden.....	145
Operational Technology Manager-Referenz.....	215
Prozessmanager Industrie.....	219

Prozessmanager Industrie erkunden.....	220
Prozessmanager Industrie konfigurieren.....	222
Prozessmanager Industrie mit Operational Technology Managerverwenden.....	245
Prozessmanager Industrie-Referenz.....	269
Operational Technology Vulnerability Response.....	275
Operational Technology Vulnerability Response erkunden.....	276
Operational Technology Vulnerability Solution Management.....	277
Operational Technology Vulnerability Response konfigurieren.....	278
Operational Technology Vulnerability Response Integrationen.....	291
Operational Technology Vulnerability Response verwenden.....	323
Operational Technology Vulnerability Response-Referenz.....	331
Incident-Management für operative Technologie.....	335
Incident-Management für operative Technologie erkunden.....	336
Incident-Management für operative Technologie konfigurieren.....	340
Incident-Management für operative Technologie verwenden.....	351
Incident-Management für operative Technologie-Referenz.....	363
Change-Management für operative Technologie.....	366
Change-Management für operative Technologie erkunden.....	367
Change-Management für operative Technologie konfigurieren.....	370
Change-Management für operative Technologie verwenden.....	381
Change-Management für operative Technologie-Referenz.....	395
Knowledge Management für operative Technologie.....	397
Knowledge Management für operative Technologie erkunden.....	398
Knowledge Management für operative Technologie konfigurieren.....	399
Knowledge Management für operative Technologie verwenden.....	408
Knowledge Management für operative Technologie-Referenz.....	416
Anforderungsmanagement für operative Technologie.....	420
Anforderungsmanagement für operative Technologie erkunden.....	421
Anforderungsmanagement für operative Technologie konfigurieren.....	422
Anforderungsmanagement für operative Technologie verwenden.....	426
Anforderungsmanagement für operative Technologie-Referenz.....	428
Industriell Arbeitsbereich.....	433
Industrial Workspace erkunden.....	434
Konfigurieren von Industriell Arbeitsbereich.....	453
Verwenden von Industriell Arbeitsbereich.....	473
Domänentrennung und Operational Technology.....	490

Operational Technology

Verwenden Sie ServiceNow® für Operational Technology, um Ihrem Unternehmen zu helfen, den Betrieb zu optimieren, die Produktivität zu steigern und die Betriebszeit von Operational Technology in der Produktion durch digitale Workflows zu maximieren.

Operational Technology – Übersicht

Sehen Sie sich die Übersicht über Operational Technology und die Lösung ServiceNow Operational Technology-Management an.

[https://player.vimeo.com/video/957122379?](https://player.vimeo.com/video/957122379?h=d9c04a0637&badge=0&autoplay=0&player_id=0&app_id=58479)

[h=d9c04a0637&badge=0&autoplay=0&player_id=0&app_id=58479](https://player.vimeo.com/video/957122379?h=d9c04a0637&badge=0&autoplay=0&player_id=0&app_id=58479)

Vorteile in Operational Technology, Core Operations und die Bevollmächtigung von Produktionsarbeitern



Operational Technology

Contextualize and safeguard your Operational Technology systems, connect to digital workflows, and respond quickly to threats.



Core Operations

Streamline and digitize standard operating procedures (SOPs) and enable shared knowledge and collaboration across the enterprise.



Factory Workers

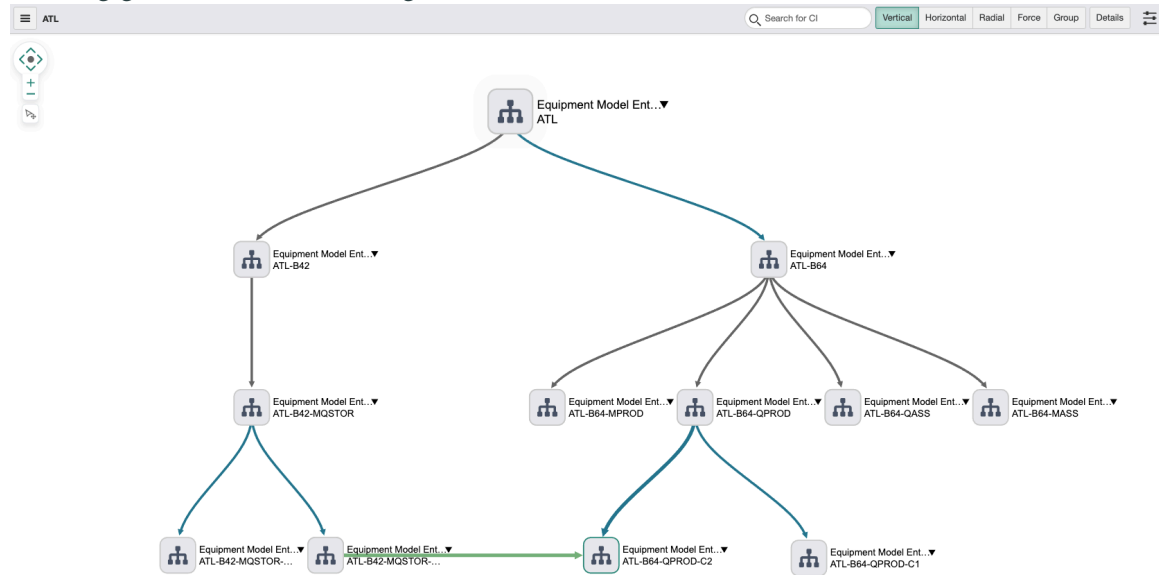
Empower the workforce with digital tools and knowledge to adapt, collaborate, and excel in fast-changing conditions.

Maximieren Sie Ihre Betriebszeit, und erstellen Sie eine organisationale Resilienz mit ServiceNow Operational Technology Management

Vor der Einführung von branchenüblicher Technologie waren Hersteller bei der Wartung ihrer Umgebungen auf manuelle Prozesse und Legacy-Wissen angewiesen. Sie fanden es herausfordernd, sich einen vollständigen Überblick über ihre Umgebung zu verschaffen und alles zu sichern, zu überwachen und zu verwalten. Mit der Lösung ServiceNow Operational Technology Management kann Ihre Industrieorganisation jetzt eine vollständige und kontextbezogene Ansicht Ihrer operativen Technologiesysteme erhalten. Mit dieser Ansicht können Sie dafür sorgen, dass Ihre Systeme sicher, betriebsbereit und mit Produktionsprozessen und digitalen Workflows verbunden sind. Sie können Ihre Organisation auch in die Lage versetzen, Ereignisse und Bedrohungen zu bewerten, zu priorisieren und darauf zu reagieren.

Automatische Übersetzung

Abhängigkeitsansicht für Anlagenmodelle



Durch die Verwendung einer digitalen Karte erhält Ihr Unternehmen einen besseren Überblick über die Prozesse, Systeme und Beziehungen von Industrial Operations. Mit dieser Zuordnung können Sie Ihre potenziellen Auswirkungen auf die Produktion einfacher und schneller verwalten und bewerten.

Hinweis:

Die Lösung Operational Technology-Management wird unter Now Mobile[®] nicht unterstützt.

Transparenz verbessern



Erhalten Sie eine vollständige und kontextbezogene Ansicht Ihrer Operational Technology-Systeme, damit Sie Ihre Systeme sicher und betriebsbereit halten können.

Digitale Workflows



Verbinden Sie Ihre Operational Technology-Systeme mit Produktionsprozessen und digitalen Workflows.

Schwachstellenmanagement



Sehen Sie alles an einem Ort, um Ereignisse und Bedrohungen zu bewerten, zu priorisieren und darauf zu reagieren.

Automatische Übersetzung

statten Sie Ihr Personal aus

Erstellen Sie Low-Code- und No-Code-Anwendungen, damit Ihre Mitarbeiter eine kollaborative Überwachung, erweiterte Fehlerbehebung, Problemlösung und eingehende Situationsanalysen durchführen können.

Einzelheiten finden Sie in der [Lösungsbeschreibung](#) .

Erste Schritte

- Über [DemoNow](#) demonstrierte Funktionen für Überwachungsuhren.
- Informationen zum Anfordern und Einrichten Operational Technology von finden Sie unter
 - [Operational Technology Manager konfigurieren](#)
 - [Prozessmanager Industrie konfigurieren](#)
 - [Operational Technology Vulnerability Response konfigurieren](#)
 - [Incident-Management für operative Technologie konfigurieren](#)
 - [Change-Management für operative Technologie konfigurieren](#)
 - [Knowledge Management für operative Technologie konfigurieren](#)
- Weitere Informationen dazu, wie Operational Technology Tabellen Gemeinsames Servicedatenmodell vom Typ verwaltet und verwendet, finden Sie unter [Operative Technologien und CSDM-Tabellen](#).
- Weitere Informationen zu den neuesten Releases für Operational Technology finden Sie unter [ServiceNow Store – Versionshinweise zu Operational Technology](#) .

Anwendungen

- [Operational Technology Manager](#)
- [Prozessmanager Industrie](#)
- [Operational Technology Vulnerability Response](#)
- [Incident-Management für operative Technologie](#)
- [Change-Management für operative Technologie](#)
- [Knowledge Management für operative Technologie](#)
- [Anforderungsmanagement für operative Technologie](#)
- [Industrial Workspace für operative Technologie](#)
- [Servicemanagement: IT Service Management](#)
- [Sicherheit: Vulnerability Response](#)
- [Transparenz: IT Operations Management](#)

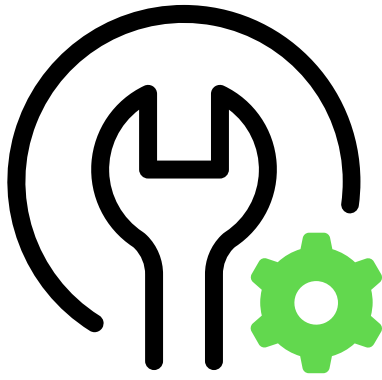
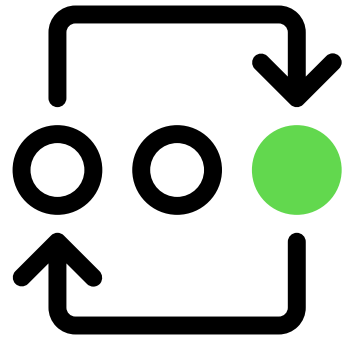
Operational Technology-Management-Lizenzierung und -Abonnements

Die Lizenzierung ServiceNow® OTM für ist ein wichtiger Aspekt von Operational Technology-Management, da sie die Nutzung von OTM -Abonnements basierend auf Abbonementseinheiten berechnet und darstellt. Diese können Faktoren wie die Anzahl der überwachten Geräte oder die Dauer des Abonnements umfassen.

Operational Technology-Management Übersicht über Lizenzierung und Abonnements

Dies ermöglicht es Unternehmen, die Compliance sicherzustellen, Ressourcen effektiv zuzuweisen und fundierte Entscheidungen über die Skalierung ihrer OTM -Fähigkeiten zu treffen, um ihre operativen Technologiesysteme zu schützen und sich an ändernde Sicherheits- und Betriebsanforderungen anzupassen. Verwenden Sie das Lizenzierungsmodul OTM, um auf abonnementbezogene Details für die OTM -Produkte zuzugreifen: ServiceNow OT Foundation, ServiceNow OT Visibility und ServiceNow OT Vulnerability and Response.

Erste Schritte

Erkunden Sie die OTM -Lizenz  Erfahren Sie mehr über abonnementbezogene Details	ITOM SU-Lizenzierung für OTM installieren  Aktualisiert die neueste Version des Plugins	Lizenzierungsreferenzen  Erfahren Sie mehr über installierte Komponenten wie geplante Aufgaben und Tabellen

Support kontaktieren

[Kontakt Kundenservice und Support](#)

Abonnements für OTM

Die Plattform ServiceNow nutzt OTM für die Lizenzverwaltung im verarbeitenden Gewerbe. OTM umfasst Lizenzen in IT Operations Managementsowie Lizenzen, die ausschließlich für die Domäne OTM gelten.

Überwachen Sie OTM -Lizenzen ähnlich wie IT Operations Management -Lizenzen. In der Instanz ServiceNow können Sie die Lizenztypen OTM in den **Metadaten der ITOM-Lizenzierungskategorie** () identifizieren.**OTM-Lizenz > Lizenzen nach CI-Typen**), auf der die Spalte **SKU-Typ** den Wert **otm**anzeigt. Standardmäßig ist der Lizenzfilter auf **SKU-Typ** enthält **otm**festgelegt.

Installieren Sie ITOM SU-Lizenzierung

Installieren oder aktualisieren Sie ServiceNow® ITOM SU-Lizenzierung [sn_itom_licensing], um sicherzustellen, dass Sie die neuesten Lizenzierungsfunktionen verwenden. Die Anwendung

enthält Demodaten und installiert die zugehörigen ServiceNow® Store-Anwendungen und Plugins, falls sie nicht bereits installiert sind.

Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter [Rufen Sie eine Berechtigung für ab ServiceNow Produkt oder Anwendung](#) .
- Überprüfen Sie den Eintrag der Anwendung [ITOM SU Licensing](#) im ServiceNow Store auf Informationen zu Abhängigkeiten, Lizenzierungs- oder Abonnementanforderungen und Release-Kompatibilität.

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Vor Q1 2022 wurde der ursprüngliche Lizenzierungsmechanismus als Teil der Familienreleases bereitgestellt. Seither wird der Lizenzierungsmechanismus mit ServiceNow® ITOM SU-Lizenzierung aus dem ServiceNow Store bereitgestellt. Das System installiert automatisch ServiceNow® ITOM SU-Lizenzierung. Sie erhalten Benachrichtigungen, wenn Updates für diese Anwendung unter ServiceNow Store verfügbar sind.

Die folgenden Elemente werden mit ITOM SU-Lizenzierung installiert:

- Regelmäßige Aufgaben
- Tabellen

Weitere Informationen finden Sie unter [Mit ITOM SU-Lizenzierung für OTMinstallierte Komponenten](#).

Prozedur

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

2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach der Anwendung (sn_itom_licensing).

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

In der Liste neben der Schaltfläche **Aktualisieren** werden die für Sie verfügbaren Versionen angezeigt.

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

Demodaten sind Beispieldatensätze, die Anwendungsfunktionen für die gängigen Anwendungsfälle veranschaulichen. Laden Sie die Demodaten, wenn Sie die Anwendung zum ersten Mal auf einer Entwicklungs- oder Testinstanz installieren.

i Wichtig:

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

6. Wählen Sie Aktualisieren.**Abonnementstatistiken für OTM anzeigen**

Zeigen Sie die Anzahl der OTM Anwendungsabonnements an, die von Ihrer Organisation erworben und genutzt wurden. Sie bieten wertvolle Einblicke für das Ressourcenmanagement und die Optimierung der operativen Technologie.

Vorbereitungen

- Stellen Sie sicher, dass Ihre Organisation über aktive Abonnements OTM verfügt.
- Stellen Sie sicher, dass Sie die neueste verfügbare Version der ITOM SU-Lizenzierung von installiert haben [ServiceNow Store](#) .

Erforderliche Rolle: sn_itom_license.reader

Warum und wann dieser Vorgang ausgeführt wird

Bewerten Sie die Zuteilung von Configuration Items (CIs) und ihre Zuteilungsebenen, um die Abonnementnutzung OTM Ihrer Organisation zu bewerten und sich auf zukünftige Abonnementanforderungen vorzubereiten.

Prozedur

1. Um Abonnementinformationen für OTM Abonnements anzuzeigen, die einzeln erworben wurden, navigieren Sie zu **OTM-Lizenz > Lizenzzusammenfassung**.
2. Überprüfen Sie die im Formular angezeigten Details, wie in [Abonnementformular für die OTM-Produkte](#) beschrieben.

Überprüfen Sie die Ressourcennutzung OTM anhand der zugewiesenen Abommementeinheiten

Überprüfen und analysieren Sie Ressourcenstatistiken, die -Produkte OTM verwalten können, und vergleichen Sie diese Informationen mit der durchschnittlichen Zuteilung von Abommementeinheiten.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Erkunden Sie detaillierte Lizenzierungsdatentrends von OTM mithilfe von [OTM Lizenzierungs-Dashboard](#). Beobachten Sie tägliche CI-Anzahl, oder zeigen Sie die Durchschnittswerte der letzten 90 täglichen Anzahl an. Diese Funktion bietet domänenspezifische Informationen und spezifische CI-Listen für jede tägliche Anzahl, sodass Sie die Ressourcennutzung im Zeitverlauf effektiv überwachen und analysieren können.

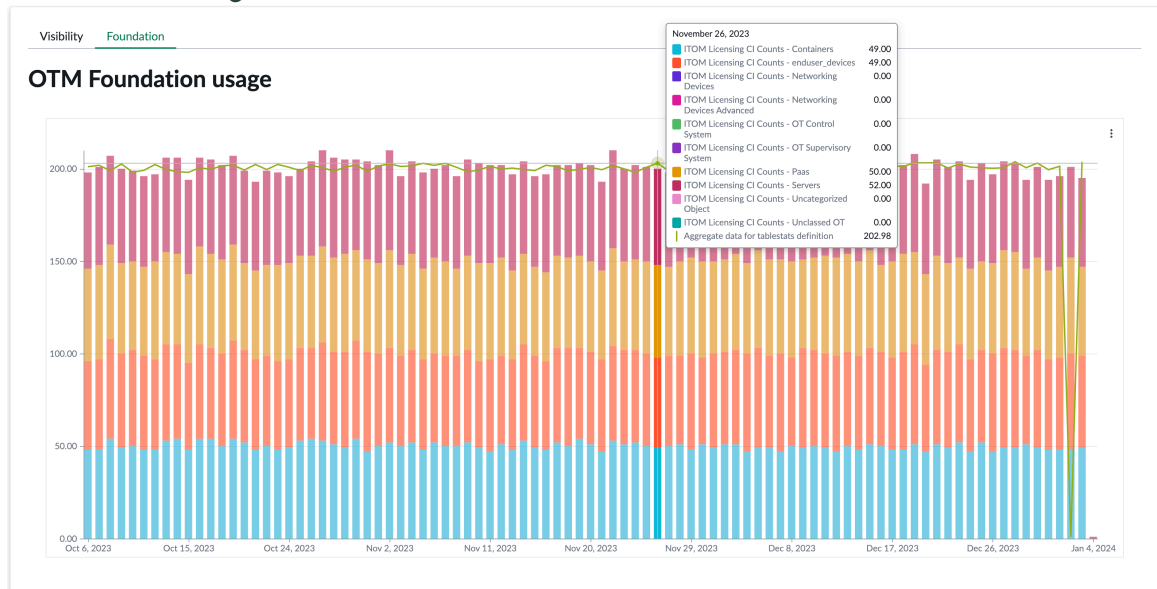
i Hinweis:

Von SG-OT Excel verwaltete CIs werden gezählt und für den Lizenzverbrauch mit last_scan-Daten aktueller als, gleich und älter als 90 Tage aufgelistet.

Prozedur

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

OTM Lizenzierungsdashboard



3. Zeigen Sie auf einen Balken, um die Anzahl der CIs in jeder Kategorie anzuzeigen.
4. Wählen Sie den Balken aus, um eine Liste der gezählten CIs anzuzeigen.
5. Überprüfen Sie das unter **OTM Lizenzierungs-Dashboard** beschriebene Dashboard.

Für OTM-Abonnements verwendete CI-Anzahl prüfen

Zeigen Sie die täglichen Anzahlen oder die Durchschnittswerte für die letzten 90 Tage der CI-Daten an. ServiceNow OT Foundation, ServiceNow OT Visibility und ServiceNow OT Vulnerability and Response bieten Einblicke in die lizenzierten Ressourcen, die OTM Anwendungen unterstützen. Ressourcen, die von OTM -Anwendungen erkannt, überwacht und bereitgestellt werden, sind Konfigurationselemente (CIs), die in der CMDB gespeichert werden. Das Lizenzierungsmodul OTM kombiniert diese CI-Informationen mit den Informationen zu den von Ihrer Organisation erworbenen Abonnements, um Statistiken zur Abonnementnutzung durch die Anwendungen OTM zu erstellen.

Vorbereitungen

- Stellen Sie sicher, dass Ihre Organisation über aktive Abonnements OTM verfügt.
- Stellen Sie sicher, dass Sie die neueste verfügbare Version der ITOM SU-Lizenzierung von installiert haben [ServiceNow Store](#) .

Erforderliche Rolle: sn_itom_license.reader

Warum und wann dieser Vorgang ausgeführt wird

ServiceNow fallen Gebühren für die Nutzung von ServiceNow OT Foundation, ServiceNow OT Visibility und ServiceNow OT Vulnerability and Response an. Weitere Informationen zu den in -Abonnements OTM von enthaltenen Produkten und Funktionen finden Sie unter [Abonnements für OTM](#).

Das Verfahren zum Sammeln und Konsolidieren von Daten für Lizenzierungszwecke umfasst die folgenden Aktionen:

1. Das OTM -Lizenzierungssystem berechnet die tägliche Anzahl der Configuration Items (CIs), die von den einzelnen OTM -Produkten verwaltet werden, und kategorisiert diese CI-Anzahl anschließend in verschiedene lizenzierbare CI-Kategorien.
2. In Fällen, in denen identische Configuration Items (CIs) von verschiedenen Funktionen innerhalb derselben OTM -Produkte verwaltet werden, werden Anpassungen vorgenommen, um Doppelungen in der CI-Anzahl zu vermeiden.
3. In Fällen, in denen IT-Konfigurationselemente (IT-CIs) als OT-Konfigurationselemente kategorisiert sind, werden die CIs nur einmal gezählt – unter OTM -Lizenzierung und nicht unter ITOM -Lizenzierung.
4. Das Lizenzierungsmodul konsolidiert CI-Anzahlen aus den Anwendungen OTM, um den Durchschnitt der täglichen CI-Anzahl für die letzten 90 Tage zu berechnen.

i Hinweis:

Von SG-OT Excel verwaltete CIs werden gezählt und für den Lizenzverbrauch mit last_scan-Daten aktueller als, gleich und älter als 90 Tage aufgelistet.

5. Das Lizenzierungsmodul gleicht die täglichen durchschnittlichen CI-Anzahlen für die Anwendungen OTM mit den im Kundenvertrag angegebenen Lizenzierungsdetails ab, um lizenzbezogene Statistiken zu generieren.

Daher können Sie Statistiken dazu anzeigen, wie Ihre Organisation die gekauften Abbonnementeinheiten verwendet.

Rufen Sie Informationen zur CI-Anzahl und zu den für jede OTM-Anwendung erworbenen Abonnements separat (à la carte) auf:

- **Gesamtanzahl:** Durchschnitt der über 90 Tage gesammelten CI-Anzahlen, kategorisiert nach CI-Typen, für jede einzelne OTM -Anwendung.

i Hinweis:

Von SG-OT Excel verwaltete CIs werden gezählt und für den Lizenzverbrauch mit last_scan-Daten aktueller als, gleich und älter als 90 Tage aufgelistet.

- **Abonnement-Einheiten-Verhältnis:** Verhältnisse bestimmen, wie viele CIs einer bestimmten CI-Kategorie ein Abonnement erfordern. Diese Verhältnisinformationen werden vom Lizenzierungsmodul aus Kundenverträgen abgerufen.
- **Insgesamt verbrauchte Abbonnementeinheiten:** Die Menge der von Ihrer Organisation für jede CI-Kategorie in jeder Anwendung von OTM verwendeten Abonnements. Diese Berechnung wird durchgeführt, indem das Abbonnementeinheitenverhältnis auf die Anzahl der CIs in der jeweiligen CI-Kategorie angewendet wird.
- **Verbrauchte Abbonnementeinheiten insgesamt:** Die Gesamtanzahl der Abbonnementeinheiten, die von allen OTM -Anwendungen zusammen verbraucht werden.

Sie können auf den Verbrauch OTM von Subscription Unit (SU) zugreifen, der nach Domäne kategorisiert ist. Diese Daten können für die Zuordnung von Verbrauch und Ausgaben verschiedener Organisationen nützlich sein.

Prozedur

1. Navigieren zu **OTM-Lizenz** > **Lizenzbericht**.

CI Category	Domain	Total Count	Subscription Unit Ratio	Total Subscription Units Consumed
Application: Visibility (6)				
Networking Devices	global	17	25:1	0
OT Control System	global	210	3:1	70
OT Field Device	global	19	10:1	1
OT Supervisory System	global	7	1:1	7
Servers	global	20	1:1	20
Unclassified OT	global	49	1:1	49
Sum				147
Sum				147

2. Wahlweise: Zeigen Sie die täglichen durchschnittlichen CI-Anzahlen der letzten 90 Tage an.

3. Wahlweise: Um die täglichen CI-Anzahlen anzuzeigen, ändern Sie den Filter so, dass **Aggregiert** auf **false** festgelegt wird.

(Optional) Bei Bedarf können Sie die Ansicht ändern, indem Sie die Spalten sortieren. In der Spalte **Erstellt** wird der Zeitstempel angezeigt, der angibt, wann die CI-Informationen zuletzt aktualisiert wurden.

OTM-Abonnementeinheiten verbrauchende CIs anzeigen

Generieren Sie eine Liste der derzeit zählbaren CIs für jede der OTM -Anwendungen: ServiceNow® OT Foundation, ServiceNow® OT Visibility und ServiceNow® OT Vulnerability and Response.

Vorbereitungen

- Stellen Sie sicher, dass Ihre Organisation über aktive Abonnements OTM verfügt.
- Stellen Sie sicher, dass Sie die neueste verfügbare Version der ITOM SU-Lizenzierung von installiert haben [ServiceNow Store](#) .

Erforderliche Rolle: sn_itom_license.reader

Warum und wann dieser Vorgang ausgeführt wird

Die generierte CI-Liste weist eine starke Korrelation mit der aktuellen täglichen CI-Anzahl auf. Es ist jedoch möglich, dass die Anzahl der CIs in der generierten Liste geringfügige Abweichungen von der letzten täglichen Zählung aufweist, wenn seit der letzten täglichen Zählung Änderungen aufgetreten sind.

Prozedur

1. Navigieren zu **Alle** > **OTM-Lizenz** > **OTM-lizenzierbare CIs melden**.

Die Seite **ITOM-lizenzierbare CIs melden** wird angezeigt.

2. Wählen Sie die Anwendung aus, für die Sie lizenzierte CIs anzeigen möchten.

- Grundlage
- Sichtbarkeit
- HLA
- Gesundheitswesen

Application	Max Results	Status	Progress	Additional Filters for CIs
Foundation	10,000	Completed	1/10000	
Health	10,000		N/A	
Visibility	10,000	Completed	1/10000	
HLA	10,000		N/A	

3. Um einen Bericht für die ausgewählten Anwendungen zu erstellen, wählen Sie **Lizenzierbare CIs ausfüllen** aus.

4. Um die Bestätigungsnachricht zu akzeptieren und den Bericht zu generieren, wählen Sie **Ja** aus.

Im neuen Bericht werden die Daten aus dem zuvor generierten Bericht ersetzt. Sie können den Bericht abbrechen, indem Sie die Anwendung auswählen und dann die Option **Auftrag abbrechen** wählen.

5. Warten Sie einige Minuten, und aktualisieren Sie dann die Seite.

Der Antragsstatus wird als **Abgeschlossen** angezeigt, sobald die Verarbeitung des Berichts abgeschlossen ist.

6. Wählen Sie die Anwendung und dann **Lizenzierbare CIs anzeigen** aus.

Auf der Seite ITOM Lizenzierbare CIs für OTM SKU wird die Liste der CIs mit einer OTM -Lizenz angezeigt.

OTM SU-Lizenzierungsreferenzen

Verwenden Sie Referenzthemen, um wertvolle Einblicke in die mit OTM der -Lizenzierung installierten Komponenten, Abonnementformulare für OTM -Produkte und eine Übersicht über das OTM -Lizenzierungs-Dashboard zu erhalten. Navigieren Sie durch die Unterthemen, um auf spezifische Anleitungen und Referenzen zu jedem dieser kritischen Aspekte zuzugreifen, die Ihnen dabei helfen, Ihre OTM -Abonnements und Lizenzierungsanforderungen effektiv zu verwalten.

Mit ITOM SU-Lizenzierung für OTM installierte Komponenten

Mit der Aktivierung des Plugins OTM SU-Lizenzierung werden verschiedene Arten von Komponenten installiert, einschließlich geplante Aufgaben und Tabellen.

Installierte geplante Aufgaben

Regelmäßige Aufgabe	Beschreibung
Speichern aktualisierter ITOM-Ausschlusstabellen	Aktualisiert die Ausschlussliste.
Speichern der ITOM-Lizenzierungszusammenfassung	Berechnet die täglichen durchschnittlichen CI-Anzahlen der letzten 90 Tage.
ITOMHealthCIReporterWithOTOMCountOTOMStore	Stellt die Liste der lizenzierbaren CIs für OTM Integrität zusammen.
ITOM Health-Lizenzierung – Speichern der Nutzungsanzahl	Berechnet die tägliche CI-Anzahl für OTM Integrität.
OTOM-Lizenzierung – Speichern der CI-Auflistung für ITOM Visibility	Stellt die Liste der lizenzierbaren CIs für OTM Visibility zusammen.
OTM Foundation Lizenzierung CI-Auflistungsspeicher	Stellt die Liste der lizenzierbaren CIs für OTM Foundation zusammen.

Regelmäßige Aufgabe	Beschreibung
OTM Foundation Licensing Store für Nutzungsanzahl	Berechnet die täglichen Anzahlen der lizenzierbaren CIs für OT Foundation.

Installierte Tabellen

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

Abonnementformular für die OTM-Produkte

Erfahren Sie mehr über die wichtigen Felder und Indikatoren im Formular „Abonnements“ für unsere Produkte. Dies sorgt für eine optimierte Abonnementverwaltung und Klarheit bei der Nutzung Ihrer OTM -Produkte.

Zeigen Sie die folgenden Abonnementstatistiken für einzeln (à la carte) erworbene Artikel an:

Name

Der Name der Anwendung OTM.

Gekauft

Die Anzahl der erworbenen Abonnements pro Anwendung.

Kapazitätsdefinitions-ID

Die ID, die zum Abrufen der täglichen Verbrauchsdaten von Abbonementseinheiten aus einer Anwendung verwendet wird.

Startdatum/Enddatum

Zeitdauer, während der dieses Abonnement aktiv bleibt.

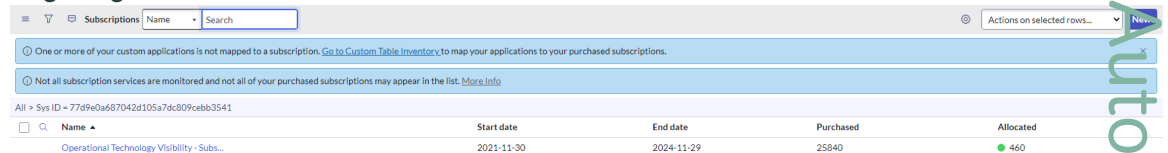
Abonnements à la carte

Das Lizenzierungsmodul berechnet den Abonnementverbrauch und zeigt ihn wie folgt an:

Abonnements à la carte

Im Fenster „Abonnements“ werden Informationen zu erworbenen und zugewiesenen Abonnements für OTM-Anwendungen angezeigt.

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



Name	Start date	End date	Purchased	Allocated
Operational Technology Visibility - Subs...	2021-11-30	2024-11-29	25840	460

OTM Lizenzierungs-Dashboard

Verwenden Sie das Lizenzierungsdashboard OTM, um den Ressourcenverbrauch und den Status in Bezug auf Ihre erworbenen Abonnements zu bewerten. Das Dashboard bietet dedizierte Berichte für jede OTM-Anwendung, die visuelle Darstellungen der täglichen Nutzungsanzahl und der durchschnittlichen Nutzung von Abbonementseinheiten über einen Zeitraum von 90 Tagen bieten. Das Lizenzierungsdashboard OTM ist ein integrierter Bestandteil der ITOM-Lizenzierungsanwendung Version 4.0 und verfügbar unter ServiceNow Store.

Apps im 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](#).

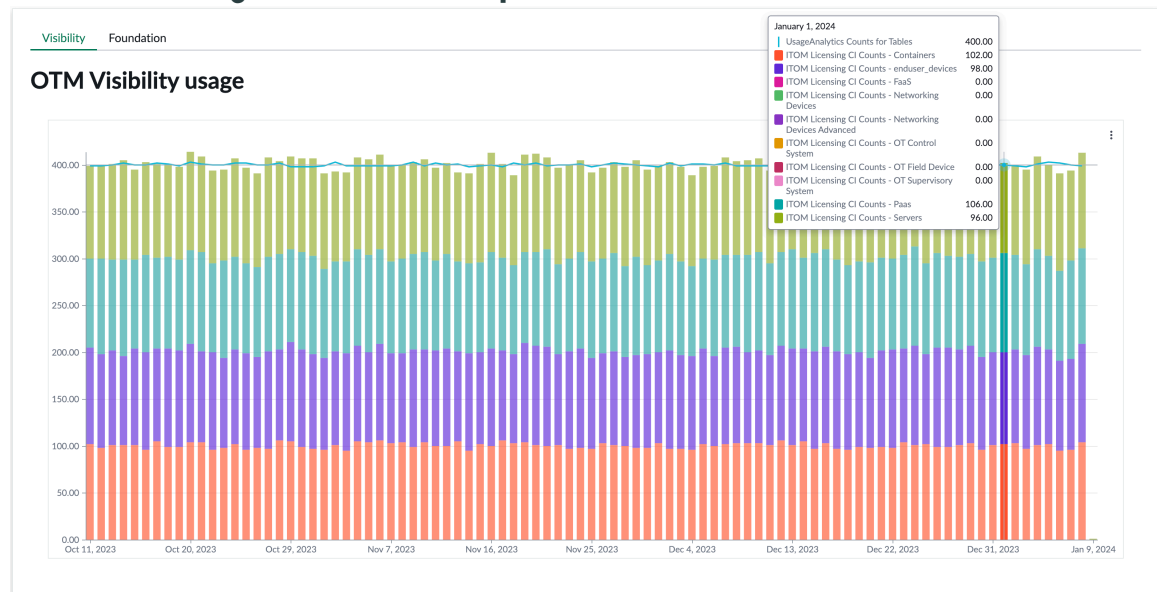
Erforderliche Now Platform-Rollen

admin

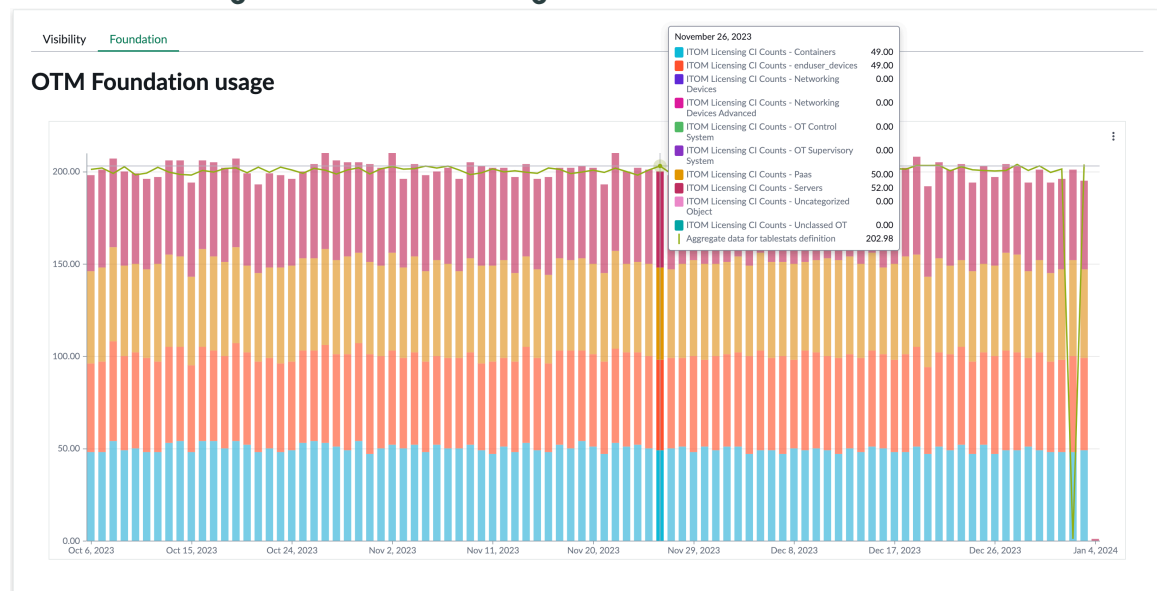
Bewertungs-Dashboard aufrufen

Um das Dashboard für OTM zu öffnen, navigieren Sie zu **Alle > OTM-Lizenz > OTM-Lizenzierungsdashboard**.

OTM Lizenzierungsdashboard – Transparenz



OTM Lizenzierungsdashboard – Grundlage



Anwendungsfälle

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

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

i Hinweis:

ServiceNow-Anwendungen beziehen sich auf Geräte und Anwendungen, die Anwendungsservices als Konfigurationselemente (Configuration Items, CIs) umfassen.

Datenvisualisierung

Das Dashboard enthält die folgende Visualisierung:

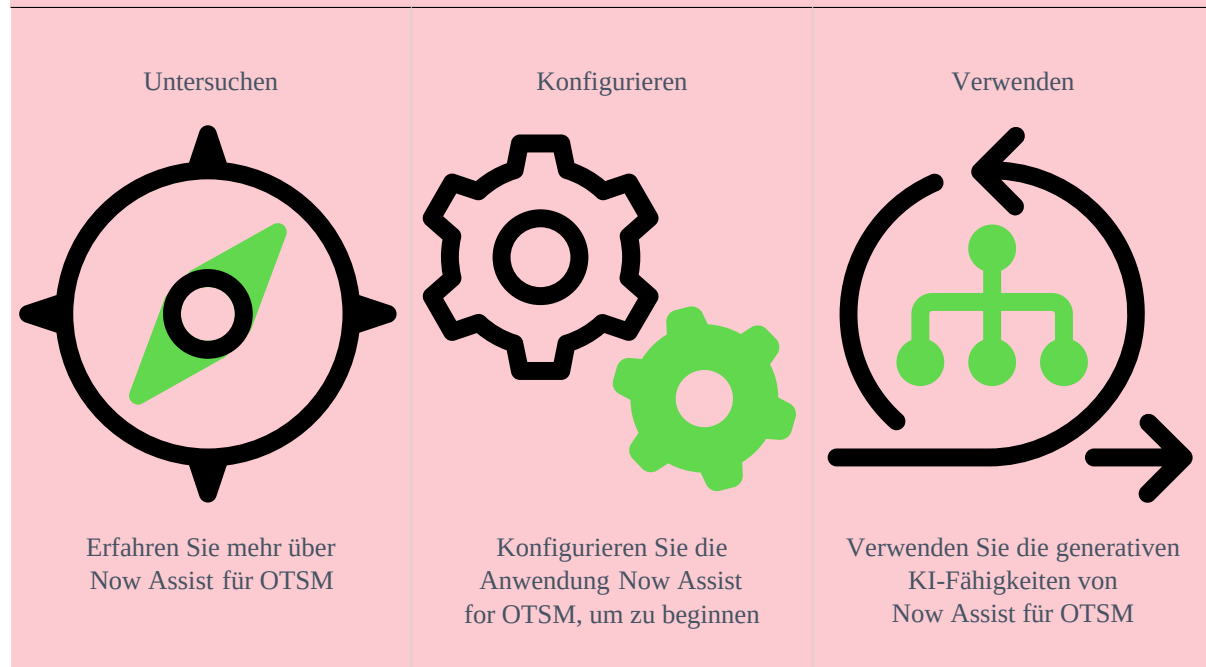
Titel	Quelltabelle	Beschreibung
OTM Transparenznutzung und OTM Grundlagennutzung	ITOM-Lizenzierungs-CI-Anzahlen [itom_lu_ci_counts] und UsageAnalytics-Anzahlen für Tabellen [usageanalytics_count]	Zeigt Balken an, die die Anzahl der CIs verschiedener lizenzierbarer Kategorien für die letzten 120 Tage pro ITOM-Anwendung darstellen. Auf dem Dashboard wird auch die Zeile angezeigt, die den durchschnittlichen Verbrauch von Abbonementseinheiten in den letzten 90 Tagen darstellt. i Hinweis: Von SG-OT Excel verwaltete CIs werden gezählt und für den Lizenzverbrauch mit last_scan-Daten aktueller als, gleich und älter als 90 Tage aufgelistet.

[store-future: BEGIN review]

Now Assist für Operational Technology Service Management (OTSM)

Verwenden Sie die Anwendung ServiceNow® Now Assist für Operational Technology Service Management (OTSM), um die OT-Incident-Informationen zusammenzufassen und Lösungshinweise für Incidents zu generieren. Sie ermöglichen Ihren Benutzern das Verständnis des Kontexts, um schneller Lösungen implementieren zu können.

Erste Schritte



Wichtig:

- Einige Now Assist -Produkte/-Funktionen sind derzeit für Kunden in FedRAMP-, NSC DOD IL5- oder Australia IRAP-geschützten Rechenzentren, für selbst gehostete Kunden oder in anderen eingeschränkten Umgebungen nicht verfügbar. Weitere Informationen finden Sie im Now Support Knowledge Base-Artikel [KB0743854](#). Achten Sie darauf, in zukünftigen Versionen nach Verfügbarkeitsaktualisierungen zu suchen.
- Einige Produkte/Funktionen Now Assist von sind derzeit nur für Kunden in bestimmten Regionen verfügbar. Weitere Informationen finden Sie in Artikel [KB1699552](#) in der Now Support Knowledge Base. Achten Sie darauf, in zukünftigen Versionen nach Verfügbarkeitsaktualisierungen zu suchen.

Problembehandlung und Hilfe

- [KI und Intelligenz in der ServiceNow-Community](#)
- [Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen](#)
- [Kontakt Kundenservice und Support](#)

KI-Beschränkungen

Diese Anwendung nutzt künstliche Intelligenz (KI) und maschinelles Lernen, zwei sich schnell entwickelnde Studienbereiche, in denen Vorhersagen auf Grundlage von Datenmustern erstellt werden. Daher liefert diese Anwendung möglicherweise nicht immer präzise, vollständige und angemessene Informationen. Darüber hinaus gibt es keine Garantie dafür, dass diese Anwendung vollständig für Ihren Anwendungsfall trainiert und getestet wurde. Um diese Probleme zu minimieren, sind Sie dafür verantwortlich, Ihre Verwendung dieser Anwendung auf Genauigkeit, Schaden und Angemessenheit für Ihren Anwendungsfall zu testen und zu bewerten, die Ausgabe von Menschen beaufsichtigen zu lassen und sich bei der Entscheidungsfindung nicht ausschließlich auf KI-generierte Ergebnisse zu verlassen Zwecke. Dies ist besonders wichtig, wenn Sie diese Anwendung in Bereichen mit weitreichenden Auswirkungen wie Gesundheitswesen, Finanzen, Recht, Beschäftigung,

Sicherheit und Infrastruktur einsetzen möchten. Sie erklären sich damit einverstanden, [die Richtlinie zur zulässigen KI-Nutzung von ServiceNow](#) einzuhalten, die von ServiceNow aktualisiert werden kann.

Datenverarbeitung

Bei dieser Anwendung müssen die Daten einzelner ServiceNow-Kundeninstanzen in eine zentrale ServiceNow-Umgebung übertragen werden, die sich in einer anderen Rechenzentrumsregion befinden kann als die, in der sich Ihre Instanz befindet, und möglicherweise an einen externen Cloud-Anbieter, z. B. Microsoft Azure. Diese Daten werden gemäß den internen Richtlinien und Verfahren von ServiceNow gehandhabt, einschließlich unserer Richtlinien, die über unser [CORE-Compliance-Portal](#) verfügbar sind.

Datenerfassung

ServiceNow sammelt und verwendet die Eingaben, Ausgaben und Ausgabenbearbeitungen dieser Anwendung, um ServiceNow-Technologien wie ServiceNow-Modelle und KI-Produkte zu entwickeln und zu verbessern. Darüber hinaus erfasst diese Anwendung Incident-Daten (für Incident-Assistent und Wissensassistent) und Chattranskripte (für Chat-Assistent). Kunden können der Datenerfassung für die Zukunft jederzeit widersprechen, wie auf der [Now Assist Abwählseite](#) beschrieben.

Weitere Informationen finden Sie unter [Now Assist Dokumentation](#).

[End]

[store-future: BEGIN review]

Now Assist für Operational Technology Service Management erkunden (OTSM)

Mit der Anwendung Now Assist für Operational Technology Service Management (OTSM) kann Ihr Team die OT-Incident-Details zusammenfassen und die Incident-Lösungshinweise generieren, um sie für andere Benutzer freizugeben.

Now Assist für Operational Technology Service Management (OTSM) Übersicht

Die folgenden generativen KI-Fähigkeiten sind für OTSM-Benutzer verfügbar:

- Eine automatisch generierte OT-Incident-Zusammenfassung, die Ihnen hilft, den OT-Incident-Kontext zu verstehen.
- Es werden automatisch Lösungshinweise für OT-Incidents generiert, die anderen Anwendern helfen, ihre Incidents zu lösen, wenn sie ein ähnliches Problem haben.

Now Assist für Operational Technology Service Management (OTSM)-Kompetenzen

Zusammenfassung von Incidents für operative Technologie (OT).

Ermöglicht Ihnen, den Fehlerbehebungsprozess für OT-Incidents zu beschleunigen, indem Sie eine Zusammenfassung überprüfen, die das Problem, die ergriffenen Maßnahmen und die Lösung enthält. Sie können eine Incident-Zusammenfassung für aktive Incidents generieren, um den Incident-Kontext zu verstehen. Sie können die Zusammenfassung auch aktualisieren, die Zusammenfassung in den Incident-Arbeitsnotizen veröffentlichen, die Zusammenfassung kopieren und Feedback zur Zusammenfassung hinterlassen.

Die Incident-Zusammenfassung enthält die folgenden Informationen:

- Kurzbeschreibung
- Beschreibung
- Arbeitsnotizen
- Zusätzliche Anmerkungen
- Priorität
- Site
- Anlagenmodell-Entität
- OT-Gerät
- OT-Incident-Aufgabe

Lösungshinweise für OT-Incidents generieren

Generiert automatisch die Lösungshinweise für einen OT-Incident und bietet Kontext für einen anderen Benutzer, der möglicherweise auf ähnliche Incidents stößt.

[End]

[store-future: BEGIN review]

Ergänzende Informationen für Now Assist für Operational Technology Service Management (OTSM)

Verschaffen Sie sich einen schnellen Überblick über wichtige Informationen im Zusammenhang mit der Anwendung Now Assist für Operational Technology Service Management (OTSM).

Unterstützte Anwenderoberflächen

Die Anwendung Now Assist für OTSM enthält die in der folgenden Tabelle aufgeführten Kompetenzen.

Von Now Assist für OTSM unterstützte Anwenderoberflächen

Schnittstelle	Kompetenz
Industrial Workspace	• Zusammenfassung von OT-Incidents • Generierung von OT-Lösungshinweisen

[End]

[store-future: BEGIN review]

Verwenden von Anwendungsfällen von KI-Agenten für Now Assist für Operational Technology Service Management (OTSM)

Verwenden Sie die KI-Mitarbeiter für Operational Technology (OT), um Aufgaben autonom abzuschließen.

Tabelle 1. Verfügbare Anwendungsfälle für KI-Agents für OT

Name des Anwendungsfalls	Beschreibung	Verfügbare KI-Agents
Generieren Sie Operational Technology KB-Artikel	Nach der Lösung des OT-Incidents erstellt der KI-Mitarbeiter automatisch einen KB-Artikel mit relevanten kontextbezogenen Informationen.	OT-Wissensgenerator

i Wichtig:

Wenn Sie diesen Anwendungsfall ändern möchten, können Sie [duplizieren](#) , passen Sie die Einstellungen an Ihre spezifischen Bedürfnisse an, und aktivieren Sie stattdessen die duplizierte Version des Anwendungsfalls.

Zum Duplizieren eines Anwendungsfalls ist mindestens die Rolle **sn_aia.admin** erforderlich. Standardmäßig ist der OT-Anwendungsfall inaktiv. Wenn Sie den OOB-Anwendungsfall verwenden möchten, können Sie den OOB-Auslöser aktivieren. Wenn Sie den Anwendungsfall jedoch anpassen möchten, müssen Sie ihn duplizieren.

[End]

[store-future: BEGIN review]

KI-Agents für den Anwendungsfall Operational Technology „KB-Artikel generieren“.

Verwenden Sie den Anwendungsfall Operational Technology „KB-Artikel generieren“, um einen KB-Artikel zu generieren, wenn ein OT-Incident gelöst wird.

Generieren Sie eine Übersicht über die Operational Technology KB-Artikel

Mit dem Anwendungsfall Operational Technology KB-Artikel generieren können Sie automatisch einen KB-Artikel für einen OT-Incident generieren, wenn der Status des incident auf **Gelöst** festgelegt ist. Der Artikel enthält die folgenden Informationen.

Site

Standort, an dem der Incident aufgetreten ist.

OT-Gerät

Betroffenes OT-Gerät an der Site.

Anlagenmodell-Entität

Betroffene Anlagenmodell-Entität am Standort.

Zusammenfassung

Die KI-generierte Zusammenfassung, die das Problem, die durchgeführten wichtigen Aktionen und ggf. OT-Incident-Aufgaben enthält.

Lösungsnotizen

KI-generierte Lösungshinweise aus der Kompetenz „OT-Lösungshinweise generieren“.

KB-Basis

Die Knowledge Base, in der der generierte KB-Artikel gespeichert wird. Die KB-Basis für den OT-Anwendungsfall ist die OT-Knowledge Base des KI-Mitarbeiters.

Autor

Der Autor, der den generierten KB-Artikel veröffentlicht. Der Autor für den OT-Anwendungsfall ist der OTSM AI Agent.

Der Artikel wird dann automatisch veröffentlicht und in der zugehörigen Liste Angehängtes Wissen des OT-Incident-Datensatzes in Industrial Workspace angezeigt. Der Prozess zur Generierung von KB-Artikeln wird nicht ausgelöst, wenn an den aktuellen OT-Incident bereits ein Artikel angehängt ist.

Im Folgenden finden Sie die Anweisungen, Service Desk-Mitarbeiter, Tools und Auslöser, die dem von ServiceNow bereitgestellten OT-Anwendungsfall zugeordnet sind. Wenn Sie diesen Anwendungsfall ändern möchten, können Sie [duplizieren](#) , passen Sie die Einstellungen an Ihre spezifischen Bedürfnisse an, und aktivieren Sie stattdessen die duplizierte Version des Anwendungsfalls.

Wichtig:

Wenn Sie einen Anwendungsfall, KI-Agenten oder ein Tool ändern, aktualisieren Sie alle Anweisungen entsprechend.

Zum Duplizieren eines Anwendungsfalls ist mindestens die Rolle **sn_aia.admin** erforderlich. Standardmäßig ist der OT-Anwendungsfall inaktiv. Wenn Sie den OOB-Anwendungsfall verwenden möchten, können Sie den OOB-Auslöser aktivieren. Wenn Sie den Anwendungsfall jedoch anpassen möchten, müssen Sie ihn duplizieren.

Anwendungsfall Operational Technology „KB-Artikel generieren

Generiert automatisch einen KB-Artikel, nachdem ein OT-Incident gelöst wurde.

So greifen Sie auf den Anwendungsfall zu:

1. Navigieren zu **Alle > AI Agent Studio > Erstellen und verwalten**.
2. Wählen Sie den Anwendungsfall **KB-Artikel bei Lösung eines OT-Incidents generieren** aus.

Auslöser für den Anwendungsfall Operational Technology „KB-Artikel generieren“.

Wenn im Bildschirm „Auslöser definieren“ die folgenden Bedingungen für den Auslöser festgelegt sind, beginnt die Ausführung des Anwendungsfalls.

- Legen Sie das Feld **Tabelle** auf „Operative Technologie-Incident“ [sn_ot_incident] fest.
- Legen Sie das Feld **Ausführen als** auf Gelöst von [Incident] fest.
- Legen Sie die folgende Bedingung fest:
 - [Status] [ändert sich in] [Gelöst]
 - [store-future: BEGIN review][End]

Wichtig:

Stellen Sie im Formular „Auslöser bearbeiten“ sicher, dass die Schaltfläche **Aktiv** aktiviert ist, um den KI-Agent autonom auszulösen.

KI-Agents, die im Anwendungsfall Operational Technology „KB-Artikel generieren verwendet werden

Der OT-Wissensgenerator-Agent wird verwendet, um einen KB-Artikel zu generieren, der sich auf einen gelösten OT-Incident bezieht.

Wichtig:

Stellen Sie auf dem Bildschirm „**Verfügbarkeit definieren**“ für den KI-Mitarbeiter sicher, dass das Feld **Status** aktiviert ist, um den KI-Mitarbeiter zu aktivieren.

Tools, die KI-Agents für den Anwendungsfall Operational Technology „KB-Artikel generieren zugeordnet sind

Alle in diesem Anwendungsfall verwendeten Tools sind vom Typ Skripts.

Tabelle 1. Tools, die im Anwendungsfall Generieren eines KB-Artikels nach Lösen eines OT-Incidents verwendet werden

Name	Ausführungsmodus	Beschreibung
Generieren und veröffentlichen Sie einen KB-Artikel für einen gelösten OT-Incident	Autonom	Generiert den KB-Artikel für einen OT-Incident, wenn der Status des Incidents auf Gelöst festgelegt ist.

Der KB-Artikel wird generiert

Im Anwendungsfalldatensatz:

- Überprüfen Sie die Informationen im Bildschirm Beschreiben und verbinden und im Bildschirm Auslöser definieren, nehmen Sie die erforderlichen Aktualisierungen vor, und wählen Sie dann **Speichern und fortfahren aus**.
- Auf dem **Bildschirm „Auswählen“** :
 - Wählen Sie aus, wo die Ausgabe des Anwendungsfalls angezeigt werden soll, verwenden Sie den Pfeil daneben, und fügen Sie Rollen hinzu, die auf den Anwendungsfall zugreifen können.

Hinweis:

Die Rolle itil wird standardmäßig hinzugefügt.

- Wählen Sie **Speichern und testenaus**.

Der Service Desk-Mitarbeiter führt die Anforderung für den Anwendungsfall aus.

[End]

[store-future: BEGIN review]

Now Assist für Operational Technology Service Management (OTSM) konfigurieren

Wenn Sie über die Administratorrolle verfügen, können Sie die Anwendung Now Assist für Operational Technology Service Management (OTSM) so konfigurieren, dass Teams die generativen KI-Fähigkeiten in Industrial Workspace für ihre Operational Technology (OT)-Incidents verwenden können.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Verwenden Sie die Now Assist-Administrator-Konsole, um Now Assist für OTSM zu konfigurieren. Diese Konsole enthält alles, was Sie benötigen, um die Plugins zu installieren und die Kompetenzen generativer KI zu konfigurieren. Weitere Informationen finden Sie unter [Now Assist Admin console](#) .

In der folgenden Tabelle sind die Funktionen und Kompetenzen aufgeführt, auf die Sie über die Now Assist-Administrator-Konsole zugreifen können.

OTSM-Funktionen und -Kompetenzen in der Konsole Now Assist-Administrator .

OTSM-Funktionen	Kompetenzen
Generative KI-Kompetenzen für OT-Incidents	• Generierung von OT-Lösungshinweisen • Zusammenfassung von OT-Incidents  Hinweis: Die Incident-Zusammenfassung gilt nur für Incidents im Status „Neu“, „In Bearbeitung“, „Warten“, „Gelöst“ oder „Geschlossen“, solange die im Basissystem bereitgestellten Incident-Statuszuordnungen nicht angepasst werden.

Prozedur

1. Installieren Sie das Plugin Now Assist für OTSM (sn_otsm_gen_ai).
 - Informationen zu den Anwendungsabhängigkeiten finden Sie unter [Ergänzende Informationen für Now Assist für Operational Technology Service Management \(OTSM\)](#).
 - Informationen zum Installationsprozess finden Sie unter [Install Now Assist plugins](#) .
2. Navigieren zu **Alle > Now Assist Admin > Funktionen** um auf die Registerkarte „Features“ der Now Assist-Administrator -Konsole zuzugreifen.
3. Aktivieren und konfigurieren Sie die Kompetenzen für die Funktionen von Now Assist für OTSM. Diese Funktionen sind unter der Workflow-Gruppe **Technologie** gruppiert. Jede Funktion hat zugehörige Kompetenzen.
4. Wählen Sie auf der Funktionskarte, die der zu aktivierenden Kompetenz zugeordnet ist, **Details anzeigen**.
5. Wählen Sie im Abschnitt „Alle verfügbaren Kompetenzen“ **Kompetenz aktivieren**.
6. Wählen Sie die Eingaben oder Auslöser für die ausgewählte Kompetenz aus.

Informationen zu den Eingaben und Auslösern für die einzelnen Kompetenzen finden Sie unter [Kompetenzeingaben und -auslöser in Now Assist für Operational Technology Service Management \(OTSM\)](#).
7. Nachdem Sie die Eingaben oder Auslöser für die ausgewählte Kompetenz konfiguriert haben, wählen Sie **Speichern und fortfahren**, um mit dem nächsten Schritt fortzufahren. Über die Schaltfläche **Zurück** können Sie zum vorhergehenden Schritt zurückkehren.
8. Wählen Sie aus, wo Sie die Kompetenz anzeigen möchten.
 - **Produktintern:** Wenn diese Option ausgewählt ist, werden die Now Assist-Kompetenzen in Formularen und Arbeitsbereichen angezeigt.
 - **Now Assist-Bereich:** Wenn diese Option ausgewählt ist, sind die Now Assist-Kompetenzen im Bereich Now Assist verfügbar. Wenn diese Option nicht angezeigt wird, müssen Sie den Bereich Now Assist aktivieren. Weitere Informationen finden Sie unter [Turn on the Now Assist panel](#) .

Wählen Sie für die Kompetenzen, die im Bereich Now Assist angezeigt werden, den Abwärtspfeil, um die Rollen zu identifizieren, die diese Kompetenzen verwenden können.

9. Nachdem Sie die Anzeige für die ausgewählte Kompetenz konfiguriert haben, wählen Sie **Speichern und fortfahren**, um mit dem nächsten Schritt fortzufahren.
10. Überprüfen Sie Ihre Auswahl, und wählen Sie **Aktivieren**, um die Konfiguration abzuschließen. Ihre Kompetenz ist konfiguriert.

Zugehörige Informationen

[Now Assist Admin console](#) 

[Configuring Now Assist settings and features](#) 

[End]

[store-future: BEGIN review]

Kompetenzeingaben und -auslöser in Now Assist für Operational Technology Service Management (OTSM)

Verschaffen Sie sich einen schnellen Überblick über die Kompetenzeingaben und -auslöser für Now Assist für Operational Technology Service Management (OTSM). Durch die Konfiguration der Eingaben oder Auslöser für eine Kompetenz können Sie bestimmen, wie und wann eine Kompetenz verwendet wird.

Now Assist für OTSM Übersicht über Kompetenzeingaben

Je nach ausgewählter Kompetenz können Sie Eingaben oder Auslöser konfigurieren. Diese Einstellungen legen fest, wie und wann eine Kompetenz verwendet wird. Eine Eingabe benennt die Daten, die für eine Kompetenz verwendet werden, z. B. die Tabelle und die Felder, die zum Generieren einer Incident-Zusammenfassung verwendet werden. Ein Auslöser initiiert eine Aktion, z. B. wenn das System Operational Technology (OT)-Lösungshinweise generiert.

Kompetenz „Zusammenfassung von OT-Incidents“.

Die Kompetenz „Zusammenfassung von OT-Incidents“ enthält die Eingaben, die die Tabelle und die Felder identifizieren, die bei der Generierung einer OT-Incident-Zusammenfassung verwendet werden.

Die folgende Tabelle enthält die Eingaben für die Kompetenz „Zusammenfassung von OT-Incidents“.

Eingaben für die Kompetenz „Zusammenfassung von OT-Incidents“.

Eingabe	Beschreibung
Eingabetabelle	OT-Incident [sn_ot_incident]
Eingabefelder	• Beschreibung • Kurzbeschreibung • Arbeitsnotizen • Zusätzliche Anmerkungen • Priorität • Site • Anlagenmodell-Entität

Eingaben für die Kompetenz „Zusammenfassung von OT-Incidents“. (Fortsetzung)

Eingabe	Beschreibung
	• OT-Gerät • OT-Incident-Aufgabe
Status der Eingabevorlage	• Neu • WIP • Gelöst • Geschlossen

Die folgende Tabelle enthält die Beschreibungen für die Kompetenz „Zusammenfassung von OT-Incidents“.

Beschreibungen für die Kompetenz „Incident-Zusammenfassung“

Beschreibung	Pflichtfeld für Eingabestatus
Problem	• Neu • WIP • Gelöst • Geschlossen
Wichtige getroffene Maßnahmen	• WIP • Gelöst • Geschlossen
Lösung	• Gelöst • Geschlossen
OT-Incident-Aufgabe	• WIP • Gelöst • Geschlossen

Kompetenz „OT-Lösungshinweise generieren“.

Die Kompetenz „OT-Lösungshinweise generieren“ enthält die Eingaben, die die Tabelle und die Felder identifizieren, die verwendet werden, wenn die Lösungshinweise für einen OT-Incident generiert werden.

Die folgende Tabelle zeigt die Eingaben für die Kompetenz „Lösungshinweise generieren“.

Eingaben für die Kompetenz „OT-Lösungshinweise generieren“.

Eingabe	Beschreibung
Eingabetabelle	OT-Incident [sn_ot_incident]
Eingabefelder	• Beschreibung • Kurzbeschreibung • Arbeitsnotizen • Zusätzliche Anmerkungen • Priorität • Site • Anlagenmodell-Entität • OT-Gerät

[End]

[store-future: BEGIN review]

Now Assist für Operational Technology Service Management (OTSM) verwenden

Sie können einen Operational Technology (OT)-Incident zusammenfassen und OT-Lösungshinweise generieren, indem Sie die Anwendung Now Assist für Operational Technology Service Management (OTSM) verwenden.

[End]

[store-future: BEGIN review]

Incident Operational Technology mithilfe von Now Assist für Operational Technology Service Management (OTSM) zusammenfassen

Mit der Kompetenz „Zusammenfassung von OT-Incidents“ in der Anwendung Now Assist für Operational Technology Service Management (OTSM) können Sie den Incident-Kontext Operational Technology (OT) schnell nachvollziehen und auf die Anfragen eines Benutzers antworten.

Vorbereitungen

Erforderliche Rolle: sn_ot_incident_write

Warum und wann dieser Vorgang ausgeführt wird

Eine OT-Incident-Zusammenfassung bietet Ihnen eine kurze Zusammenfassung eines incident. Die Zusammenfassung basiert auf dem Status des OT-Incident und wird aus den folgenden Informationen generiert:

- Kurzbeschreibung
- Beschreibung
- Arbeitsnotizen
- Zusätzliche Anmerkungen
- Priorität

- Site
- Anlagenmodell-Entität
- OT-Gerät
- OT-Incident-Aufgabe

Prozedur

1. Navigieren zu **Alle > Industrial Workspace**.
2. Öffnen Sie die Listenansicht Industrial Workspace.
3. Wählen Sie im Modul OT Incidents eine der verfügbaren Listen aus.
4. Öffnen Sie den OT-Incident-Datensatz, den Sie zusammenfassen möchten.
5. Wählen Sie im OT-Incident-Datensatz die Schaltfläche **Zusammenfassen**.
6. **Wahlweise:** Wenn die Zusammenfassung eines OT-Incidents fertig ist, können Sie sie den Arbeitsnotizen hinzufügen, erweitern oder reduzieren, Feedback geben, ihn kopieren oder Informationen dazu anzeigen.

[End]

[store-future: BEGIN review]

Generieren Sie Lösungshinweise für einen Operational Technology -Incident

Aktualisiert die Lösungshinweise für einen Operational Technology (OT)-Incident automatisch. Sie können die Qualität der Lösungshinweise verbessern, indem Sie eine Zusammenfassung der zur Lösung des Problems unternommenen Schritte dokumentieren. Durch Generieren von Lösungshinweisen können Sie anderen Benutzern, die möglicherweise auf ähnliche Probleme stoßen, Informationen zur Incident-Lösung bereitstellen.

Vorbereitungen

Erforderliche Rolle: sn_ot_incident_write

Warum und wann dieser Vorgang ausgeführt wird

Lösungshinweise für OT-Incidents werden aus den folgenden Informationen generiert:

- Kurzbeschreibung
- Beschreibung
- Arbeitsnotizen
- Zusätzliche Anmerkungen
- Status
- Site
- Anlagenmodell-Entität
- OT-Gerät

Prozedur

1. Navigieren zu **Alle > Industrial Workspace**.
2. Öffnen Sie die Listenansicht Industrial Workspace.
3. Wählen Sie im Modul OT Incidents eine der verfügbaren Listen aus.

4. Öffnen Sie den OT-Incident-Datensatz, für den Sie Lösungshinweise generieren möchten.
5. Wählen Sie im Feld **Lösungshinweise** die **Schnellaktion Now Assist zum Generieren von Notizen verwenden** () aus.
6. Wählen Sie **Lösungshinweise generieren** aus.
7. **Wahlweise:** Überprüfen Sie die Lösungszusammenfassung im Feld **Lösungshinweise**, und nehmen Sie die erforderlichen Korrekturen vor.

i Hinweis:

Da die Informationen in diesen Feldern automatisch generiert werden, empfiehlt es sich, den Text zu prüfen und eventuelle Fehler zu korrigieren.

8. **Wahlweise:** Wenn Sie mit dem Generieren von OT-Lösungshinweisen fertig sind, können Sie die Lösungshinweise einfügen, die Lösungshinweise verfeinern, Feedback geben, sie kopieren oder Informationen dazu anzeigen.
9. Aktualisieren Sie im Feld **Lösungscode** den Lösungscode, und wählen Sie **Lösen** aus.
Ein Lösungscode kategorisiert, wie der Incident gelöst wird. Zum Beispiel als Known Error bzw. als dauerhaft gelöst.
Die Lösungsinformationen werden aktualisiert, und der Status des OT-Incident wird auf **Gelöst** gesetzt.

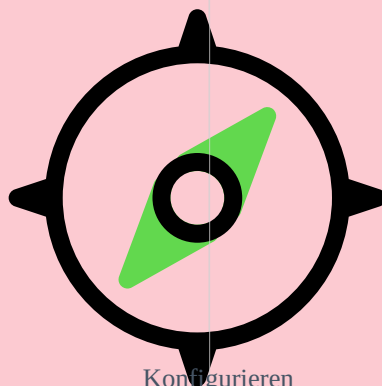
[End]

[store-future: BEGIN review]

Empfohlene Aktionen für Operational Technology Service Management (OTSM)

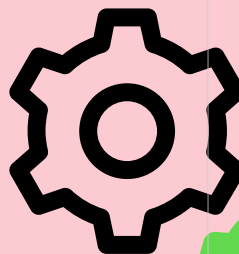
Mit Recommended Actions for Operational Technology Service Management (OTSM) können Sie umsetzbare Echtzeitempfehlungen einrichten und anwenden, um den Selektierungsprozess zu beschleunigen und Probleme schnell für verschiedene Datensätze in Industrial Workspace zu lösen, einschließlich Operational Technology (OT) Incidents.

Erste Schritte



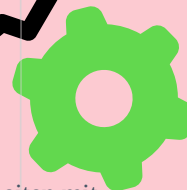
Untersuchen

Erfahren Sie, wie empfohlene Aktionen für OTSM Ihnen

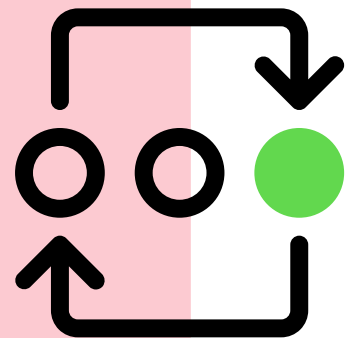


Konfigurieren

Richten Sie „Empfohlene Aktionen für OTSM“ ein



Arbeiten mit



Automatische Übersetzung

bei der Verwaltung Ihres
OT-Systems helfen können.

und konfigurieren Sie
sie, um Ihre spezifischen
Anforderungen zu erfüllen.

Verwalten Sie Ihre OTSM-
Datensätze mit Empfohlene
Aktionen für OTSM.

Hilfreiche Ressourcen

Einige ServiceNow -Ressourcen, die Ihnen hilfreiche Informationen liefern können, sind:



ServiceNow Community

[ServiceNow Community](#)



Customer Success Center

[Customer Success Center](#)



Entwickler

developer.servicenow.com



Impact

<http://impact.servicenow.com>



ServiceNow University

[ServiceNow University](#)



NowCreate

[Now Create](#)



Partner

<https://www.servicenow.com/partners.html>



ServiceNow

<https://www.servicenow.com/>



ServiceNow Store

https://store.servicenow.com/sn_appstore_store.do#!/store/home



Unterstützung

- <https://support.servicenow.com/now>
- [Known Error-Portal](#)

[End]

[store-future: BEGIN review]

Empfohlene Aktionen für Operational Technology Service Managementerkunden

Mit Recommended Actions for Operational Technology Service Management (OTSM) können Sie umsetzbare Echtzeitempfehlungen einrichten und anwenden, um den Selektierungsprozess zu beschleunigen und Probleme schnell für verschiedene Datensätze zu lösen, einschließlich Incidents Operational Technology von (OT).

Empfohlene Aktionen für OTSM – Übersicht

Empfehlungen werden als umsetzbare Echtzeitempfehlung im Seitenbereich angezeigt, während OT Incident-Datensätze in Industrial Workspace aktualisiert oder erstellt werden. Sie können auf Empfehlungen in Industrial Workspace zugreifen, indem Sie im Seitenbereich das Symbol **für Empfehlungen** () wählen.

Empfohlene Aktionen für OTSM- Workflow

Der Workflow für Recommended Actions for OTSM enthält den Kontext verwenden. Verwenden Sie den OT-Incident-Kontext, um die Empfehlungen in Industrial Workspace zu suchen und zu verwenden.

Hinweis:

Für OT-Incidents können Sie anleitungsbasierte Empfehlungen im Bereich **Empfehlungen** verwenden.

[End]

[store-future: BEGIN review]

Übersicht über empfohlene Aktionen für Operational Technology Service Management

Empfohlene Aktionen für Operational Technology Service Management (OTSM) enthält die folgenden Kontextkomponenten, die zum Konfigurieren von empfohlenen Aktionen für verschiedene Datensätze in Industrial Workspace verwendet werden, einschließlich Incidents für Operational Technology (OT).

Kontexte in „Empfohlene Aktionen für OTSM“.

Ein Kontext ermöglicht es Ihnen, Empfehlungen für einen bestimmten Datensatztyp anzuzeigen, wenn bestimmte Regeln erfüllt sind. Diese Empfehlungen können Ihnen helfen, indem sie basierend auf dem Datensatzkontext Aktionen vorschlagen. Weitere Informationen finden Sie unter [Contexts in Recommended Actions](#) .

Der OTSM-Kontext übermittelt den in der folgenden Tabelle beschriebenen OT-Incident-Kontext.

Kontextbeschreibung

Kontext	Beschreibung
OT-Incident-Kontext	Hier werden alle gültigen Empfehlungen zu OT-Incidents basierend auf den aktiven Empfehlungen in Industrial Workspace angezeigt.

Hinweis:

Informationen zum Erstellen eines Kontexts finden Sie unter [Create a context in Recommended Actions](#) .

Suchergebniszuordnungen

Die Suchergebniszuordnungen werden in den KI-Suchergebnissen für OT-Incident-Datensätze im Industrial Workspace angezeigt.

Der OTSM-Kontext enthält die folgenden Suchergebniszuordnungen basierend auf dem Kontexttyp:

OT-Incident: Wissen [kb_knowledge], OT-Incident [sn_ot_incident]

Anwendungskonfiguration durchsuchen

Der OTSM-Kontext enthält die **[AIS] Empfohlene Aktionen für OTSM-Suchkonfiguration**. Diese Anwendung unterstützt die KI-Suche nach verschiedenen Datensätzen in Industrial Workspace, einschließlich OT-Incidents.

[End]

[store-future: BEGIN review]

Empfohlene Aktionen für Operational Technology Service Management in der konfigurieren Industrial Workspace

Aktivieren Sie einen Anwender, der an den relevanten Empfehlungen arbeitet, die von Recommended Actions for Operational Technology Service Management (OTSM) bereitgestellt werden.

„Empfohlene Aktionen für OTSM“ wird als neue Funktion für die Anwendung Incident-Management für operative Technologie bereitgestellt.

[End]

[store-future: BEGIN review]

Richten Sie empfohlene Aktionen für Operational Technology Service Management ein

Richten Sie empfohlene Aktionen ein, um relevante Empfehlungen in Industrial Workspace anzuzeigen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Erstellen Sie eine Regel in Recommended Actions for OTSM.

Mit OTSM können Sie neue Regeln erstellen. Weitere Informationen finden Sie unter [Create a rule in Recommended Actions](#) .

2. Erstellen Sie eine Empfehlung.

Mit OTSM können Sie neue Empfehlungen erstellen. Weitere Informationen finden Sie unter [Create a recommendation in Recommended Actions](#) .

3. Erstellen Sie einen Ressourcengenerator.

Mit OTSM können Sie neue Ressourcengeneratoren erstellen. Weitere Informationen finden Sie unter [Create a resource generator in Recommended Actions](#) .

4. Erstellen Sie Anleitungen und Feldempfehlungen.

Mit OTSM können Sie Anleitungen und Feldempfehlungen konfigurieren oder erstellen. Weitere Informationen finden Sie unter [Creating guidance and field recommendation in Recommended Actions](#) .

[End]

[store-future: BEGIN review]

KI-Suche für Operational Technology Service Management konfigurieren

Konfigurieren Sie KI-Suche für Empfohlene Aktionen für Operational Technology Service Management (OTSM), um intelligente Abfragefunktionen zu aktivieren, mit denen Sie schnell die benötigten Antworten für OT-Incidents finden können.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Für Operational Technology Service Management -Benutzer müssen Sie die OT-Incident-Tabelle [sn_ot_incident] als indizierte Quelle definieren, um KI-Suche für OT-Incident-Datensätze zu verwenden. Weitere Informationen zur Indexierung finden Sie unter [Indexed sources in AI Search](#).

Hinweis:

Knowledge [kb_know] wird auch als indizierte Quelle für Recommended Actions for OSTM verwendet, Knowledge ist jedoch bereits indiziert.

Um indizierte Quellen zu definieren, können Sie Geführtes Setup für KI-Suche verwenden. Im folgenden Verfahren wird beschrieben, wie Sie auf die Aufgabe **Indizierte Quellen definieren** zugreifen. Weitere Informationen zu Geführtes Setup für KI-Suche finden Sie unter [Configuring AI Search](#).

Prozedur

1. Navigieren zu **KI-Suche > Geführtes Setup**.
2. Wählen Sie im Abschnitt „**Durchsuchbaren Inhalt definieren**“ die Aufgabe **Indizierte Quellen definieren aus**.
3. Wählen Sie **Konfigurieren**.
4. Wählen Sie in der Liste „**Indizierte Quellen der KI-Suche**“ den OT Incident-Datensatz aus.
5. Klicken Sie auf die Schaltfläche **Ausgewählte Tabelle(n) indizieren**.

[End]

[store-future: BEGIN review]

Empfohlene Aktionen für Operational Technology Service Management verwenden

Nachdem Sie alle erforderlichen Setup-Aufgaben für Empfohlene Aktionen für Operational Technology Service Management (OTSM) abgeschlossen haben, können Benutzer mit der Verwendung empfohlener Aktionen für OT-Incidents beginnen.

[End]

[store-future: BEGIN review]

Wenden Sie Empfohlene Aktionen auf Ihre Operational Technology Incidents an

Wenden Sie Empfohlene Aktionen auf Ihre Operational Technology (OT)-Incidents an, um Benutzern basierend auf dem Kontext eines OT-Incident-Datensatzes relevante Aktionen anzuzeigen.

Vorbereitungen

Erforderliche Rolle: sn_ot_incident_write

Hinweis:

Sie können die empfohlenen Aktionen für einen OT-Incident nur anzeigen, wenn sich der OT-Incident auf eine Site bezieht, auf die Sie Zugriff haben, oder wenn der Incident sich nicht im Status „**Geschlossen**“ oder „**Abgebrochen**“ befindet.

Warum und wann dieser Vorgang ausgeführt wird

Sie können den Bereich Empfehlungen und die KI-Suche verwenden, wenn Sie einen OT-Incident-Datensatz anzeigen, um relevante Aktionen im Zusammenhang mit Ihrem Incident anzuzeigen und auszuwählen.

Weitere Informationen zu empfohlenen Aktionen finden Sie unter [Using the Recommended Actions application](#) .

Prozedur

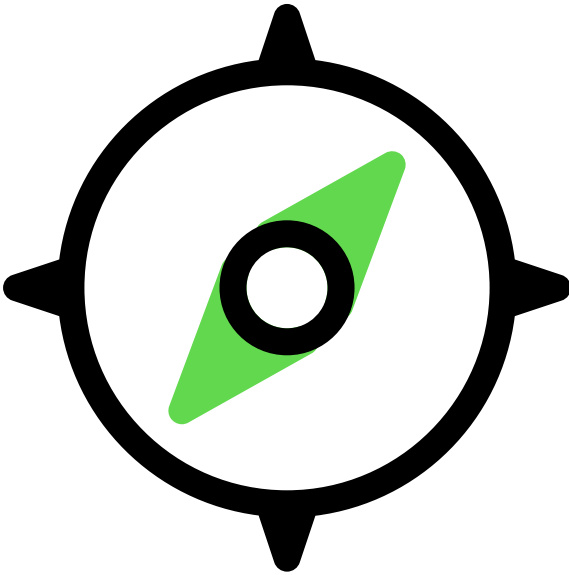
1. Navigieren zu **Alle > Industrial Workspace**.
2. Öffnen Sie die Listenansicht Industrial Workspace.
3. Wählen Sie im Listenmodul OT Incidents eine der verfügbaren Listen aus.
4. Öffnen Sie den Incident-Datensatz, für den Sie die empfohlenen Aktionen überprüfen möchten.
5. Wählen Sie das Symbol **Empfohlene Aktionen** () aus.
6. Überprüfen Sie im Bereich **Empfehlungen** die empfohlenen Aktionen, und wählen Sie sie aus.

[End]

Operational Technology Manager

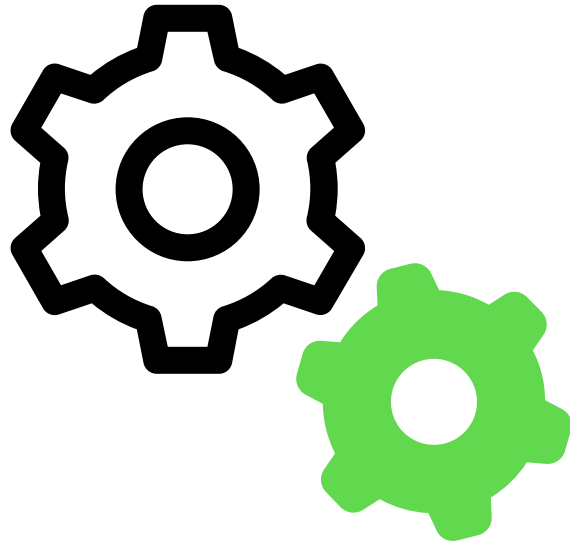
Die Anwendung Operational Technology Manager erstellt die grundlegenden Daten und Beziehungen, die es Ihrer Organisation ermöglichen, die Lösung ServiceNow® Operational Technology zu verwenden. Operational Technology Manager unterstützt die Verwendung der Anwendungen Configuration Management Database (CMDB), Service Graph Connectors und Discovery in Now Platform.

Untersuchen



Erfahren Sie, wie Hersteller den verwenden
Operational Technology Manager

Konfigurieren



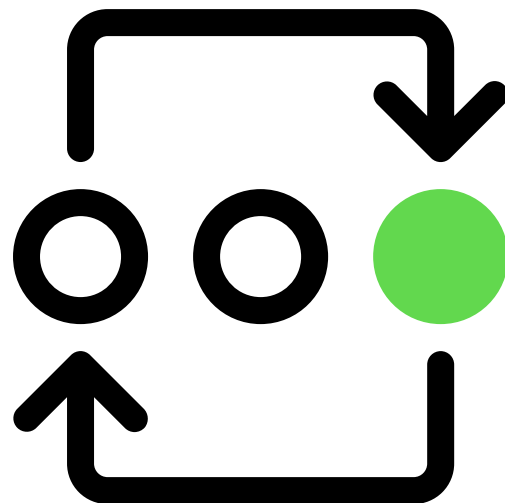
Planen und konfigurieren
Sie Ihre -Implementierung

Verwenden



Sie können Operational Technology-Geräte
importieren, erkennen und überprüfen

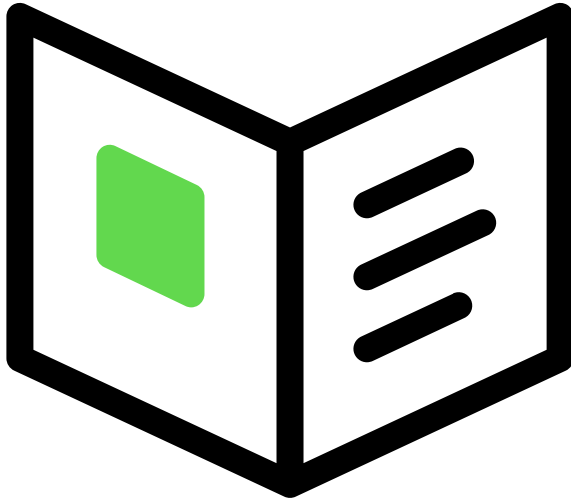
integrieren



Erweitern Sie Operational Technology Manager
durch die Integration mit anderen Anwendungen

Automatische Übersetzung

Referenz



Erhalten Sie Details zu zugehörigen
Informationen und Anwendungen.

Operational Technology Manager erkunden

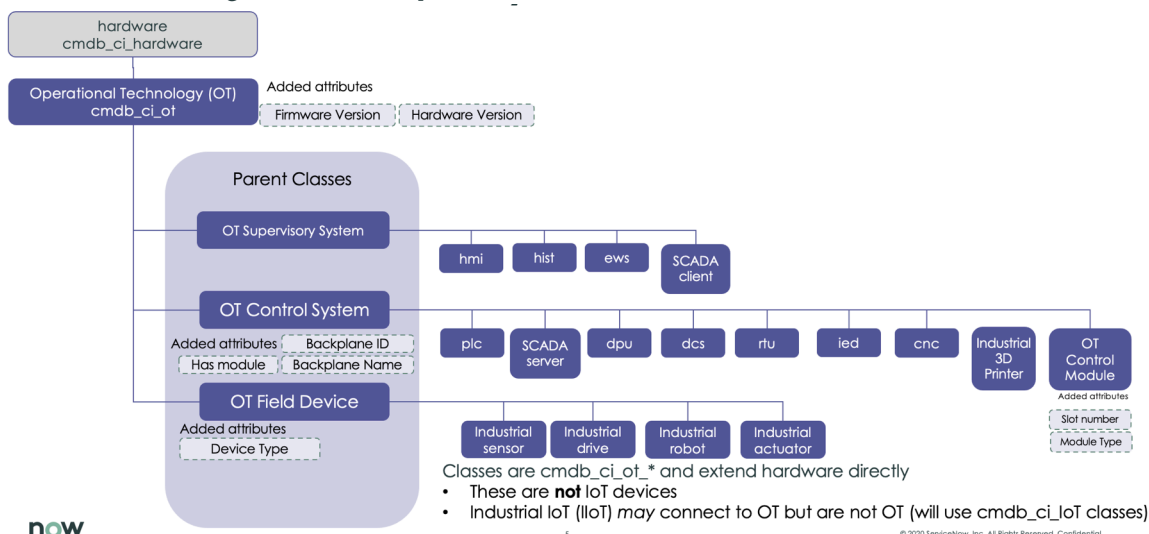
Erfahren Sie, wie Sie mit der Anwendung Operational Technology Manager die grundlegenden Daten und Beziehungen erstellen können, die Ihr Unternehmen für die Nutzung der Lösung ServiceNow® Operational Technology benötigen.

Operational Technology Manager unterstützt die Verwendung der Anwendungen Configuration Management Database (CMDB), Service Graph Connectors und Discovery in Now Platform.

Operational Technology Manager (OT) Configuration Item-Erweiterungsklassen

Operational Technology Manager verwendet Operational Technology (OT) Configuration Item (CI)-Erweiterungsklassen, die die Klassenhierarchie CMDB erweitern (siehe folgende Abbildung).

OT-CI-Erweiterungsklassen entsprechen OT-Geräten



Operational Technology Manager enthält Klassenbeschreibungen, Identifizierungsregeln, Identifier-Einträge und abhängige Beziehungen, falls zutreffend. Die Anwendungen Service Graph verwenden diese Klassenerweiterungen, um CIs auszufüllen und verschiedene Technologien und Software zu erkennen. Weitere Informationen finden Sie [unter Erweiterungsklassen für Operation Technology \(OT\)](#).

CMDB-CI-Klassen für Operational Technology Manager

Operational Technology Manager fügt diese Configuration Management Database (CMDB) Configuration Item (CI)-Klassen hinzu, die Teil der Anwendung CMDB CI Class Models (CMDB CI-Klassenmodelle) sind.

i Hinweis:

Weitere Informationen zu dieser Anwendung finden Sie unter der Anwendung CMDB CI-Klassenmodelle im [ServiceNow ServiceNow](#).

CMDB-CI-Klassen für Operational Technology Manager -Workflows

Klasse	Beschreibung	CI-Klasse erweitert
Erkennungssystem für Netzwerkangriffe	Die Klasse des Netzwerkangriffserkennungssystems (Network Intrusion Detection System, NIDS) [cmdb_ci_nids] erstellt die Beziehungen zwischen passiven Netzwerküberwachungsgeräten und den Geräten im Netzwerk, die erkannt werden.	cmdb_ci_nids

Import und Erkennung von OT-Gerät-Daten

Zum Hochladen Ihrer vorhandenen Operational Technology -Gerätedaten in Now Plattform stehen mehrere Methoden zur Verfügung.

Service Graph Connector (Excel)

Sie können die Funktion Service Graph Connector (Excel) verwenden, um Ihre Daten Operational Technology aus einer ausgefüllten Excel-Tabelle Microsoft Azure

Event Hubs zu importieren. Sie verwenden die Tabelle in IntegrationHub Transformationslast extrahieren (ETL), um diese Daten in CMDB hochzuladen. Weitere Informationen finden Sie unter [Service Graph Connector für Operational Technology \(Excel\)](#).

Discovery für Operational Technology

Um Operational Technology -Geräte in festgelegten Purdue-Ebenen in Ihren ICS-Netzwerken (Industrial Control System) zu erkennen, führen Sie die Funktion Discovery für Operational Technology regelmäßig aus. Er funktioniert ähnlich wie die Standardprozesse Discovery. Der Discovery findet jedoch normalerweise in den Purdue-Ebenen 3 bis 3.5 statt, je nachdem, welche Ebene Sie beim Erstellen eines OT-Discovery-Zeitplans auswählen. Weitere Informationen finden Sie unter [Discovery für Operational Technology](#).

i Hinweis:

Weitere Informationen zu Purdue-Ebenen in Industrial Control Systems finden Sie unter https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lv1sec10/the-purdue-model-for-industrial-control-systems .

Service Graph Connectors von ServiceNow Partnern

ServiceNow Partner bieten auch Service Graph Connectors an, mit denen Sie Ihre vorhandenen OT-Daten hochladen können.

Unterschiede zwischen OT- und Standard-IT-Netzwerken

Es gibt Unterschiede im Umgang mit Geräten in Operational Technology Configuration Management Database (CMDB) -Netzwerken und in Standard-IT-Netzwerken (Information Technology).

Konfigurationselemente (CIs), die unter Information Technology Operations Management (ITOM) verwaltet werden, werden in CMDB als Typ IT klassifiziert. Sie existieren auf den Ebenen 4 und 5 des Purdue-Modells oder auf der Unternehmensebene.

Geräte, die unter dem OT-Datenmodell verwaltet werden, befinden sich auf den Ebenen 0 bis 3,5 des Purdue-Modells, und es gibt zwei Hauptkomponenten von OT-Geräten:

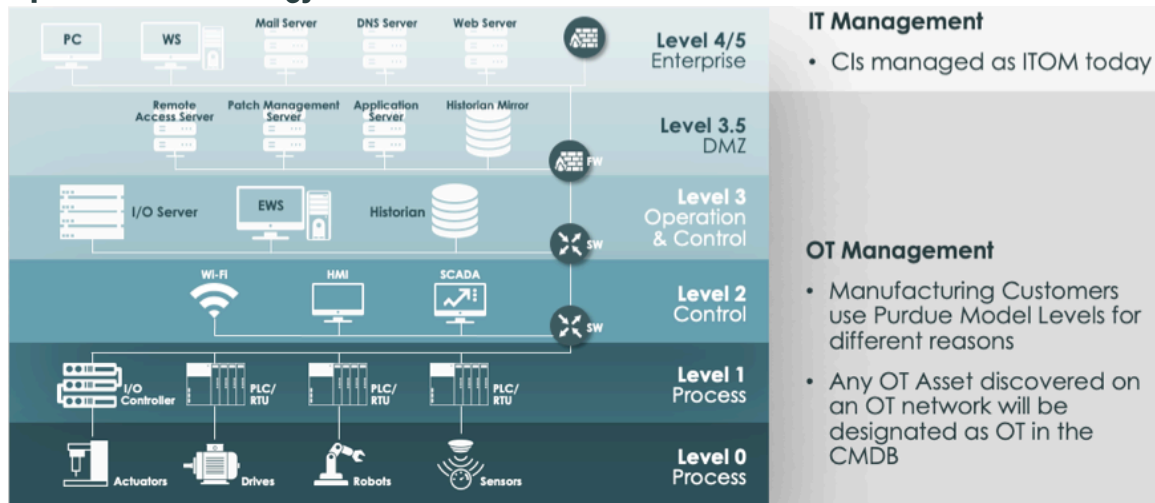
1. Ein CI-Klassendatensatz. Dies kann ein IT- oder ein OT-Klassen-CI sein.
2. Ein OT-Gerät-Detaildatensatz. Dies beschreibt den OT-Gerät-Typ (Funktion) und andere OT-spezifische Attribute.

i Hinweis:

Weitere Informationen zum OT-Datenmodell und zu den Erweiterungsklassen finden Sie unter [Operational Technology \(OT\) extension classes](#) .

Die folgende Grafik veranschaulicht diese Unterschiede.

Operational Technology CMDB Klassenmodelle unterstützen Purdue-Ebenen



i Hinweis:

Weitere Informationen zu Purdue-Ebenen finden Sie unter https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lv1sec10/the-purdue-model-for-industrial-control-systems.

Operational Technology Manager konfigurieren

Konfigurieren Sie die Anwendung Operational Technology Manager, um die Datengrundlage für die Lösung ServiceNow® Operational Technology zu erstellen.

Aufgabe	Zweck
1. Installieren Sie Erweiterungsklassen für Operational Technology (OT).	Erweitern Sie die Klassenhierarchie Configuration Management Database (CMDB) zur Verwendung bei der Verarbeitung von Operational Technology.
2. Installieren Sie Operational Technology Manager.	Installieren Sie die Anwendung Operational Technology Manager.
3. Weisen Sie Operational Technology Rollen zu.	Weist Rollen zu, um die für jeden Benutzer verfügbaren Aktionen zu steuern.
4. Bereiten Sie eine Microsoft Azure Event Hubs Excel-Tabelle für den Import von Service Graph Connector vor.	Erstellen Sie eine Excel-Tabelle Microsoft Azure Event Hubs, und füllen Sie sie mit Ihren vorhandenen Daten Operational Technology aus, um sie in Now Plattformhochzuladen. Weitere Informationen finden Sie unter Bereiten Sie Ihr Tool zur Überprüfung von OT-Arbeitsblatteinträgen vor dem Import für den Import von Service Graph Connector vor.
5. Importieren Sie Ihre Excel-Tabelle.	Laden Sie Ihre Operational Technology -Daten in Configuration Management Database (CMDB)hoch. Weitere Informationen finden Sie unter Importieren Sie die Excel-Vorlage.

Aufgabe	Zweck
6. Führen Sie die Funktion Discovery für Operational Technology aus.	Erkennen Sie Operational Technology (OT)-Geräte in den festgelegten Purdue-Ebenen in Ihren ICS-Netzwerken (Industrial Control System). Weitere Informationen zu Discovery für Operational Technology finden Sie unter Discovery für Operational Technology .
7. Installieren Sie Service Graph Connectors, die von ServiceNow®-Partnern bereitgestellt werden.	Installieren Sie ServiceNow, Inc. -Connectors, die von Partnern bereitgestellt werden, sobald sie in ServiceNow® Store verfügbar sind.
8. Verwenden Sie die Auswahlmöglichkeiten Alle OT-Geräte oder Alle OT-Geräte nach IP-Adresse im Menü Operational Technology (OT) .	Bearbeiten oder zeigen Sie detaillierte Informationen für die OT-Geräte in Ihrem Unternehmen an, nachdem Sie Ihre Excel-Tabelle importiert oder die Funktion Discovery für Operational Technology ausgeführt haben.

Framework CSDM für Operational Technology implementieren

Wenn Sie das CSDM -Framework befolgen, wird sichergestellt, dass Sie Ihr primäres Ziel einer konsistenten Genauigkeit bei Berichten und Analysen erreichen, damit Sie Ihre Operational Technology (OT)-Umgebung effektiv verwalten können.

CSDM Framework für OT

Sie müssen die Implementierung für das -Framework CSDM schrittweise abschließen. Weitere Informationen finden Sie unter [Implementing the CSDM framework in stages](#) .

Operational Technology-Produktübersicht

Operational Technology umfasst Produkte, die Aspekte der Verwaltung von OT-Geräten und Produktionsprozessen in verschiedenen Phasen des Lebenszyklus behandeln. Diese Produktansicht soll Ihnen dabei helfen zu verstehen, wie Operational Technology -Schlüsselentitäten mit dem Core-Framework Gemeinsames Servicedatenmodell (CSDM) funktionieren.

Operational Technology Manager

Erstellt die grundlegenden Daten und Beziehungen, die Ihrem Unternehmen die Verwendung der Lösung Operational Technology ermöglichen. Weitere Informationen finden Sie unter [Operational Technology Manager](#).

Prozessmanager Industrie

Ermöglicht Ihnen das Erstellen der Datengrundlage des Anlagenmodells nach ISA-95, die für die Lösung Operational Technology erforderlich ist. Weitere Informationen finden Sie unter [Prozessmanager Industrie](#).

Operational Technology Vulnerability Response

Ermöglicht die effektive Priorisierung und Behebung von OT-Gerät-Schwachstellen auf Site-Ebene. Weitere Informationen finden Sie unter [Operational Technology Vulnerability Response](#).

Incident-Management für operative Technologie

Ermöglicht Ingenieuren, Probleme mit OT-Geräten und Produktionsprozessen schnell zu lösen. Weitere Informationen finden Sie unter [Incident-Management für operative Technologie](#).

Change-Management für operative Technologie

Ermöglicht Ihrem Unternehmen, Änderungen an OT-Geräten und Produktionsprozessen zu implementieren. Weitere Informationen finden Sie unter [Change-Management für operative Technologie](#).

Knowledge Management für operative Technologie

Ermöglicht Ihrer Organisation, Informationen über Ihr OT-System in Wissensartikeln zu erfassen, die sich auf OT-Incidents beziehen. Weitere Informationen finden Sie unter [Knowledge Management für operative Technologie](#).

Anforderungsmanagement für operative Technologien

Ermöglicht Ihnen den Zugriff auf den OT-Servicekatalog, um OT-Katalogelemente anzufordern und basierend auf den definierten Flows zu erfüllen. OT-Mitarbeiter können dann eine OT-Anforderung aus einem Katalogelement erstellen und übermitteln, was zu einer konsistenten Experience beiträgt und funktionsübergreifende Anforderungen erleichtert. Weitere Informationen finden Sie unter [Anforderungsmanagement für operative Technologie](#).

Operational Technology und CSDM-Tabellen

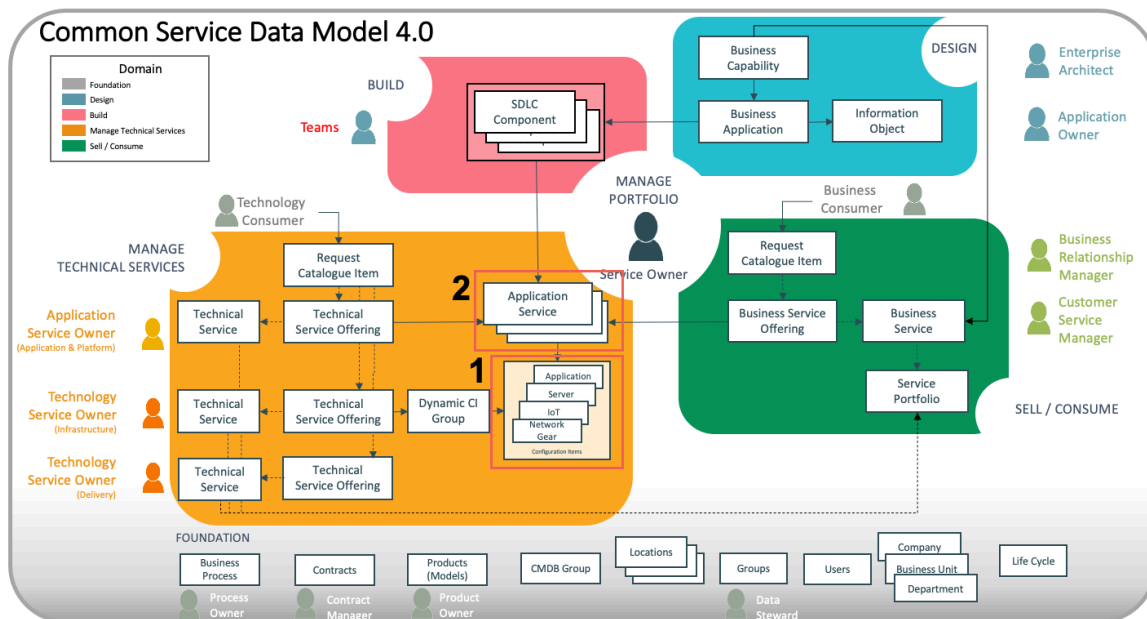
Operational Technology verwaltet und verwendet CSDM-Tabellen. Mehrere ServiceNow-Produkte profitieren von Operational Technology und fügen der Anwendung Mehrwert hinzu.

Von Operational Technology verwaltete CSDM-Tabellen

Es gibt zwei primäre Kategorien von Tabellen, die von Operational Technology (OT) verwaltet werden:

- Operational Technology device: Konfigurationselemente, die in einem OT-Netzwerk (ICS oder PCN) gefunden wurden.
- Entität für Anlagenmodell nach ISA: Industrieprozess automatisiert durch OT-Geräte.

Die Zahlen in dieser Abbildung entsprechen den von CSDM verwalteten Tabellen Incident-Management.

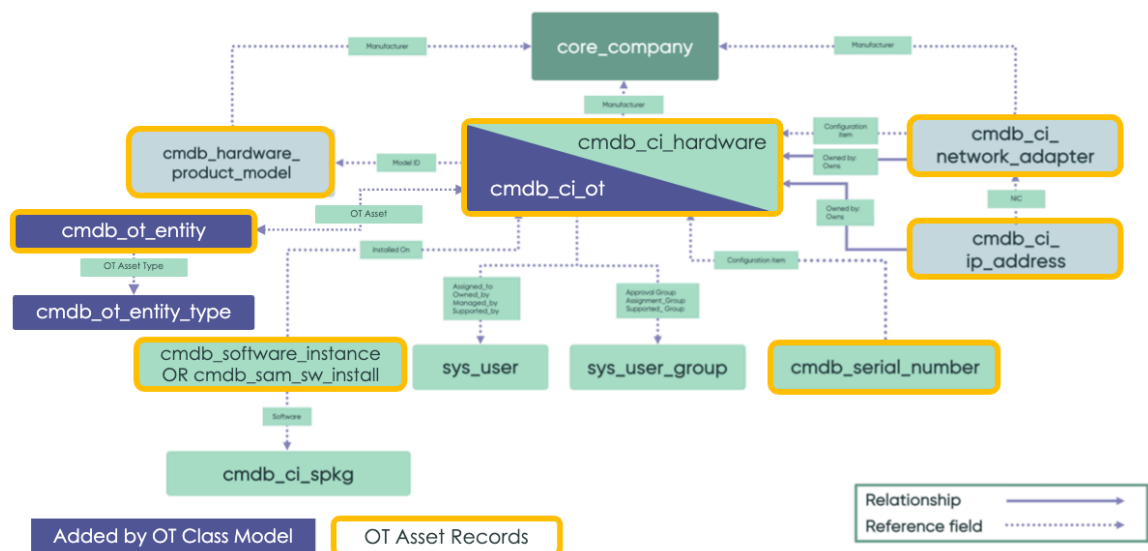


CSDM-Tabellen, die von Operational Technology verwendet werden

1. OT-Geräte:

- a.** Für Operational Technology Hardwareklassen (cmdb_ci_ot) wurden Konfigurationselementklassen durch Erweitern von Hardware erstellt. Details siehe [Operational Technology \(OT\) extension classes](#) .
- b.** Jede CI-Klasse (jede relevante vorhandene Hardwareklasse sowie neue OT-Klassen) kann als OT-Geräte festgelegt werden, indem OT-Gerät-Details unter Verwendung der Referenz OT-Gerät-Details (cmdb_ot_entity) zur Tabelle cmdb_ot_entity hinzugefügt werden. OT-Gerät-Details enthalten OT-spezifische Merkmale wie Purdue-Ebene und OT-Gerät-Typ.
- c.** OT-Gerät-Typen beschreiben die Funktion jedes CI, das einen Industrie- oder Produktionsprozess automatisiert. Die Tabelle cmdb_ot_entity_type beschreibt diese Funktionen oder Rollen.

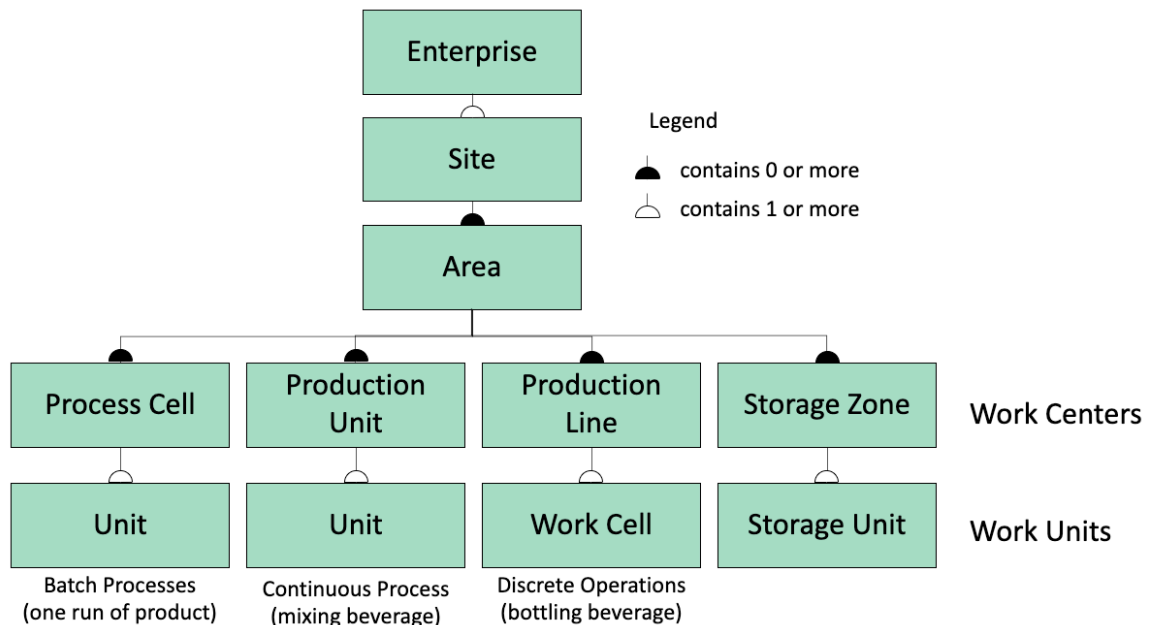
Wie hier gezeigt, wird ein einzelnes OT-Gerät durch mindestens zwei Datensätze dargestellt: einen CI- und einen OT-Entitätsdatensatz. Das Gerät kann sechs oder mehr Datensätze in bis zu sechs Tabellen enthalten (z. B. wenn das CI mehr als eine IP- und MAC-Adresse hat).



2. Anlagenmodell-Entitäten:

- a. Die Anlagenmodell-Entitätsklasse erweitert den berechneten Anwendungsservice und wird verwendet für:
 - i. Stellen Sie den Standort einer beliebigen OT-Gerät- oder Anlagenmodell-Entität dar. Ein Datensatz in der Tabelle „Anlagenmodell-Entität“ (cmdb_ci_ot_isa_entity) ohne übergeordnetes Element wird als Site betrachtet.
 - ii. Stellt die Entität des Anlagenmodells nach ISA für einen Teil des Produktionsprozesses dar.
- b. Sie können Anlagenmodell-Vorlagen (isa_entity_template) verwenden, um die Beziehungen zwischen Anlagenmodell-Entitäten in einer industriellen Umgebung genauer zu beschreiben.

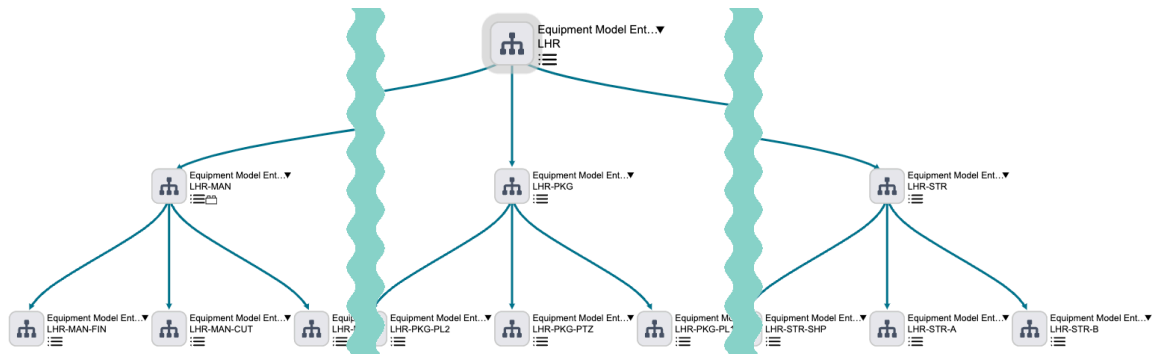
- i. Ebenen (isa_entity_level) beschreiben die hierarchische Ebene der Anlagenmodell-Entität. Bei der Standardvorlage ISA-95 sind die hier gezeigten Ebenen (Bereich, Arbeitsplatz und Arbeitseinheiten) in Basissystemen enthalten.
- ii. Ebenentypen (isa_entity_type) beschreiben die Art des Prozesses, der von den Anlagenmodell-Entitäten auf einer bestimmten Ebene dargestellt wird. Für die Standardvorlage ISA-95 sind die hier gezeigten Typen (Prozesszelle, Produktionseinheit, Produktionslinie und Lagerzone) in Basissystemen enthalten.



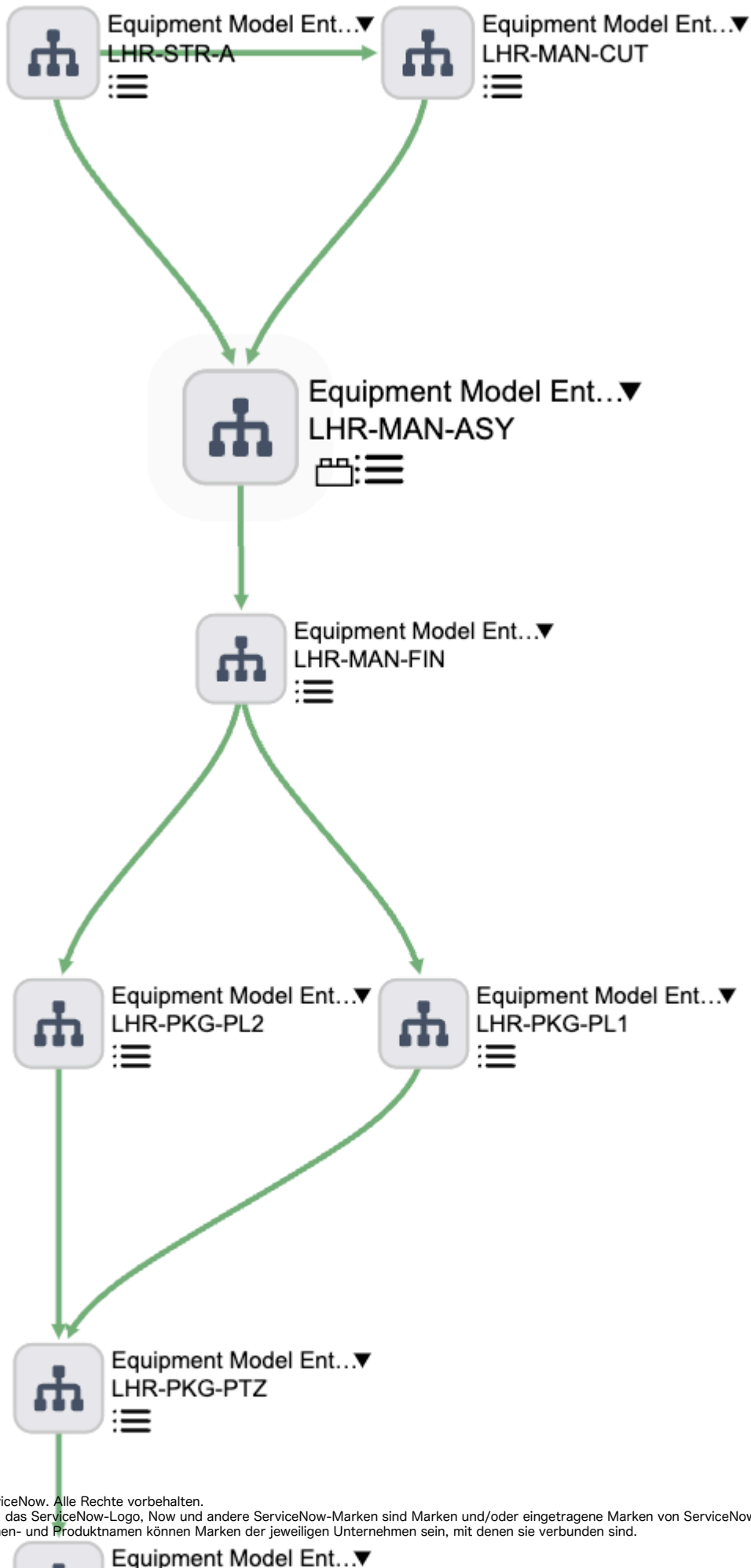
CSDM enthält Beziehungstypen (spezifisch für Operational Technology), die genauer unterscheiden, wie OT-Geräte und Anlagenmodell-Entitäten miteinander in Beziehung stehen:

- **Ersteller für::Verbraucher von:** Beschreibt den Produktionsprozess (Materialfluss) zwischen Anlagenmodell-Entitäten.
- **Enthält Element::Element von:** Beschreibt die hierarchische Beziehung zwischen Anlagenmodell-Entitäten.
- **Automatisiert von::Automatisiert:** Beschreibt die Beziehung zwischen einem OT-Gerät und einer Anlagenmodell-Entität, die das OT-Gerät automatisiert.
- **Erkennt::Erkannt von:** Beschreibt, welche NIDS-Klasse (Network Intrusion Detection System) (cmdb_ci_nids) ein OT-Gerät in einem OT-Netzwerk erkannt hat.
- **Besitzt::Im Besitz von:** Beschreibt die Beziehung, wenn ein OT-Steuerungsmodul im Besitz eines OT-Steuerungssystems ist (SPS, DCS usw.)

Die folgenden Abhängigkeitskarten zeigen die Beziehungen zwischen OT-Geräten und Anlagenmodell-Entitäten:



Automatische Übersetzung



Automatische Übersetzung

Produkte, die Operational Technology Mehrwert hinzufügen

Wenn Sie OT mit einem der folgenden ServiceNow -Produkte verwenden, erhöhen Sie den Wert, den Sie von OT erhalten.

Discovery für Operational Technology

Discovery für Operational Technology enthält Details zu IT-klassifizierten Hardware- und Software-CIs und kann so konfiguriert werden, dass zusätzlicher OT-Gerätekontext wie Purdue-Ebene und Standort auf einer Pro-OT-Zeitplanbasis bereitgestellt werden. Discovery für OT ist Teil des Produkts Operational Technology Manager.

Prozessmanager Industrie

Wenn OT-Geräte einer Anlagenmodell-Entität zugewiesen werden, werden *automated by::automates* -Beziehungen zwischen ihnen erstellt. Dies kann manuell in Industriell Arbeitsbereich erfolgen oder über die Beziehung zwischen OT-Subnetzen und Anlagenmodell-Entitäten mithilfe der Funktion Automatische Zuordnung über zonenbasierte IP-Netzwerkgruppen hinweg (AMAZING) im Menüelement OT-Subnetz-zuordnung.

Operational Technology Vulnerability Response

Wenn Datensätze für angreifbare Elemente (VIT) durch Importieren von Datensätzen aus einer OT-zertifizierten Integration mit einer Drittanbieter-Sicherheitsplattform erstellt werden, werden OT-Geräte dem VIT zugeordnet. Dadurch werden die beiden folgenden Fähigkeiten aktiviert:

- Risikoberechnung basierend auf der Relevanz der zugeordneten Anlagenmodell-Entität.
- Zuweisung von VITs an das entsprechende lokale Team zur Korrektur über standortbasierte Zuweisungsgruppen.

Incident-Management für operative Technologie

Incident-Management für OT wird für die meisten OT-Geräte getrennt von IT ausgeführt. OT-Incident-Datensätze ermöglichen einen standortbasierten Zugriff und Ansichten für Probleme, die sich auf OT-Geräte beziehen.

Change-Management für operative Technologie

OT-Change-Anforderungen ermöglichen Änderungen an OT-Geräten oder industriellen Anlagenkonfigurationen.

Knowledge Management für operative Technologie

Knowledge Management für operative Technologie Mit können Sie Informationen über Ihr OT-System in Wissensartikeln erfassen, die sich auf OT-Incidents beziehen.

Anforderungsmanagement für operative Technologien

Ermöglicht Ihnen den Zugriff auf den OT-Servicekatalog, um OT-Katalogelemente anzufordern und basierend auf den definierten Flows zu erfüllen. OT-Mitarbeiter können dann eine OT-Anforderung aus einem Katalogelement erstellen und übermitteln, was zu einer konsistenten Experience beiträgt und funktionsübergreifende Anforderungen erleichtert.

Produkte, die von Operational Technology profitieren

IT Service Management (ITSM)

Services erhalten den Kontext des Standorts, des Produktionsprozesses und der OT-Geräte sowie die zugrunde liegenden Informationen und Technologien.

Information Technology Operations Management (ITOM)

Versteht den Geschäftskontext für die Produktionsprozesse zusammen mit der verwalteten OT-Gerät-Hardware und -Software.

Security Operations

Versteht den Geschäftskontext für die Produktionsprozesse sowie die zu sichernde OT-Gerätehardware und -software.

Governance, Risk und Compliance (GRC)

Auditoren können Produktionsprozess-Flows und zugehörige Informationsobjekte besser nutzen. Das hilft Auditoren, zur Designzeit die Sensibilität der Daten zu verstehen, um den Auditumfang zu definieren, Risiken zu messen und Auditaktivitäten zu verwalten.

Asset-Management

Verwaltet die Auswirkungen des Software- und Hardware-Lebenszyklusprozesses auf die Produktionsprozesse.

Operational Technology Manager – Anwendungsfall

In diesem Abschnitt werden die Anwendungsfälle Operational Technology Manager beschrieben.

Operational Technology Manager – Anwendungsfall

Die Anwendung Operational Technology Manager erstellt die grundlegenden Daten und Beziehungen, die Ihrem Unternehmen die Verwendung der Lösung Operational Technology ermöglichen. Es unterstützt die Verwendung der Anwendungen Configuration Management Database (CMDB), Service Graph Connectors und Discovery in Now Platform.

Das OT-Transparenz-Dashboard in Industrial Workspace fasst Ihren OT-Gerätebestand zusammen. Weitere Informationen zum Dashboard finden Sie unter [Operational Technology Transparenz-Dashboard](#).

Schlüsselfunktionen

- Operational Technology Manager verwendet Erweiterungsklassen für OT Configuration Item (CI), die die Klassenhierarchie CMDB erweitern.
- Discovery für OT ist auf OT-spezifische Rollen beschränkt, und OT-bezogene Metadaten können einem OT-Discovery-Zeitplan hinzugefügt werden.
- Der Connector Service Graph (Excel) importiert OT-Daten aus einer ausgefüllten Microsoft Excel-Faltdatentabelle. Diese Daten werden validiert und dann in die entsprechenden Tabellendatensätze und -beziehungen umgewandelt, um OT-Geräte-Details in CMDB darzustellen.

Ergebnisse

Mit dem Anwendungsfall Operational Technology Manager können Sie:

- Visualisieren Sie Abhängigkeiten von OT-Geräten in der industriellen Umgebung.
- Verwalten Sie den Lebenszyklus von OT-Geräten für jeden Standort mit einem standortspezifischen RBAC
- Erstellen Sie eine solide Datengrundlage, und definieren Sie kritische Infrastrukturebenen.

Prozessmanager Industrie – Anwendungsfall

Verwenden Sie die Anwendung Prozessmanager Industrie, um die Datengrundlage des Anlagenmodells nach ISA-95 zu erstellen, die für die Lösung Operational Technology erforderlich ist.

Schlüsselfunktionen

Im Arbeitsbereich Prozessmanager Industrie können Sie die folgenden Vorgänge ausführen:

- Verwenden Sie ISA-95-Modelle, um den Produktionsprozess an jedem Standort in der industriellen Umgebung zu beschreiben.
- Verwalten Sie Anlagenmodell-Entitäten und ihre Beziehungen untereinander und zu OT-Geräten.
- Ordnen Sie die Beziehung aller OT-Geräte automatisch der Anlagenmodell-Entität zu, die mithilfe der Beziehung zwischen OT-Subnetz und Anlagenmodell-Entität automatisiert wird.

Ergebnisse

Mit Prozessmanager Industrie können Sie eine anwenderdefinierte Version der Anlagenmodelle an jedem Ihrer Sites erstellen.

Operational Technology Vulnerability Response – Anwendungsfall

Operational Technology Vulnerability Response Mit können Sie OT-Geräte-Schwachstellen auf Site-Ebene effektiv priorisieren und beheben.

Schlüsselfunktionen

- Der Arbeitsbereich des Korrekturverantwortlichen ordnet angreifbare Elemente (VITs) dem Produktionsprozess zu.
- Die Risikoberechnung für OT VITs kann auf der Relevanz der vom OT-Gerät automatisierten Anlagenmodell-Entität basieren.
- Automatische Zuweisung von VITs zu Korrekturbesitzern basierend auf der Site, die dem OT-Gerät mit der VIT zugewiesen ist.

Ergebnisse

Durch die Nutzung der CMDB -Beziehungen von OT-Geräten können Sie angreifbare Geräte oder Elemente basierend auf der Relevanz des von ihnen automatisierten Produktionsprozesses priorisieren.

Als OT-Ingenieur oder OT-Schwachstellenmanager können Sie Operational Technology Vulnerability Response mit Antworten auf folgende Fragen finden:

- Was sind meine OT-Geräte-Schwachstellen?☒
- Wie kann ich die Nachbesserung von Schwachstellen mit OT-spezifischem Risiko priorisieren?
- Welche Fortschritte machen wir bei der Behebung von OT-Schwachstellen?

Das OTVR (PA)-Dashboard und das OT-Schwachstellenrisiko-Rollup-Dashboard in Industrial Workspace fassen die Schwachstellen in Ihrem System zusammen. Weitere Informationen zum OTVR (PA)-Dashboard finden Sie unter [Operational Technology Vulnerability Response \(PA\)-Dashboard](#). Weitere Informationen zum Dashboard für OT-Schwachstellenrisiko-Rollup finden Sie unter [Operational Technology Dashboard „Schwachstellenrisiko-Rollup“](#)..

Incident-Management für operative Technologie – Anwendungsfall

OT-Incidents treten auf, wenn eine Serviceunterbrechung durch ein OT-Gerät in einem OT-Netzwerk auftritt. Manchmal ist das OT-Gerät möglicherweise nicht bekannt, wenn der Incident zum ersten Mal erstellt wird. Incident-Management für operative Technologie ermöglicht es Ingenieuren, Probleme mit OT-Geräten und Produktionsprozessen schnell zu lösen.

Schlüsselfunktionen

Wenn ein Benutzer einen OT-Incident aus Industriell Arbeitsbereichen erstellt, wird dem Incident automatisch der Netzwerktyp OT zugewiesen, um einen OT-Incident von einem IT-Incident zu unterscheiden. Das Feld wird standardmäßig nicht angezeigt.

Ergebnisse

Incident-Management für operative Technologie ermöglicht es Ingenieuren, Probleme mit OT-Geräten und Produktionsprozessen schnell zu lösen. Sie können OT-Incidents getrennt von IT-Incidents verwalten.

Change-Management für operative Technologie – Anwendungsfall

Change-Management für operative Technologie Mit können Ihre Teammitglieder gemeinsam an Änderungen an Konfigurationen von OT-Geräten oder Industrieanlagen arbeiten.

Schlüsselfunktionen

- Digitalisierter Change-Workflow, der alle Stakeholder verbindet
- Sites mit unterschiedlichen Change-Management-Prozessen (Workflows).
- IT Change Management und Change-Management für operative Technologie getrennt, aber bei Bedarf kombinierbar.
- Workflow Change-Management für operative Technologie mit den Anwendungen Incident-Management für operative Technologie und Operational Technology Vulnerability Response integriert.
- Ausgerichtete Änderungen der Werksverkaufsfläche für die Anlagenmodell-Entitäten mit Ausfallzeitplänen.

Ergebnisse

Die folgenden Beispiele zeigen, wie Sie Change-Management für operative Technologie auf Ihre Organisation anwenden können:

- Ein Besitzer der OT-Nachbesserung, der für die Behebung von Schwachstellen in OT-Geräten verantwortlich ist, möchte einen Change initiieren, um eine Gruppe von Schwachstellen zu beheben.
- Ein OT-Techniker, der für OT-Konfigurationen und Anlagen-Engineering-Aktivitäten verantwortlich ist, möchte einen Change ausführen, um einen defekten Roboterarm in der Industriewerkstatt zu reparieren.
- Ein Werksleiter, der für die gesamte Produktionsaktivität verantwortlich ist, möchte eine vom Engineering-Team angeforderte Änderung überprüfen und genehmigen.

Knowledge Management für operative Technologie – Anwendungsfall

Knowledge Management für operative Technologie hilft Ihnen, Informationen über Ihr Operational Technology (OT)-System in Wissensartikeln zu erfassen, die sich auf OT-Incidents beziehen. Ihre Organisation kann diese Wissensartikel dann verwenden, um Ihren Anwendern zu helfen, auf die richtigen Informationen zuzugreifen, und Fehlkommunikation mit Ihren Anwendern verhindert.

Schlüsselfunktionen

- Fähigkeit, den vorhandenen Wissensmanagement Funktionen der Now Platform mit der Lösung Operational Technology-Management zu verwenden.
- Möglichkeit, alle Knowledge Base-Artikel zu durchsuchen, die sich auf einen OT-Incident beziehen, und Wissensartikel direkt aus einem Incident-Datensatz zu erstellen.
- Fähigkeit, eine OT-Wissensdatenbank für Wissensmanager und Wissensanwender zu konfigurieren.

- Fähigkeit, Wissensartikel in Industriell Arbeitsbereich zu erstellen.
- Möglichkeit, Genehmigungen zum Veröffentlichen, Bearbeiten, Deaktivieren oder Löschen eines Wissensartikels anzufordern.
- Möglichkeit, vorhandene Wissensartikel mit aktualisierten Informationen zu bearbeiten.

Ergebnisse

Die folgenden Beispiele zeigen, wie Knowledge Management für operative Technologie auf Ihr Team angewendet wird:

- Ein OT-Ingenieur mit mehrjähriger Erfahrung möchte sein Wissen über OT-Geräte an einem Ort für Guide Worker und Nachfolgetechniker erfassen.
- Außendienstmitarbeiter und Techniker, die für den Betrieb des Produktionsprozesses verantwortlich sind, haben ein Problem in der Produktionsanlage festgestellt und benötigen einen Wissensartikel, in dem die Behebung erläutert wird.

Anforderungsmanagement für operative Technologie – Anwendungsfall

Anforderungsmanagement für operative Technologie Mit können Sie auf den OT-Servicekatalog zugreifen, um OT-Katalogelemente anzufordern und basierend auf den definierten Flows zu erfüllen. OT-Mitarbeiter können dann eine OT-Anforderung aus einem Katalogelement erstellen und übermitteln, was zu einer konsistenten Experience beiträgt und funktionsübergreifende Anforderungen erleichtert.

Schlüsselfunktionen

- Bietet eine zentrale Ansicht für die effiziente Verwaltung mehrerer Kataloganforderungen ☒
- Fördert Transparenz, beschleunigt Anforderungsprozesse und minimiert Verzögerungen durch automatische Benachrichtigungen und Genehmigungen.
- Verwaltet das Produkt- und Servicemenü, das Sie zum Erstellen und Aktualisieren von Kataloganforderungen verwenden können.

Ergebnisse

Die folgenden Beispiele zeigen, wie Anforderungsmanagement für operative Technologie auf Ihr Team angewendet wird:

- OT-Ingenieure können OT-Anforderungen für verschiedene OT-Produkte und -Services an einem Ort einreichen und verwalten.
- Ein Werksleiter oder ein Vorgesetzter kann mit dem richtigen Team zusammenarbeiten, um einen im Werk gemeldeten Incident zu beheben.

Operational Technology - und CSDM -Elemente

Begriffe im Zusammenhang mit der Verwaltung von Geschäftsanwendungen mit Elementen von CSDM.

Begriffe aus dem Bereich der operativen Technologie

Benennung	Definition
Anlagenmodell	Die Servicedatensätze, die beschreiben, wie ein Industriebetrieb zur Herstellung einer Ausgabe oder eines Produkts organisiert ist.
Produktionsprozess	Die Beziehungen zwischen Anlagenmodell-Entitäten und den verschiedenen Phasen des Workflows vom Rohmaterial bis zum fertigen Produkt.

Begriffe aus dem Bereich der operativen Technologie (Fortsetzung)

Benennung	Definition
Site	Ein übergeordneter Anlagenmodell-Entitätsdatensatz, der kein übergeordnetes Element hat. Dies ist ein spezieller Anlagenmodell-Entitätsdatensatz, da er verwendet wird, um den OT-Geräten, die der Site zugewiesen sind, Lese- oder Schreibzugriff auf Ebene zuzuweisen.
OT-Gerät (Standortzuweisung)	Die Site-Zuweisung ist für die rollenbasierte Sicherheit (RBAC) von OT-Geräten erforderlich. Dies wird als Auswahllisten-Referenzfeld im Tabellenteil „OT-Gerät-Details“ (cmdb_ot_entity) des OT-Gerät-Datensatzes implementiert, da ein OT-Gerät nur zu einem Standort gehören kann.
OT-Gerät (automatisiert::automatisiert)	Die Beziehung automates::automated by beschreibt, wie das OT-Gerät mit dem Produktionsprozess zusammenhängt, der mehr als eine Anlagenmodell-Entität enthalten kann.
Windows	Sowohl in OT- als auch in IT-Netzwerken wird der Server Windows im cmdb_ci_win_server-Server dargestellt. Darüber hinaus hat der Server Windows im OT-Netzwerk eine Referenz im Feld „cmdb_ci_win_server.cmdb_ot_entity“, die auf einen Datensatz in der Tabelle „cmdb_ot_entity“ verweist, der seine Funktion in OT und andere OT-Merkmale wie Purdue-Ebene, Site usw. beschreibt.

Operational Technology Häufig gestellte Fragen

Bei der Implementierung des Frameworks CSDM haben Sie möglicherweise Fragen.

Was ist der Unterschied zwischen einem Produktionsprozess und einer Anlagenmodell-Entität?

Anlagenmodell-Entitäten sind die Servicedatensätze, die verwendet werden, um zu beschreiben, wie ein Industriebetrieb zur Herstellung einer Ausgabe oder eines Produkts organisiert ist. Der Produktionsprozess beschreibt die Beziehungen zwischen Anlagenmodell-Entitäten als Materialflows vom Roheingabematerial zum fertigen Produkt.

Was ist eine Website?

Ein Standort ist ein übergeordneter Anlagenmodell-Entitätsdatensatz, der selbst kein übergeordnetes Element aufweist. Eine Site ist ein spezieller Anlagenmodell-Entitätsdatensatz, da er verwendet wird, um den OT-Geräten, die der Site zugewiesen sind, Lese- oder Schreibzugriff auf Ebene zuzuweisen.

Warum verfügt ein OT-Gerät sowohl über eine Standortzuweisung als auch über -Beziehungen::Automatisiert durch?

Die Standortzuweisung ist für die rollenbasierte Sicherheit (RBAC) der OT-Geräte erforderlich. Dies wird als Auswahllisten-Referenzfeld im Tabellenteil „OT-Gerät-Details“ (cmdb_ot_entity) des OT-Gerät-Datensatzes implementiert, da ein OT-Gerät nur zu einem Standort gehören kann.

Die Beziehung *automates::automated by* beschreibt, wie das OT-Gerät mit dem Produktionsprozess zusammenhängt, der mehr als eine Anlagenmodell-Entität enthalten kann.

Was ist der Unterschied zwischen einem Windows -Server in einem OT-Netzwerk und einem in einem IT-Netzwerk?

In beiden Netzwerktypen wird der Server Windows durch den Server `cmdb_ci_win_server` dargestellt. Darüber hinaus hat der Server Windows im OT-Netzwerk eine Referenz im Feld „`cmdb_ci_win_server.cmdb_ot_entity`“, die auf einen Datensatz in der Tabelle „`cmdb_ot_entity`“ verweist, der seine Funktion in OT und andere OT-Merkmale wie Purdue-Ebene, Site usw. beschreibt.

Operational Technology Installation von Erweiterungsklassen für (OT).

Sie müssen die Erweiterungsklassen Operational Technology (OT) installieren, die die Grundlage von Operational Technology Manager bilden.

Diese Klassenmodelle erweitern die Klassenhierarchie Configuration Management Database (CMDB), die Klassenbeschreibungen, Identifizierungsregeln, Identifizierungseinträge und abhängige Beziehungen enthält, falls zutreffend. Anwendungen wie die Connectors Discovery und Service Graph verwenden diese Klassenerweiterungen, um CIs zu füllen und verschiedene Technologien und Software zu erkennen.

Weitere Informationen finden Sie [unter Erweiterungsklassen für operative Technologie \(OT\)](#). 

Operational Technology Manager installieren

Wenn Sie über die Administratorrolle verfügen, können Sie die Anwendung Operational Technology Manager installieren. Die Anwendung enthält Demodaten und Installationen, bei denen es sich um zugehörige ServiceNow® Store -Anwendungen und -Plugins handelt, sofern sie nicht bereits installiert sind.

Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter [Rufen Sie eine Berechtigung für ab ServiceNow Produkt oder Anwendung](#) .

Hinweis:

Weitere Informationen zu den für Operational Technology Manager erforderlichen Abonnements finden Sie [unter Abonnements für Operational Technology Management \(OTM\)](#)

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

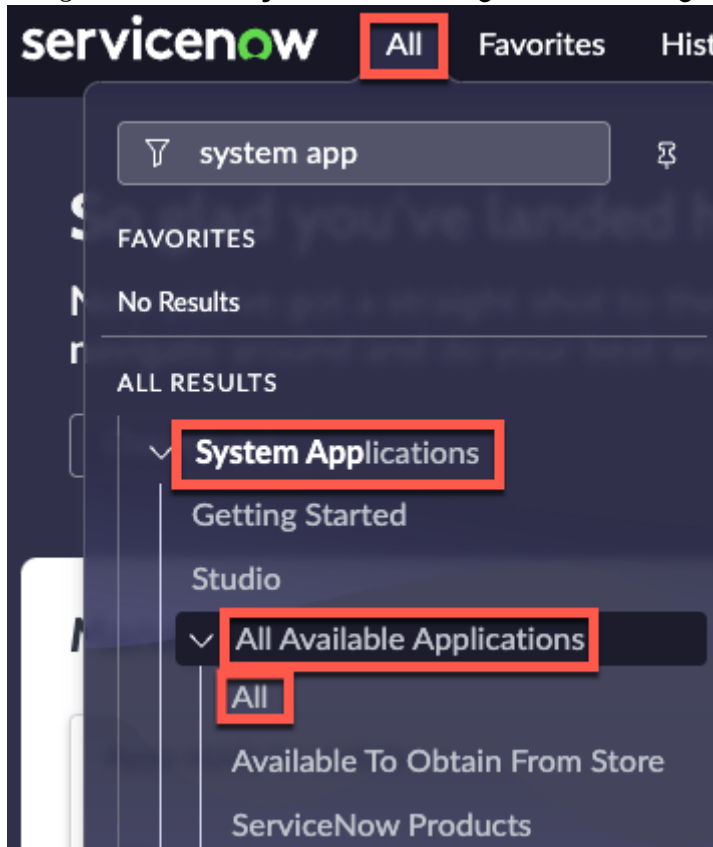
Die folgenden Elemente werden mit Operational Technology Manager installiert:

- Plugins
- Store-Anwendungen
- Rollen
- Tabellen
- Skripteinbindungen

Weitere Informationen zum Anzeigen von mit Operational Technology Manager installierten Komponenten finden Sie unter [Mit Operational Technology Manager installierte Komponenten](#).

Prozedur

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



2. Suchen Sie die Anwendung Operational Technology Manager über die Filterkriterien und die Suchleiste.

Sie können nach der Anwendung anhand ihres Namens oder ihrer ID suchen. Wenn Sie die 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. Überprüfen Sie im Dialogfeld „Anwendungsinstallation“ die Anwendungsabhängigkeiten.

Abhängige Plugins und Anwendungen werden angezeigt, wenn sie installiert werden, derzeit installiert sind oder installiert werden müssen. Wenn Plugins oder Anwendungen installiert werden müssen, müssen Sie diese Installation durchführen, bevor Sie Operational Technology Manager installieren können.

4. **Wahlweise:** Wenn Demodaten verfügbar sind und Sie diese installieren möchten, aktivieren Sie das Kontrollkästchen **Demodaten laden**.

Demodaten sind Beispieldatensätze, die Anwendungsfunktionen für die gängigen Anwendungsfälle veranschaulichen. Laden Sie die Demodaten, wenn Sie die Anwendung zum ersten Mal auf einer Entwicklungs- oder Testinstanz installieren.

i Wichtig:

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

5. Wählen Sie **Installieren** aus.

Mit Operational Technology Manager installierte Skripteinbindungen

Mit dem Plugin Operational Technology Manager werden die folgenden Skripteinbindungen installiert.

Name	Beschreibung
BaseDAO	Basis-DAO-Klasse, die von allen DAO-Klassen erweitert werden soll.
NIDSUtils	Dienstprogramme für cmdb_ci_nids-Geräte.
OTDevicesMigrationUtils	Migrieren Sie Datensätze aus den angegebenen Klassen in aktualisierte Klassentabellen. Weitere Informationen finden Sie unter Operational Technology (OT)-Erweiterungsklassen .
OTDevice	Implementierungsklasse zum Ausführen von Vorgängen in der Tabelle [cmdb_ot_entity] und den zugehörigen Tabellen [cmdb_ci] und [cmdb_rel_ci].
OTDeviceDAO	Utilities zur Unterstützung bei der Verwendung von Discovery für Operational Technology -Geräte.
OTBaseDAO	Basis-DAO-Klasse, die alle DAO-Klassen in Operational Technology erweitern sollen.
OTGrundlagenKonstanten	Eine Sammlung von Konstanten, die von anderen Skripteinbindungen verwendet werden.
OTUtils	Eine Sammlung von Operational Technology Dienstprogrammmethoden.
SGOTDeviceConstants	Eine Sammlung von Konstanten, die von Operational Technology Service Graph Connectors verwendet werden.
SGOTDeviceTransformUtil	Eine Sammlung von Transformationsdienstprogramm-Methoden für Operational Technology Service Graph Connectors.
SGOTDataStreamBase	Basismuster zum Aufrufen eines bestimmten Datenstroms mit den angegebenen Eingaben.
SGOTroubleSkillHelper	Hilfsmethoden zum Validieren der Konfigurationen von Service Graph Connector.
OTAassetFilterAjax	Ein Dienstprogramm-Client-Skript zum Herausfiltern von Anwendungsdatensätzen und OT-Steuerungsmodulen aus der Listenansicht „Alle OT-Geräte“ in Industriell Arbeitsbereich.
OTBulkEditHandler	Serverseitiges Skript zur Verarbeitung der Massенbearbeitung von IT in OT und der Massенbearbeitung von OT-Gerät-Details, die über

Name	Beschreibung
	die Flow-Aktionen und geplanten Aufgaben ausgelöst werden.
Erweiterungspunkte	
SGOTDeviceImportExtensionPoint	SG-OT-Geräteimport-Erweiterungspunkt, der zwei Methoden enthält: 1. getDeviceCMDBClassNameWithSysId; 2. getComputerType.

Weisen Sie Operational Technology Manager Rollen zu

Weisen Sie Ihren Benutzern Rollen zu, damit Sie ihren Zugriff auf die Funktionen, Fähigkeiten und Daten in der Anwendung Operational Technology Manager steuern können.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Benutzer mit den in der folgenden Tabelle aufgeführten Rollen können die Anwendung Operational Technology Manager verwenden.

Wenn Sie Site-Benutzer konfigurieren möchten, können Sie Anwenderkriterien für Site-Benutzer der Anlagenmodell-Entität erstellen und zuweisen. Weitere Informationen finden Sie unter [Gewähren Sie Nicht-Administratoren Zugriff auf den Anlagenmodell-Standort, oder entfernen Sie ihn](#).

Rolle	Beschreibung
Operational Technology Discovery -Administrator [ot_discovery_admin]	Kann den Prozess Discovery für den Prozess Operational Technology ausführen, aber nicht auf Configuration Management Database (CMDB) zugreifen, um die Configuration Items (CIs) und die zugehörigen Entitäten Operational Technology (OT) anzuzeigen, die aus erkannten Elementen erstellt wurden. Weitere Informationen finden Sie unter Erstellen Sie einen Discovery-Zeitplan Operational Technology, und führen Sie den Prozess Discovery aus .
Operational Technology Manager Betrachter [cmdb_ot_viewer]	Schreibgeschützter Zugriff auf Gerätedatensätze von Operational Technology (OT).
Operational Technology Manager -Editor [cmdb_ot_editor]	Erstellen, Lesen, Aktualisieren und Löschen von Zugriffsrechten für Erweiterungsklassen von Operation Technology (OT)  .
Operational Technology Manager Administrator [cmdb_ot_admin]	Zugriffsrechte für Operational Technology (OT)-Gerätedatensätze erstellen, lesen, aktualisieren und löschen. Kann auch bestimmte Konfigurationen im OT-Entitätstyp bearbeiten und verwalten. Weitere Informationen finden Sie unter Erweiterungsklassen für Operation Technology (OT)  .

Prozedur

Weisen Sie Benutzern und Gruppen mit der Benutzerverwaltungsfunktion Now Platform Rollen zu.

Operational Technology Manager Integrationen

Die Anwendung Operational Technology Manager unterstützt Drittanbieterintegrationen.

Die folgenden Drittanbieterintegrationen werden derzeit unterstützt.

- Service Graph Connector Integration for Claroty CTD
- Service Graph Connector für Microsoft Defender for IoT (Azure)
- Service Graph Connector für Microsoft Defender for IoT (lokale Verwaltungskonsole)

Service Graph Connector Integration for Claroty CTD

Integrieren Sie Claroty Continuous Threat Detection (CTD) in die Anwendung ServiceNow Operational Technology Manager, um erkannte Geräte und Claroty CTD-Sites (Sensor oder Netzwerkangriffserkennungssystem-Appliances) zu importieren.

Apps im Store anfordern

Besuchen Sie die Website [ServiceNow Store](#) , um sich alle verfügbaren Apps anzusehen 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](#) .

Unterstützte Versionen

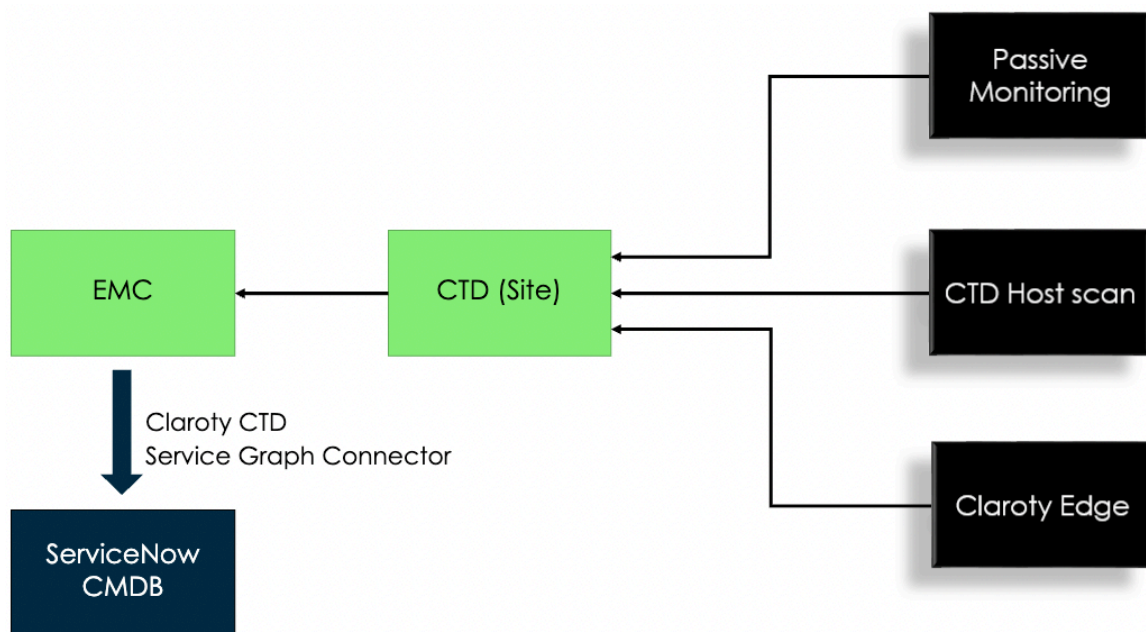
- Claroty CTD Version: 2.0.1 oder höher
- Unterstützte ServiceNow Versionen:
 - Utah
 - Vancouver
 - Washington
 - Xanadu
 - Yokohama

Anwendungsfälle

Verwenden Sie Service Graph Connector-Integration für die kontinuierliche Bedrohungserkennung mit Claroty mit der Anwendung Operational Technology Manager, um die folgenden Informationen in Configuration Management Database (CMDB) zu importieren.

- Sites
- Von jedem Standort erkannte Geräte
- Verbindungen (oder Baselines)
- Installierte Programme

Die folgende Abbildung zeigt die Erkennungsmethode für den Import von Claroty CTD-Daten in CMDB.



Geführtes Setup

Das geführte Setup für Service Graph Connector Integration for Claroty CTD bietet eine organisierte Abfolge von Aufgaben zum Konfigurieren der Integration in Ihrer -Instanz. Informationen zum Zugriff auf das geführte Setup finden Sie unter [Konfigurieren Sie das geführte Setup](#).

Dashboard für CMDB-Integrationen

Die Store-App Gemeinsame Komponenten für CMDB-Integrationen bietet ein Dashboard mit einer zentralen Ansicht des Status, der Verarbeitungsergebnisse und der Verarbeitungsfehler aller installierten Integrationen. Sie können Metriken für alle Integrationsausführungen anzeigen. Sie können die Ansicht nach einer bestimmten CMDB Integration, einer bestimmten Zeitdauer oder einer bestimmten Integrationsausführung filtern. Weitere Informationen zur Überwachung von Integrationen im Integrations-Dashboard CMDB finden Sie unter [Integration Commons for CMDB](#) .

Datenzuordnung

Daten aus den Claroty CTD-Datenquellen werden zugeordnet und mithilfe der Robust Transform Engine (RTE) in die Klassendefinitionen der ServiceNow CMDB Configuration Item(CI)-Klasse umgewandelt. Daten werden mithilfe der Identification and Reconciliation Engine (IRE) in ServiceNow CMDB eingefügt.

In der folgenden Tabelle sind die für Service Graph Connector Integration for Claroty CTD enthaltenen Datenquellen und die entsprechenden Bereitstellungstabellen aufgelistet, in die die importierten Daten geladen werden.

Datenquellen und Bereitstellungstabellen für Claroty CTD

Datenquelle	Bereitstellungstabelle
SG-OT Claroty CTD-Geräte	SG-OT Claroty – Import von CTD-Geräten [sn_clarotycdsgc_sg_ot_claroty_ctd_devices_import]

Datenquellen und Bereitstellungstabellen für Claroty CTD (Fortsetzung)

Datenquelle	Bereitstellungstabelle
SG-OT Claroty – CTD-Baselines	SG-OT Claroty – Import von CTD-Baselines [sn_clarotyctdsgc_sg_ot_claroty_ctd_baselines_import]
SG-OT Claroty CTD – Programme	SG-OT Claroty – Import von CTD-Programmen [sn_clarotyctdsgc_sg_ot_claroty_ctd_programs_import]
SG-OT Claroty – CTD-Sites	SG-OT Claroty CTD – Sites importieren [sn_clarotyctdsgc_sg_ot_claroty_ctd_sites_import]

Die aus den Bereitstellungstabellen importierten Daten werden dann in die folgenden Zieltabellen eingefügt:

- Computer [cmdb_ci_computer]
- Hardware [cmdb_ci_hardware]
- IP-Adresse [cmdb_ci_ip_address]
- Netzwerkadapter [cmdb_ci_network_adapter]
- OT-Gerät-Details [cmdb_ot_entity]
- OT-Steuerungsmodul [cmdb_ci_ot_control_module]
- OT-Steuerungssystem [cmdb_ci_ot_control]
- Seriennummer [cmdb_serial_number]

Weitere Informationen finden Sie unter [Angestrebte CMDB-Klassen](#).

Standardmäßige Abfrageparameter für Service Graph Connector Integration for Claroty CTD

Service Graph Connector Integration for Claroty CTD standardmäßig mit Abfrageparameterfiltern geliefert. Sie können ihre Werte basierend auf den Berechtigungen ServiceNow ändern, die Sie für das IntegrationHub Enterprise-Paket haben.

Wenn Sie mit dem Importieren der Daten aus Claroty CTD beginnen, verwendet Service Graph Connector Integration for Claroty CTD die standardmäßigen Abfrageparameterfilter, die in der folgenden Tabelle aufgeführt sind.

Standardmäßige Abfrageparameterfilter

Abfrageparameterfilter	Wert	Beschreibung
approve_exact	wahr	Nicht genehmigte Geräte in Claroty CTD werden nicht importiert, da der Wert von approve_exact auf „wahr“ festgelegt ist.
valid_exact	wahr	Ungültige Geräte in Claroty CTD werden nicht importiert, da der Wert von „valid_exact“ auf „wahr“ festgelegt ist.

Standardmäßige Abfrageparameterfilter (Fortsetzung)

Abfrageparameterfilter	Wert	Beschreibung
special_hinweis_exakt	0	Adresstypen, die in Claroty CTD nicht auf 0 (Unicast) festgelegt sind, werden nicht importiert.
host_exact	falsch	Wenn in Claroty CTD ein Gerät vorhanden ist, das als Geist klassifiziert ist, wird es von der Service Graph Connector-Integration für Claroty CTD nicht importiert, da der Standardwert auf „false“ festgelegt ist.

Konfigurieren Sie die Eigenschaften Service Graph Connector Integration for Claroty CTD

Lassen Sie sich vom geführten Setup für Service Graph Connector Integration for Claroty CTD durch die Integrationsschritte führen.

Vorbereitungen

Abhängigkeiten und Anforderungen:

- Die Store-App [Integration Commons for CMDB](#), die automatisch installiert wird.
- [CMDB CI Class Models](#), das automatisch installiert wird.
- Plugin „ITOM Discovery License“ (com.snc.itom.discovery.license). Sie müssen dieses Plugin aktivieren.
- ITOM-Lizenzierungs-Plugin (com.snc.itom.license). Weitere Informationen finden Sie unter [Discovery anfordern](#).
- Das Plugin „Datastream Action“ (com.glide.hub.action_type.datastream), das automatisch installiert wird.

Erforderliche Rolle: Administrator

Hinweis:

Wenn Sie eine frühere Version von Service Graph Connector Integration for Claroty CTD haben, migrieren Sie keine Daten aus dem alten Connector. Sie müssen die vorherige Version deinstallieren und die neue Integration ausführen.

Prozedur

1. Stellen Sie mithilfe der Anwendungsauswahl sicher, dass die Anwendung auf Service Graph Connector Integration for Claroty CTD festgelegt ist.
Weitere Informationen finden Sie unter [Application picker](#).
2. Navigieren zu **Alle > Service Graph Connector – Claroty CTD > Geführtes Setup**.
3. Wählen Sie auf der Seite „Erste Schritte“ **Erste Schritte** aus.
4. Führen Sie zum Konfigurieren eines MID-Server Folgendes aus:
 - a. Wählen Sie im Abschnitt „Verbindungen und Anmeldeinformationen einrichten“ die Aufgabe MID-Server konfigurieren aus.
 - b. Wählen Sie **Als abgeschlossen markieren** aus, sobald Sie die Konfiguration MID-Server abgeschlossen haben.
5. Führen Sie zum Einrichten der Verbindungsdatensätze Folgendes aus:

- a. Wählen Sie im Abschnitt „Verbindungen und Anmeldeinformationen einrichten“ die Aufgabe Verbindungen konfigurieren aus.
 - b. Wählen Sie **Konfigurieren**.
 - c. Öffnen Sie den Claroty CTD API-Datensatz in der Verbindungstabelle.
 - d. Geben Sie im Feld **Verbindungs-URL** den Namen der URL für Ihre Claroty CTD Enterprise Management Console (EMC) ein.
Beispiel: <https://192.168.1.100> .
 - e. Wenn Sie MID-Server verwenden, aktivieren Sie das Kontrollkästchen **MID-Server verwenden** im -Datensatz.
- i Hinweis:**
Wenn Sie kein MID-Server verwenden, fahren Sie mit Schritt 5g fort.
- f. Wählen Sie in der zugehörigen Liste Erweiterte Konfiguration MID-Server eine MID-Server und eine MID-Auswahl aus.
 - g. Wählen Sie **Aktualisieren**.
 - h. Wiederholen Sie die Schritte 5a bis 5h, um den Datensatz „**Claroty CTD EMC Base Auth**“ zu aktualisieren.
6. Führen Sie zum Einrichten der Anmeldeinformationsdatensätze Folgendes aus:
- a. Wählen Sie im Abschnitt „Verbindungen und Anmeldeinformationen einrichten“ die Aufgabe Anmeldeinformationen konfigurieren aus.
 - b. Wählen Sie **Konfigurieren**.
 - c. Öffnen Sie den Datensatz „Claroty CTD EMC Base Auth“ in der Tabelle „Anmeldeinformationen“.
 - d. Geben Sie im Feld **Anwendername** den Anwendernamen ein, mit dem Sie sich bei Claroty CTD EMC angemeldet haben.
 - e. Geben Sie im Feld **Passwort** das Passwort ein, mit dem Sie sich bei Claroty CTD EMC angemeldet haben.
 - f. Wählen Sie **Aktualisieren**.
7. Um die Verbindung zu testen, führen Sie Folgendes aus:
- a. Wählen Sie im Abschnitt „Verbindungen und Anmeldeinformationen einrichten“ die Aufgabe Verbindung testen/validieren aus.
 - b. Wählen Sie im Datenquellen-Datensatz für Sensoren im Abschnitt „Zugehörige Links“ die UI-Aktion **Verbindung testen** aus.
Zeigen Sie nach Abschluss des Verbindungstests die Ergebnisse an. Sie müssen die vorgeschlagenen Problembehandlungsschritte ausführen, bis das Testergebnis **Erfolg** zurückgibt.
 - c. Überprüfen Sie, ob der Verbindungsmanager über ein gültiges Zertifikat verfügt.

Für eine Produktionsumgebung muss ein gültiges Zertifikat installiert sein. Für eine Instanz außerhalb der Produktion oder für eine Proof of Concept-Instanz (POC) können Sie die Systemeigenschaften so konfigurieren, dass die Integration funktioniert, wenn der Verbindungsmanager nicht über ein gültiges Zertifikat verfügt. In der folgenden Tabelle sind die Systemeigenschaften aufgeführt, die Sie für eine Umgebung außerhalb der Produktion konfigurieren können.

Systemeigenschaften für eine Umgebung außerhalb der Produktion

Eigenschaft	Wert
com.glide.communications.httpclient.verify_hostname	Auf „ false “ festlegen.
com.glide.communications.httpclient.verify_revoked_certificate	Auf „ false “ festlegen. Wenn Sie diese Systemeigenschaft hinzufügen müssen, finden Sie weitere Informationen unter Systemeigenschaft hinzufügen  .
com.glide.communications.trustmanager_trust_all	Auf wahr festlegen.

d. Überprüfen Sie die MID-Sicherheitsrichtlinie.

Überprüfen Sie im Intranetdatensatz, ob die Spalten in der folgenden Tabelle die angegebenen Werte anzeigen.

Intranet-Datensatzwerte

Spalte	Wert
Zertifikatkettenprüfung	false
Hostnamenprüfung	false
Widerrufsprüfung	false

Weitere Informationen finden Sie [unter Richtlinien für MID-Server-Zertifikatprüfung](#) .

8. Um die Systemeigenschaften festzulegen, mit denen die API-Ressourcenpfade, Paginierungsgrößen und Ablaufzeiten der API-Schlüssel konfiguriert werden, gehen Sie wie folgt vor:

a. Wählen Sie im Abschnitt Konfigurieren von Systemeigenschaften **die Option Konfigurieren aus**.

b. Konfigurieren Sie die Systemeigenschaften in der folgenden Tabelle:

Eigenschaft	Beschreibung
sn_clarotyctdsgc.resourcepath.site	Eigenschaft zum Festlegen des Ressourcenpfads für die Sites:

Eigenschaft	Beschreibung
	i Hinweis: Der Ressourcenpfad für die Sites wird standardmäßig für die API-Version Claroty CTD Enterprise Management Console (EMC) V4.4.3 für die CTD-Sites und -Geräte bereitgestellt. Wenn Sie eine andere API-Version verwenden möchten, können Sie die Pfade überschreiben.
sn_clarotyctdsgc.resourcepath.device	Eigenschaft zum Festlegen des Ressourcenpfads für die Geräte: i Hinweis: Der Ressourcenpfad für die Geräte wird standardmäßig für die API-Version CTD EMC V4.4.3 für die CTD-Sites und -Geräte bereitgestellt. Wenn Sie eine andere API-Version verwenden möchten, können Sie die Pfade überschreiben.
sn_clarotyctdsgc.pagesize.device	Eigenschaft zum Festlegen der Anzahl der Gerätedatensätze, die in einem paginierten REST-Aufruf an die Claroty CTD EMC abgerufen werden sollen. Der Standardwert beträgt 500 Datensätze pro Seite. i Hinweis: Die maximale Anzahl von Geräten pro Seite beträgt 500.
sn_clarotyctdsgc.resourcepath.baseline	Eigenschaft zum Festlegen des Ressourcenpfads für die Baselines: i Hinweis: Der Ressourcenpfad für die Baselines wird standardmäßig für die API-Version CTD EMC V4.4.3 für die CTD-Sites und -Geräte bereitgestellt. Wenn Sie eine andere API-Version verwenden möchten, können Sie die Pfade überschreiben.
sn_clarotyctdsgc.pagesize.baseline	Eigenschaft zum Festlegen der Anzahl der Baseline-Datensätze, die in einem paginierten REST-Aufruf an die Claroty

Eigenschaft	Beschreibung
	CTD EMC abgerufen werden sollen. Der Standardwert beträgt 500 Datensätze pro Seite.
sn_clarotyctdsgc.get_all_baselines	Eigenschaft zum Abrufen aller Datensätze für Baselines oder nur der neuen Datensätze seit der Startzeit des letzten erfolgreichen Imports. i Hinweis: Wenn Sie Baselines zum ersten Mal importieren, werden alle Datensätze unabhängig von der Einstellung für diese Eigenschaft importiert.
sn_clarotyctdsgc.resourcepath.entity	Eigenschaft zum Festlegen des Ressourcenpfads für die Entitäten: i Hinweis: Der Ressourcenpfad für die Entitäten wird standardmäßig für die API-Version CTD EMC V4.4.3 für die CTD-Sites und -Geräte bereitgestellt. Wenn Sie eine andere API-Version verwenden möchten, können Sie die Pfade überschreiben.
sn_clarotyctdsgc.resourcepath.program	Eigenschaft zum Festlegen des Ressourcenpfads für die installierten Programme: i Hinweis: Der Ressourcenpfad für die installierten Programme wird standardmäßig für die API-Version CTD EMC V4.4.3 für die CTD-Sites und -Geräte bereitgestellt. Wenn Sie eine andere API-Version verwenden möchten, können Sie die Pfade überschreiben.
sn_clarotyctdsgc.pagesize.entity	Eigenschaft zum Festlegen der Anzahl der Entitätsdatensätze, die in einem paginierten REST-Aufruf an die Claroty CTD EMC abgerufen werden sollen. Der Standardwert beträgt 500 Datensätze pro Seite.
sn_clarotyctdsgc.pagesize.program	Eigenschaft zum Festlegen der Anzahl der Programm datensätze, die in einem paginierten REST-Aufruf an die Claroty CTD EMC abgerufen werden sollen. Der

Eigenschaft	Beschreibung
	Standardwert beträgt 500 Datensätze pro Seite.
sn_clarotyctdsgc.api_token_life_in_minutes	Eigenschaft zum Festlegen der Anzahl der Minuten, für die die API als aktiv betrachtet wird. Nach Ablauf der Zeit ruft der Service Graph Connector beim nächsten Import einen neuen API-Schlüssel ab. Der Standardwert ist 0, und für jeden REST-Aufruf wird ein neues Token abgerufen. i Hinweis: Sie können den Wert so ändern, dass dasselbe Token maximal 24 Stunden lang beibehalten und die Anzahl der REST-Aufrufe reduziert wird.
sn_clarotyctdsgc.classify_based_on_os	Eigenschaft, um eine Liste von Klassen bereitzustellen, die die Klassifizierung nach Betriebssystem als Teil von Service Graph Connector Integration for Claroty CTD unterstützen. Wenn die Kennzeichnung auf true festgelegt ist, wird die Klassifizierung nach Betriebssystem unterstützt. Wenn sie auf false festgelegt ist, klassifiziert der Service Graph Connector nicht mehr nach Betriebssystem. Zum Beispiel: <pre>{ "cmdb_ci_ip_switch":true, "cmdb_ci_nids":false }</pre>
sn_clarotyctdsgc.filter.asset_type_code	Eigenschaft zum Bereitstellen einer Liste von Codes für Gerätetypen, getrennt durch das Trennzeichen (\$). Weitere Informationen zu Claroty-Typen und -Codes finden Sie unter Angestrebte CMDB-Klassen. Um beispielsweise nur SPS- und HMI-Gerätetypen zu importieren, geben Sie den Claroty-Typcode als 0\$1 ein.
sn_clarotyctdsgc.filter.asset_purdue_level	Eigenschaft, um eine Liste von Purdue-Ebenen bereitzustellen, getrennt durch das Trennzeichen (\$). Um beispielsweise nur Geräte mit den Purdue-Ebenen 1 und 2 zu filtern, legen Sie, um nur Geräte mit den Purdue-Ebenen 1 und 2 zu filtern, den Wert 1.0\$2.0 fest.

c. Wählen Sie **Speichern.**

9. Um CTD-Sites zu importieren, gehen Sie wie folgt vor:

- a. Wählen Sie im Abschnitt „CTD-Sites konfigurieren“ die Aufgabe CTD-Sites importieren aus.
 - b. Wählen Sie **Konfigurieren**.
 - c. Klicken Sie auf die Schaltfläche **Jetzt ausführen**.
- 10.** Führen Sie zum Konfigurieren von Netzwerkangriffserkennungssystemen (NIDS) Folgendes aus:
- a. Wählen Sie im Abschnitt „CTD-Sites konfigurieren“ die Aufgabe Konfigurieren von NIDS aus.
 - b. Wählen Sie **„Als abgeschlossen markieren“** aus, sobald Sie das NIDS eingerichtet haben, das zum Abrufen von Geräten von Claroty CTD verwendet wird.
- 11.** Führen Sie die folgenden Schritte aus, um die Importzeitpläne für die Ausführung der Sites, Geräte, Baselines und installierten Programme zu konfigurieren:
- a. Wählen Sie im Abschnitt Importzeitpläne konfigurieren die Aufgabe Importzeitplan für Sites konfigurieren aus.
 - b. Wählen Sie **Konfigurieren**.
 - c. Wählen Sie in der Tabelle „Geplante Datenimporte“ **Geplanter Import von SG-OT CTD-Sites** aus.
 - Standardmäßig ist der Importzeitplan für Sites so konfiguriert, dass er jeden Tag um Mitternacht ausgeführt wird.
 - Sie müssen die CTD-Sites importieren und validieren, bevor Sie die Geräte importieren.
 - d. Führen Sie die folgenden Aktionen nach Bedarf aus, um den Importzeitplan nach Bedarf zu überprüfen oder zu ändern:

Aktion	Beschreibung
Geben Sie ein bedingtes Skript ein	Geben Sie ein bedingtes Skript ein, das bestimmt, ob ein geplanter Import ausgeführt werden soll, indem Sie Bedingung auswählen.
Ändern Sie den standardmäßigen Importzeitplan	Ändern Sie den standardmäßigen Importzeitplan, indem Sie das Feld Ausführen nach Bedarf festlegen.
Verweisen Sie in der Benutzertabelle auf einen Benutzer	Verweisen Sie in der Tabelle „Benutzer“ auf einen Benutzer, indem Sie ihn im Feld Wird ausgeführt als auswählen. i Hinweis: Standardmäßig ist dieses Feld auf „Systemadministrator“ festgelegt. Dem ausgewählten Anwender muss die Administratorrolle zugewiesen werden, damit der Import erfolgreich ist. Wenn leer gelassen, verwendet der Importzeitplan die Rollen des angemeldeten Benutzers.
Import ausführen	Führen Sie einen Import aus, indem Sie „Jetzt ausführen“ auswählen. Sie können entweder

Aktion	Beschreibung
	alle Datensätze oder nur neue Datensätze seit der Startzeit des letzten erfolgreichen Imports importieren, basierend auf den konfigurierten Systemeigenschaften. Weitere Informationen finden Sie unter Konfigurieren Sie das geführte Setup .
Aktivieren Sie den Import	Aktivieren Sie den Import, indem Sie das Kontrollkästchen Aktiv aktivieren.
Speichern Sie alle Zeitplanänderungen	Speichern Sie alle Zeitplanänderungen, indem Sie Aktualisieren auswählen.

- e. Wählen Sie im Abschnitt „Importzeitpläne konfigurieren“ die Aufgabe Importzeitplan für Geräte konfigurieren aus.
- f. Wählen Sie **Konfigurieren**.
- g. Wählen Sie in der Tabelle „Geplante Datenimporte“ **Geplanter Import von SG-OT CTD-Geräten** aus, um den Importzeitplan für Ihre Geräte zu überprüfen oder zu ändern.
- Standardmäßig ist der Zeitplan für den Geräteimport so konfiguriert, dass er jeden Tag um Mitternacht ausgeführt wird.
 - Geräte werden von der CTD-Site abgefragt. Der Service Graph Connector fragt nur Geräte ab, die von validierten CTD-Sites erkannt wurden.
- h. Führen Sie die folgenden Aktionen nach Bedarf aus, um den Importzeitplan nach Bedarf zu überprüfen oder zu ändern:

Aktion	Beschreibung
Geben Sie ein bedingtes Skript ein	Geben Sie ein bedingtes Skript ein, das bestimmt, ob ein geplanter Import ausgeführt werden soll, indem Sie Bedingung auswählen.
Ändern Sie den standardmäßigen Importzeitplan	Ändern Sie den standardmäßigen Importzeitplan, indem Sie das Feld Ausführen nach Bedarf festlegen.
Verweisen Sie in der Benutzertabelle auf einen Benutzer	Verweisen Sie in der Tabelle „Benutzer“ auf einen Benutzer, indem Sie ihn im Feld Wird ausgeführt als auswählen. i Hinweis: Standardmäßig ist dieses Feld auf „Systemadministrator“ festgelegt. Dem ausgewählten Anwender muss die Administratorrolle zugewiesen werden, damit der Import erfolgreich ist. Wenn leer gelassen, verwendet der Importzeitplan die Rollen des angemeldeten Benutzers.

Aktion	Beschreibung
Import ausführen	Führen Sie einen Import aus, indem Sie „Jetzt ausführen“ auswählen. Sie können entweder alle Datensätze oder nur neue Datensätze seit der Startzeit des letzten erfolgreichen Imports importieren, basierend auf den konfigurierten Systemeigenschaften. Weitere Informationen finden Sie unter Konfigurieren Sie das geführte Setup .
Aktivieren Sie den Import	Aktivieren Sie den Import, indem Sie das Kontrollkästchen Aktiv aktivieren.
Speichern Sie alle Zeitplanänderungen	Speichern Sie alle Zeitplanänderungen, indem Sie Aktualisieren wählen.

- i. Wählen Sie im Abschnitt „Importzeitpläne konfigurieren“ die Aufgabe Importzeitplan für Baselines konfigurieren aus.
- j. Wählen Sie **Konfigurieren**.
- k. Wählen Sie in der Tabelle „Geplante Datenimporte“ **SG-OT CTD-Baselines Geplanter Import** aus, um den Importzeitplan für die Baselines zu überprüfen oder zu ändern.
Standardmäßig ist der Importzeitplan für Baselines so konfiguriert, dass er nach der Ausführung des übergeordneten OT-Steuerungssystems ausgeführt wird.
- l. Führen Sie die folgenden Aktionen nach Bedarf aus, um den Importzeitplan nach Bedarf zu überprüfen oder zu ändern.

Aktion	Beschreibung
Geben Sie ein bedingtes Skript ein	Geben Sie ein bedingtes Skript ein, das bestimmt, ob ein geplanter Import ausgeführt werden soll, indem Sie Bedingung auswählen.
Ändern Sie den standardmäßigen Importzeitplan	Ändern Sie den standardmäßigen Importzeitplan, indem Sie das Feld Ausführen nach Bedarf festlegen.
Verweisen Sie in der Benutzertabelle auf einen Benutzer	Verweisen Sie in der Tabelle „Benutzer“ auf einen Benutzer, indem Sie ihn im Feld Wird ausgeführt als auswählen. i Hinweis: Standardmäßig ist dieses Feld auf „Systemadministrator“ festgelegt. Dem ausgewählten Anwender muss die Administratorrolle zugewiesen werden, damit der Import erfolgreich ist. Wenn leer gelassen, verwendet der Importzeitplan die Rollen des angemeldeten Benutzers.
Import ausführen	Führen Sie einen Import aus, indem Sie „Jetzt ausführen“ auswählen. Sie können entweder

Aktion	Beschreibung
	alle Datensätze oder nur neue Datensätze seit der Startzeit des letzten erfolgreichen Imports importieren, basierend auf den konfigurierten Systemeigenschaften. Weitere Informationen finden Sie unter Konfigurieren Sie das geführte Setup .
Aktivieren Sie den Import	Aktivieren Sie den Import, indem Sie das Kontrollkästchen Aktiv aktivieren.
Speichern Sie alle Zeitplanänderungen	Speichern Sie alle Zeitplanänderungen, indem Sie Aktualisieren wählen.

m. Wählen Sie im Abschnitt „Importzeitpläne konfigurieren“ die Aufgabe Importzeitplan für installierte Sites konfigurieren aus.

n. Wählen Sie **Konfigurieren**.

o. Wählen Sie in der Tabelle „Geplante Datenimporte“ **SG-OT CTD Geplanter Import von installierten Programmen** aus, um den Zeitplan für den Import von installierten Programmen zu überprüfen oder zu ändern.
Standardmäßig ist der Importzeitplan für installierte Programme so konfiguriert, dass er jeden Tag um Mitternacht ausgeführt wird.

p. Führen Sie die folgenden Aktionen nach Bedarf aus, um den Importzeitplan nach Bedarf zu überprüfen oder zu ändern.

Aktion	Beschreibung
Geben Sie ein bedingtes Skript ein	Ändern Sie den standardmäßigen Importzeitplan, indem Sie das Feld Ausführen nach Bedarf festlegen.
Ändern Sie den standardmäßigen Importzeitplan	Ändern Sie den standardmäßigen Importzeitplan, indem Sie das Feld Ausführen nach Bedarf festlegen.
Verweisen Sie in der Benutzertabelle auf einen Benutzer	Verweisen Sie in der Tabelle „Benutzer“ auf einen Benutzer, indem Sie ihn im Feld Wird ausgeführt als auswählen. i Hinweis: Standardmäßig ist dieses Feld auf „Systemadministrator“ festgelegt. Dem ausgewählten Anwender muss die Administratorrolle zugewiesen werden, damit der Import erfolgreich ist. Wenn leer gelassen, verwendet der Importzeitplan die Rollen des angemeldeten Benutzers.
Import ausführen	Führen Sie einen Import aus, indem Sie „Jetzt ausführen“ auswählen. Sie können entweder alle Datensätze oder nur neue Datensätze seit

Aktion	Beschreibung
	der Startzeit des letzten erfolgreichen Imports importieren, basierend auf den konfigurierten Systemeigenschaften. Weitere Informationen finden Sie in Schritt 7c.
Aktivieren Sie den Import	Aktivieren Sie den Import, indem Sie das Kontrollkästchen Aktiv aktivieren.
Speichern Sie alle Zeitplanänderungen	Speichern Sie alle Zeitplanänderungen, indem Sie Aktualisieren wählen.

12. Wahlweise: Wenn Konfigurationselemente (CIs) in CMDB erstellt werden, werden Asset-Datensätze erstellt.

Der Asset-Datensatz enthält die Modellkategorie des CI. Weitere Informationen zu den Modellkategorien für Operational Technology (OT) finden Sie unter [Modellkategorien für Operational Technology](#). Führen Sie Folgendes aus, um die Modellkategorie für ein OT-Gerät anzuzeigen:

- a. Navigieren zu **Alle > Operative Technologien (OT) > Alle OT-Geräte**.
- b. Wählen Sie das OT-Gerät aus, für das Sie den Asset-Datensatz anzeigen möchten.
- c. Wählen Sie neben dem Feld **Asset** das Symbol **Vorschau auf diesen Datensatz anzeigen** () aus.
- d. Wählen Sie **Datensatz öffnen**.

13. Wahlweise: Führen Sie Folgendes aus, um Probleme mit Service Graph Connector Integration for Claroty CTD zu beheben:

- a. Wählen Sie den Abschnitt [OPTIONAL] Problembehandlung bei Service Graph Connector für Claroty CTD aus.
- b. Wählen Sie in der Aufgabe Geplante Validierungen ausführen die Option **Konfigurieren aus**.
- c. Wählen Sie **Jetzt ausführen**.
Dieser Auftrag führt Aufgaben aus, um die Konfigurationen für SGC und die Verbindung zu Claroty CTD zu validieren. Wenn Konfigurationsprobleme gefunden werden, melden die Validierungsergebnisse das Problem und schlagen Problembehandlungsschritte vor. Warten Sie, bis die geplante Aufgabe abgeschlossen ist.
- d. Navigieren Sie nach Abschluss der geplanten Aufgabe zurück zum Abschnitt [OPTIONAL] Problembehandlung bei Service Graph Connector für Claroty CTD.
- e. Wählen Sie in der Aufgabe Validierungsergebnisse überprüfen **die Option Konfigurieren aus**.
Dieser Schritt öffnet die Ausführungsprotokolle und Vorschläge der letzten Problembehandlung, damit Sie sie anzeigen können.

f. Behandeln Sie die Vorschläge nach Bedarf.

Hinweis:

Sie können das geplante Skript jederzeit nach der Erstkonfiguration von Service Graph Connector Integration for Claroty CTD verwenden. Um Validierungen auszulösen, navigieren Sie zu **Alle > Service Graph Connector für Claroty CTD > Problembehandlung > Problembehandlung ausführen**. Um die Validierungsergebnisse anzuzeigen, navigieren Sie zu **Alle > Service Graph Connector für Claroty CTD > Problembehandlung > Ergebnisse**.

Weitere Informationen zur Behebung von Problemen bei der Verwendung von Service Graph Connector Integration for Claroty CTD finden Sie unter [Problembehandlungsszenarien für die Service Graph Connector-Integration für Claroty CTD \(KB1502041\)](#) .

Validiert NIDS-Sensoren

Validiert die Netzwerk-IDS-Sensoren (NIDS) nach dem Import zur Vorbereitung des Geräteimports. Die Sensoren können die Validierung nur bestehen, wenn sie sich nicht im Lernmodus befinden, da solche Sensoren nicht für den Geräteimport geeignet sind.

Vorbereitungen

Es wird empfohlen, das CSDM-Plugin zu installieren. Der Service Graph Connector ist an den Lebenszyklusdatenmodellen gemäß den CMDB-Standards ausgerichtet. Weitere Informationen finden Sie unter [Implementing the CSDM framework in stages](#) .

Erforderliche Rolle: cmdb_nids_admin

Warum und wann dieser Vorgang ausgeführt wird

Die Felder „**Lebenszyklusphase**“ und „**Status der Lebenszyklusphase**“ werden verwendet, um den Lernmodus eines Sensors zu erfassen. Wenn das Feld Lebenszyklusphase auf **Funktionsfähig** und der Status der Lebenszyklusphase auf **Lernmodus** festgelegt ist, ist die Validierung nicht erfolgreich. Wenn das Feld Status der Lebenszyklusphase auf **In Gebrauch** festgelegt ist, ist die Validierung erfolgreich.

Prozedur

1. Navigieren zu **Alle > Netzwerk-IDS-Appliances (NIDS) > Sensoren**.
2. Wählen Sie den Sensordatensatz aus, den Sie validieren möchten.
3. Fügen Sie im Abschnitt „NIDS Assigned Meta Data“ (NIDS zugewiesene Metadaten) Werte für den Sensor hinzu, der den erkannten Geräten zugewiesen werden soll.
4. Stellen Sie im Abschnitt „NIDS-Administratorkonfiguration“ sicher, dass der Wert des Felds „**Status der Lebenszyklusphase**“ nicht **Lernmodus** lautet.
Andernfalls schlägt die Validierung fehl.
5. Stellen Sie sicher, dass das Feld „**NIDS-Netzwerktyp**“ auf Grundlage des Standorts des NIDS-Netzwerks festgelegt ist.
Sie können beispielsweise den NIDS-Netzwerktyp „**IT**“ für eine Rechenzentrumsbereitstellung des NIDS oder den NIDS-Netzwerktyp „**OT**“ für eine industrielle Bereitstellung in einem Industrie-/OT-Netzwerk auswählen.

Wenn Sie OT auswählen, werden die OT-Gerät-Details für alle Geräte erstellt.

6. Wenn die Attribute korrekt ausgefüllt sind, wählen Sie **Validieren** aus.

i Hinweis:

HINWEIS: Die Attribute, die vom Sensor an die Geräte übergeben werden, sind in der Systemeigenschaft `sn_cmdb_ci_class.nids_map_fields` definiert. Die folgende Liste ist die Standardliste der Attribute.

- assigned_to
- location
- Unternehmen
- owned_by
- managed_by
- supported_by
- change_control
- support_group
- managed_by_group
- assignment_group
- Zone
- isa_entity_site (nur verfügbar, wenn Sie die Anwendung Prozessmanager Industrie installiert haben)

Verwenden Sie das Verbindungs-Framework Service Graph .

Verwenden Sie das Verbindungs-Framework Service Graph, um die zugehörigen Datenquellen, Systemeigenschaften und geplanten Datenimporte, die für Claroty CTD erstellt wurden, an einem Ort zu sammeln.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Es stehen Anwendungsmodule für die separate Navigation zu den Datenquellen, Systemeigenschaften und geplanten Datenimporten für Service Graph Connector Integration for Claroty CTD zur Verfügung. Das neue Service Graph -Verbindungs-Framework ermöglicht es jedoch, alle zugehörigen Datenquellen und geplanten Datenimporte, die für Claroty CTD erstellt wurden, an einem Ort zu sammeln. Sie können die Verbindung zur Quelle (Claroty CTD) auch im Abschnitt „Zugehörige Links“ testen.

Prozedur

1. Stellen Sie mithilfe der Anwendungsauswahl sicher, dass der Anwendungsbereich auf die Anwendung **Service Graph Connector-Integration für Claroty CTD** festgelegt ist.
2. Navigieren zu **Alle > Service Graph Connector für Claroty CTD > Claroty CTD SGC-Verbindung**.
3. Wählen Sie auf der Seite „Service Graph-Verbindungen“ **SG-OT Claroty CTD – Standardverbindung** aus.
4. **Wahlweise:** Um auf die Systemeigenschaften zuzugreifen, wählen Sie die Registerkarte **Service Graph-Verbindungseigenschaften**.

- 5. Wahlweise:** Um auf die Datenquellen zuzugreifen, wählen Sie die Registerkarte **Service Graph-Verbindungsdatenquellen**.
- 6. Wahlweise:** Um auf die geplanten Datenimporte zuzugreifen, wählen Sie die Registerkarte **Geplante Datenimporte für Service Graph-Verbindungen**.
- 7. Wahlweise:** Um Ihre Verbindung mit der Claroty CTD-Plattform zu testen, wählen Sie den zugehörigen Link **Verbindung testen** aus.
Sie können Ihre Verbindung jederzeit testen. Wenn der Verbindungstest abgeschlossen ist, finden Sie den Status und Vorschläge zur Problembehandlung der fehlgeschlagenen Schritte unter **Status** bzw. **Vorschlag** auf derselben Seite.

CMDB Klassen, die in der anvisiert werden Service Graph Connector Integration for Claroty CTD

Wenn Sie die Setupaufgaben abschließen, können Sie die Integration regelmäßig so konfigurieren, dass Daten aus Claroty CTD abgerufen werden. Die Daten werden in Tabellen gespeichert, die sich auf die Tabelle Configuration Item [cldb_ci] beziehen.

Computer [cldb_ci_computer]

Die folgenden Attribute in der Tabelle „Computer“ [cldb_ci_computer] werden durch gesammelte Daten gefüllt:

Attributbezeichnung	Attributname
Neuester Discovery-Scan	last_discovered
Betriebssystem	os
BS-Version	os_version

Externe Systemmetadaten [cldb_key_value_v2]

Die folgenden Attribute in der Tabelle „Externe Systemmetadaten“ [cldb_key_value_v2] werden durch gesammelte Daten gefüllt:

Attributbezeichnung	Attributname
Discovery-Quelle	discovery_source
Key	key
Quellschlüssel	source_key
URL-Wert	url_value
Werttyp	value_type

Hardware [cldb_ci_hardware]

Die folgenden Attribute in der Tabelle „Hardware“ [cldb_ci_hardware] werden durch gesammelte Daten gefüllt:

Attributbezeichnung	Attributname
Change-Gruppe	assignment_group

Attributbezeichnung	Attributname
Support-Gruppe	support_group
Unternehmen	Unternehmen
Lieferant	Lieferant
Name	name
Seriennummer	serial_number
Klasse	sys_class_name
Zuerst erkannt	first_discovered
Standort	location
Modellnummer	model_number
Neuester Discovery-Scan	last_discovered
Support durch	supported_by
Zugewiesen an	assigned_to
Verwaltet nach Gruppe	managed_by_group
Verwaltet von	managed_by
Modell-ID	model_id
Freigabegruppe	change_control
Eigentum von	owned_by
Hersteller	manufacturer

Für Hardware erstellte Beziehungen

Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
Hardware [cmdb_ci_hardware]	Eigentümer von::Eigentum von	Netzwerkadapter [cmdb_ci_network_adapter]
Hardware [cmdb_ci_hardware]	Eigentümer von::Eigentum von	IP-Adresse [cmdb_ci_ip_address]
Hardware [cmdb_ci_hardware]	Referenz	OT-Gerät [cmdb_ot_entity]
Hardware [cmdb_ci_hardware]	Referenz	Externe Systemmetadaten [cmdb_key_value_v2]
Hardware [cmdb_ci_hardware]	Referenz	Softwareinstallation [cmdb_sam_sw_install]

IP-Adresse [cmdb_ci_ip_address]

Die folgenden Attribute in der Tabelle „IP-Adresse“ [cmdb_ci_ip_address] werden durch gesammelte Daten gefüllt:

Attributbezeichnung	Attributname
Im Besitz von Konfigurationselement	owned_by_cmdb_ci
IP-Adresse	ip_address

Attributbezeichnung	Attributname
IP-Version	ip_version

Für die IP-Adresse erstellte Beziehungen

Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
IP-Adresse [cmdb_ci_ip_address]		Erkennungssystem für Netzwerkangriffe [cmdb_ci_nids]
IP-Adresse [cmdb_ci_ip_address]		Hardware [cmdb_ci_hardware]

Netzwerkadapter [cmdb_ci_network_adapter]

Die folgenden Attribute in der Tabelle „Netzwerkadapter“ [cmdb_ci_network_adapter] werden durch gesammelte Daten gefüllt:

Attributbezeichnung	Attributname
MAC-Adresse	mac_address
Name	name

Für den Netzwerkadapter erstellte Beziehungen

Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
Netzwerkadapter [cmdb_ci_network_adapter]	Referenz	Hardware [cmdb_ci_hardware]

Erkennungssystem für Netzwerkangriffe [cmdb_ci_nids]

Die folgenden Attribute in der Tabelle „Netzwerkangriffserkennungssystem“ [cmdb_ci_nids] werden durch gesammelte Daten gefüllt:

Attributbezeichnung	Attributname
Hersteller	manufacturer
Name	name
Korrelations-ID	correlation_id
Beschreibung	short_description
Firmware-Version	firmware_version
Verbindungsstatus des NIDS-Managers	connection_state
Status der Lebenszyklusphase	life_cycle_stage_status
Lebenszyklusphase	life_cycle_stage
Überprüft	überprüft

Für NIDS erstellte Beziehungen

Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
Erkennungssystem für Netzwerkangriffe [cmdb_ci_nids]	Eigentümer von::Eigentum von	IP-Adresse [cmdb_ci_ip_address]
Erkennungssystem für Netzwerkangriffe [cmdb_ci_nids]	Erkennt::Erkannt von	Hardware [cmdb_ci_hardware]

Operative Technologien (OT) [cmdb_ci_ot]

Die folgenden Attribute in der Tabelle „Operative Technologie (OT)“ [cmdb_ci_ot] werden durch gesammelte Daten gefüllt:

Attributbezeichnung	Attributname\
Firmware-Version	firmware_version
Neuester Discovery-Scan	last_discovered

OT-Gerät [cmdb_ot_entity]

Die folgenden Attribute in der Tabelle „OT-Gerät“ [cmdb_ot_entity] werden durch gesammelte Daten gefüllt:

Attributbezeichnung	Attributname
Purdue-Ebene	purdue_level
ISA-Entitätsstandort	isa_entity_site
OT-Erkennungsquellen-ID	ot_correlation_id
Gerät-Relevanz	business_criticality
Zone	Zone
OT-Gerätetyp	ot_asset_type

OT-Steuerungsmodul [cmdb_ci_ot_control_module]

Die folgenden Attribute in der Tabelle „OT-Steuerungsmodul“ [cmdb_ci_ot_control_module] werden durch gesammelte Daten ausgefüllt:

Attributbezeichnung	Attributname
Standort	location
Support durch	supported_by
Name	name
Seriennummer	serial_number
Slot-Nummer	slot_number
Hersteller	manufacturer
Firmware-Version	firmware_version

Attributbezeichnung	Attributname
Freigabegruppe	change_control
Zugewiesen an	assigned_to
Neuester Discovery-Scan	last_discovered
Modell-ID	model_id
Modellnummer	model_number
Unternehmen	Unternehmen
Eigentum von	owned_by
Verwaltet von	managed_by
Support-Gruppe	support_group
Verwaltet nach Gruppe	managed_by_group
Change-Gruppe	assignment_group
Lieferant	Lieferant

Für das OT-Steuerungsmodul erstellte Beziehungen

Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
OT-Steuerungsmodul [cmdb_ci_ot_control_module]	Referenz	OT-Gerät [cmdb_ot_entity]

OT-Steuerungssystem [cmdb_ci_ot_control]

Die folgenden Attribute in der Tabelle „OT-Steuerungssystem“ [cmdb_ci_ot_control] werden durch gesammelte Daten ausgefüllt:

Attributbezeichnung	Attributname
Hat Modul	has_module
Neuester Discovery-Scan	last_discovered

Für OT-Steuerungssystem erstellte Beziehungen

Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
OT-Steuerungssystem [cmdb_ci_ot_control]	Eigentümer von::Eigentum von	OT-Steuerungsmodul [cmdb_ci_ot_control_module]

Seriennummer [cmdb_serial_number]

Die folgenden Attribute in der Tabelle „Seriennummer“ [cmdb_serial_number] werden durch gesammelte Daten gefüllt:

i Hinweis:

Ein Korrekturskript wird automatisch angewendet, um die Seriennummern-Datensätze [cmdb_serial_number] zu bereinigen, die aus Service Graph Connector in die Tabelle sys_object_source importiert wurden. Das Skript stellt sicher, dass keine Nullzeiger-Ausnahme auftritt, wenn Seriennummer und MAC-Adresse identisch sind.

Dieses Korrekturskript wird nur einmal während des Upgrades von Service Graph Connector Integration for Claroty CTD ausgeführt, nicht jedoch auf zBoot-Instanzen oder Neuinstallationen. Dies hat keine Auswirkungen auf die Funktionalität oder führt zu Datenverlust.

Attributbezeichnung	Attributname
Seriennummer	serial_number
Seriennummertyp	serial_number_type
Gültig	gültig

Für die Seriennummer erstellte Beziehungen

Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
Seriennummer [cmdb_serial_number]	Referenz	Hardware [cmdb_ci_hardware]

Software [cmdb_ci_spkg]

Die folgenden Attribute in der Tabelle „Software“ [cmdb_ci_spkg] werden durch gesammelte Daten gefüllt:

Attributbezeichnung	Attributname
Key	key
Version	version
Hersteller	manufacturer
Name	name

Für Software erstellte Beziehungen

Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
Software [cmdb_ci_spkg]	Referenz	Softwareinstanz [cmdb_software_instance]

Softwareinstanz [cmdb_software_instance]

Die folgenden Attribute in der Tabelle „Softwareinstanz“ [cmdb_software_instance] werden durch gesammelte Daten gefüllt:

Attributbezeichnung	Attributname
Installationsdatum	install_date

Attributbezeichnung	Attributname
Installiert auf	installed_on
Name	name

Für die Software-Instanz erstellte Beziehungen

Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
Softwareinstanz [cmdb_software_instance]	Referenz	Hardware [cmdb_ci_hardware]

Softwareinstallation [cmdb_sam_sw_install]

Die folgenden Attribute in der Tabelle „Softwareinstallation“ [cmdb_sam_sw_install] werden durch gesammelte Daten gefüllt:

Attributbezeichnung	Attributname
Anzeigename	display_name
Version	version
Discovery-Quelle	discovery_source

Für die Softwareinstallation erstellte Beziehungen

Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
Softwareinstanz [cmdb_software_instance]	Referenz	Hardware [cmdb_ci_hardware]

Standardmäßige Klassenzuordnung

Eine Standardklassenzuordnung ist im Lieferumfang der Anwendung Service Graph Connector Integration for Claroty CTD enthalten.

Hinweis:

Sie finden die Klassenzuordnung im Skript **sn_clarotyctdsgc.SGOTClarotyCTDConstants**.

Claroty CTD-Typ	ServiceNow-Typ	Klasse	OT-Entitätstyp	Claroty-Typen und -Codes
eAAAServer	(Leer)	cmdb_ci_server		eAAAServer = 61
eAccessControl	(Leer)	cmdb_ci_iot		eAccessControl = 50
eAccessPoint	(Leer)	cmdb_ci_ip_Switch		eAccessPoint = 60
eADServer	(Leer)	cmdb_ci_server		eADServer = 33
eAutonomousVehicle	OT-Feldgerät	cmdb_ci_ot_field_device	ot_field_device	eAutonomousVehicle = 58
eAVServer	(Leer)	cmdb_ci_server		eAVServer = 32

Claroty CTD-Typ	ServiceNow-Typ	Klasse	OT-Entitätstyp	Claroty-Typen und -Codes
eBarcodeScanner	OT-Feldgerät	cmdb_ci_ot_field_device	ot_field_device	eBarcodeScanner = 48
eBluetoothDevice	(Leer)	cmdb_ci_iot		eBluetoothDevice = 41
eBroadcast	(Leer)	cmdb_ci_netgear		eBroadcast = 4
eKamera	OT-Feldgerät	cmdb_ci_ot_field_device	ot_field_device	eKamera = 42
ecleaningdevice	OT-Feldgerät	cmdb_ci_ot_field_device	ot_field_device	eCleaningDevice = 55
eController	OT-Steuerungssystem	cmdb_ci_ot_control	ot_control_system	eController = 20
eDataLogger	OT-Steuerungssystem	cmdb_ci_ot_control	ot_control_system	eDataLogger = 66
eDBServer	(Leer)	cmdb_ci_server		eDBServer = 35
eDomainController	(Leer)	cmdb_ci_server		eDomainController = 5
eElektrischeAntrieb	Industrial Drive	cmdb_ci_ot_industrial_drive	induserielle_Laufwerk	eElektrischeAntrieb = 68
eEndpunkt	Gerät der operativen Technologie	cmdb_ci_ot	ot_base	eEndpunkt = 2
eEngineeringStation	EWS	cmdb_ci_ot_ews	EWS	eEngineeringStation = 14
eFileServer	(Leer)	cmdb_ci_server		eFileServer = 10
eFirewall	(Leer)	cmdb_ci_ip_firewall		eFirewall = 31
eFrontEndProcessor	OT-Steuerungssystem	cmdb_ci_ot_control	ot_control_system	eFrontEndProcessor = 26
eGateway	(Leer)	cmdb_ci_ip_Switch		eGateway = 15
eGPSClock	Gerät der operativen Technologie	cmdb_ci_ot	ot_base	eGPSClock = 37
eGPSDevice	Gerät der operativen Technologie	cmdb_ci_ot	ot_base	eGPSDevice = 62
eHistoria	Aufzeichnung	cmdb_ci_ot_historian	-Historiker	eHistorant = 9
eHMI	HMI	cmdb_ci_ot_hmi	hmi	eHMI = 1
eHomeAssist	(Leer)	cmdb_ci_iot		eHomeAssistant = 53
eIED	IED	cmdb_ci_ot_ied	geb	eIED = 19
eInFusionPumpe	(Leer)	cmdb_ci_iot		eInFusionPump = 46
eMediaServer	(Leer)	cmdb_ci_server		eMediaServer = 54
eMedicalDevice	(Leer)	cmdb_ci_iot		eMedicalDevice = 47

Claroty CTD-Typ	ServiceNow-Typ	Klasse	OT-Entitätstyp	Claroty-Typen und -Codes
eMicroscope	(Leer)	cmdb_ci_iot		eMicroscope = 49
eModem	(Leer)	cmdb_ci_netgear		eModem = 27
eMotoStarter	Industrielaufwerk	cmdb_ci_ot_industrial_line	industrielle_Laufwerke	eMotoStarter = 69
eNetworkAccessStorage	(Leer)	cmdb_ci_server		eNetworkAccessStorage = 30
eNetwork	(Leer)	cmdb_ci_netgear		eNetwork = 3
eNTPServer	(Leer)	cmdb_ci_server		eNTPServer = 21
eOPCServer	OPC-Server	cmdb_ci_ot_opc_server	opc_server	eOPCServer = 16
eOT	Gerät der operativen Technologie	cmdb_ci_ot	ot_base	eOT = 17
ePLC	SPS	cmdb_ci_ot_plc	SPS	ePLC = 0
eDrucker	(leer)	cmdb_ci_printer		eDrucker = 6
eProxyServer	(leer)	cmdb_ci_netgear		eProxyServer = 28
eRemoteIO	OT-Feldgerät	cmdb_ci_ot_field_device	ot_field_device	eRemoteIO = 13
eReverseProxyServer	(Leer)	cmdb_ci_netgear		eReverseProxyServer = 29
eRobot	Industrierobot	cmdb_ci_ot_industrial_line	industrielle_robot	eRobot = 57
eRouter	Router	cmdb_ci_ip_router		eRouter = 11
eRTU	RTU	cmdb_ci_ot_rtu	rtu	eRTU = 18
eSCADAClient	SCADA-Client	cmdb_ci_ot_scada_client	scada_client	eSCADAClient = 7
eSCADAMaster	SCADA-Server	cmdb_ci_ot_scada_server	scada_server	eSCADAMaster = 38
eSCADAServer	SCADA-Server	cmdb_ci_ot_scada_server	scada_server	eSCADAServer = 8
eSensor	Industriesensor	cmdb_ci_ot_industrial_line	industrielle_sensor	eSensor = 67
eSmartLight	(Leer)	cmdb_ci_iot		eSmartLight = 51
eSmartPhone	(Leer)	cmdb_ci_iot		eSmartPhone = 44
eSmartWatch	(Leer)	cmdb_ci_iot		eSmartWatch = 45
eStorageArray	(Leer)	cmdb_ci_server		eStorageArray = 36
eStreamer	(Leer)	cmdb_ci_iot		eStreamer = 52
eSwitch	(Leer)	cmdb_ci_ip_Switch		eSwitch = 12
eSyslogServer	(Leer)	cmdb_ci_server		eSyslogServer = 25
eTerminalServer	(Leer)	cmdb_ci_server		eTerminalServer = 24
eTVBildschirm	(Leer)	cmdb_ci_iot		eTVBildschirm = 40
eUPS	(Leer)	cmdb_ci_ups		eUPS = 63
eUserConsole	HMI	cmdb_ci_ot_hmi	hmi	eUserConsole = 22

Claroty CTD-Typ	ServiceNow-Typ	Klasse	OT-Entitätstyp	Claroty-Typen und -Codes
eUserWorkstation	HMI	cmdb_ci_ot_hmi	hmi	eUserWorkstation = 23
eVendingMachine	(Leer)	cmdb_ci_iot		eVendingMachine = 43
eVideoRecorder	(Leer)	cmdb_ci_server		eVideoRecorder = 64
eVirtualizationServer	(Leer)	cmdb_ci_server		eVirtualizationServer = 65
eVoipPhone	(Leer)	cmdb_ci_comm_hardware		eVoipPhone = 39
eVoipServer	(Leer)	cmdb_ci_server		eVoipServer = 56
eWebServer	(Leer)	cmdb_ci_server		eWebServer = 34
eWirelessLanController	(Leer)	cmdb_ci_netgear		eWirelessLanController = 59
eBarcodeReader	(Leer)	cmdb_ci_iot		eBarcodeReader = 77
eBimetricScanner	(Leer)	cmdb_ci_iot		eBimetricScanner = 74
eDNSServer	(Leer)	cmdb_ci_server		eDNSServer = 75
eSNMPScanner	(Leer)	cmdb_ci_server		eSNMPScanner = 73
eSNMPServer	(Leer)	cmdb_ci_server		eSNMPServer = 72
eVisionCamera	OT-Feldgerät	cmdb_ci_ot_field_device	ot_field_device	eVisionCamera = 76
eVisionController	OT-Steuerungssystem	cmdb_ci_ot_control	ot_control_system	eVisionController = 78
eVisionSensor	OT-Feldgerät	cmdb_ci_ot_field_device	ot_field_device	eVisionSensor = 79
eVOIPAccessPoint	(Leer)	cmdb_ci_ip_Switch		eVOIPAccessPoint = 71
eVulnerabilityScanner	(Leer)	cmdb_ci_server		eVulnerabilityScanner = 70

Service Graph Connector für Microsoft Defender for IoT (Azure)

Integrieren Sie Microsoft Defender for IoT in die Anwendung ServiceNow® Operational Technology Manager, um den Import von OT-Geräten und Sensor-Appliances zu automatisieren.

Apps im Store anfordern

Besuchen Sie die Website [ServiceNow Store](#) , um sich alle verfügbaren Apps anzusehen 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](#) .

Unterstützte Versionen

- Unterstützt Microsoft Defender for IoT -Sensorversionen:
 - 22.2.3.22
 - 22.2.5.9
- Unterstützte ServiceNow -Versionen:
 - Utah
 - Vancouver
 - Washington
 - Xanadu
 - Yokohama

Anwendungsfälle

Sie können den Service Graph Connector für Microsoft Defender for IoT (Azure) mit der Anwendung ServiceNow® Operational Technology Manager verwenden, um OT-Geräte und Sensor-Appliances zu importieren.

Geführtes Setup

Das geführte Setup für den Service Graph Connector für Microsoft Defender for IoT (Azure) bietet eine organisierte Abfolge von Aufgaben zum Konfigurieren der Integration in Ihrer -Instanz. Informationen zum Zugriff auf das geführte Setup finden Sie unter [Konfigurieren Sie das geführte Setup](#).

CMDB Dashboard für Integrationen

Die Store-App Gemeinsame Komponenten für CMDB-Integrationen bietet ein Dashboard mit einer zentralen Ansicht des Status, der Verarbeitungsergebnisse und der Verarbeitungsfehler aller installierten Integrationen. Sie können Metriken für alle Integrationsausführungen anzeigen. Sie können die Ansicht nach einer bestimmten CMDB Integration, einer bestimmten Zeitdauer oder einer bestimmten Integrationsausführung filtern. Weitere Informationen zur Überwachung von Integrationen im Integrations-Dashboard CMDB finden Sie unter [Integration Commons for CMDB](#) .

Datenzuordnung

Daten aus den Datenquellen Microsoft Defender for IoT (Azure) werden zugeordnet und mithilfe der Robust Transform Engine (RTE) in die Klassendefinitionen der ServiceNow CMDB Configuration Item(CI)-Klasse umgewandelt. Daten werden mithilfe der Identification and Reconciliation Engine (IRE) in ServiceNow CMDB eingefügt.

Wenn Sie das Setup abgeschlossen haben, können Sie die Integration so konfigurieren, dass regelmäßig Daten aus der Anwendung Microsoft Defender for IoT (Azure) abgerufen werden.

In der folgenden Tabelle sind die Datenquellen aufgeführt, die für ein Microsoft Defender for IoT -Projekt (Azure) enthalten sind, und die entsprechenden Bereitstellungstabellen, in die die importierten Daten geladen werden.

Datenquellen und Bereitstellungstabellen für Microsoft Defender for IoT (Azure)

Datenquelle	Bereitstellungstabelle
SG-OT Azure D4IoT – Geräteimport	SG-OT Azure D4IoT – Geräteimport [sn_msftd4iotazsgc_sg_ot_azure_d4iot_devices_import]
SG-OT Azure D4IoT – Sensorenimport	SG-OT Msft D4IoT – Sensorenimport [sn_msftd4iotazsgc_sg_ot_azure_d4iot_sensors_import]

Die aus den Bereitstellungstabellen importierten Daten werden dann in die folgenden Zieltabellen eingefügt:

- AIX-Server [cmdb_ci_aix_server]
- Computer [cmdb_ci_computer]
- Konfigurationselement [cmdb_ci]
- DCS [cmdb_ci_ot_dcs]
- ESX-Server [cmdb_ci_esx_server]
- EWS [cmdb_ci_ot_ews]
- Externe Systemmetadaten [cmdb_key_value_v2]
- Spielkonsole [cmdb_ci_quest_console]
- Handcomputergerät [cmdb_ci_handgehalten_computing]
- Historian [cmdb_ci_ot_historian]
- HMI [cmdb_ci_ot_hmi]
- HP-UX-Server [cmdb_ci_hpux_server]
- HLK-Geräte [cmdb_ci_hvac]
- HyperV-Server [cmdb_ci_hyper_v_server]
- IED [cmdb_ci_ot_ied]
- Industrieaktuator [cmdb_ci_ot_industrial_actuator]
- Industrielaufwerk [cmdb_ci_ot_industrial_drive]
- Industrierobot [cmdb_ci_ot_industrial_robot]
- Industriesensor [cmdb_ci_ot_industrial_sensor]
- IoT-Gerät [cmdb_ci_iot]
- IP-Adresse [cmdb_ci_ip_address]
- IP-Kamera [cmdb_ci_ip_kamera]
- IP-Firewall [cmdb_ci_ip_firewall]
- IP-Telefon [cmdb_ci_ip_phone]
- Linux-Server [cmdb_ci_linux_server]
- Netgear [cmdb_ci_netgear]
- Netzwerkadapter [cmdb_ci_network_adapter]
- Erkennungssystem für Netzwerkangriffe [cmdb_ci_nids]
- Operative Technologien (OT) [cmdb_ci_ot]

- OSX-Server [cmdb_ci_osx_server]
- OT-Steuerungsmodul [cmdb_ci_ot_control_module]
- OT-Steuerungssystem [cmdb_ci_ot_control]
- OT-Gerät-Details [cmdb_ot_entity]
- OT-Feldgerät [cmdb_ci_ot_field_device]
- SPS [cmdb_ci_ot_plc]
- Drucker [cmdb_ci_printer]
- RTU [cmdb_ci_ot_rtu]
- Seriennummer [cmdb_serial_number]
- Server [cmdb_ci_server]
- Server [cmdb_ci_server]
- Solaris-Server [cmdb_ci_solaris_server]
- Quelle [sys_object_source]
- Unix-Server [cmdb_ci_unix_server]
- Unterbrechungsfreie Stromversorgung (USV) [cmdb_ci_ups]
- Drahtloser Zugriffspunkt [cmdb_ci_wap_network]

Weitere Informationen zum Speicherort von Daten beim Abrufen von Daten aus einem Microsoft Defender for IoT (Azure) -Projekt finden Sie unter [Angestrebte CMDB-Klassen](#).

Konfigurieren Sie den Service Graph Connector für Microsoft Defender for IoT (Azure)

Verwenden Sie das geführte Setup für den Service Graph Connector für Microsoft Defender for IoT (Azure), um sich durch die Integrationsschritte führen zu lassen.

Vorbereitungen

Abhängigkeiten und Anforderungen:

- Die Store-App [Integration Commons for CMDB](#) , die automatisch installiert wird.
- [CMDB CI Class Models](#) , das automatisch installiert wird.
- Plugin „ITOM Discovery License“ (com.snc.itom.discovery.license). Sie müssen dieses Plugin aktivieren.
- ITOM-Lizenzierungs-Plugin (com.snc.itom.license). Weitere Informationen finden Sie unter [Discovery anfordern](#) .
- Das Plugin „Datastream Action“ (com.glide.hub.action_type.datastream), das automatisch installiert wird.

Erforderliche Rolle: Administrator

Hinweis:

Wenn Sie eine frühere Version des Service Graph Connector für Microsoft Defender for IoT (Azure) haben, migrieren Sie keine Daten aus dem alten Connector. Sie müssen die vorherige Version deinstallieren und die neue Integration ausführen.

Prozedur

1. Stellen Sie mithilfe der Anwendungsauswahl sicher, dass der Anwendungsbereich auf die Anwendung Service Graph Connector für Microsoft Defender for IoT (Azure) festgelegt ist.
Weitere Informationen finden Sie unter [Application picker](#) .
2. Navigieren zu **Alle > Service Graph für MSFT D4IoT (Azure) > Geführtes Setup**.
3. Wählen Sie auf der Seite „Erste Schritte “ **Erste Schritte** aus.
4. Um auf die Ressourcen Azure zuzugreifen, gehen Sie wie folgt vor:
 - a. Wählen Sie die Aufgabe Zugriff auf Ressourcen Azure aus.
 - b. Wenn Sie die Anweisungen in der Beschreibung abgeschlossen haben, wählen Sie **Als abgeschlossen markieren** aus.
5. Führen Sie zum Einrichten der Verbindungen und Anmeldeinformationen Folgendes aus:
 - a. Wählen Sie im Abschnitt Verbindungen und Anmeldeinformationen konfigurieren die Aufgabe Verbindungen und Anmeldeinformationen einrichten aus.
 - b. Wählen Sie **Konfigurieren**.
 - c. Wählen Sie den Datensatz **SG-OT Azure Connection (SG-OT-Azure-Verbindung)** aus.
 - d. Wählen Sie den zugehörigen Link Neue Verbindung und Anmeldeinformationen erstellen aus.
 - e. Füllen Sie im Fenster „Verbindungen und Anmeldeinformationen erstellen“ die folgenden Felder aus.

Feld	Beschreibung
Verbindungsname	Anzeigenname für den Verbindungsdatensatz
Verbindungs-URL	Azure-URL
OAuth-Client-ID	Client-ID (Anwendungs-ID) oder Dienstprinzipal-ID
OAuth-Client-Geheimnis	Geheimer Clientschlüssel, der dem Dienstprinzipal zugeordnet ist
OAuth-Token-URL	URL zum Abrufen des Autorisierungstokens. Ersetzen <tenantid> in der URL mit dem Mandanten-ID-Wert.

Hinweis:

Wenn eine Tokengenerierung erfolgreich ist, wird ein neues Fenster mit einer Erfolgsmeldung angezeigt. Wenn die Tokengenerierung nicht erfolgreich ist, wird ein neues Fenster mit der Fehlermeldung „OAuth-Flow fehlgeschlagen“ angezeigt. Überprüfen Sie die angegebenen Details, und versuchen Sie es erneut, indem Sie den von Ihnen erstellten Datensatz bearbeiten.

- f. Wählen Sie **OAuth-Token erstellen und abrufen** aus.
6. Um die Verbindung zu testen, führen Sie Folgendes aus:

- a. Wählen Sie im Abschnitt „Verbindungen und Anmeldeinformationen einrichten“ die Aufgabe Verbindung testen/validieren aus.
 - b. Wählen Sie im Datenquellen-Datensatz für Sensoren im Abschnitt „Zugehörige Links“ die UI-Aktion **Verbindung testen** aus.
Zeigen Sie nach Abschluss des Verbindungstests die Ergebnisse an. Sie müssen die vorgeschlagenen Problembehandlungsschritte ausführen, bis das Testergebnis **Erfolg** zurückgibt.
7. Führen Sie zum Konfigurieren der Systemeigenschaften Folgendes aus:
- a. Wählen Sie im Abschnitt Konfigurieren von Systemeigenschaften **die Option Konfigurieren** aus.
 - b. Konfigurieren Sie die folgenden Systemeigenschaften.

Eigenschaft	Beschreibung
sn_msft4iotazsgc.resource_path	Legen Sie die Ressourcenpfadeigenschaft fest. Der standardmäßige Ressourcenpfad für die ARG-REST-API-Version vom 01.03.2021 lautet/providers/Microsoft.ResourceGraph/resources.
sn_msft4iotazsgc.pagesize.sensor	Legen Sie die Seitengrößeneigenschaft für Sensoren fest. - Da die Azure ARG-REST-API Paginierung unterstützt, können Sie die Anzahl der Datensätze pro Seite für jede API auswählen. - Der Standardwert ist 1000 Datensätze pro Seite. i Hinweis: 1000 ist auch die maximale Anzahl von Datensätzen pro Seite.
sn_msft4iotazsgc.pagesize.device	Legen Sie die Seitengrößeneigenschaft für Geräte fest. - Da die Azure ARG-REST-API Paginierung unterstützt, können Sie die Anzahl der Datensätze pro Seite für jede API auswählen. - Der Standardwert ist 1000 Datensätze pro Seite. i Hinweis: 1000 ist auch die maximale Anzahl von Datensätzen pro Seite.
sn_msft4iotazsgc.get_all_devices	Bei Geräten können Sie wählen, ob alle Datensätze (Kontrollkästchen aktiviert) oder die Delta-Datensätze

Eigenschaft	Beschreibung
	(Kontrollkästchen deaktiviert) abgerufen werden sollen. Das DELTA ruft alle Datensätze ab, die seit der Startzeit des letzten erfolgreichen Imports in CMDB erstellt oder aktualisiert wurden.  Hinweis: Wenn Sie die Geräteintegration zum ersten Mal ausführen, werden alle Datensätze unabhängig von dieser Eigenschaft importiert.
sn_msft4iotazsgc.convert_sensor_names_to_lower	Legen Sie diese Eigenschaft für den Geräteimport fest. - Diese Systemeigenschaft wird verwendet, um die von Microsoft Azure bereitgestellten Sensornamen beim Importieren von Geräten in Kleinbuchstaben zu konvertieren. - Dies ist erforderlich, da Microsoft Azure Daten für die Abfrage in Kleinbuchstaben erwartet.
sn_msft4iotazsgc.filter.device_sub_types	Legen Sie diese Eigenschaft fest, um die Geräte während des Geräteimports nach Untertyp zu filtern. - Kommagetrennte Liste von Microsoft Azure -Untertypen zum Filtern der Geräte. - Beispiel: Um nur SPS und Server zu importieren, geben Sie den Wert aus dem Attribut „DeviceSubType“ von Microsoft Azure als Server, SPS an.
sn_msft4iotazsgc.filter.device_tags	Legen Sie diese Eigenschaft fest, um die Geräte während des Geräteimports nach Geräte-Tag zu filtern. - Kommagetrennte Liste von Tags, bei denen die Groß-/Kleinschreibung zu beachten ist, die zum Filtern von Geräten erforderlich sind. - Beispiel: Um Geräte mit bestimmten Tags zu importieren, geben Sie eine Liste von Werten aus dem Attribut „DeviceTags“ in Microsoft Azure an.
sn_msft4iotazsgc.filter.custom_query	Legen Sie diese Eigenschaft fest, um neben den Filtern „Geräteuntertyp“ und „Geräte-Tags“ weitere Filter für den Geräteimport hinzuzufügen.

Eigenschaft	Beschreibung
	- Abfrage zum Filtern basierend auf anderen Attributen. - Dies ermöglicht die Filterung nach anderen Attributen. Weitere Informationen finden Sie unter Azure-Abfragesprache .

c. Wählen Sie **Speichern**.

8. Um Sensoren zu importieren, gehen Sie wie folgt vor:

- a. Wählen Sie im Abschnitt „Configure Sensors (NIDS)“ (Sensoren konfigurieren (NIDS)) die Aufgabe Sensoren importieren aus.
- b. Wählen Sie **Konfigurieren**.
- c. Wählen Sie **Aktiv** aus, um den geplanten Datenimportauftrag zu aktivieren.

9. Führen Sie zum Konfigurieren des NIDS Folgendes aus:

- a. Wählen Sie im Abschnitt „Configure Sensors (NIDS)“ (Sensoren konfigurieren (NIDS)) die Aufgabe Sensoren importieren aus.
- b. Wählen Sie **Als abgeschlossen markieren** aus, sobald Sie die in der Beschreibung verknüpfte NIDS-Konfiguration abgeschlossen haben.

10. Führen Sie die folgenden Schritte aus, um Importzeitpläne zu konfigurieren:

- a. Wählen Sie im Abschnitt Importzeitpläne konfigurieren **die Option Konfigurieren aus**.
- b. Wählen Sie „**SG-OT Microsoft Azure D4IoT – Geplanter Import der Sensoren**“ aus, um den Importzeitplan für Sensoren nach Bedarf zu überprüfen oder zu ändern.
 - i. Wählen Sie **Aktiv** aus, um den Zeitplan für den Sensorenimport zu aktivieren.
 - ii. Standardmäßig ist der Zeitplan für den Sensorenimport so konfiguriert, dass er täglich um Mitternacht ausgeführt wird. Ändern Sie den Zeitplan mithilfe der Felder **Ausführung** und **Zeit**.
 - iii. Aktivieren Sie das Kontrollkästchen **Bedingt**, um diesen Zeitplan als bedingt festzulegen.
 - iv. Wählen Sie **Jetzt ausführen** aus, um einen manuellen Import zu starten.
- c. Wählen Sie **Geplanter Import von SG-OT Microsoft Azure D4IoT-Geräten** aus, um den Importzeitplan für Geräte nach Bedarf zu überprüfen oder zu ändern.
 - i. Wählen Sie **Aktiv** aus, um den Zeitplan für den Sensorenimport zu aktivieren.
 - ii. Standardmäßig ist der Zeitplan für den Sensorenimport so konfiguriert, dass er täglich um Mitternacht ausgeführt wird. Ändern Sie den Zeitplan mithilfe der Felder **Ausführung** und **Zeit**.

- iii. Aktivieren Sie das Kontrollkästchen **Bedingt**, um diesen Zeitplan als bedingt festzulegen.
- iv. Wählen Sie **Jetzt ausführen** aus, um einen manuellen Import zu starten.

** Hinweis:**

Geräte werden pro Sensor abgefragt. Der Service Graph Connector fragt nur Geräte ab, die von einem validierten Sensor erkannt wurden. Weitere Informationen finden Sie in Schritt 9.

- 11. Wahlweise:** Wenn Konfigurationselemente (CIs) in CMDB erstellt werden, werden Asset-Datensätze erstellt.
Der Asset-Datensatz enthält die Modellkategorie des CI. Weitere Informationen zu den Modellkategorien für Operational Technology (OT) finden Sie unter [Modellkategorien für Operational Technology](#). Führen Sie Folgendes aus, um die Modellkategorie für ein OT-Gerät anzuzeigen:

- a. Navigieren zu **Alle > Operative Technologien (OT) > Alle OT-Geräte**.
- b. Wählen Sie das OT-Gerät aus, für das Sie den Asset-Datensatz anzeigen möchten.
- c. Wählen Sie neben dem Feld **Asset** das Symbol **Vorschau auf diesen Datensatz anzeigen** () aus.
- d. Wählen Sie **Datensatz öffnen**.

- 12. Wahlweise:** Um Probleme mit dem Service Graph Connector für Microsoft Defender for IoT (Azure) zu beheben, gehen Sie wie folgt vor:

- a. Wählen Sie den Abschnitt [OPTIONAL] Problembehandlung bei Service Graph Connector für Microsoft Defender for IoT (Azure) aus.
- b. Wählen Sie in der Aufgabe Geplante Validierungen ausführen die Option **Konfigurieren aus**.
- c. Wählen Sie **Jetzt ausführen**.
Dieser Auftrag führt Aufgaben aus, um die Konfigurationen für SGC und die Verbindung zu Microsoft Azure zu validieren. Wenn Konfigurationsprobleme gefunden werden, melden die Validierungsergebnisse das Problem und schlagen Problembehandlungsschritte vor. Warten Sie, bis die geplante Aufgabe abgeschlossen ist.
- d. Sobald die geplante Aufgabe abgeschlossen ist, navigieren Sie zurück zum Abschnitt [OPTIONAL] Problembehandlung bei Service Graph Connector für Microsoft Defender for IoT (Azure).
- e. Wählen Sie in der Aufgabe Validierungsergebnisse überprüfen die Option **Konfigurieren aus**.
Dieser Schritt öffnet die Ausführungsprotokolle und Vorschläge der letzten Problembehandlung, damit Sie sie anzeigen können.
- f. Behandeln Sie die Vorschläge nach Bedarf.

** Hinweis:**

Sie können das geplante Skript jederzeit nach der Erstkonfiguration von Service Graph Connector Integration for Claroty CTD verwenden. Um Validierungen auszulösen, navigieren Sie zu **Alle > Service Graph für MSFT D4IoT (Azure) > Problembehandlung > Problembehandlung ausführen**. Um die Validierungsergebnisse anzuzeigen, navigieren Sie zu **Alle > Service Graph für MSFT D4IoT (Azure) > Problembehandlung > Ergebnisse**.

Nächste Maßnahme

Sie können jetzt Microsoft Defender for IoT (Azure) mit dem ServiceNow Service Graph Connector für Microsoft Defender for IoT (Azure) verbinden. Weitere Informationen finden Sie unter [Ihr Microsoft Defender for IoT \(Azure\)-Abonnement wird mit ServiceNow Service Graph Connector für Microsoft Defender for IoT \(Azure\) verbunden \(KB1587770\)](#) .

Validiert NIDS-Sensoren

Validiert die Netzwerk-IDS-Sensoren (NIDS) nach dem Import zur Vorbereitung des Geräteimports. Sensoren bestehen die Validierung nur, wenn sie sich nicht im Lernmodus befinden, da sie nicht für den Geräteimport geeignet sind.

Vorbereitungen

Es wird empfohlen, das CSDM-Plugin zu installieren. Der Service Graph Connector ist an den Lebenszyklusdatenmodellen gemäß den CMDB-Standards ausgerichtet. Weitere Informationen finden Sie unter [Implementing the CSDM framework in stages](#) .

Erforderliche Rolle: cmdb_nids_admin

Hinweis:

Ein NIDS-Gerät in ServiceNow stellt einen Microsoft Defender for IoT -Sensor (Azure) dar.

Warum und wann dieser Vorgang ausgeführt wird

Die Felder „**Lebenszyklusphase**“ und „**Status der Lebenszyklusphase**“ werden verwendet, um den Lernmodus eines Sensors zu erfassen. Wenn das Feld Lebenszyklusphase auf **Funktionsfähig** und der Status der Lebenszyklusphase auf **Lernmodus** festgelegt ist, ist die Validierung nicht erfolgreich. Wenn das Feld Status der Lebenszyklusphase auf **In Gebrauch** festgelegt ist, ist die Validierung erfolgreich.

Prozedur

1. Navigieren zu **Alle > Netzwerk-IDS-Appliances (NIDS) > Sensoren**.
2. Wählen Sie den Sensordatensatz aus, den Sie validieren möchten.
3. Fügen Sie im Abschnitt „NIDS Assigned Meta Data“ (NIDS zugewiesene Metadaten) Werte für den Sensor hinzu, der den erkannten Geräten zugewiesen werden soll.
4. Stellen Sie im Abschnitt „NIDS-Administratorkonfiguration“ sicher, dass der Wert des Felds „**Status der Lebenszyklusphase**“ nicht **Lernmodus** lautet.
Andernfalls schlägt die Validierung fehl.
5. Stellen Sie sicher, dass das Feld „**NIDS-Netzwerktyp**“ auf Grundlage des Standorts des NIDS-Netzwerks festgelegt ist.
Sie können beispielsweise den NIDS-Netzwerktyp „**IT**“ für eine Rechenzentrumsbereitstellung des NIDS oder den NIDS-Netzwerktyp „**OT**“ für eine industrielle Bereitstellung in einem Industrie-/OT-Netzwerk auswählen.

Wenn Sie OT auswählen, werden die OT-Gerät-Details für alle Geräte erstellt.

6. Wenn die Attribute korrekt ausgefüllt sind, wählen Sie **Validieren** aus.

i Hinweis:

HINWEIS: Die Attribute, die vom Sensor an die Geräte übergeben werden, sind in der Systemeigenschaft `sn_cmdb_ci_class.nids_map_fields` definiert. Die folgende Liste ist die Standardliste der Attribute.

- assigned_to
- location
- Unternehmen
- owned_by
- managed_by
- supported_by
- change_control
- support_group
- managed_by_group
- assignment_group
- Zone
- isa_entity_site (nur verfügbar, wenn Sie die Anwendung Prozessmanager Industrie installiert haben)

Verwenden Sie das Verbindungs-Framework Service Graph .

Verwenden Sie das Verbindungs-Framework Service Graph, um die zugehörigen Datenquellen, Systemeigenschaften und geplanten Datenimporte, die für Microsoft Azure erstellt wurden, an einem Ort zu sammeln.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Es sind Anwendungsmodule verfügbar, um separat zu den Datenquellen, Systemeigenschaften und geplanten Datenimporten für den Service Graph Connector für Microsoft Defender for IoT (Azure) zu navigieren. Das neue Service Graph -Verbindungs-Framework ermöglicht es jedoch, alle zugehörigen Datenquellen und geplanten Datenimporte, die für Microsoft Azure erstellt wurden, an zentraler Stelle zu sammeln. Sie können die Verbindung zur Quelle (Microsoft Azure) auch im Abschnitt „Zugehörige Links“ testen.

Prozedur

1. Stellen Sie mithilfe der Anwendungsauswahl sicher, dass der Anwendungsbereich auf die Anwendung Service Graph Connector für Microsoft Defender for IoT (Azure) festgelegt ist.
2. Navigieren zu **Alle > Service Graph für MSFT D4IoT (Azure) > Azure SGC-Verbindung**.
3. Wählen Sie auf der Seite „Service Graph-Verbindungen“ den Datensatz **SG-OT Azure SGC-Standardverbindung** aus.
4. **Wahlweise:** Um auf die Systemeigenschaften zuzugreifen, wählen Sie die Registerkarte **Service Graph-Verbindungseigenschaften**.

- 5. Wahlweise:** Um auf die Datenquellen zuzugreifen, wählen Sie die Registerkarte **Service Graph-Verbindungsdatenquellen**.
- 6. Wahlweise:** Um auf die geplanten Datenimporte zuzugreifen, wählen Sie die Registerkarte **Geplante Datenimporte für Service Graph-Verbindungen**.
- 7. Wahlweise:** Um Ihre Verbindung mit der Plattform Microsoft Azure zu testen, wählen Sie den zugehörigen Link **Verbindung testen** aus.
Sie können Ihre Verbindung jederzeit testen. Wenn der Verbindungstest abgeschlossen ist, finden Sie den Status und Vorschläge zur Problembehandlung der fehlgeschlagenen Schritte unter **Status** bzw. **Vorschlag** auf derselben Seite.

CMDB Klassen im Ziel von Service Graph Connector für Microsoft Defender for IoT (Azure)

Wenn Sie das geführte Setup abschließen, können Sie die Integration so konfigurieren, dass regelmäßig Daten aus einem Microsoft Defender for IoT (Azure)-Projekt abgerufen werden. Die Daten werden in Tabellen gespeichert, die sich auf die Tabelle Configuration Item [cmdb_ci] beziehen.

Computer [cmdb_ci_computer]

Die folgenden Attribute in der Tabelle „Computer“ [cmdb_ci_computer] werden durch gesammelte Daten gefüllt:

Attribute für Computer [cmdb_ci_computer].

Attributbezeichnung	Attributname
Neuester Discovery-Scan	last_discovered
Betriebssystem	os
OS-Adressbreite (Bit)	os_address_width
BS-Domäne	os_domain
BS-Version	os_version

Externe Systemmetadaten [cmdb_key_value_v2]

Die folgenden Attribute in der Tabelle „Externe Systemmetadaten“ [cmdb_key_value_v2] werden durch gesammelte Daten gefüllt:

Attribute für externe Systemmetadaten [cmdb_key_value_v2].

Attributbezeichnung	Attributname
Discovery-Quelle	discovery_source
Key	key
Quellschlüssel	source_key
Zeichenfolgenwert	string_value
URL-Wert	url_value
Werttyp	value_type

Hardware [cmdb_ci_hardware]

Die folgenden Attribute in der Tabelle „Hardware“ [cmdb_ci_hardware] werden durch gesammelte Daten gefüllt:

Attribute für Hardware [cmdb_ci_hardware].

Attributbezeichnung	Attributname
Klasse	sys_class_name
Modellnummer	model_number
Neuester Discovery-Scan	last_discovered
Standort	location
Modell-ID	model_id
Hersteller	manufacturer
Zuerst erkannt	first_discovered
Eigentum von	owned_by
Freigabegruppe	change_control
Verwaltet nach Gruppe	managed_by_group
Verwaltet von	managed_by
Name	name
Unternehmen	Unternehmen
Support-Gruppe	support_group
Change-Gruppe	assignment_group
Zugewiesen an	assigned_to
Support durch	supported_by

Für Hardware erstellte Beziehungen

Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
Hardware [cmdb_ci_hardware]	Eigentümer von::Eigentum von	IP-Adresse [cmdb_ci_ip_address]
Hardware [cmdb_ci_hardware]	Eigentümer von::Eigentum von	Netzwerkadapter [cmdb_ci_network_adapter]
Hardware [cmdb_ci_hardware]	Referenz	Externe Systemmetadaten [cmdb_key_value_v2]
Hardware [cmdb_ci_hardware]	Referenz	OT-Gerät [cmdb_ot_entity]

IP-Adresse [cmdb_ci_ip_address]

Die folgenden Attribute in der Tabelle „IP-Adresse“ [cmdb_ci_ip_address] werden durch gesammelte Daten gefüllt:

IP-Adressenattribute [cmdb_ci_ip_address].

Attributbezeichnung	Attributname
IP-Adresse	ip_address
IP-Version	ip_version
Im Besitz von Konfigurationselement	owned_by_cmdb_ci

Für die IP-Adresse erstellte Beziehungen

Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
IP-Adresse [cmdb_ci_ip_address]	Referenz	Erkennungssystem für Netzwerkangriffe [cmdb_ci_nids]
IP-Adresse [cmdb_ci_ip_address]	Referenz	Hardware [cmdb_ci_hardware]

Netzwerkadapter [cmdb_ci_network_adapter]

Die folgenden Attribute in der Tabelle „Netzwerkadapter“ [cmdb_ci_network_adapter] werden durch gesammelte Daten gefüllt:

Attribute für den Netzwerkadapter [cmdb_ci_network_adapter].

Attributbezeichnung	Attributname
MAC-Adresse	mac_address
Name	name
Discovery-Quelle	discovery_source

Für den Netzwerkadapter erstellte Beziehungen

Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
Netzwerkadapter [cmdb_ci_network_adapter]	Referenz	Erkennungssystem für Netzwerkangriffe [cmdb_ci_nids]
Netzwerkadapter [cmdb_ci_network_adapter]	Referenz	Hardware [cmdb_ci_hardware]

Erkennungssystem für Netzwerkangriffe [cmdb_ci_nids]

Die folgenden Attribute in der Tabelle „Netzwerkangriffserkennungssystem“ [cmdb_ci_nids] werden durch gesammelte Daten gefüllt:

Attribute für das Netzwerkangriffserkennungssystem [cmdb_ci_nids].

Attributbezeichnung	Attributname
Zuerst erkannt	first_discovered
NIDS-Quellenname	source_name
Lebenszyklusphase	life_cycle_stage

Attribute für das Netzwerkangriffserkennungssystem [cmdb_ci_nids]. (Fortsetzung)

Attributbezeichnung	Attributname
Status der Lebenszyklusphase	life_cycle_stage_status
Name	name
Korrelations-ID	correlation_id
Firmware-Version	firmware_version
Vollqualifizierter Domänenname	fqdn
NIDS-Zuweisungszone	Zone
Verbindungsstatus des NIDS-Managers	connection_state
Überprüft	überprüft
Hersteller	manufacturer

Für NIDS erstellte Beziehungen

Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
Erkennungssystem für Netzwerkangriffe [cmdb_ci_nids]	Erkennt::Erkannt von	Hardware [cmdb_ci_hardware]
Erkennungssystem für Netzwerkangriffe [cmdb_ci_nids]	Eigentümer von::Eigentum von	IP-Adresse [cmdb_ci_ip_address]
Erkennungssystem für Netzwerkangriffe [cmdb_ci_nids]	Eigentümer von::Eigentum von	Netzwerkadapter [cmdb_ci_network_adapter]

Operative Technologien (OT) [cmdb_ci_ot]

Die folgenden Attribute in der Tabelle „Operative Technologie (OT)“ [cmdb_ci_ot] werden durch gesammelte Daten gefüllt:

Attribute für Operational Technology (OT) [cmdb_ci_ot].

Attributbezeichnung	Attributname
Neuester Discovery-Scan	last_discovered

OT-Steuerungsmodul [cmdb_ci_ot_control_module]

Die folgenden Attribute in der Tabelle „OT-Steuerungsmodul“ [cmdb_ci_ot_control_module] werden durch gesammelte Daten ausgefüllt:

Attribute des OT-Steuerungsmoduls [cmdb_ci_ot_control_module].

Attributbezeichnung	Attributname
Lieferant	Lieferant
Support-Gruppe	support_group
Seriennummer	serial_number

Attribute des OT-Steuerungsmoduls [cmdb_ci_ot_control_module]. (Fortsetzung)

Attributbezeichnung	Attributname
Klasse	sys_class_name
Zuerst erkannt	first_discovered
Freigabegruppe	change_control
Verwaltet von	managed_by
Verwaltet nach Gruppe	managed_by_group
Change-Gruppe	assignment_group
Unternehmen	Unternehmen
Racknummer	rack_number
Slot-Nummer	slot_number
Standort	location
Name	name
Firmware-Version	firmware_version
Neuester Discovery-Scan	last_discovered
Zugewiesen an	assigned_to
Eigentum von	owned_by
Support durch	supported_by
Modell-ID	model_id

Für das OT-Steuerungsmodul erstellte Beziehungen

Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
OT-Steuerungsmodul [cmdb_ci_ot_control_module]	Referenz	OT-Gerät [cmdb_ot_entity]

OT-Steuerungssystem [cmdb_ci_ot_control]

Die folgenden Attribute in der Tabelle „OT-Steuerungssystem“ [cmdb_ci_ot_control] werden durch gesammelte Daten ausgefüllt:

Attribute für OT-Steuerungssystem [cmdb_ci_ot_control].

Attributbezeichnung	Attributname
Hat Modul	has_module
Neuester Discovery-Scan	last_discovered

Für OT-Steuerungssystem erstellte Beziehungen

Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
OT-Steuerungssystem [cmdb_ci_ot_control]	Eigentümer von::Eigentum von	OT-Steuerungsmodul [cmdb_ci_ot_control_module]

OT-Gerät [cmdb_ot_entity]

Die folgenden Attribute in der Tabelle „OT-Gerät“ [cmdb_ot_entity] werden durch gesammelte Daten gefüllt:

OT-Gerät-Attribute [cmdb_ot_entity].

Attributbezeichnung	Attributname
ISA-Entitätsstandort	isa_entity_site
OT-Erkennungsquellen-ID	ot_correlation_id
Gerät-Relevanz	business_criticality
Purdue-Ebene	purdue_level
Zone	Zone
OT-Gerätetyp	ot_asset_type

SPS [cmdb_ci_ot_plc]

Die folgenden Attribute in der Tabelle „SPS“ [cmdb_ci_ot_plc] werden durch gesammelte Daten gefüllt:

SPS-Attribute [cmdb_ci_ot_plc].

Attributbezeichnung	Attributname
Neuester Discovery-Scan	last_discovered
Schalterposition	switch_position
Remote wechseln	switch_remote_mode

Seriennummer [cmdb_serial_number]

Die folgenden Attribute in der Tabelle „Seriennummer“ [cmdb_serial_number] werden durch gesammelte Daten gefüllt:

Attribute für Seriennummer [cmdb_serial_number].

Attributbezeichnung	Attributname
Seriennummer	serial_number
Seriennummertyp	serial_number_type
Gültig	gültig

Für die Seriennummer erstellte Beziehungen

Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
Seriennummer [cmdb_serial_number]	Referenz	Hardware [cmdb_ci_hardware]
Netzwerkadapter [cmdb_ci_network_adapter]	Referenz	Hardware [cmdb_ci_hardware]

Attributzuordnung und -klassifizierung für Service Graph Connector für Microsoft Defender for IoT (Azure)

In den folgenden Tabellen wird die Attributzuordnung und -klassifizierung für Sensoren und Geräte beschrieben.

Attributzuordnung für Sensoren

Feldname für Nutzlast	Datentyp	Der Tabelle zugeordnet	Zu Feld zugeordnet	Beschreibung
id	Zeichenfolgenformat: /subscriptions/<subscription-id> /Provider/<provider> /Standorte/<location> /sites/<site> /sensor/<sensor-name>	• sys_object_source • cmdb_ci_nids	esnk in „sys_object_source“ • correlation_id	Eindeutige ID für den Sensor.
name	Zeichenfolge	cmdb_ci_nids	name	Name des Sensors.
properties.hostname	Zeichenfolge	cmdb_ci_nids	fqdn	Hostname des Sensors.
properties.ip	Zeichenfolge	cmdb_ci_ip_address	ip_address	IP-Adresse des Sensors.
properties.learningMode	Boolean	cmdb_ci_nids	Falsch oder nicht verfügbar: Lebenszyklusphase (life_cycle_stage): Status der operativen Lebenszyklusphase (life_cycle_stage_status): Wird verwendet Wahr: Lebenszyklusphase (life_cycle_stage): Status der operativen Lebenszyklusphase	Lernmodusstatus des IoT-Sensors.

Attributzuordnung für Sensoren (Fortsetzung)

Feldname für Nutzlast	Datentyp	Der Tabelle zugeordnet	Zu Feld zugeordnet	Beschreibung
			(life_cycle_stage_status): Lernen	
properties.mac	Zeichenfolge	cmdb_ci_network_adapter	name, mac_address	MAC-Adresse des Sensors.
properties.sensorStatus	Zeichenfolge	cmdb_ci_nids	connection_state	Status des IoT-Sensors.
properties.sensorVersion	Zeichenfolge	cmdb_ci_nids	firmware_version	Version des IoT-Sensors.
properties.upSince_utc	Datum und Uhrzeit als Zeichenfolge	cmdb_ci_nids	first_discovered	Startzeit
properties.zone	Zeichenfolge	cmdb_ci_nids	Zone	Zone des IoT-Sensors.

Attributzuordnung für Geräte

Feldname für Nutzlast	Datentyp	Der Tabelle zugeordnet	Zu Feld zugeordnet	Beschreibung
id	Zeichenfolgenformat: / subscriptions/ subscription-id>/providers/ <providers-id> /Standort/ <location> / deviceGroups/ <device-Group> / devices/<name-field>	• sys_object_source in „sys_object_source“. • cmdb_ot_entity • cmdb_key_value_v2 in cmdb_ot_entity	discovery_source_id	Eindeutige ID für das Gerät.
resourceGroup	(leer)	cmdb_key_value_v2	(leer)	Ressourcengruppe
tenantId	(leer)	cmdb_key_value_v2	(leer)	Mandanten-ID
properties.authorizedStatus	Zeichenfolge	cmdb_key_value_v2	(leer)	Autorisierter Status des Geräts
properties.criticality	Zeichenfolge	cmdb_ot_entity	business_criticality	Relevanz des Geräts
properties.deviceName	Zeichenfolge	cmdb_ci	name	Der Name des Geräts.
properties.deviceSubtypeName	Zeichenfolge	cmdb_ci	sys_class_name	Anzeigenname des Geräteuntertyps.
properties.firstSeen	Datum und Uhrzeit als Zeichenfolge	• cmdb_ci • cmdb_ci_ot_control_module (falls	first_discovered	Zeitpunkt, zu dem das Gerät zum ersten Mal angezeigt wurde.

Attributzuordnung für Geräte (Fortsetzung)

Feldname für Nutzlast	Datentyp	Der Tabelle zugeordnet	Zu Feld zugeordnet	Beschreibung
		Steuerungsmodul vorhanden sind)		
properties.lastSeen	Datum und Uhrzeit als Zeichenfolge	- cmdb_ci - cmdb_ci_ot_control_module (falls Steuerungsmodul vorhanden sind)	mod_recent_discovery	Zeitpunkt, zu dem das Gerät zuletzt angezeigt wurde.
properties.purdueLevel	Zeichenfolge	cmdb_ot_entity	purdue_level	Purdue-Ebene des Geräts.
Eigenschaften.Betriebssystem	Zeichenfolge	cmdb_ci_computer	os	BS-Verteilung
Eigenschaften.Betriebssystemversion	Zeichenfolge	cmdb_ci_computer	os_version	BS-Version
Eigenschaften.Betriebssystemplattform	Zeichenfolge	cmdb_ci_computer	os_domain	BS-Plattform
Eigenschaften.Betriebssystemarchitektur	Zeichenfolge	cmdb_ci_computer	os_address_width	BS-Architektur
properties.additionalFields.plcKeyState	(leer)	cmdb_ci_ot_plc	switch_position	SPS-Schlüsselstatus
properties.additionalFields.plcRunState	(leer)	cmdb_ci_ot_plc	switch_remote_mode	SPS- Ausführungsstatus
properties.hardware	Objekt	(leer)	(leer)	Daten zur Gerätehardware
Eigenschaften.Hardwaremodell	Zeichenfolge	cmdb_ci	(leer)	Hardwaremodell
properties.hardware.serialNumber	Zeichenfolge	cmdb_serial_number	serial_number	Hardware- Seriennummer
Eigenschaften.Hardwarelieferant	Zeichenfolge	cmdb_ci	manufacturer	Hardware-Lieferant
properties.nics	Array von Objekten	(leer)	(leer)	Liste der Netzwerkschnittstellenkarten des Geräts.
properties.nics[{}]	Objekt	(leer)	(leer)	Eigenschaften der Netzwerkschnittstellenkarte
properties.nics[{}].ipv4Address	Zeichenfolge	cmdb_ci_ip_address	ip_address	IPv4-Adresse
properties.nics[{}].macAddress	Zeichenfolge	cmdb_ci_network_adapter	name, Mac	MAC-Adresse
Eigenschaften Steckplatz	Array von Objekten	(leer)	(leer)	Liste des Gerätesteckplatzes in der Backplane.
Eigenschaften Steckplatz[{}]	Objekt	(leer)	(leer)	Slot-Daten in der SPS-Backplane.
properties.slots[{}].firmwareVersion	Zeichenfolge	cmdb_ci_ot_control_module	firmware_version	Firmware-Version des Slots.

Automatische Übersetzung

Attributzuordnung für Geräte (Fortsetzung)

Feldname für Nutzlast	Datentyp	Der Tabelle zugeordnet	Zu Feld zugeordnet	Beschreibung
properties.slots[{}].model	Zeichenfolge	cmdb_ci_ot_control	model_id	Modell des Steckplatzes.
Eigenschaften.SteckplatzRackNumber	Ganzzahl	cmdb_ci_ot_control	rack_number	Racknummer in der Backplane
properties.slots[{}].serial	Zeichenfolge	cmdb_ci_ot_control	serial_number	Seriennummer des Slots
properties.slots[{}].slot_number	Ganzzahl	cmdb_ci_ot_control	slot_number	Steckplatznummer im Rack.
properties.slots[{}].hardware_vendor	Zeichenfolge	cmdb_ci_ot_control	manufacturer	Hardware-Lieferant des Slots.

Klassifizierung des Gerätetyps

Microsoft Azure Name des Geräteuntertyps	Microsoft Azure Name des Gerätetyps	Betriebssystem/ Firmware	NOW-Kurs	NOW-Tabelle	NOW O
Alarmsirene	(leer)	(leer)	IoT-Gerät	cmdb_ci_iot	NULL
Alarmsystem	(leer)	(leer)	OT-Steuerungssystem	cmdb_ci_ot_control	OT-Steuerung
Geldautomat	(leer)	(leer)	IoT-Gerät	cmdb_ci_iot	NULL
Sicherungsserver	(leer)	(leer)	Server	cmdb_ci_server	NULL
Strichcode-Scanner	(leer)	(leer)	IoT-Gerät	cmdb_ci_iot	NULL
DB-Server	(leer)	(leer)	Server	cmdb_ci_server	NULL
DCS-Controller	Industriell	(leer)	DCS	cmdb_ci_ot_dcs	NULL
Domain Controller	(leer)	(leer)	Server	cmdb_ci_server	NULL
Türsteuerungsfeld	(leer)	(leer)	IoT-Gerät	cmdb_ci_iot	NULL
VR	(leer)	(leer)	IoT-Gerät	cmdb_ci_iot	NULL
Aufzug	(leer)	(leer)	IoT-Gerät	cmdb_ci_iot	NULL
Engineering-Station	Industriell	(leer)	EWS	cmdb_ci_ot_ews	EWS
Feueralarm	(leer)	(leer)	IoT-Gerät	cmdb_ci_iot	NULL
Feuermelder	(leer)	(leer)	IoT-Gerät	cmdb_ci_iot	NULL
Firewall	(leer)	(leer)	IP-Firewall	cmdb_ci_ip_firewall	NULL
Spielkonsole	(leer)	(leer)	Spielkonsole	cmdb_ci_spiel_konsole	NULL
Aufzeichnung	(leer)	(leer)	Aufzeichnung	cmdb_ci_ot_historian	Aufzeichn
HMI	Industriell	(leer)	HMI	cmdb_ci_ot_hmi	HMI
Feuchtigkeitssensor	(leer)	(leer)	IoT-Gerät	cmdb_ci_iot	NULL

Klassifizierung des Gerätetyps (Fortsetzung)

Microsoft Azure Name des Geräteuntertyps	Microsoft Azure Name des Gerätetyps	Betriebssystem/ Firmware	NOW-Kurs	NOW-Tabelle	NOW O
HLK	(leer)	(leer)	HLK-Zubehör	cmdb_ci_hvac	NULL
I/O-Adapter	(leer)	(leer)	Netzwerkadapter	(leer)	NA
IED	(leer)	(leer)	IED	cmdb_ci_ot_ied	geb
Industrielles Verpackungssystem	(leer)	(leer)	OT-Feldgerät	cmdb_ci_ot_field_device	OT-Feld
Industrieroboter	(leer)	(leer)	Industrieroboter	cmdb_ci_ot_industrial_robot	Industrie
Industrielle Skala	(leer)	(leer)	OT-Feldgerät	cmdb_ci_ot_field_device	OT-Feld
Gegensprechanlage	(leer)	(leer)	IoT-Gerät	cmdb_ci_iot	NULL
IP-Kamera	(leer)	(leer)	IP-Kamera	cmdb_ci_ip_kamera	NULL
IP-Telefon	(leer)	(leer)	IP-Telefon	cmdb_ci_ip_phone	NULL
Laufschrift	(leer)	(leer)	IoT-Gerät	cmdb_ci_iot	NULL
Zähler	(leer)	(leer)	Industriesensor	cmdb_ci_ot_industrial_sensor	Industrie
Bewegungsmelder	(leer)	(leer)	IoT-Gerät	cmdb_ci_iot	NULL
Multicast/Broadcast	(leer)	(leer)	Netgear	cmdb_ci_netgear	NULL
NTP-Server	(leer)	(leer)	Server	cmdb_ci_server	NULL
Personenzähler- System	(leer)	(leer)	IoT-Gerät	cmdb_ci_iot	NULL
Physischer Speicherort	(leer)	(leer)	(leer)	(leer)	NULL
SPS	Industriell	(leer)	SPS	cmdb_ci_ot_plc	SPS
pneumatisches Gerät	(leer)	(leer)	Industrieaktuator	cmdb_ci_ot_industrial_actuator	Industrie
Drucker	(leer)	(leer)	Drucker	cmdb_ci_printer	NULL
Protokollkonverter	(leer)	(leer)	Netgear	cmdb_ci_netgear	NULL
Stempeluhr	(leer)	(leer)	IoT-Gerät	cmdb_ci_iot	NULL
Robot-Controller	(leer)	(leer)	OT- Steuerungssystem	cmdb_ci_ot_control	OT- Steuerung
Router	(leer)	(leer)	IP-Router	cmdb_ci_ip_router	NULL
RTU	(leer)	(leer)	RTU	cmdb_ci_ot_rtu	NULL
Server	Server	(leer)	Server	cmdb_ci_server	NULL
Stellt Laufwerk ein	(leer)	(leer)	Industrieaktuator	cmdb_ci_ot_industrial_actuator	Industrie
Steckplatz	(leer)	(leer)	OT- Steuerungsmodul	cmdb_ci_ot_control_module	OT- Steuerung
Intelligentes Licht	(leer)	(leer)	IoT-Gerät	cmdb_ci_iot	NULL

Automatische Übersetzung

Klassifizierung des Gerätetyps (Fortsetzung)

Microsoft Azure Name des Geräteuntertyps	Microsoft Azure Name des Gerätetyps	Betriebssystem/ Firmware	NOW-Kurs	NOW-Tabelle	NOW O
Smartphone	(leer)	(leer)	Handcomputergerät	cmdb_ci_handgehalten_computing	NULL
Intelligenter Switch	(leer)	(leer)	IoT-Gerät	cmdb_ci_iot	NULL
Smart TV	(leer)	(leer)	Smart TV	cmdb_ci_stv	NULL
Speicher	(leer)	(leer)	Server	cmdb_ci_server	NULL
Switch	Netzwerkgerät	(leer)	IP-Switch	cmdb_ci_ip_switch	NULL
Tablet	(leer)	(leer)	Handcomputergerät	cmdb_ci_handgehalten_computing	NULL
Terminal-Station	(leer)	(leer)	Computer	cmdb_ci_computer	NULL
Raumtempererator	(leer)	(leer)	IoT-Gerät	cmdb_ci_iot	NULL
Drehkreuz	(leer)	(leer)	IoT-Gerät	cmdb_ci_iot	NULL
Unterbrechungsfreie Stromversorgung	(leer)	(leer)	UPS	cmdb_ci_ups	NULL
Frequenzumrichter	(leer)	(leer)	Industrielaufwerk	cmdb_ci_ot_industrial_drive	Industrie
VPN Gateway	(leer)	(leer)	Netgear	cmdb_ci_netgear	NULL
WLAN-Ananas	(leer)	(leer)	Netgear	cmdb_ci_netgear	NULL
Drahtloser Zugriffspunkt	(leer)	(leer)	Drahtloser Zugriffspunkt	cmdb_ci_wap_network	NULL
WLAN- Zugriffspunkt	Netzwerkgerät	(leer)	Drahtloser Zugriffspunkt	cmdb_ci_wap_network	NULL
Arbeitsplatz-PC	Arbeitsplatz- PC	(leer)	Computer	cmdb_ci_computer	NULL
Unbekannt	Alle	(leer)	Operative Technologien (OT)	cmdb_ci_ot	Operativ Technol (OT)
Nicht klassifiziert	„Nicht klassifiziert“ oder „Alle“.	(leer)	Operative Technologien (OT)	cmdb_ci_ot	Operativ Technol (OT)
Jeder andere Typ	(leer)	(leer)	Operative Technologien (OT)	cmdb_ci_ot	Operativ Technol (OT)
Beliebiger obiger Typwert außer mit der Bezeichnung „Netzwerk und IoT“.	(leer)	• Windows- Server • Windows Server, Version 2004[8] • Windows Server, Version 1909[9]	Windows-Server	cmdb_ci_linux_server	Identisch Fall, we Betriebs nicht vo ist.

Automatische Übersetzung

Klassifizierung des Gerätetyps (Fortsetzung)

Microsoft Azure Name des Geräteuntertyps	Microsoft Azure Name des Gerätetyps	Betriebssystem/ Firmware	NOW-Kurs	NOW-Tabelle	NOW O
		• Windows Server, Version 1903[9] • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2 • Windows Server 2008 • Windows Server 2003 R2 • Windows Server 2003 • Windows 2000-Server • Windows nt 4.0 Server • Windows nt 3.51 Server • Windows nt 3.5 Server • Windows nt 3.1 Server			
Beliebiger obiger Typwert außer mit der Bezeichnung „Netzwerk und IoT“.	(leer)	• Linux • arch • centos • Debian • Bucket Hat • suse	Linux-Server	cmdb_ci_linux_server	Identisch Fall, we Betriebs nicht vo ist.

Automatische Übersetzung

Klassifizierung des Gerätetyps (Fortsetzung)

Microsoft Azure Name des Geräteuntertyps	Microsoft Azure Name des Gerätetyps	Betriebssystem/ Firmware	NOW-Kurs	NOW-Tabelle	NOW O
		• Red Hat • RHEL • ubuntu • Oracle			
Beliebiger obiger Typwert außer mit der Bezeichnung „Netzwerk und IoT“.	(leer)	aix	AIX-Server	cmdb_ci_aix_server	Identisch Fall, wenn Betriebs- system nicht vor- handen ist.
Beliebiger obiger Typwert außer mit der Bezeichnung „Netzwerk und IoT“.	(leer)	esx	ESX-Server	cmdb_ci_esx_server	Identisch Fall, wenn Betriebs- system nicht vor- handen ist.
Beliebiger obiger Typwert außer mit der Bezeichnung „Netzwerk und IoT“.	(leer)	• HP/UX • HPUX	HP-UX Server	cmdb_ci_hpux_server	Identisch Fall, wenn Betriebs- system nicht vor- handen ist.
Beliebiger obiger Typwert außer mit der Bezeichnung „Netzwerk und IoT“.	(leer)	• Hyper-V • Hyperv • Hyper	HyperV-Server	cmdb_ci_hyper_v_server	Identisch Fall, wenn Betriebs- system nicht vor- handen ist.
Beliebiger obiger Typwert außer mit der Bezeichnung „Netzwerk und IoT“.	(leer)	• Solaris • Sunos • Sunos	Solaris-Server	cmdb_ci_solaris_server	Identisch Fall, wenn Betriebs- system nicht vor- handen ist.
Beliebiger obiger Typwert außer mit der Bezeichnung „Netzwerk und IoT“.	(leer)	• MacOS X- Server • MacOS-Server • BS x • OSX	OSX-Server	cmdb_ci_osx_server	Identisch Fall, wenn Betriebs- system nicht vor- handen ist.
Beliebiger obiger Typwert außer mit der Bezeichnung	(leer)	• Unix • GNU	Unix-Server	cmdb_ci_unix_server	Identisch Fall, wenn Betriebs-

Automatische Übersetzung

Klassifizierung des Gerätetyps (Fortsetzung)

Microsoft Azure Name des Geräteuntertyps	Microsoft Azure Name des Gerätetyps	Betriebssystem/ Firmware	NOW-Kurs	NOW-Tabelle	NOW O
„Netzwerk und IoT“.					nicht vo ist.
Beliebiger obiger Typwert außer mit der Bezeichnung „Netzwerk und IoT“.	(leer)	• Gewinn • windows • Microsoft • Windows 1.0, 1.02, 1.03, 1.04, 2.03, 2.10, 2.11, 3.0, 3.1, 3.2, 7, 8, 8.1, 10, 98, 95 • Windows 2000 • Windows für Arbeitsgruppen 3.11 • Fenster mich • Windows nt 3.1, 3.5, 3.51, 4.0 • Windows Visa • Windows XP • Windows XP Professional x64-Edition	Basiscomputerklasse	cmdb_ci_computer	Identisch Fall, we Betriebs nicht vo ist.
Beliebiger obiger Typwert außer mit der Bezeichnung „Netzwerk und IoT“.	(leer)	Server	Basisserverklasse	cmdb_ci_server	Identisch Fall, we Betriebs nicht vo ist.

Automatische Übersetzung

Service Graph Connector für Microsoft Defender for IoT (lokale Verwaltungskonsole)

Integrieren Sie Microsoft Defender for IoT (lokale Verwaltungskonsole) in die Anwendung ServiceNow® Operational Technology Manager, um den Import von Sensor-Appliances, OT-Geräten und Netzwerkverbindungen zu automatisieren.

Apps im Store anfordern

Besuchen Sie die Website [ServiceNow Store](#), um sich alle verfügbaren Apps anzusehen 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](#) .

Unterstützte Versionen

- Microsoft Defender for IoT (Lokale Verwaltungskonsole) Version: 10.5.2 oder höher
- Unterstützte ServiceNow -Versionen:
 - Utah
 - Vancouver
 - Washington
 - Xanadu

Anwendungsfälle

Sie können den Service Graph Connector für Microsoft Defender for IoT (lokale Verwaltungskonsole) mit der Anwendung ServiceNow® Operational Technology Manager verwenden, um Sensor-Appliances, OT-Geräte und Netzwerkverbindungen zu importieren.

Geführtes Setup

Das geführte Setup für den Service Graph Connector für Microsoft Defender for IoT (lokale Managementkonsole) bietet eine organisierte Abfolge von Aufgaben zum Konfigurieren der Integration in Ihrer Instanz. Informationen zum Zugriff auf das geführte Setup finden Sie unter [Konfigurieren Sie das geführte Setup](#).

CMDB Dashboard für Integrationen

Die Store-App Gemeinsame Komponenten für CMDB-Integrationen bietet ein Dashboard mit einer zentralen Ansicht des Status, der Verarbeitungsergebnisse und der Verarbeitungsfehler aller installierten Integrationen. Sie können Metriken für alle Integrationsausführungen anzeigen. Sie können die Ansicht nach einer bestimmten CMDB Integration, einer bestimmten Zeitdauer oder einer bestimmten Integrationsausführung filtern. Weitere Informationen zur Überwachung von Integrationen im Integrations-Dashboard CMDB finden Sie unter [Integration Commons for CMDB](#) .

Datenzuordnung

Daten aus den Datenquellen Microsoft Defender for IoT (lokale Managementkonsole) werden zugeordnet und mithilfe der Robust Transform Engine (RTE) in die Klassendefinitionen der Configuration Items (CI) ServiceNow CMDB umgewandelt. Daten werden mithilfe der Identification and Reconciliation Engine (IRE) in ServiceNow CMDB eingefügt.

Wenn Sie das Setup abschließen, können Sie die Integration so konfigurieren, dass in regelmäßigen Abständen Daten aus der Anwendung Microsoft Defender for IoT (lokale Verwaltungskonsole) abgerufen werden.

In der folgenden Tabelle sind die für ein Microsoft Defender for IoT -Projekt (lokale Managementkonsole) enthaltenen Datenquellen und die entsprechenden Bereitstellungstabellen aufgelistet, in die die importierten Daten geladen werden.

Datenquellen und Bereitstellungstabellen für Microsoft Defender for IoT (lokale Verwaltungskonsole)

Datenquelle	Bereitstellungstabelle
SG-OT Microsoft D4IoT – Verbindungsimport	SG-OT Msft D4IoT – Verbindungsimport [sn_msftd4iotsgc_sg_ot_msft_d4iot_connections_import]
SG-OT Microsoft D4IoT – Geräteimport	SG-OT Msft D4IoT – Geräteimport [sn_msftd4iotsgc_sg_ot_msft_d4iot_devices_import]
SG-OT Microsoft D4IoT – Sensorenimport	SG-OT Msft D4IoT – Sensorenimport [sn_msftd4iotsgc_sg_ot_msft_d4iot_sensors_import]

Die aus den Bereitstellungstabellen importierten Daten werden dann in die folgenden Zieltabellen eingefügt:

- AIX-Server [cmdb_ci_aix_server]
- Computer [cmdb_ci_computer]
- Konfigurationselement [cmdb_ci]
- DCS [cmdb_ci_ot_dcs]
- ESX-Server [cmdb_ci_esx_server]
- EWS [cmdb_ci_ot_ews]
- Externe Systemmetadaten [cmdb_key_value_v2]
- Spielkonsole [cmdb_ci_quest_console]
- Handcomputergerät [cmdb_ci_handgehalten_computing]
- Historian [cmdb_ci_ot_historian]
- HMI [cmdb_ci_ot_hmi]
- HP-UX-Server [cmdb_ci_hpux_server]
- HLK-Geräte [cmdb_ci_hvac]
- HyperV-Server [cmdb_ci_hyper_v_server]
- IED [cmdb_ci_ot_ied]
- Industrieaktuator [cmdb_ci_ot_industrial_actuator]
- Industrielaufwerk [cmdb_ci_ot_industrial_drive]
- Industrierobot [cmdb_ci_ot_industrial_robot]
- Industriesensor [cmdb_ci_ot_industrial_sensor]
- IoT-Gerät [cmdb_ci_iot]
- IP-Adresse [cmdb_ci_ip_address]
- IP-Kamera [cmdb_ci_ip_kamera]
- IP-Firewall [cmdb_ci_ip_firewall]
- IP-Telefon [cmdb_ci_ip_phone]
- Linux-Server [cmdb_ci_linux_server]
- Netgear [cmdb_ci_netgear]
- Netzwerkadapter [cmdb_ci_network_adapter]

- Erkennungssystem für Netzwerkangriffe [cmdb_ci_nids]
- Operative Technologien (OT) [cmdb_ci_ot]
- OSX-Server [cmdb_ci_osx_server]
- OT-Steuerungsmodul [cmdb_ci_ot_control_module]
- OT-Steuerungssystem [cmdb_ci_ot_control]
- OT-Gerät-Details [cmdb_ot_entity]
- OT-Feldgerät [cmdb_ci_ot_field_device]
- SPS [cmdb_ci_ot_plc]
- Drucker [cmdb_ci_printer]
- RTU [cmdb_ci_ot_rtu]
- Seriennummer [cmdb_serial_number]
- Server [cmdb_ci_server]
- Server [cmdb_ci_server]
- Solaris-Server [cmdb_ci_solaris_server]
- Quelle [sys_object_source]
- Unix-Server [cmdb_ci_unix_server]
- Unterbrechungsfreie Stromversorgung (USV) [cmdb_ci_ups]
- Drahtloser Zugriffspunkt [cmdb_ci_wap_network]

Weitere Informationen zum Speicherort von Daten beim Abrufen von Daten aus einem Microsoft Defender for IoT -Projekt (lokale Managementkonsole) finden Sie unter [Angestrebte CMDB-Klassen](#).

Den Service Graph Connector für Microsoft Defender for IoT konfigurieren (lokale Verwaltungskonsole)

Verwenden Sie das geführte Setup für den Service Graph Connector für Microsoft Defender for IoT (lokale Verwaltungskonsole), um sich durch die Integrationsschritte führen zu lassen.

Vorbereitungen

Abhängigkeiten und Anforderungen:

- Die Store-App [Integration Commons for CMDB](#), die automatisch installiert wird.
- [CMDB CI Class Models](#), das automatisch installiert wird.
- Plugin „ITOM Discovery License“ (com.snc.itom.discovery.license). Sie müssen dieses Plugin aktivieren.
- ITOM-Lizenzierungs-Plugin (com.snc.itom.license). Weitere Informationen finden Sie unter [Discovery anfordern](#).
- Das Plugin „DataStream Action“ (com.glide.hub.action_type.datastream), das automatisch installiert wird.

Erforderliche Rolle: Administrator

i Hinweis:

Wenn Sie eine frühere Version des Service Graph Connector für Microsoft Defender for IoT (lokale Verwaltungskonsole) haben, migrieren Sie keine Daten vom alten Connector. Sie müssen die vorherige Version deinstallieren und die neue Integration ausführen.

Prozedur

1. Stellen Sie mithilfe der Anwendungsauswahl sicher, dass der Anwendungsbereich auf die Anwendung Service Graph Connector für Microsoft Defender for IoT (On-premises Management Console) festgelegt ist. Weitere Informationen finden Sie unter [Application picker](#) .
2. Navigieren zu **Alle > Service Graph Connector Microsoft D4IoT > Geführtes Setup**.
3. Wählen Sie auf der Seite „Erste Schritte“ **Erste Schritte** aus.
4. Führen Sie zum Konfigurieren eines MID-Servers Folgendes aus:
 - a. Wählen Sie im Abschnitt „Verbindungen und Anmeldeinformationen einrichten“ die Aufgabe MID-Server konfigurieren aus.
 - b. Wählen Sie **Als abgeschlossen markieren** aus, sobald Sie die in der Beschreibung verknüpfte Konfiguration MID-Server abgeschlossen haben.
5. Führen Sie die folgenden Schritte aus, um den Datensatz „Alias für Verbindungen und Anmeldeinformationen“ zu aktualisieren:
 - a. Wählen Sie im Abschnitt „Verbindungen und Anmeldeinformationen einrichten“ die Aufgabe Verbindungen und Anmeldeinformationen aus.
 - b. Wählen Sie **Konfigurieren**.
 - c. Öffnen Sie den Standarddatensatz **Microsoft D4IoT Base API**.
 - d. Wählen Sie in der zugehörigen Liste „Verbindungen“ **Neu** aus, um einen neuen HTTP(S)-Verbindungsdatensatz zu erstellen.
 - e. Geben Sie im Feld **Verbindungs-URL** den Namen für die URL Ihres Microsoft Defender for IoT Central Manager ein.
Beispiel: `https://192.168.1.100`.
 - f. **Wahlweise:** Wenn Sie ein MID-Server verwenden, wählen Sie alle der folgenden Optionen aus:
 - **MID-Server-Feld verwenden**
 - **MID-Server** aus der zugehörigen Liste „Erweiterte MID-Server-Konfiguration“.
 - **MID-Auswahl** aus der Liste
 - g. Wählen Sie im Feld **Anmeldeinformationen** das Suchsymbol aus, um die Liste der Anmeldeinformationsdatensätze zu öffnen.
 - h. Wählen Sie **Neu** aus, um einen neuen Datensatz zu erstellen.
 - i. Wählen Sie den **Anmeldeinformationstyp API-Schlüssel** aus.
 - j. Geben Sie im Feld **API-Schlüssel** einen Namen und den API-Schlüssel ein, der von Ihrer Microsoft Defender for IoT -Verwaltungskonsole bereitgestellt wurde.

- k. Wählen Sie **Absenden aus**, um den Anmeldeinformationsdatensatz zu erstellen.
Informationen zum Erstellen eines API-Schlüssels in der -Verwaltungskonsolle Microsoft Defender for IoT finden Sie in der Produktdokumentation Microsoft Azure Event Hubs : <https://docs.microsoft.com/de-de/azure/defender-for-iot/organizations/references-work-with-defender-for-iot-apis> [↗](#) .

- l. Wählen Sie im Formular „Verbindung“ **Absenden aus**, um die Erstellung des Verbindungsdatensatzes abzuschließen.

6. Um die Verbindung zu testen, führen Sie Folgendes aus:

- a. Wählen Sie im Abschnitt „Verbindungen und Anmeldeinformationen einrichten“ die Aufgabe Verbindung testen/validieren aus.
- b. Wählen Sie im Datenquellen-Datensatz für Sensoren im Abschnitt „Zugehörige Links“ die UI-Aktion **Verbindung testen** aus.
Zeigen Sie nach Abschluss des Verbindungstests die Ergebnisse an. Sie müssen die vorgeschlagenen Problembehandlungsschritte ausführen, bis das Testergebnis **Erfolg** zurückgibt.

- c. Überprüfen Sie, ob der Verbindungsmanager über ein gültiges Zertifikat verfügt.

Für eine Produktionsumgebung muss ein gültiges Zertifikat installiert sein. Für eine Instanz außerhalb der Produktion oder für eine Proof of Concept-Instanz (POC) können Sie die Systemeigenschaften so konfigurieren, dass die Integration funktioniert, wenn der Verbindungsmanager nicht über ein gültiges Zertifikat verfügt. In der folgenden Tabelle sind die Systemeigenschaften aufgeführt, die Sie für eine Umgebung außerhalb der Produktion konfigurieren können.

Systemeigenschaften für eine Umgebung außerhalb der Produktion

Eigenschaft	Wert
com.glide.communications.httpclient.verify_hostname	Auf „false“ festlegen.
com.glide.communications.httpclient.verify_revoked_certificate	Auf „false“ festlegen. Wenn Sie diese Systemeigenschaft hinzufügen müssen, finden Sie weitere Informationen unter Systemeigenschaft hinzufügen ↗ .
com.glide.communications.trustmanager_trust_all	Auf wahr festlegen.

- d. Überprüfen Sie die MID-Sicherheitsrichtlinie.
Überprüfen Sie im Intranetdatensatz, ob die Spalten in der folgenden Tabelle die angegebenen Werte anzeigen.

Intranet-Datensatzwerte

Spalte	Wert
Zertifikatkettenprüfung	false
Hostnamenprüfung	false

Spalte	Wert
Widerrufsprüfung	false

Weitere Informationen finden Sie [unter Richtlinien für MID-Server-Zertifikatprüfung](#) .

Die Verbindung zeigt, dass sie richtig eingestellt ist, wenn im Fortschrittsfenster Abschlusscode **Erfolg** angezeigt wird und die Anzahl der verarbeiteten Datensätze als die gleiche Anzahl von Sensoren im Verbindungsmanager angezeigt wird.

7. Führen Sie zum Konfigurieren der Systemeigenschaften Folgendes aus:

a. Wählen Sie im Abschnitt Konfigurieren von Systemeigenschaften **die Option Konfigurieren aus**.

b. Konfigurieren Sie die folgenden Systemeigenschaften.

Eigenschaft	Beschreibung
sn_msftd4iotsgc.resourcepath.sensor	Legen Sie den Ressourcenpfad für Sensoren fest. - Der Ressourcenpfad für Sensoren wird standardmäßig für die V3-API-Version bereitgestellt. - Wenn Sie eine andere API-Version verwenden möchten, können Sie den Pfad überschreiben.
sn_msftd4iotsgc.resourcepath.device	- Der Geräteressourcenpfad wird standardmäßig für die V3-API-Version bereitgestellt. - Wenn Sie eine andere API-Version verwenden möchten, können Sie den Pfad überschreiben.
sn_msftd4iotsgc.resourcespfad.verbindung	- Der Verbindungsressourcenpfad wird standardmäßig für die V3-API-Version bereitgestellt. - Wenn Sie eine andere API-Version verwenden möchten, können Sie den Pfad überschreiben.
sn_msftd4iotsgc.pagesize.device	Geben Sie die Anzahl der Datensätze ein, die pro Seite für jede Geräte- und Verbindungs-API angezeigt werden sollen. Standardwert: 50 Datensätze pro Seite
sn_msftd4iotsgc.pagesize.connection	Wenn Sie einen anderen Verbindungsalias verwenden möchten als die Microsoft D4IoT-Basis-API, die beim Einrichten der Datensätze für Verbindungen und Anmeldeinformationen konfiguriert wurde, können Sie die sys_id Ihres anwenderdefinierten Verbindungsalias-

Eigenschaft	Beschreibung
	Datensatzes in diesem Eigenschaftsfeld eingeben. Der Standardwert dieser Eigenschaft ist leer. Wenn dieses Eigenschaftsfeld leer gelassen wird, wird standardmäßig der Microsoft D4IoT-Basis-API-Verbindungsalias verwendet.
sn_msftd4iotsgc.get_all_devices	Wählen Sie aus, ob alle Datensätze für Geräte oder nur die neuen Datensätze seit der Startzeit des letzten erfolgreichen Imports abgerufen werden sollen. i Hinweis: Wenn Sie Geräte zum ersten Mal importieren, werden alle Datensätze unabhängig von der Einstellung für diese Eigenschaft importiert.
sn_msftd4iotsgc.get_all_connections	Wählen Sie aus, ob alle Datensätze für Verbindungen oder nur neue Datensätze seit der Startzeit des letzten erfolgreichen Imports in CMDB abgerufen werden sollen. i Hinweis: Wenn Sie Verbindungen zum ersten Mal importieren, werden alle Datensätze unabhängig von der Einstellung für diese Eigenschaft importiert.
sn_msftd4iotsgc.ot.vr.integration.id	Wenn Sie die Anwendung Operational Technology Vulnerability Response mit der Integration Service Graph für Microsoft Defender for IoT verwenden, geben Sie die Sys-ID des OT VR-Importdatensatzes an. i Hinweis: Wenn das Plugin Operational Technology Vulnerability Response installiert ist und dieses Eigenschaftsfeld leer gelassen wird, wird die Microsoft D4IoT Devices CVE-Integration (Delta Import) ausgeführt, wenn „Aktiv“ für den Datensatz auf „wahr“ festgelegt ist.

c. Wählen Sie **Speichern.**

8. Um Sensoren zu importieren, gehen Sie wie folgt vor:

- a. Wählen Sie im Abschnitt „Configure Sensors (NIDS)“ (Sensoren konfigurieren (NIDS)) die Aufgabe Sensoren importieren aus.
 - b. Wählen Sie **Konfigurieren**.
 - c. Wählen Sie **Aktiv** aus, um den geplanten Datenimportauftrag zu aktivieren.
9. Führen Sie zum Konfigurieren des NIDS Folgendes aus:
- a. Wählen Sie im Abschnitt „Configure Sensors (NIDS)“ (Sensoren konfigurieren (NIDS)) die Aufgabe Sensoren importieren aus.
 - b. Wählen Sie **Als abgeschlossen markieren** aus, sobald Sie die in der Beschreibung verknüpfte NIDS-Konfiguration abgeschlossen haben.
10. Führen Sie die folgenden Schritte aus, um Importzeitpläne zu konfigurieren:
- a. Wählen Sie im Abschnitt Importzeitpläne konfigurieren **die Option Konfigurieren aus**.
 - b. Wählen Sie **Geplanter Import von Sensoren in SG-OT Microsoft D4IoT** aus, um den Importzeitplan für Sensoren nach Bedarf zu überprüfen oder zu ändern.
 - Standardmäßig ist der Zeitplan für den Sensorenimport so konfiguriert, dass er täglich um Mitternacht ausgeführt wird.
 - Importieren Sie Sensoren, bevor Sie Geräte oder Verbindungen importieren.
 - c. Wählen Sie **Aktiv** aus, um den Zeitplan für den Sensorenimport zu aktivieren.
 - d. Wählen Sie **Geplanter Import von SG-OT Microsoft D4IoT-Geräten** aus, um den Importzeitplan für Geräte nach Bedarf zu überprüfen oder zu ändern.
 - Standardmäßig ist der Importzeitplan für Geräte so konfiguriert, dass er täglich um Mitternacht ausgeführt wird.
 - Geräte werden nach Sensor abgefragt. Der Connector Service Graph fragt Geräte ab, die von validierten Sensoren erkannt wurden. Informationen zum Konfigurieren von NIDS-Geräten (Network Intrusion Detection System) finden Sie unter [Validieren Sie das NIDS](#).
 - e. Wählen Sie **Aktiv** aus, um den Importzeitplan für Geräte zu aktivieren.
 - f. Wählen Sie **Geplanter Import von SG-OT Microsoft D4IoT-Verbindungen** aus, um den Importzeitplan für Verbindungen nach Bedarf zu überprüfen oder zu ändern.
 - Standardmäßig ist der Zeitplan für den Verbindungsimport so konfiguriert, dass er nach dem Geräteimport ausgeführt wird (**Nach übergeordneten Ausführungen**).
 - Verbindungen werden nur importiert, wenn sich beide Geräte (Quelle und Ziel in der Microsoft-API oder übergeordnetes und untergeordnetes Element in der CMDB) bereits in der CMDB befinden.
 - Importieren Sie Geräte, bevor Sie Verbindungen importieren.

CMDB Klassen im Service Graph Connector für Microsoft Defender for IoT (lokale Managementkonsole)

Wenn Sie das geführte Setup abschließen, können Sie die Integration so konfigurieren, dass regelmäßig Daten aus einem Microsoft Defender for IoT -Projekt (lokale Verwaltungskonsole)

abgerufen werden. Die Daten werden in Tabellen gespeichert, die sich auf die Tabelle Configuration Item [cmdb_ci] beziehen.

Computer [cmdb_ci_computer]

Die folgenden Attribute in der Tabelle „Computer“ [cmdb_ci_computer] werden durch gesammelte Daten gefüllt:

Attribute für Computer [cmdb_ci_computer].

Attributbezeichnung	Attributname
Neuester Discovery-Scan	last_discovered
Betriebssystem	os
OS-Adressbreite (Bit)	os_address_width
BS-Domäne	os_domain
BS-Version	os_version

Externe Systemmetadaten [cmdb_key_value_v2]

Die folgenden Attribute in der Tabelle „Externe Systemmetadaten“ [cmdb_key_value_v2] werden durch gesammelte Daten gefüllt:

Attribute für externe Systemmetadaten [cmdb_key_value_v2].

Attributbezeichnung	Attributname
Discovery-Quelle	discovery_source
Key	key
Quellschlüssel	source_key
Zeichenfolgenwert	string_value
URL-Wert	url_value
Werttyp	value_type

Hardware [cmdb_ci_hardware]

Die folgenden Attribute in der Tabelle „Hardware“ [cmdb_ci_hardware] werden durch gesammelte Daten gefüllt:

Attribute für Hardware [cmdb_ci_hardware].

Attributbezeichnung	Attributname
Klasse	sys_class_name
Modellnummer	model_number
Neuester Discovery-Scan	last_discovered
Standort	location
Modell-ID	model_id

Attribute für Hardware [cmdb_ci_hardware]. (Fortsetzung)

Attributbezeichnung	Attributname
Hersteller	manufacturer
Zuerst erkannt	first_discovered
Eigentum von	owned_by
Freigabegruppe	change_control
Verwaltet nach Gruppe	managed_by_group
Verwaltet von	managed_by
Name	name
Unternehmen	Unternehmen
Support-Gruppe	support_group
Change-Gruppe	assignment_group
Zugewiesen an	assigned_to
Support durch	supported_by

Für Hardware erstellte Beziehungen

Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
Hardware [cmdb_ci_hardware]	Eigentümer von::Eigentum von	IP-Adresse [cmdb_ci_ip_address]
Hardware [cmdb_ci_hardware]	Eigentümer von::Eigentum von	Netzwerkadapter [cmdb_ci_network_adapter]
Hardware [cmdb_ci_hardware]	Referenz	Externe Systemmetadaten [cmdb_key_value_v2]
Hardware [cmdb_ci_hardware]	Referenz	OT-Gerät [cmdb_ot_entity]

IP-Adresse [cmdb_ci_ip_address]

Die folgenden Attribute in der Tabelle „IP-Adresse“ [cmdb_ci_ip_address] werden durch gesammelte Daten gefüllt:

IP-Adressenattribute [cmdb_ci_ip_address].

Attributbezeichnung	Attributname
IP-Adresse	ip_address
IP-Version	ip_version
Im Besitz von Konfigurationselement	owned_by_cmdb_ci

Für die IP-Adresse erstellte Beziehungen

Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
IP-Adresse [cmdb_ci_ip_address]	Referenz	Erkennungssystem für Netzwerkangriffe [cmdb_ci_nids]

Für die IP-Adresse erstellte Beziehungen (Fortsetzung)

Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
IP-Adresse [cmdb_ci_ip_address]	Referenz	Hardware [cmdb_ci_hardware]

Netzwerkadapter [cmdb_ci_network_adapter]

Die folgenden Attribute in der Tabelle „Netzwerkadapter“ [cmdb_ci_network_adapter] werden durch gesammelte Daten gefüllt:

Attribute für den Netzwerkadapter [cmdb_ci_network_adapter].

Attributbezeichnung	Attributname
MAC-Adresse	mac_address
Name	name
Discovery-Quelle	discovery_source

Für den Netzwerkadapter erstellte Beziehungen

Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
Netzwerkadapter [cmdb_ci_network_adapter]	Referenz	Erkennungssystem für Netzwerkangriffe [cmdb_ci_nids]
Netzwerkadapter [cmdb_ci_network_adapter]	Referenz	Hardware [cmdb_ci_hardware]

Erkennungssystem für Netzwerkangriffe [cmdb_ci_nids]

Die folgenden Attribute in der Tabelle „Netzwerkangriffserkennungssystem“ [cmdb_ci_nids] werden durch gesammelte Daten gefüllt:

Attribute für das Netzwerkangriffserkennungssystem [cmdb_ci_nids].

Attributbezeichnung	Attributname
Zuerst erkannt	first_discovered
NIDS-Quellenname	source_name
Lebenszyklusphase	life_cycle_stage
Status der Lebenszyklusphase	life_cycle_stage_status
Name	name
Korrelations-ID	correlation_id
Firmware-Version	firmware_version
Vollqualifizierter Domänenname	fqdn
NIDS-Zuweisungszone	Zone
Verbindungsstatus des NIDS-Managers	connection_state
Überprüft	überprüft

Attribute für das Netzwerkangriffserkennungssystem [cmdb_ci_nids]. (Fortsetzung)

Attributbezeichnung	Attributname
Hersteller	manufacturer

Für NIDS erstellte Beziehungen

Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
Erkennungssystem für Netzwerkangriffe [cmdb_ci_nids]	Erkennt::Erkannt von	Hardware [cmdb_ci_hardware]
Erkennungssystem für Netzwerkangriffe [cmdb_ci_nids]	Eigentümer von::Eigentum von	IP-Adresse [cmdb_ci_ip_address]
Erkennungssystem für Netzwerkangriffe [cmdb_ci_nids]	Eigentümer von::Eigentum von	Netzwerkadapter [cmdb_ci_network_adapter]

Operative Technologien (OT) [cmdb_ci_ot]

Die folgenden Attribute in der Tabelle „Operative Technologie (OT)“ [cmdb_ci_ot] werden durch gesammelte Daten gefüllt:

Attribute für Operational Technology (OT) [cmdb_ci_ot].

Attributbezeichnung	Attributname
Neuester Discovery-Scan	last_discovered

OT-Steuerungsmodul [cmdb_ci_ot_control_module]

Die folgenden Attribute in der Tabelle „OT-Steuerungsmodul“ [cmdb_ci_ot_control_module] werden durch gesammelte Daten ausgefüllt:

Attribute des OT-Steuerungsmoduls [cmdb_ci_ot_control_module].

Attributbezeichnung	Attributname
Lieferant	Lieferant
Support-Gruppe	support_group
Seriennummer	serial_number
Klasse	sys_class_name
Zuerst erkannt	first_discovered
Freigabegruppe	change_control
Verwaltet von	managed_by
Verwaltet nach Gruppe	managed_by_group
Change-Gruppe	assignment_group
Unternehmen	Unternehmen
Racknummer	rack_number

Attribute des OT-Steuerungsmoduls [cmdb_ci_ot_control_module]. (Fortsetzung)

Attributbezeichnung	Attributname
Slot-Nummer	slot_number
Standort	location
Name	name
Firmware-Version	firmware_version
Neuester Discovery-Scan	last_discovered
Zugewiesen an	assigned_to
Eigentum von	owned_by
Support durch	supported_by
Modell-ID	model_id

Für das OT-Steuerungsmodul erstellte Beziehungen

Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
OT-Steuerungsmodul [cmdb_ci_ot_control_module]	Referenz	OT-Gerät [cmdb_ot_entity]

OT-Steuerungssystem [cmdb_ci_ot_control]

Die folgenden Attribute in der Tabelle „OT-Steuerungssystem“ [cmdb_ci_ot_control] werden durch gesammelte Daten ausgefüllt:

Attribute für OT-Steuerungssystem [cmdb_ci_ot_control].

Attributbezeichnung	Attributname
Hat Modul	has_module
Neuester Discovery-Scan	last_discovered

Für OT-Steuerungssystem erstellte Beziehungen

Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
OT-Steuerungssystem [cmdb_ci_ot_control]	Eigentümer von::Eigentum von	OT-Steuerungsmodul [cmdb_ci_ot_control_module]

OT-Gerät [cmdb_ot_entity]

Die folgenden Attribute in der Tabelle „OT-Gerät“ [cmdb_ot_entity] werden durch gesammelte Daten gefüllt:

OT-Gerät-Attribute [cmdb_ot_entity].

Attributbezeichnung	Attributname
ISA-Entitätsstandort	isa_entity_site

OT-Gerät-Attribute [cmdb_ot_entity]. (Fortsetzung)

Attributbezeichnung	Attributname
OT-Erkennungsquellen-ID	ot_correlation_id
Gerät-Relevanz	business_criticality
Purdue-Ebene	purdue_level
Zone	Zone
OT-Gerätetyp	ot_asset_type

SPS [cmdb_ci_ot_plc]

Die folgenden Attribute in der Tabelle „SPS“ [cmdb_ci_ot_plc] werden durch gesammelte Daten gefüllt:

SPS-Attribute [cmdb_ci_ot_plc].

Attributbezeichnung	Attributname
Neuester Discovery-Scan	last_discovered
Schalterposition	switch_position
Remote wechseln	switch_remote_mode

Seriennummer [cmdb_serial_number]

Die folgenden Attribute in der Tabelle „Seriennummer“ [cmdb_serial_number] werden durch gesammelte Daten gefüllt:

Attribute für Seriennummer [cmdb_serial_number].

Attributbezeichnung	Attributname
Seriennummer	serial_number
Seriennummertyp	serial_number_type
Gültig	gültig

Für die Seriennummer erstellte Beziehungen

Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
Seriennummer [cmdb_serial_number]	Referenz	Hardware [cmdb_ci_hardware]
Netzwerkadapter [cmdb_ci_network_adapter]	Referenz	Hardware [cmdb_ci_hardware]

Attributzuordnung und -klassifizierung für den Service Graph Connector für Microsoft Defender for IoT (lokale Verwaltungskonsole)

In den folgenden Tabellen wird die Attributzuordnung und -klassifizierung für Sensoren und Geräte beschrieben.

Attributzuordnung für Sensoren

Feldname für Nutzlast	Datentyp	Der Tabelle zugeordnet	Zu Feld zugeordnet	Beschreibung
id	Zeichenfolgenformat: /subscriptions/<subscription-id> /Provider/<provider> /Standorte/<location> /sites/<site> /sensor/<sensor-name>	• sys_object_source • cmdb_ci_nids	• correlation_id	Eindeutige ID für den Sensor.
name	Zeichenfolge	cmdb_ci_nids	name	Name des Sensors.
properties.hostname	Zeichenfolge	cmdb_ci_nids	fqdn	Hostname des Sensors.
properties.ip	Zeichenfolge	cmdb_ci_ip_address	ip_address	IP-Adresse des Sensors.
properties.learningMode	Boolean	cmdb_ci_nids	Falsch oder nicht verfügbar: Lebenszyklusphase (life_cycle_stage): Status der operativen Lebenszyklusphase (life_cycle_stage_status): Wird verwendet Wahr: Lebenszyklusphase (life_cycle_stage): Status der operativen Lebenszyklusphase (life_cycle_stage_status): Lernen	Lernmodusstatus des IoT-Sensors.
properties.mac	Zeichenfolge	cmdb_ci_network_adapter	name, mac_address	MAC-Adresse des Sensors.
properties.sensorStatus	Zeichenfolge	cmdb_ci_nids	connection_state	Status des IoT-Sensors.
properties.sensorVersion	Zeichenfolge	cmdb_ci_nids	firmware_version	Version des IoT-Sensors.
properties.upSince_utc	Datum und Uhrzeit als Zeichenfolge	cmdb_ci_nids	first_discovered	Startzeit
properties.zone	Zeichenfolge	cmdb_ci_nids	Zone	Zone des IoT-Sensors.

Attributzuordnung für Geräte

Feldname für Nutzlast	Datentyp	Der Tabelle zugeordnet	Zu Feld zugeordnet	Beschreibung
id	Zeichenfolgenformat: /subscriptions/subscription-id>/providers/<providers-id> /Standort/<location> /deviceGroups/<device-Group> /devices/<name-field>	• sys_object_source • cmdb_ot_entity • cmdb_key_value_v2	esnk in „sys_object_source“. • discovery_source_id in cmdb_ot_entity	Eindeutige ID für das Gerät.
resourceGroup	(leer)	cmdb_key_value_v2	(leer)	Ressourcengruppe
tenantId	(leer)	cmdb_key_value_v2	(leer)	Mandanten-ID
properties.authorizedState	Zeichenfolge	cmdb_key_value_v2	(leer)	Autorisierter Status des Geräts
properties.criticality	Zeichenfolge	cmdb_ot_entity	business_criticality	Relevanz des Geräts
properties.deviceName	Zeichenfolge	cmdb_ci	name	Der Name des Geräts.
properties.deviceSubType	Zeichenfolge	cmdb_ci	sys_class_name	Anzeigenname des Geräteuntertyps.
properties.firstSeen	Datum und Uhrzeit als Zeichenfolge	• cmdb_ci • cmdb_ci_ot_control_module (falls Steuerungsmodule vorhanden sind)	first_discovered	Zeitpunkt, zu dem das Gerät zum ersten Mal angezeigt wurde.
properties.lastSeen	Datum und Uhrzeit als Zeichenfolge	• cmdb_ci • cmdb_ci_ot_control_module (falls Steuerungsmodule vorhanden sind)	mod_recent_discovery	Zeitpunkt, zu dem das Gerät zuletzt angezeigt wurde.
properties.purdueLevel	Zeichenfolge	cmdb_ot_entity	purdue_level	Purdue-Ebene des Geräts.
Eigenschaften.Betriebsystem	Zeichenfolge	cmdb_ci_computer	os	BS-Verteilung
Eigenschaften.Betriebsystemversion	Zeichenfolge	cmdb_ci_computer	os_version	BS-Version
Eigenschaften.Betriebsystemplattform	Zeichenfolge	cmdb_ci_computer	os_domain	BS-Plattform
Eigenschaften.Betriebsystemarchitektur	Zeichenfolge	cmdb_ci_computer	os_address_width	BS-Architektur
properties.additionalFields.plcKeyState	(leer)	cmdb_ci_ot_plc	switch_position	SPS-Schlüsselstatus

Attributzuordnung für Geräte (Fortsetzung)

Feldname für Nutzlast	Datentyp	Der Tabelle zugeordnet	Zu Feld zugeordnet	Beschreibung
properties.additionalFields.plcRunState	Boolean	cmdb_ci_ot_plc	switch_remote_mode	SPS-Ausführungsstatus
properties.hardware	Objekt	(leer)	(leer)	Daten zur Gerätehardware
Eigenschaften.Hardware.Zeichenfolge	Zeichenfolge	cmdb_ci	(leer)	Hardwaremodell
properties.hardware.serialNumber	Zeichenfolge	cmdb_serial_number	serial_number	Hardware-Seriennummer
Eigenschaften.Hardware.Zeichenfolge	Zeichenfolge	cmdb_ci	manufacturer	Hardware-Lieferant
properties.nics	Array von Objekten	(leer)	(leer)	Liste der Netzwerkschnittstellenkarten des Geräts.
properties.nics[{}]	Objekt	(leer)	(leer)	Eigenschaften der Netzwerkschnittstellenkarte
properties.nics[{}].ipv4Address	Zeichenfolge	cmdb_ci_ip_address	ip_address	IPv4-Adresse
properties.nics[{}].macAddress	Zeichenfolge	cmdb_ci_network_adapter	Name, Mac	MAC-Adresse
Eigenschaften.Steckplätze	Array von Objekten	(leer)	(leer)	Liste des Gerätesteckplatzes in der Backplane.
Eigenschaften.Steckplätze[{}]	Objekt	(leer)	(leer)	Slot-Daten in der SPS-Backplane.
properties.slots[{}].firmwareVersion	Zeichenfolge	cmdb_ci_ot_control_module	firmware_version	Firmware-Version des Slots.
properties.slots[{}].modelName	Zeichenfolge	cmdb_ci_ot_control_module	model_id	Modell des Steckplatzes.
Eigenschaften.Steckplätze[{}].RackNumber	Zeichenfolge	cmdb_ci_ot_control_module	rack_number	Racknummer in der Backplane
properties.slots[{}].serialNumber	Zeichenfolge	cmdb_ci_ot_control_module	serial_number	Seriennummer des Slots
properties.slots[{}].slotNumber	Nummer	cmdb_ci_ot_control_module	slot_number	Steckplatznummer im Rack.
properties.slots[{}].hardwareManufacturer	Zeichenfolge	cmdb_ci_ot_control_module	manufacturer	Hardware-Lieferant des Slots.

Automatische Übersetzung

Klassifizierung des Gerätetyps

Microsoft Azure Name des Geräteuntertyps	Microsoft Azure Name des Gerätetyps	Betriebssystem/ Firmware	NOW-Kurs	NOW-Tabelle	NOW O
Alarmsirene	(leer)	(leer)	IoT-Gerät	cmdb_ci_iot	NULL

Klassifizierung des Gerätetyps (Fortsetzung)

Microsoft Azure Name des Geräteuntertyps	Microsoft Azure Name des Gerätetyps	Betriebssystem/ Firmware	NOW-Kurs	NOW-Tabelle	NOW O
Alarmsystem	(leer)	(leer)	OT- Steuerungssystem	cmdb_ci_ot_control	OT- Steuerung
Geldautomat	(leer)	(leer)	IoT-Gerät	cmdb_ci_iot	NULL
Sicherungsserver	(leer)	(leer)	Server	cmdb_ci_server	NULL
Strichcode-Scanner	(leer)	(leer)	IoT-Gerät	cmdb_ci_iot	NULL
DB-Server	(leer)	(leer)	Server	cmdb_ci_server	NULL
DCS-Controller	Industriell	(leer)	DCS	cmdb_ci_ot_dcs	NULL
Domain Controller	(leer)	(leer)	Server	cmdb_ci_server	NULL
Türsteuerungsfeld	(leer)	(leer)	IoT-Gerät	cmdb_ci_iot	NULL
VR	(leer)	(leer)	IoT-Gerät	cmdb_ci_iot	NULL
Aufzug	(leer)	(leer)	IoT-Gerät	cmdb_ci_iot	NULL
Engineering-Station	Industriell	(leer)	EWS	cmdb_ci_ot_ews	EWS
Feueralarm	(leer)	(leer)	IoT-Gerät	cmdb_ci_iot	NULL
Feuermelder	(leer)	(leer)	IoT-Gerät	cmdb_ci_iot	NULL
Firewall	(leer)	(leer)	IP-Firewall	cmdb_ci_ip_firewall	NULL
Spielkonsole	(leer)	(leer)	Spielkonsole	cmdb_ci_spiel_konsole	NULL
Aufzeichnung	(leer)	(leer)	Aufzeichnung	cmdb_ci_ot_historian	Aufzeichn
HMI	Industriell	(leer)	HMI	cmdb_ci_ot_hmi	HMI
Feuchtigkeitssensor	(leer)	(leer)	IoT-Gerät	cmdb_ci_iot	NULL
HLK	(leer)	(leer)	HLK-Zubehör	cmdb_ci_hvac	NULL
I/O-Adapter	(leer)	(leer)	Netzwerkadapter	(leer)	NA
IED	(leer)	(leer)	IED	cmdb_ci_ot_ied	geb
Industrielles Verpackungssystem	(leer)	(leer)	OT-Feldgerät	cmdb_ci_ot_field_device	OT-Feld
Industrieroboter	(leer)	(leer)	Industrieroboter	cmdb_ci_ot_industrial_robot	Industrie
Industrielle Skala	(leer)	(leer)	OT-Feldgerät	cmdb_ci_ot_field_device	OT-Feld
Gegensprechanlage	(leer)	(leer)	IoT-Gerät	cmdb_ci_iot	NULL
IP-Kamera	(leer)	(leer)	IP-Kamera	cmdb_ci_ip_kamera	NULL
IP-Telefon	(leer)	(leer)	IP-Telefon	cmdb_ci_ip_phone	NULL
Laufschrift	(leer)	(leer)	IoT-Gerät	cmdb_ci_iot	NULL
Zähler	(leer)	(leer)	Industriesensor	cmdb_ci_ot_industrial_sensor	Industrie
Bewegungsmelder	(leer)	(leer)	IoT-Gerät	cmdb_ci_iot	NULL

Automatische Übersetzung

Klassifizierung des Gerätetyps (Fortsetzung)

Microsoft Azure Name des Geräteuntertyps	Microsoft Azure Name des Gerätetyps	Betriebssystem/ Firmware	NOW-Kurs	NOW-Tabelle	NOW O
Multicast/Broadcast	(leer)	(leer)	Netgear	cmdb_ci_netgear	NULL
NTP-Server	(leer)	(leer)	Server	cmdb_ci_server	NULL
Personenzähler-System	(leer)	(leer)	IoT-Gerät	cmdb_ci_iot	NULL
Physischer Speicherort	(leer)	(leer)	(leer)	(leer)	NULL
SPS	Industriell	(leer)	SPS	cmdb_ci_ot_plc	SPS
pneumatisches Gerät	(leer)	(leer)	Industrieaktuator	cmdb_ci_ot_industrial_actuator	Industrie
Drucker	(leer)	(leer)	Drucker	cmdb_ci_printer	NULL
Protokollkonverter	(leer)	(leer)	Netgear	cmdb_ci_netgear	NULL
Stempeluhr	(leer)	(leer)	IoT-Gerät	cmdb_ci_iot	NULL
Robot-Controller	(leer)	(leer)	OT-Steuerungssystem	cmdb_ci_ot_control	OT-Steuerung
Router	(leer)	(leer)	IP-Router	cmdb_ci_ip_router	NULL
RTU	(leer)	(leer)	RTU	cmdb_ci_ot_rtu	NULL
Server	Server	(leer)	Server	cmdb_ci_server	NULL
Stellt Laufwerk ein	(leer)	(leer)	Industrieaktuator	cmdb_ci_ot_industrial_actuator	Industrie
Steckplatz	(leer)	(leer)	OT-Steuerungsmodul	cmdb_ci_ot_control_module	OT-Steuerung
Intelligentes Licht	(leer)	(leer)	IoT-Gerät	cmdb_ci_iot	NULL
Smartphone	(leer)	(leer)	Handcomputergerät	cmdb_ci_handgehalten_computing	NULL
Intelligenter Switch	(leer)	(leer)	IoT-Gerät	cmdb_ci_iot	NULL
Smart TV	(leer)	(leer)	Smart TV	cmdb_ci_stv	NULL
Speicher	(leer)	(leer)	Server	cmdb_ci_server	NULL
Switch	Netzwerkgerät	(leer)	IP-Switch	cmdb_ci_ip_switch	NULL
Tablet	(leer)	(leer)	Handcomputergerät	cmdb_ci_handgehalten_computing	NULL
Terminal-Station	(leer)	(leer)	Computer	cmdb_ci_computer	NULL
Raumtempererator	(leer)	(leer)	IoT-Gerät	cmdb_ci_iot	NULL
Drehkreuz	(leer)	(leer)	IoT-Gerät	cmdb_ci_iot	
Unterbrechungsfreie Stromversorgung	(leer)	(leer)	UPS	cmdb_ci_ups	NULL
Frequenzumrichter	(leer)	(leer)	Industrielaufwerk	cmdb_ci_ot_industrial_drive	Industrie
VPN Gateway	(leer)	(leer)	Netgear	cmdb_ci_netgear	NULL

Automatische Übersetzung

Klassifizierung des Gerätetyps (Fortsetzung)

Microsoft Azure Name des Geräteuntertyps	Microsoft Azure Name des Gerätetyps	Betriebssystem/ Firmware	NOW-Kurs	NOW-Tabelle	NOW O
WLAN-Ananas	(leer)	(leer)	Netgear	cmdb_ci_netgear	NULL
Drahtloser Zugriffspunkt	(leer)	(leer)	Drahtloser Zugriffspunkt	cmdb_ci_wap_network	NULL
WLAN- Zugriffspunkt	Netzwerkgerät	(leer)	Drahtloser Zugriffspunkt	cmdb_ci_wap_network	NULL
Arbeitsplatz-PC	Arbeitsplatz- PC	(leer)	Computer	cmdb_ci_computer	NULL
Unbekannt	Alle	(leer)	Operative Technologien (OT)	cmdb_ci_ot	Operativ Technol (OT)
Nicht klassifiziert	„Nicht klassifiziert“ oder „Alle“.	(leer)	Operative Technologien (OT)	cmdb_ci_ot	Operativ Technol (OT)
Jeder andere Typ	(leer)	(leer)	Operative Technologien (OT)	cmdb_ci_ot	Operativ Technol (OT)
Beliebiger obiger Typwert außer mit der Bezeichnung „Netzwerk und IoT“.	(leer)	• Windows- Server • Windows Server, Version 2004[8] • Windows Server, Version 1909[9] • Windows Server, Version 1903[9] • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2 • Windows Server 2008	Windows-Server	cmdb_ci_linux_server	Identisch Fall, we Betriebs nicht vo ist.

Automatische Übersetzung

Klassifizierung des Gerätetyps (Fortsetzung)

Microsoft Azure Name des Geräteuntertyps	Microsoft Azure Name des Gerätetyps	Betriebssystem/ Firmware	NOW-Kurs	NOW-Tabelle	NOW O
		• Windows Server 2003 R2 • Windows Server 2003 • Windows 2000-Server • Windows nt 4.0 Server • Windows nt 3.51 Server • Windows nt 3.5 Server • Windows nt 3.1 Server			
Beliebiger obiger Typwert außer mit der Bezeichnung „Netzwerk und IoT“.	(leer)	• Linux • arch • centos • Debian • Bucket Hat • suse • Red Hat • RHel • ubuntu • Orakel	Linux-Server	cmdb_ci_linux_server	Identisch Fall, we Betriebs nicht vo ist.
Beliebiger obiger Typwert außer mit der Bezeichnung „Netzwerk und IoT“.	(leer)	aix	AIX-Server	cmdb_ci_aix_server	Identisch Fall, we Betriebs nicht vo ist.
Beliebiger obiger Typwert außer mit der Bezeichnung „Netzwerk und IoT“.	(leer)	esx	ESX-Server	cmdb_ci_esx_server	Identisch Fall, we Betriebs nicht vo ist.

Automatische Übersetzung

Klassifizierung des Gerätetyps (Fortsetzung)

Microsoft Azure Name des Geräteuntertyps	Microsoft Azure Name des Gerätetyps	Betriebssystem/ Firmware	NOW-Kurs	NOW-Tabelle	NOW O
Beliebiger obiger Typwert außer mit der Bezeichnung „Netzwerk und IoT“.	(leer)	• HP/UX • HPUX	HP-UX Server	cmdb_ci_hpux_server	Identisch Fall, we Betriebs nicht vo ist.
Beliebiger obiger Typwert außer mit der Bezeichnung „Netzwerk und IoT“.	(leer)	• Hyper-V • Hyperv • Hyper	HyperV-Server	cmdb_ci_hyper_v_server	Identisch Fall, we Betriebs nicht vo ist.
Beliebiger obiger Typwert außer mit der Bezeichnung „Netzwerk und IoT“.	(leer)	• Solaris • Sunos • Sunos	Solaris-Server	cmdb_ci_solaris_server	Identisch Fall, we Betriebs nicht vo ist.
Beliebiger obiger Typwert außer mit der Bezeichnung „Netzwerk und IoT“.	(leer)	• MacOS X- Server • MacOS-Server • BS x • osx	OSX-Server	cmdb_ci_osx_server	Identisch Fall, we Betriebs nicht vo ist.
Beliebiger obiger Typwert außer mit der Bezeichnung „Netzwerk und IoT“.	(leer)	• Unix • GNU	Unix-Server	cmdb_ci_unix_server	Identisch Fall, we Betriebs nicht vo ist.
Beliebiger obiger Typwert außer mit der Bezeichnung „Netzwerk und IoT“.	(leer)	• Gewinn • windows • Microsoft • Windows 1.0, 1.02, 1.03, 1.04, 2.03, 2.10, 2.11, 3.0, 3.1, 3.2, 7, 8, 8.1, 10, 98, 95 • Windows 2000 • Windows für Arbeitsgruppen 3.11	Basiscomputerklasse	cmdb_ci_computer	Identisch Fall, we Betriebs nicht vo ist.

Automatische Übersetzung

Klassifizierung des Gerätetyps (Fortsetzung)

Microsoft Azure Name des Geräteuntertyps	Microsoft Azure Name des Gerätetyps	Betriebssystem/ Firmware	NOW-Kurs	NOW-Tabelle	NOW O
		• Fenster mich • Windows nt 3.1, 3.5, 3.51, 4.0 • Windows Visa • Windows XP • Windows XP Professional x64-Edition			
Beliebiger obiger Typwert außer mit der Bezeichnung „Netzwerk und IoT“.	(leer)	Server	Basisserverklasse	cmdb_ci_server	Identisch Fall, we Betriebs nicht vo ist.

Service Graph Connector für SIEMENS IAH

Integrieren Sie „Siemens IAH“ mit der Anwendung ServiceNow Operational Technology Manager, um Siemens IAH-Assets zu importieren.

Apps im Store anfordern

Besuchen Sie die Website [ServiceNow Store](#), um sich alle verfügbaren Apps anzusehen 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](#).

Geführtes Setup

Das geführte Setup für Service Graph Connector für SIEMENS IAH bietet eine organisierte Abfolge von Aufgaben zum Konfigurieren der Integration in Ihrer -Instanz. Informationen zum Zugriff auf das geführte Setup finden Sie unter [Konfigurieren Sie das geführte Setup](#).

CMDB Dashboard für Integrationen

Die Store-App Gemeinsame Komponenten für CMDB-Integrationen bietet ein Dashboard mit einer zentralen Ansicht des Status, der Verarbeitungsergebnisse und der Verarbeitungsfehler aller installierten Integrationen. Sie können Metriken für alle Integrationsausführungen anzeigen. Sie können die Ansicht nach einer bestimmten CMDB Integration, einer bestimmten Zeitdauer oder einer bestimmten Integrationsausführung filtern. Weitere Informationen zur Überwachung von Integrationen im Integrations-Dashboard CMDB finden Sie unter [Integration Commons for CMDB](#).

Datenzuordnung

Daten aus den Siemens IAH-Datenquellen werden zugeordnet und mithilfe der Robust Transform Engine (RTE) in die Klassendefinitionen der ServiceNow CMDB Configuration Item(CI)-Klasse umgewandelt. Daten werden mithilfe der Identification and Reconciliation Engine (IRE) in ServiceNow CMDB eingefügt.

In der folgenden Tabelle sind die für Service Graph Connector für SIEMENS IAH enthaltene Datenquelle und die entsprechenden Bereitstellungstabellen aufgeführt, in die die importierten Daten geladen werden.

Datenquelle und Bereitstellungstabelle für SIEMENS IAH

Datenquelle	Bereitstellungstabelle
Bereitstellung des SG-SiemensIAH-Assets	sn_siemensiahsgc_staging_asset

Verwaltung des Industrial Asset Hub (IAH)

Weitere Informationen zur Verwaltung der Siemens IAH finden Sie unter [Administrationsdokumentation](#) .

Installieren Sie Service Graph Connector für SIEMENS IAH

Installieren Sie Service Graph Connector von ServiceNow Store.

Vorbereitungen

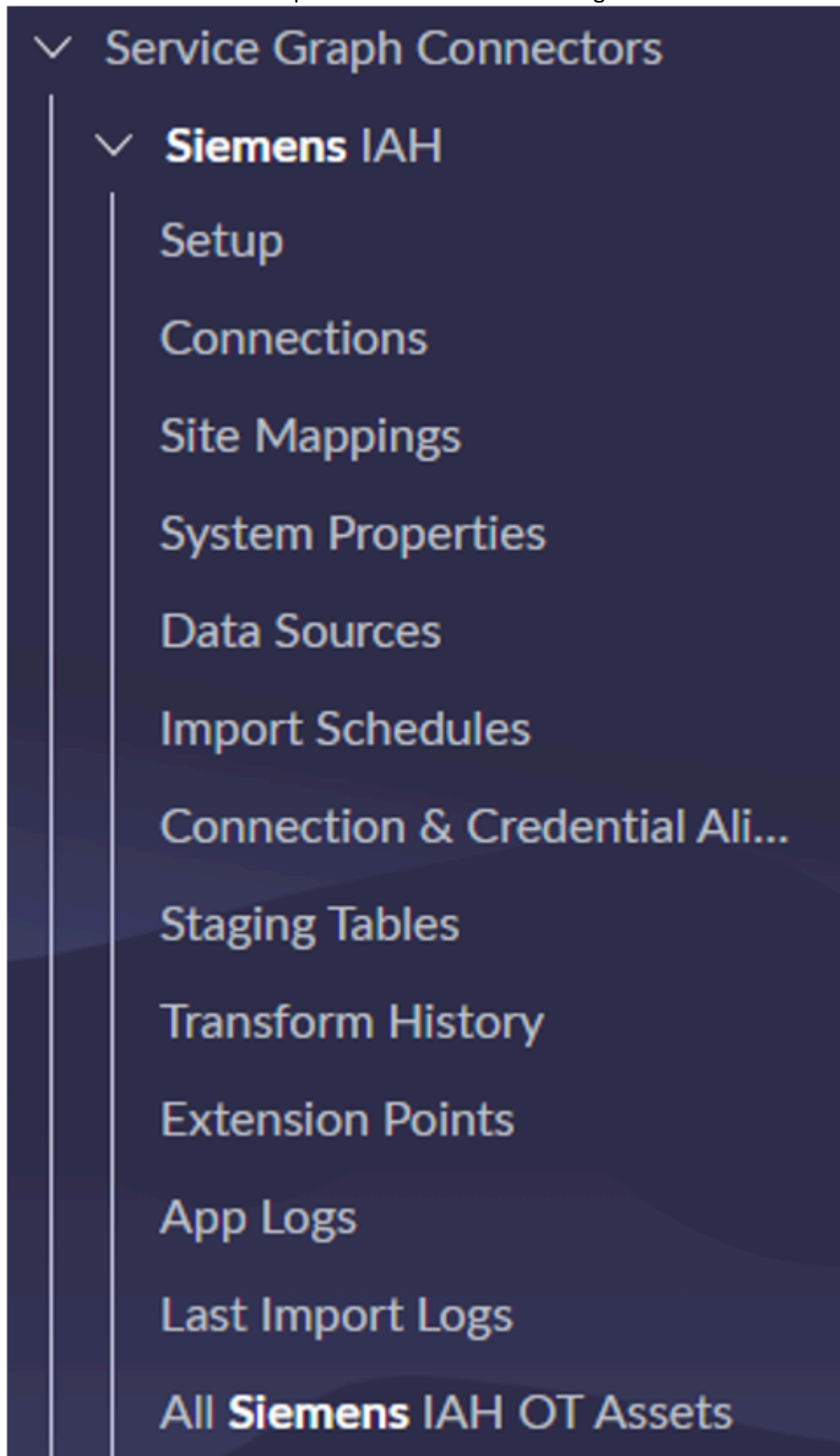
Erforderliche Rolle: Administrator

Prozedur

1. Wählen Sie in ServiceNow Store die **Option Zugriff** auf Store-Seite Service Graph Connector für Siemens IAH abrufen aus, um die Integration für eine oder mehrere Instanzen ServiceNow zu berechtigen.
2. Melden Sie sich nach der Berechtigung bei Ihrer -Instanz an.
3. Navigieren zu **Systemanwendungen > Alle verfügbaren Anwendungen > Alle**.
4. Suchen Sie nach Service Graph Connector für „Siemens IAH“, und wählen Sie **Installieren** aus.

Ergebnisse

Nachdem die Installation abgeschlossen ist, können Sie Ihren Browser aktualisieren und im Filternavigator „Siemens“ eingeben, um die



anzuzeigen.

Konfigurieren Sie Service Graph Connector für Siemens IAH

Verwenden Sie Geführtes Setup für Service Graph Connector für SIEMENS IAH, um sich durch die Integrationsschritte führen zu lassen.

Automatische Übersetzung

- a. Wählen Sie im Abschnitt Tabellenberechtigungen konfigurieren **die Option Erste Schritte aus.**
- b. Wählen Sie neben der Aufgabe „Geplanter Datenimport“ **Konfigurierenaus.**
- c. Stellen Sie auf der Registerkarte „Anwendungszugriff“ sicher, dass „Kann lesen“, „Kann erstellen“ und „Kann aktualisieren“ aktiviert

sind.

- d. Kehren Sie zum geführten Setup zurück.
- e. Wählen Sie neben der Aufgabe „Geplanter Datenimport“ die **Option Als abgeschlossen markierenaus.**

5. Datenquelle

- a. Wählen Sie neben der Aufgabe „Datenquelle“ **Konfigurierenaus.**
- b. Stellen Sie auf der Registerkarte „Anwendungszugriff“ sicher, dass „Kann lesen“, „Kann erstellen“ und „Kann aktualisieren“ aktiviert

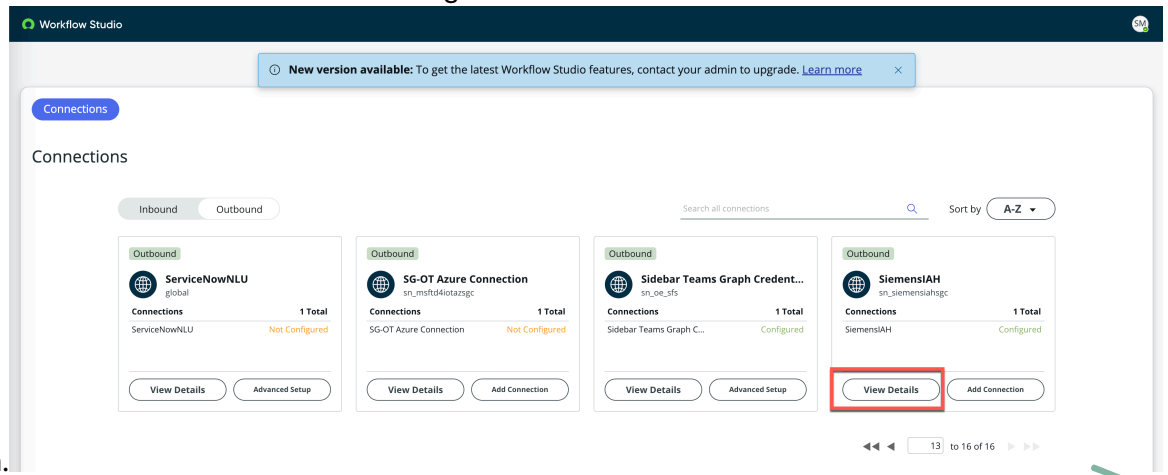
sind.

- c. Kehren Sie zu Geführtes Setup zurück.
- d. Wählen Sie neben der Datenquellenaufgabe **Als abgeschlossen markieren aus.**

6. Konfigurieren Sie die Siemens IAH-Verbindungen und -Anmeldeinformationen

- a. Ändern Sie die Anwendung mithilfe der Anwendungsauswahl in Service Graph Connector für SIEMENS IAH.
- b. Wählen Sie im Abschnitt Verbindung konfigurieren die **Option Erste Schritte aus.**
- c. Wählen Sie neben der Aufgabe „Siemens IAH-Verbindung und -Anmeldeinformationen konfigurieren“ **die Option Konfigurierenaus.** Je nach ServiceNow -Version werden Sie zur Liste Workflow-Studio oder Workflow-Studio weitergeleitet.

d. Wählen Sie in den SIEMENSIAH-Verbindungen **Details**



anzeigen.

e. Wählen Sie im Datensatz „SiemensIAH-Verbindungen“ **Konfigurieren aus**.

f. Füllen Sie die Verbindungsdetails aus.

AWSIAH-Verbindungsdatensatz

Feld	Beschreibung
Verbindungsinformation	
Verbindungsname	Die Standardverbindung ist schreibgeschützt. Wenn Sie zusätzliche Verbindungen verwenden möchten, geben Sie einen eindeutigen Namen für die Verbindung ein. Dieses Feld ist ein Pflichtfeld.
Verbindungs-URL	Geben Sie die Basis-URL für die API ein. Dieses Feld ist ein Pflichtfeld.
MID-Server verwenden	Optional können Sie dieses Kontrollkästchen aktivieren, um einen MID-Server für die Verbindung zu verwenden.
MID-Server	Wählen Sie optional einen MID-Server für die Verbindung aus.
Mandant	Geben Sie eine Siemenem IAH-Mandanten-ID ein. Dieses Feld ist ein Pflichtfeld.
Anmeldedaten	
OAuth-Entitätsname	Geben Sie einen eindeutigen Namen für die OAuth-Entität ein. Beispiel: SIEMENSIAH OAuth. Dieses Feld ist ein Pflichtfeld.
OAuth-Client-ID	Geben Sie die Client-ID-Anmeldeinformationen für die Verbindung ein. Dieses Feld ist ein Pflichtfeld.

Automatische Übersetzung

Feld	Beschreibung
OAuth-Client-Geheimnis	Geben Sie die geheimen Client-Anmeldeinformationen für die Verbindung ein. Dieses Feld ist ein Pflichtfeld.
OAuth-Token-URL	Geben Sie die URL ein, die zum Abrufen des Tokens für die API verwendet wird. Dieses Feld ist ein Pflichtfeld.

- g. Wählen Sie **Konfigurieren und OAuth-Token abrufen aus**. Wenn das OAuth-Token erfolgreich abgerufen wurde, wird die folgende Meldung angezeigt:

SiemensIAH Default Connection Edit

- Connection Name: SiemensIAH
- Endpoint: cloud.eu1.sws.siemens.com
- Credential Name: SiemensIAH.Credential
- Credential Type: OAuth 2.0

OAuth Access token is available but will expire soon at 2024-03-25 15:34:46. Verify the OAuth configuration and click 'Get OAuth Token' to request a new token. [Get OAuth Token](#)

Wenn das OAuth-Token während der Verbindungskonfiguration nicht erfolgreich abgerufen wurde, klicken Sie auf **OAuth-Token abrufen**, um das OAuth-Token für die Verbindung abzurufen. Danach sollte die in Schritt 4g angegebene Meldung angezeigt werden.

Wenn Probleme mit den Anmeldeinformationen auftreten, wird beim Abrufen des OAuth-Tokens eine Fehlermeldung angezeigt. Überprüfen Sie die Fehlermeldung, und aktualisieren Sie Ihre Anmeldeinformationen.

- h. Wenn Sie weitere Verbindungen wünschen, wählen Sie „**Verbindung hinzufügen**“ und wiederholen Sie die Schritte 4a bis 4g.
- i. Wenn Sie fertig sind, kehren Sie zu Geführtes Setup zurück.
- j. Wählen Sie neben der Aufgabe „Siemens IAH-Verbindung und -Anmeldeinformationen konfigurieren“ **die Option Als abgeschlossen markieren** aus.

7. Importe generieren

- a. Wählen Sie neben der Aufgabe Importe generieren **die Option Konfigurieren aus**.
- b. Wählen Sie auf der Seite „Importe für die SIEMENS IAH-Verbindungen generieren“ im Feld **Als Benutzer ausführen** einen Benutzer aus dem Menü aus.
- c. Legen Sie im Feld **Name des Asset-Importauftrags** den Auftragsnamen fest. Beispiel: [SiemensIAH] SG-SiemensIAH Asset.
- d. Wählen Sie für jede Verbindung **Generieren** aus.

e. Wählen Sie anschließend **Back to Guided Setup (Zurück zum geführten**

Setup) aus.

f. Wählen Sie neben der Aufgabe Importe generieren **die Option Als abgeschlossen markieren aus.**

8. Validieren Sie die Verbindung

a. Wählen Sie neben der Aufgabe Validate the connection (Verbindung validieren) **die Option Konfigurieren aus.**

b. Wählen Sie in der Liste die erste Datenquelle

aus.

Name	Active	Connection Alias	Message	Status	Status Code	Suggestion	Application	Updated
SiemensIAH	true	sn_siemensiahgc:SiemensIAH	Successfully queried Asset from the Siem...	Success	200		Service Graph Connector for Siemens IAH	2024-04-04 10:48:41

c. Wählen Sie im Abschnitt „Zugehörige Links“ **Verbindung testenaus.**

Das Testen der Verbindung dauert einige Minuten. Sobald dies abgeschlossen ist, wird die Seite aktualisiert, um die Testergebnisse anzuzeigen. Wenn die Verbindung erfolgreich ist, lautet der HTTP-Statuscode

Wenn ein Fehlercode und eine Fehlermeldung angezeigt werden, ist die Verbindung fehlgeschlagen und erfordert eine Problembehandlung.

- d. Wiederholen Sie die Schritte 6a bis 6c für jede aufgeführte Datenquelle.
- e. Wenn Sie fertig sind, kehren Sie zu Geführtes Setup zurück.
- f. Wählen Sie neben der Aufgabe Datenquelle validieren die **Option Als abgeschlossen markieren aus**.

9. Konfigurieren Sie die Siemens IAH-Standortzuordnungen

- a. Wählen Sie im Abschnitt Import konfigurieren die **Option Erste Schritte aus**.
- b. Wählen Sie neben der Aufgabe „Siemens IAH-Standortzuordnungen konfigurieren“ die **Option Konfigurierenaus**.
- c. Wählen Sie **Neu**.
- d. Fügen Sie im Feld **Verbindungsalias** den Alias für Verbindungen und Anmeldeinformationen für die von Ihnen konfigurierte Verbindung hinzu.
- e. Geben Sie im Feld **Standort** die ISA-Standortentität ein, die der Verbindung entspricht.
- f. Füllen Sie die anderen Felder nach Bedarf

- aus. **Submit**
- g. Wählen Sie **Absenden**.
- h. Wiederholen Sie die Schritte 8a bis 8g für jede Verbindung.
- i. Wenn Sie fertig sind, kehren Sie zu Geführtes Setup zurück.
- j. Wählen Sie neben der Aufgabe „Siemens IAH-Standortzuordnungen konfigurieren“ die **Option Als abgeschlossen markierenaus**.

10. Wahlweise: Überprüfen Sie die Systemeigenschaften

- a. Wählen Sie neben der Aufgabe Systemeigenschaften überprüfen (optional) die **Option Konfigurierenaus**.
- b. Überprüfen Sie die Einstellungen im Dialogfeld, und passen Sie sie nach Bedarf für Ihre Instanzkonfiguration an.
- c. Wählen Sie **Speichern**.
- d. Wenn Sie fertig sind, kehren Sie zu Geführtes Setup zurück.
- e. Wählen Sie neben der Aufgabe Systemeigenschaften überprüfen (optional) die **Option Als abgeschlossen markierenaus**.

11. Geplante Aufgaben konfigurieren

- a. Wählen Sie neben der Aufgabe Konfigurierte geplante Aufgaben die Option **Konfigurierenaus**.
- b. Wählen Sie in der Liste „Geplante Aufgaben“ den ersten Datensatz aus.

- c. Um den Auftrag zu aktivieren, aktivieren Sie das Kontrollkästchen neben dem Feld **Aktiv**.
- d. Geben Sie im Feld **Ausführen** ein, wie häufig die Aufgabe ausgeführt werden soll. Wählen Sie beispielsweise **Täglich** aus, um die Aufgabe täglich auszuführen.
- e. Geben Sie in den Feldern **Zeit** ein, wann die Aufgabe ausgeführt werden soll. Geben Sie beispielsweise 00 00 00 ein, um die Aufgabe um Mitternacht

Scheduled Data Import
[SiemensIAH] SG-SiemensIAH Asset

Name: [SiemensIAH] SG-SiemensIAH Asset

Data source: [SiemensIAH] SG-SiemensIAH Asset

Run as: System Administrator

Active: ☒

Application: Service Graph Connector for Siemens IAH

Run: Daily

Time: Hours 00 Minutes 00 Seconds 00

Conditional: ☒

Condition:

```
1 var settings = new SCSiemensIAHSettings();
2 var importStatus = settings.checkIfImportRunning("ab40f9db979a391088ae3e6e6253af76");
3 if(importStatus && importStatus.importRunning){
4   gs.info("SG-SiemensIAH: An import could not be started because a scheduled import is already running. Reason: "+importStatus);
5   answer = false;
6 }else{
7   answer = true;
8 }
```

Concurrent Import: ☒

Partition Method: Custom size

* Partition Size: 15,000

Execute pre-import script: ☒

Pre-script:

```
1 gs.info("SG-SiemensIAH: Asset Import For Connection: siemensiah started");
2 var jobDuration = new SCSiemensIAHsScheduledJobDuration("sn_siemensiahgc.scheduled_job_duration");
3 jobDuration.start();
4 new SCSiemensIAHSettings().setLastImportTimeTemp("siemensiah");
```

auszuführen.

- f. Wählen Sie **Aktualisieren**.
- g. Wiederholen Sie die Schritte 10a bis 10f für jede aufgeführte geplante Aufgabe.
- h. Wenn Sie fertig sind, kehren Sie zu Geführtes Setup zurück.
- i. Wählen Sie neben der Aufgabe Konfigurierte geplante Aufgaben die Option **Als abgeschlossen markieren** aus.

12. Überprüfen Sie die importierten Daten

- a. Entweder warten, bis die geplante Aufgabe oder die Aufträge gemäß ihrem Zeitplan abgeschlossen sind. Oder öffnen Sie zur Ausführung bei Bedarf den Datensatz der geplanten Aufgabe, und wählen Sie **Jetzt ausführen aus**.
- b. Sobald die geplante Aufgabe bzw. die geplanten Aufgaben abgeschlossen sind, wählen Sie **Konfigurieren** neben der Aufgabe Importierte Daten überprüfen aus.
- c. Überprüfen Sie die importierten CMDB

Configuration Items

Class

Search

All > Discovery source = SG-SiemensIAH

-Daten.

d. Wenn Sie fertig sind, kehren Sie zu Geführtes Setup zurück.

e. Wählen Sie neben der Aufgabe Importierte Daten überprüfen die **Option Als abgeschlossen markieren** aus.

13. Wahlweise: Konfigurieren Sie einen Asset-Erweiterungspunkt

Weitere Informationen finden Sie unter [Erweiterte Konfiguration für Asset-Erweiterungspunkt](#).

14. Verbindung mit externen Systemen

Diese Service Graph Connector -Integration basiert auf einer Verbindung zur Siemens IAH-API. Die Integration ist meist vorkonfiguriert, um eine Verbindung mit dem externen SIEMENS IAH-System herzustellen. Konfigurieren Sie die Verbindung mithilfe des geführten Setups. Um eine Verbindung zum Siemens IAH herzustellen, überprüfen und schließen Sie Schritt 5 ab.

15. Konfiguration testen

Weitere Informationen finden Sie unter [Testen Sie die Siemens IAH-Konfiguration](#).

Nächste Maßnahme

Um die Operational Technology (OT-)Geräte anzuzeigen, die während des Imports erstellt wurden, navigieren Sie zu **Alle > Service Graph Connectors > SIEMENS IAH > Alle SIEM-IAH-OT-Assets**.

Erweiterte Konfiguration für Asset-Erweiterungspunkt

Vor der Transformation durch Robust Transformator (RTE) und IntegrationHub ETL werden die Assets aus der Siemens IAH-API in ein Standardformat reduziert. Wenn Sie zusätzliche Attribute in das reduzierte Asset aufnehmen möchten, verwenden Sie das Skript für den Asset-Erweiterungspunkt. Sobald Sie den Erweiterungspunkt implementiert haben, werden die zusätzlichen anwenderdefinierten Attribute mithilfe von IntegrationHub ETL transformiert und zugeordnet.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle > Service Graph Connectors > SIEMENS IAH > Erweiterungspunkte**.
2. Wählen Sie den Datensatz `sn_siemensiahsgc.SGSiemensIAHAssetExtension` aus.
3. Wählen Sie im Abschnitt „Zugehörige Links“ **die Option Implementierung erstellen** aus.
4. Aktualisieren Sie in der Skripteinbindung die Prozessfunktion, um die gewünschten zusätzlichen Attribute mit Javascript-Code einzubeziehen.

Im folgenden Beispiel wird dem reduzierten Asset ein **custom_attribute**

Script Include
SGSiemensIAHAssetExtension

You are editing a record in the Service Graph Connector for Siemens IAH application (cancel)

Name: SGSiemensIAHAssetExtension

API Name: sn_siemensiahsg:SGSiemensIAHAssetExtension

Application: Service Graph Connector for Siemens IAH

Accessible from: This application scope only

Client callable: ☐

Active: ☒

Description: Implements extension point sn_siemensiahsg:SGSiemensIAHAssetExtension
This extension allows users to have an intersection point between getting Asset from SiemensIAH and inserting it into the staging table. Here you can modify or add additional properties

Script

```
1 var SGSiemensIAHAssetExtension = Class.create();
2 SGSiemensIAHAssetExtension.prototype = {
3   initialize: function() {
4   },
5
6   process: function(flattenedAsset, apiAsset) {
7
8     //Modify or add additional properties to the flattenedAsset before returning flattenedAsset which will be inserted in
9     flattenedAsset.custom_attribute = apiAsset.extensions.customAttributes;
10
11   },
12   return flattenedAsset;
13 },
14 type: 'SGSiemensIAHAssetExtension'
15 };
16
```

Protection policy: -- None --

Update Delete

hinzugefügt.

5. Führen Sie einen Testladen aus, um die Daten zu validieren.
Weitere Informationen finden Sie in Schritt 7 in [Konfigurieren Sie das geführte Setup](#).
6. Sobald die Testlast ausgeführt wurde, navigieren Sie zu **Alle > System-Importsätze > Importsatztabellen > Bereitstellung des SG-SiemensIAH-Assets**.
7. Validieren Sie anhand der Daten, dass die **Datenspalte** das hinzugefügte anwenderdefinierte Attribut enthält.
Wenn das anwenderdefinierte Attribut nicht in der Spalte enthalten ist, vergleichen Sie die api_data mit den -Daten, und korrigieren Sie Ihren Code.
8. Nach der Validierung transformieren Sie das custom_attribute-Element und ordnen Sie es der RTE-Transformation mithilfe von IntegrationHub ETL zu.
 - a. Navigieren zu **Konfiguration > IntegrationHub ETL**.
 - b. Wählen Sie unter **CMDB-Anwendung: SG-SiemensIAH** den Asset-Datensatz SG-SiemensIAH aus.
 - c. Wählen Sie im Abschnitt 1. Grundlegende Details angeben die **Option Quelldaten importieren und Grundlegende Details angeben aus**.
 - d. Vergewissern Sie sich, dass im Feld **Beispiel-Importsatz** ein Beispiel-Importsatz mit hinzugefügtem anwenderdefiniertem Attribut verwendet wird. Oder scrollen Sie nach unten, und wählen Sie **Neuen Importsatz automatisch abrufen aus**.
 - e. Um den Importsatz abzurufen, wählen Sie **Speichern** und **als abgeschlossen markieren aus**.

Hinweis:

Wenn Sie zurück zum Assistenten für ETL-Transformationszuordnungen navigieren, werden möglicherweise Fehlermeldungen angezeigt. Normalerweise können Sie die Fehlermeldungen ignorieren.

- f. Um das anwenderdefinierte Attribut zu transformieren und zuzuordnen, führen Sie die Aufgaben **Vorschau und Datenvorbereitung** sowie **CMDB-Klassen zum Zuordnen von Quelldaten auswählen aus**. Weitere Informationen finden Sie unter [IntegrationHub ETL](#).

Testen Sie die Siemens IAH-Konfiguration

Testen Sie die Siemens IAH-Konfiguration, um zu validieren, ob die Daten reduziert und von der Siemens IAH-API abgerufen wurden.

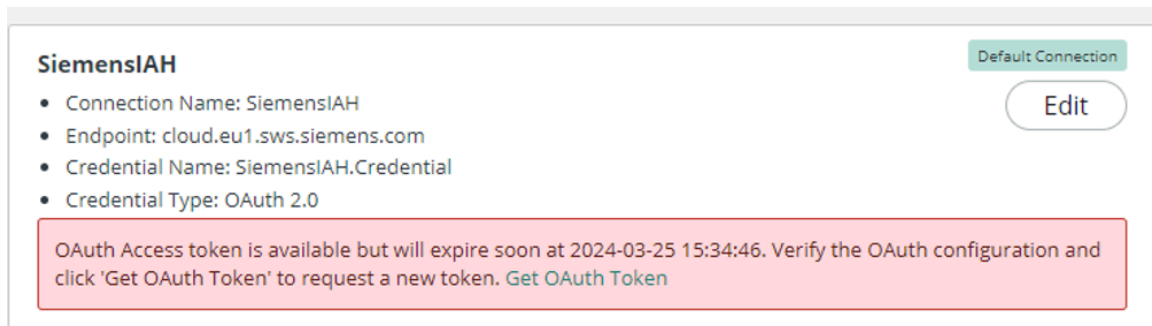
Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

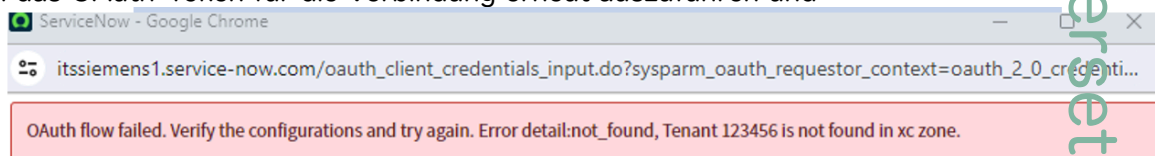
1. Testen Sie den Flow „Siemens IAH Test OAuth“.

- Navigieren zu **Alle > Service Graph Connectors > SIEMENS IAH > Setup**.
- Öffnen Sie den Abschnitt Verbindung konfigurieren.
- Wählen Sie neben der Aufgabe „Siemens IAH-Verbindung und -Anmeldeinformationen konfigurieren“ **die Option Konfigurieren** aus.
- Wählen Sie unter der SiemensIAH-Verbindung **Details anzeigen** aus.
- Wählen Sie **OAuth-Token abrufen** aus. Wenn das OAuth-Token erfolgreich abgerufen wurde, wird die folgende Meldung angezeigt:



Wenn Probleme mit den Anmeldeinformationen auftreten, wird beim Abrufen des OAuth-Tokens im Popup-Fenster eine Fehlermeldung angezeigt. Überprüfen Sie die Fehlermeldung, und aktualisieren Sie Ihre Anmeldeinformationen. Im folgenden Beispiel wurde der Mandant nicht gefunden oder ist falsch. Sie müssen den Mandanten aktualisieren und **auf „OAuth-Token abrufen“** klicken, um das OAuth-Token für die Verbindung erneut auszuführen und

abzurufen.



2. Testen Sie die Siemens IAH-Verbindung

- Navigieren zu **Alle > Service Graph Connectors > SIEMENS IAH > Setup**.
- Öffnen Sie den Abschnitt Verbindung konfigurieren.
- Validieren Sie die Verbindung. Weitere Informationen zum Validieren der Verbindung finden Sie in Schritt 7 in [Konfigurieren Sie das geführte Setup](#).

3. Testen Sie das Laden der Datenquelle „Siemens IAH“.

- Navigieren zu **Alle > Service Graph Connectors > SIEMENS IAH > Datenquellen**.
- Wählen Sie eine Datenquelle aus.
- Wählen Sie im Abschnitt „Zugehörige Links“ die Option **Testladen 20 Datensätze** aus.
- Sobald das Laden des Tests abgeschlossen ist, navigieren Sie zu **Alle > System-Importsätze > Importsatztabellen > Bereitstellung des SG-SiemensIAH-Assets**.
- Überprüfen Sie in der **Datenspalte**, ob die Daten reduziert und von der API abgerufen wurden.

- f. Wenn Sie die Systemeigenschaften so konfiguriert haben, dass API-Rohdaten in die Bereitstellungstabelle geladen werden, zeigen Sie die API-Rohdaten an, indem Sie einen Datensatz öffnen und das Feld **api_data** überprüfen. Weitere Informationen zu den Systemeigenschaften finden Sie in Schritt 9 [Konfigurieren Sie das geführte Setup](#).

Systemeigenschaften für Service Graph Connector für SIEMENS IAH

Als Administrator können Sie die Funktionen von Service Graph Connector für SIEMENS IAH über die Systemeigenschaften konfigurieren.

Sie können auf die Systemeigenschaften zugreifen, indem Sie zu navigieren **Alle > Service Graph Connectors > SIEMENS IAH > Systemeigenschaften**. In der folgenden Tabelle werden die für Service Graph Connector verfügbaren Systemeigenschaften beschrieben.

Systemeigenschaften für Service Graph Connector für SIEMENS IAH

Systemeigenschaft	Beschreibung
sn_siemensiahsgc.api_page_size	API-Seitengröße Maximale Anzahl von Zeilen, die von einem einzelnen REST-Aufruf zurückgegeben werden sollen.
sn_siemensiahsgc.api_max_timeout	Maximale API-Zeitüberschreitung Maximale Zeit zum Warten auf eine Antwort bei REST-Aufrufen an SIEMENS IAH. Standardwert: 30000
sn_siemensiahsgc.scope	Umfang der Einträge. Gültige Werte: „onboarded_assets“, „unknown_assets“ oder „ignored_assets“.
sn_siemensiahsgc.ignore_types	Kommagetrennte Liste des Typs von Assets oder Geräten, die während des Imports ignoriert werden sollen.
sn_siemensiahsgc.append_mac_to_name	Wenn Sie Ja auswählen, wird die MAC-Adresse bis an den Namen im Format @ {MAC-Adresse} angehängt. Wenn Sie Nein auswählen, wird der Name auf MAC-Adresse festgelegt.
sn_siemensiahsgc.load_raw_api_item_into_staging	Laden Sie API-Rohdaten in die Bereitstellungstabelle. Wenn Sie Ja auswählen, werden die API-Rohdaten für jede Zeile neben den analysierten Daten in die Bereitstellungstabellen aufgenommen. Dies ist nützlich, wenn Sie versuchen, die importierten Daten in ServiceNow mit den in der Siemens IAH-API verfügbaren Daten zu vergleichen.
sn_siemensiahsgc.ging.verbosity	Protokolle können sich auf der Ebene Fehler , Warn , Info und Debuggen befinden.

Fehlerbehebung bei Service Graph Connector für SIEMENS IAH

In diesem Abschnitt erfahren Sie, wie Sie Probleme bei der Konfiguration und Verwendung von Service Graph Connector für SIEMENS IAH beheben.

Verbindungsprobleme

Beim Einrichten der Integration gibt es einen Schritt zum Testen der Verbindung, nachdem Sie Ihre URL und die Anmeldeinformationen für die Standardauthentifizierung konfiguriert haben. Wenn alles richtig konfiguriert ist, sollte ein erfolgreicher Verbindungstest ohne Fehler angezeigt werden. Wenn während der Verbindung ein Fehler aufgetreten ist, stellt Service Graph Connector die Fehlermeldung, den Fehlercode und den Antworttext von der API bereit. Die folgende Abbildung zeigt den Abschlusscode eines erfolgreichen Verbindungstests.

Service Graph Connections
SiemensIAH

Name: SiemensIAH

Connection Alias: sn_siemensiahgc.SiemensIAH

Active: ☒

Status: Success

Status Code: 200

Application: Service Graph Connector for Siemens IAH

Message: Successfully queried Asset from the Siemens IAH API

Suggestion:

Unter Ausgehende HTTP-Anforderungen können Sie den von der API zurückgegebenen Statuscode anzeigen, indem Sie zu navigieren **Alle > Systemprotokolle > Ausgehende HTTP-Anforderungen**. In der Listenansicht sollte der URL-Hostname angezeigt werden, den Sie beim Einrichten der Verbindungsparameter angegeben haben. Sie können diesen Datensatz öffnen, um die Verbindungsdetails anzuzeigen. Die folgende Abbildung zeigt ein Beispiel für einen ausgehenden HTTP-

Outbound HTTP Log
Created 2023-11-15 06:43:40

HTTP method: POST

Created: 2023-11-15 06:43:40

URL: https://lahprod.eu1.sws.siemens.com/oauth/token

Response status: 200

Response time (ms): 118

Log Level: All

Anforderungsdatensatz.

Standardmäßig ist die Protokollebene auf **Standard** festgelegt, sodass der Antwort- oder Aufgabentext nicht angezeigt wird. Das Feld **Antwortstatus** gibt Ihnen jedoch einen Hinweis auf das Problem. Beispielsweise weist ein 401 im Feld **Antwortstatus** auf eine nicht autorisierte Anforderung hin. Um dieses Problem zu beheben, öffnen Sie die Verbindung, und vergewissern Sie sich, dass die Client-ID und der Clientschlüssel eingegeben wurden. Weitere Informationen zum Bearbeiten des Verbindungsdatensatzes finden Sie unter Schritt 5 in [Konfigurieren Sie das geführte Setup](#).

Wenn Sie eine weitere Diagnose durchführen müssen, können Sie die Protokollebene über die Systemeigenschaften überschreiben, um weitere Informationen bereitzustellen. Sie können alle verfügbaren Systemeigenschaften überprüfen, indem Sie zu navigieren **Alle > Systemeigenschaften > Alle Eigenschaften**. Ändern Sie beispielsweise die Systemeigenschaft „glide.outbound_http_log.override“ in „**True**“, und aktualisieren Sie die Systemeigenschaft „glide.outbound_http_log.override.level“ auf einen geeigneten Wert, z. B. all. Die folgende Abbildung zeigt die bearbeiteten

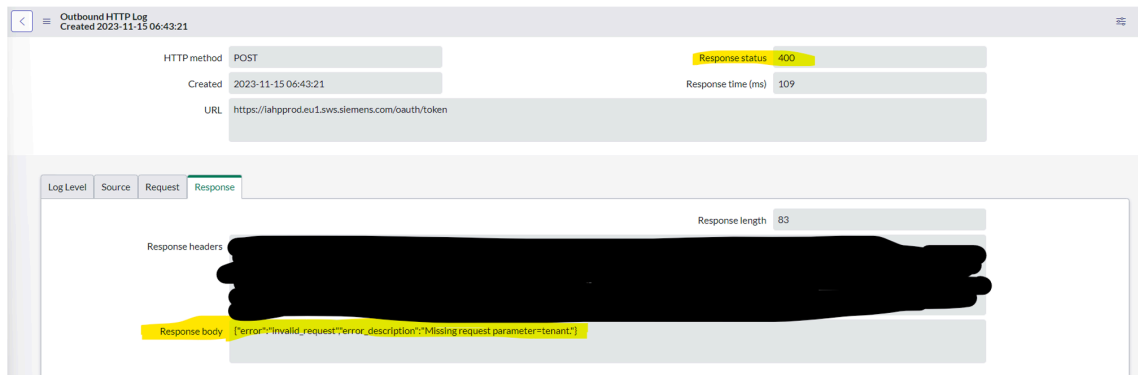
Name	Value	Type	Application	Description	Updated	Updated by
*glide.outbound_http_log.override	Search	Search	Search	Search	Search	Search
glide.outbound_http_log.override	true	true false	Global		2023-10-12 10:14:49	Jessica.Hanrahan
glide.outbound_http_log.override.level	all	string	Global		2023-10-12 10:13:48	Jessica.Hanrahan

Eigenschaften.

Hinweis:

Stellen Sie sicher, dass Sie dies nur für einen begrenzten Zeitraum tun, und ändern Sie sie zurück, sobald das Problem gelöst ist.

Wenn die erweiterte Protokollierung aktiviert ist, können zusätzliche Details für Anforderungen bereitgestellt werden, um mehr Kontext für das Problem zu bieten. Im folgenden ausgehenden HTTP-Protokoll lautet der **Antwortstatus** beispielsweise 400, und der **Antworttext** gibt an, dass der Mandant leer war.



Sie können dieses Problem beheben, indem Sie im Flow Designer zu der Verbindung navigieren und sicherstellen, dass Sie im Feld **Mandant** den erwarteten Wert eingeben. Weitere Informationen zum Zugriff auf die Verbindung in Workflow-Studio finden Sie in Schritt 5 in [Konfigurieren Sie das geführte Setup](#).

Asset-Reduzierung oder Probleme mit fehlenden Daten

Wenn Probleme mit der Reduzierung des Assets oder fehlende Daten in der API auftreten, können Sie eine Testlast ausführen, die reduzierten Daten in der Bereitstellungstabelle validieren und mit „api_data“ vergleichen, um zu sehen, ob die Daten von der API bereitgestellt wurden. Weitere Informationen finden Sie unter [Testen Sie die Siemens IAH-Konfiguration](#).

Operational Technology Manager verwenden

Nachdem Sie alle erforderlichen Einrichtungsaufgaben abgeschlossen haben, einschließlich der Installation der Erweiterungsklassen Operational Technology (OT) und des Zuweisens von Anwenderrollen, führen Sie die folgenden Aufgaben aus, um die grundlegenden Daten und Beziehungen für die Lösung ServiceNow® Operational Technology zu erstellen.

Aufgabe	Zweck
1. Füllen Sie eine Excel-Tabelle MicrosoftMicrosoft Azure Event Hubs mit Ihren vorhandenen Daten Operational Technology aus.	Positioniert Ihre vorhandenen Daten in den richtigen Spalten einer MicrosoftMicrosoft Azure Event Hubs Excel-Tabelle, um den erfolgreichen Daten-Upload sicherzustellen.
2. Importieren Sie Ihre Excel-Tabelle.	Lädt Ihre vorhandenen Operational Technology -Daten in den Configuration Management Database (CMDB)hoch.
3. Führen Sie die Funktion Discovery für Operational Technology aus.	Erkennt Geräte vom Operational Technology Typ (OT) in festgelegten Purdue-Ebenen in Ihren ICS-Netzwerken (Industrial Control System).

Aufgabe	Zweck
4. Verwenden Sie die Auswahlmöglichkeiten im Menü Operational Technology (OT).	Ermöglicht das Bearbeiten oder Anzeigen detaillierter Informationen für die OT-Geräte in Ihrem Unternehmen.

Service Graph Connector für Operational Technology (Excel)

Mit der Funktion des Connectors Service Graph (Excel) können Sie Ihre vorhandenen Operational Technology -Daten aus einer ausgefüllten Excel-Tabelle Microsoft Azure Event Hubs importieren. Sie verwenden ihn im IntegrationHub Extrahieren der Transformationslast (ETL), um diese Daten in den Configuration Management Database (CMDB) hochzuladen.

Bevor Sie den Importvorgang ausführen können, müssen Sie die Excel-Tabelle Microsoft Azure Event Hubs mit Ihren vorhandenen Daten Operational Technology füllen. Wenn Sie Ihre Excel-Tabelle Microsoft Azure Event Hubs mit IntegrationHub ETL importieren, werden die richtigen Configuration Item (CI)-Datensätze in Configuration Management Database (CMDB) erstellt. Weitere Informationen finden Sie [unter Erweiterungsklassen für Operation Technology \(OT\)](#) .

Zugehörige Informationen

[IntegrationHub](#)

[IntegrationHub ETL](#)

Konfigurieren von Service Graph Connector für Microsoft Azure Event Hubs Excel

Konfigurieren Sie den Service Graph Connector für Microsoft Azure Event Hubs Excel, um Ihre vorhandenen Operational Technology-Daten aus einer ausgefüllten Microsoft Azure Event Hubs Excel-Faltdateitabelle zu importieren.

Verwenden Sie das geführte Setup für Service Graph Connector für Microsoft Azure Event Hubs Excel, und führen Sie die Aufgaben der Reihe nach aus, um Service Graph Connector für Microsoft Azure Event Hubs Excel zu konfigurieren.

Navigieren zu **Alle > Industrial Workspace-Administrator > Geführtes Setup**, öffnen Sie die folgenden geführten Setups, und führen Sie die Aufgaben aus.

Weitere Informationen zur Verwendung des geführten Setups finden Sie unter [Geführtes Setup](#) .

Aufgabe	Zweck
Anwender	Weist Rollen zu, um die für jeden Benutzer verfügbaren Aktionen zu steuern.
Überprüfen Sie die Klassenzuordnungen	Überprüfen und aktualisieren Sie die für den Service Graph Connector für Microsoft Excel verfügbaren Klassenzuordnungen.

Aufgabe	Zweck
	 Hinweis: Um die verfügbaren Klassenzuordnungen zu überprüfen, müssen Sie das Plugin „Industrial Core“ installieren, das die Tabellen mit den Klassenzuordnungsvorlagen für OT Service Graph Connectors enthält. Weitere Informationen zum Plugin „Industrial Core“ finden Sie unter List of plugins (Yokohama) .
Konfiguration der Bereitstellungstabelle	Konfigurieren Sie, um zu bestimmen, welche Faktoren bei der Identifizierung eines eindeutigen Namens für ein CI ausmachen. Weitere Informationen zu Systemeigenschaften finden Sie unter Systemeigenschaften, die sich auf die Verarbeitung des Excel-Imports für SG-OT-Geräte auswirken.
Daten vorbereiten	Erstellen Sie die Tabelle, und bereiten Sie sie vor, indem Sie Ihre vorhandenen Daten in den richtigen Spalten positionieren. Weitere Informationen zur Vorbereitung der Daten finden Sie unter Bereiten Sie Ihr Tool zur Überprüfung von OT-Arbeitsblatteinträgen vor dem Import für den Import von Service Graph Connector vor.
Erstellen Sie neue OT-Geräte	Erstellen Sie manuell ein neues OT-Gerät, indem Sie in der Listenansicht der Bereitstellungstabelle auf die Schaltfläche Neu klicken. Weitere Informationen zum Erstellen neuer OT-Geräte finden Sie unter
Datensätze validieren	Führen Sie Validierungen für die importierten Daten durch, um die Validierungsphase der Datensätze zu aktualisieren und Validierungskommentare bereitzustellen.  Hinweis: Sie müssen keine Datensätze in der Liste auswählen, um Validierungen auszuführen. Validierungen werden für alle in der Bereitstellungstabelle vorhandenen Datensätze ausgeführt. Weitere Informationen zum Validieren von Datensätzen finden Sie unter Validierungen verwalten.
Import planen	Importieren Sie Daten aus der Bereitstellungstabelle in die

Aufgabe	Zweck
	Importsatztabelle, und überprüfen Sie sie in den OT-Listenansichten und im Arbeitsbereich.

Weisen Sie Rollen für die Überprüfung von OT-Arbeitsblatteinträgen vor dem Import zu

Weisen Sie den Anwendern oder Anwendergruppen Rollen zu, damit Sie die Excel Service Graph Connector-Bereitstellungstabelle und ETL verwalten können.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Benutzer mit den in der folgenden Tabelle aufgeführten Rollen können die Anwendung Operational Technology Manager verwenden.

Rolle	Beschreibung
-Administrator [cmdb_inst_admin]	• Kann die ETL-Datei anzeigen oder bearbeiten • Kann die Datensätze in der Bereitstellungstabelle anzeigen.
[cmdb_OT_admin]	Kann die Datensätze in der Bereitstellungstabelle anzeigen oder bearbeiten.

Prozedur

Weisen Sie Benutzern und Gruppen mit der Benutzerverwaltungsfunktion Now Platform Rollen zu.

Zeigen Sie eine Vorschau vorhandener OT-Datensätze im an CMDB

Zeigen Sie eine Vorschau vorhandener Operational Technology (OT)-Gerätedatensätze in Configuration Management Database (CMDB) an, bevor Sie neue Datensätze aus der Bereitstellungstabelle importieren. Durch die Vorschau vorhandener Datensätze können Sie vermeiden, dass nicht zugehörige Datensätze abgeglichen oder zusammengeführt werden.

Vorbereitungen

Erforderliche Rolle: cmdb_ot_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn sich beim Importieren von OT-Geräten aus der Bereitstellungstabelle ein passendes Configuration Item (CI) in CMDB befindet, können vorhandene Datensätze mit neuen Datensätzen abgeglichen oder zusammengeführt werden. Übereinstimmende CIs umfassen den Hostnamen, die MAC-Adresse oder die Seriennummer. Um zu vermeiden, dass Datensätze versehentlich abgeglichen oder zusammengeführt werden, können Sie eine Vorschau der vorhandenen Datensätze anzeigen, die die übereinstimmenden CIs mit den Datensätzen in der Bereitstellungstabelle gemeinsam nutzen.

Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > OT-Manager > OT-Geräte importieren – Staging-Tabelle**.

In den Validierungskommentaren wird das gefundene übereinstimmende CI erläutert, und es wird ein Link zum entsprechenden CI angezeigt. Wenn in CMDB ein passendes CI gefunden wird, wird der Status Validierung auf **Teilweise gültig** gesetzt. In der folgenden Tabelle sind die entsprechenden CI-Validierungskommentare aufgeführt.

Übereinstimmende CI-Validierungskommentare

Übereinstimmendes CI	Validierungskommentar
Host-Name	Derselbe transformierte Name wurde für ein anderes CI gefunden: <Link to CI>
MAC-Adresse	Dieselbe MAC-Adresse [MAC-Adresse] für anderes CI gefunden: <Link to CI>
Seriennummer	Dieselbe Seriennummer [Seriennummer] für anderes CI gefunden: <Link to CI>

2. **Wahlweise:** Zeigen Sie das übereinstimmende CI an, indem Sie es aus der Liste Übereinstimmendes CI in der CMDB-Spalte auswählen.

Überprüfen Sie die Klassenzuordnungen

Überprüfen und aktualisieren Sie die für Service Graph Connector für Microsoft Excel verfügbaren Klassenzuordnungen.

Vorbereitungen

- Stellen Sie sicher, dass das Plugin „Industrial Core“ installiert ist, damit Sie die verfügbaren Klassenzuordnungstabellen anzeigen können.
- Erforderliche Rolle: admin oder cmdb_ot_admin

Warum und wann dieser Vorgang ausgeführt wird

Service Graph Connector für Microsoft Excel verwendet die in der Excel-SGC-Klassenzuordnungstabelle [excel_sgc_class_mapping] verfügbare Konfiguration, um die beste ServiceNow Configuration Management Database (CMDB) Klasse zu bestimmen, in die jedes Konfigurationselement (Configuration Item, CI) platziert werden soll. Sie können diese Einstellungen jederzeit ändern. Überprüfen Sie jedoch am besten die aktuelle Konfiguration, bevor Sie den ersten Import ausführen.

Prozedur

1. Navigieren zu **Alle > OT-Manager-Administrator > Excel SGC-Klassenzuordnungen**.

2. Überprüfen und aktualisieren Sie bei Bedarf die folgenden Felder in den Klassenzuordnungsdatensätzen.

Felder für Klassifizierungseinstellungen

Feld	Beschreibung
Quellklasse	Klasse des Quell-CI.
Zielklasse CMDB	Die erwartete ServiceNow -Klasse für das CI.

Feld	Beschreibung
OT-Gerätetyp	Der Kategorietyt, als der das OT-Gerät klassifiziert ist. Der Gerätetyp ist auch die Funktion, die das Gerät im OT-Netzwerk spielt. Zum Beispiel: Ein IT-Gerät, z. B. ein Server, kann in ein OT-Gerät umgewandelt werden, und die Funktion, die es im Netzwerk ausübt, ist ein HMI. Daher ist seine Klasse „Server“ und sein Gerätetyp ist „HMI“. i Hinweis: In einigen Fällen gibt es OT-Geräte ohne OT-Funktion oder OT-Geräte, bei denen der Gerätetyp unbekannt ist. Wählen Sie für OT-Geräte ohne OT-Funktion Keine OT-Funktion aus. Wählen Sie für OT-Geräte, bei denen der Gerätetyp unbekannt ist, Unbekannt aus.
Lassen Sie die Betriebssystemklassifizierung zu	Wenn auf True festgelegt und ein Betriebssystem für das CI gefunden wird, wird das Ziel von der Zielklasse CMDB zu einer Klasse ServiceNow gewechselt, die dem Betriebssystem entspricht.
Aktiv	Wenn diese Option aktiviert ist, wird die Klassenzuordnung auf Aktiv festgelegt.

Einfacher Import

Der einfache Import ist ein vereinfachter Importprozess, mit dem Sie nur die gewünschten Spalten importieren können.

Nur Benutzer mit der Administratorrolle können den einfachen Import verwenden. Sie können Daten in Tabellen innerhalb des aktuellen Bereichs sowie in Tabellen importieren, die anderen Anwendungen Schreibzugriff gewähren.

Laden Sie die Excel-Vorlage herunter

Laden Sie die Excel-Vorlage Microsoft Azure Event Hubs herunter, um eine Excel-Tabelle Microsoft Azure Event Hubs zu erstellen und mit Ihren vorhandenen Daten Operational Technology auszufüllen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > OT-Manager > OT-Geräte importieren: Bereitstellungstabelle**.
2. Klicken Sie mit der rechten Maustaste auf den Spaltentitel, und wählen Sie **Importieren** aus dem Listenmenü aus.
3. Wählen Sie aus, ob Sie Datensätze **einfügen** oder **aktualisieren** möchten.

Vorlage importieren

Vorlage	Beschreibung
Einfügen	Verwenden Sie diese Vorlage, um einer Tabelle neue Datensätze hinzuzufügen.
Aktualisieren	Verwenden Sie diese Vorlage, um Werte innerhalb vorhandener Datensätze in einer Tabelle zu ändern. Diese Vorlage enthält eine Zeile für jeden Datensatz in der Liste. Der aktuelle Listenfilter bestimmt, welche Datensätze die Vorlage enthält.

Insert new records or update existing records using an Excel template file. Click Upload to preview the data to be imported. [More Info](#)

Import external data into SG OT Excel Staging

Do you want to insert or update data ? ☒ Insert ☐ Update

Do you want to create an Excel template to enter data ? ☒

Step 1: Create an Excel template file to enter data

Include all fields in the template? ☒

[Create Excel template](#)

Step 2: Upload the template file

Excel template file [Choose file](#) No file chosen

[Upload](#)

4. Deaktivieren Sie das Kontrollkästchen **Alle Felder in Vorlage einschließen**, um nur die Spalten einzubeziehen, die in der Liste in der Vorlage angezeigt werden.

Bestimmte Felder in der Tabelle werden von Systemprozessen aktualisiert, und Sie können keine Werte in sie importieren. Ein Beispiel ist das Feld **Erstellt von**, das während des Imports mit dem angemeldeten Benutzer gefüllt wird, der den Import durchführt.

Lassen Sie dieses Kontrollkästchen aktiviert, um alle Spalten aus der Tabelle in die Vorlage aufzunehmen, auch die in der Liste ausgeblendeten Spalten.

5. Wählen Sie **Excel-Vorlage erstellen aus**.

6. Wählen Sie auf der Seite „Export abgeschlossen“ **Herunterladen** aus, um die Excel-Tabelle Microsoft Azure Event Hubs herunterzuladen.

Nächste Maßnahme

Öffnen Sie die Tabelle mit Ihrer bevorzugten Anwendung.

Hinweis:

Die Vorlage enthält eine Registerkarte **Richtungen**, die beschreibt, wie die Vorlage verwendet wird.

Bereiten Sie Ihr Tool zur Überprüfung von OT-Arbeitsblatteinträgen vor dem Import für den Import von Service Graph Connector vor

Bereiten Sie Ihre Tabelle vor, indem Sie Ihre vorhandenen Daten in den richtigen Spalten positionieren. Dies ist für den Erfolg des Uploads entscheidend.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Füllen Sie die folgenden Spalten in der Microsoft Excel-Tabelle aus:

i Hinweis:

Spaltennamen können nicht geändert werden. Der Bereitstellungstabelle können zusätzliche Spalten hinzugefügt werden. Weitere Informationen zum Hinzufügen einer neuen anwenderdefinierten Feldzuordnung in der Bereitstellungstabelle finden Sie unter [Fügen Sie in der Bereitstellungstabelle eine anwenderdefinierte Feldzuordnung für hinzu Service Graph](#).

Anleitungen zum Ausfüllen der Tabelle finden Sie in den folgenden Tabellen. Die Tabelle enthält viele Spalten. Die Beispiele und Feldbeschreibungen sind in mehrere Abschnitte unterteilt.

- Ausfüllen der Spalten A bis K
- Ausfüllen der Spalten L bis Y
- Ausfüllen der Spalten Z bis KI
- Ausfüllen der Spalten AJ bis AT
- Ausfüllen der Spalten AU bis BD
- Ausfüllen der Spalten BE bis BR
- Spalten BS bis BW werden ausgefüllt
- Ausfüllen der Spalten 1 bis 8

Spalten A bis K

Spalte	Erforderlicher Spaltenname	Typ	Beschreibung und Beispiel
A	Gerät-Relevanz	Zeichenfolge	Maß dafür, wie kritisch oder wichtig das OT-Gerät basierend auf seiner Rolle ist. Beispiele: ○ „Hoch“ oder „Sehr kritisch“. ○ Mittel oder kritisch ○ Niedrig oder Weniger kritisch ○ Keine oder nicht kritisch
B	Zugewiesen an	Zeichenfolge	E-Mail-Adresse des Anwenders, der dieses OT-Gerät zugewiesen ist. Beispiel: bob@example.com
C	Backplane-ID	Zeichenfolge	Eindeutige ID, die für die Identifizierung der Backplane und die Zuordnung zu Steuerungsmodulen verwendet wird. Beispiel: BPSN123

Spalte	Erforderlicher Spaltenname	Typ	Beschreibung und Beispiel
D	Backplane-Name	Zeichenfolge	Name der Backplane, falls vorhanden, für das OT-Gerät. Beispiele: Backplane Nr. 51, SPS1-Backplane
E	Übergeordnete ID des Steuerungsmoduls	Zeichenfolge	Eindeutige ID, die für die Identifizierung der Steuerungsmodule gegenüber der Backplane des übergeordneten Steuerungssystems verwendet wird. Beispiel: 482bb239-05e8-4bad-ba59-925eb87ff06e
F	Korrelations-ID	Zeichenfolge	Eindeutige ID, die zur Identifizierung des OT-Geräts verwendet wird. Geben Sie für die Korrelations-ID eine Zeichenfolge ein. Beispiele: 482bb239-05e8-4bad-ba59-925eb87ff06e oder 5123456. Dieser Spalteneintrag ist erforderlich. ○ Jedes importierte OT-Gerät muss eine eindeutige Korrelations-ID (correlation_id) aufweisen. ○ Die OT-Gerät-Daten, die Sie normalerweise importieren, stammen aus einem externen Quellsystem, das normalerweise jedem Datensatz einen eindeutigen Bezeichner zuweist.
G	Anwenderdefiniertes Feld 1	Zeichenfolge	(Optional) Anwenderdefinierte Daten für das OT-Gerät werden im Feld Attribute im CI gespeichert. Sie können diese Spalte verwenden, um dem OT-Gerät Freiformdaten zur Kategorisierung oder für andere Zwecke zuzuordnen. Beispiele: Überholt, Gebraucht
H	Anwenderdefiniertes Feld 2	Zeichenfolge	(Optional) Anwenderdefinierte Daten für das OT-Gerät werden im Feld Attribute im CI gespeichert. Sie können diese Spalte verwenden, um dem OT-Gerät Freiformdaten zur Kategorisierung oder für andere Zwecke zuzuordnen. Beispiele: Malen, Stempeln
I	Anwenderdefiniertes Feld 3	Zeichenfolge	(Optional) Anwenderdefinierte Daten für das OT-Gerät werden im Feld Attribute im CI gespeichert. Sie können diese Spalte verwenden, um dem OT-Gerät Freiformdaten zur Kategorisierung oder für andere Zwecke zuzuordnen.
J	Anwenderdefiniertes Feld 4	Zeichenfolge	(Optional) Anwenderdefinierte Daten für das OT-Gerät werden im Feld Attribute im CI gespeichert. Sie können diese Spalte verwenden, um dem OT-Gerät Freiformdaten zur Kategorisierung oder für andere Zwecke zuzuordnen.
K	Anwenderdefiniertes Feld 5	Zeichenfolge	(Optional) Anwenderdefinierte Daten für das OT-Gerät werden im Feld Attribute im CI gespeichert. Sie können diese Spalte verwenden, um dem OT-Gerät Freiformdaten zur Kategorisierung oder für andere Zwecke zuzuordnen.

Spalten L bis Y

Spalte	Erforderlicher Spaltenname	Typ	Beschreibung und Beispiel
L	Anzeigename	Zeichenfolge	Wird verwendet, um den Anzeigenamen von OT-Geräten auszufüllen.
M	Anlagenmodell-Entitätspfad	Zeichenfolge	Pfad der Anlagenmodell-Entität, der das OT-Gerät zugeordnet ist.
N	Firmware-Version	Zeichenfolge	Firmware-Version des OT-Geräts, falls vorhanden. Beispiel: 12.0
O	Zuerst erkannt	Datum/Uhrzeit	ISO-formatierter Zeitstempel des ersten Zeitpunkts, zu dem das OT-Gerät zum ersten Mal in Ihrem Netzwerk erkannt wurde. Beispiel: JJJJ-MM-TT HH:MM:SS.
P	Hardware-Version	Zeichenfolge	Hardware-Version des OT-Geräts, falls vorhanden. Beispiel: 13.2
Q	Hat Modul	Boolean	Bei Steuerungssystemen mit Modulen gibt an, dass dieses System über Module verfügt. Beispiele: Wahr, Falsch
R	E/A-Typ des Feldgeräts	Zeichenfolge	Ob dieses Gerät ein Feldgerät ist, gibt an, ob es für die Eingabe, Ausgabe oder beides verwendet wird. Beispiele: ○ Eingabe ○ Ausgabe ○ input_output Das Gerät fungiert gleichzeitig als Eingabe und Ausgabe.

Spalte	Erforderlicher Spaltenname	Typ	Beschreibung und Beispiel
S	IP-Adresse 1	Zeichenfolge	Erste IP-Adresse, falls vorhanden, die dem OT-Gerät zugeordnet ist. Wenn mehrere IP-Adressen vorhanden sind, verwenden Sie die nächste IP-Adressspalte (IP-Adresse 2). Beispiele: 10.0.0.22, 10.0.0.12
T	IP-Adresse 2	Zeichenfolge	Zweite IP-Adresse, falls vorhanden, die dem OT-Gerät zugeordnet ist. Beispiele: 192.168.100.1, 192.168.100.5
U	IP-Adresse 3	Zeichenfolge	Dritte IP-Adresse, falls vorhanden, die dem OT-Gerät zugeordnet ist.
V	IP-Adresse 4	Zeichenfolge	Vierte IP-Adresse, falls vorhanden, die dem OT-Gerät zugeordnet ist.
W	IP-Adresse 5	Zeichenfolge	Fünfte IP-Adresse, falls vorhanden, die dem OT-Gerät zugeordnet ist.
X	IP-Adresse 6	Zeichenfolge	Sechste IP-Adresse, falls vorhanden, die dem OT-Gerät zugeordnet ist.
Y	IP-Adresse 7	Zeichenfolge	Siebte IP-Adresse, falls vorhanden, die dem OT-Gerät zugeordnet ist.

Spalten Z bis AI

Spalte	Erforderlicher Spaltenname	Typ	Beschreibung und Beispiel
Z	IP-Adresse 8	Zeichenfolge	Achtende IP-Adresse, falls vorhanden, die dem OT-Gerät zugeordnet ist.
AA	IP-Adresse 9	Zeichenfolge	Neunte IP-Adresse, falls vorhanden, die dem OT-Gerät zugeordnet ist.

Spalte	Erforderlicher Spaltenname	Typ	Beschreibung und Beispiel
AB	MAC-Adresse 1	Zeichenfolge	Erste MAC-Adresse, falls vorhanden, die dem OT-Gerät zugeordnet ist. Wenn mehrere MAC-Adressen vorhanden sind, verwenden Sie die nächste MAC-Adressspalte (MAC-Adresse 2). Beispiele: 94:94:1d:01:6d:5f, CC:7c:4a:fb:20:71 i Hinweis: Für ein OT-Gerät müssen Sie einen Eintrag in mindestens einer dieser drei Tabellenspalten erstellen. Alle Werte in diesen Spalten müssen für die Tabelle eindeutig sein: - MAC-Adresse 1 - Name - Seriennummer
Wechselstrom	MAC-Adresse 2	Zeichenfolge	Zweite MAC-Adresse, falls vorhanden, die dem OT-Gerät zugeordnet ist. Beispiel: e5:4d:c8:36:b1:2d
AD	MAC-Adresse 3	Zeichenfolge	Dritte MAC-Adresse, falls vorhanden, die dem OT-Gerät zugeordnet ist.
AE	MAC-Adresse 4	Zeichenfolge	Vierte MAC-Adresse, falls vorhanden, die dem OT-Gerät zugeordnet ist.
AF	MAC-Adresse 5	Zeichenfolge	Fünfte MAC-Adresse, falls vorhanden, die dem OT-Gerät zugeordnet ist.
AG	MAC-Adresse 6	Zeichenfolge	Sechste MAC-Adresse, falls vorhanden, die dem OT-Gerät zugeordnet ist.
AH	MAC-Adresse 7	Zeichenfolge	Siebte MAC-Adresse, falls vorhanden, die dem OT-Gerät zugeordnet ist.

Spalte	Erforderlicher Spaltenname	Typ	Beschreibung und Beispiel
KI	MAC-Adresse 8	Zeichenfolge	Achtende MAC-Adresse, falls vorhanden, die dem OT-Gerät zugeordnet ist.

Spalten AJ bis AT

Spalte	Erforderlicher Spaltenname	Typ	Beschreibung und Beispiel
AJ	MAC-Adresse 9	Zeichenfolge	Neunte MAC-Adresse, falls vorhanden, die dem OT-Gerät zugeordnet ist.
AK	Hersteller	Zeichenfolge	Name des Herstellers des OT-Geräts. Beispiele: Blackwell Automation, Dell
AL	Seriennummer der Speicherkarte 1	Zeichenfolge	Zugewiesene Seriennummer der ersten im OT-Gerät installierten Speicherkarte, falls vorhanden. Wenn mehrere Speicherkarten vorhanden sind, verwenden Sie die nächste Seriennummerspalte der Speicherkarte (Seriennummer der Speicherkarte 2). Beispiele: MMC DA362131, MemSN123
AM	Seriennummer der Speicherkarte 2	Zeichenfolge	Zugewiesene Seriennummer der zweiten Speicherkarte, die im OT-Gerät installiert ist, falls vorhanden. Beispiel: MemSN123
AN	Seriennummer der Speicherkarte 3	Zeichenfolge	Zugewiesene Seriennummer der dritten Speicherkarte, die ggf. im OT-Gerät installiert ist.
AO	Arbeitsspeichergröße 1	Zeichenfolge	Größe der ersten Speicherkarte, die im OT-Gerät installiert ist, falls vorhanden. Beispiele: 256 GB oder 1 GB
AP	Arbeitsspeichergröße 2	Zeichenfolge	Größe der zweiten Speicherkarte, die im OT-Gerät installiert ist, falls vorhanden. Beispiele: 256 GB oder 1 GB
AQ	Arbeitsspeichergröße 3	Zeichenfolge	Größe der dritten Speicherkarte, die im OT-Gerät installiert ist, falls vorhanden. Beispiele: 256 GB oder 1 GB
AR	Arbeitsspeichertyp 1	Zeichenfolge	Typ der Speicherkarte, die im OT-Gerät installiert ist. Wenn mehrere Speicherkarten vorhanden sind, verwenden Sie mehrere Spalten. Beispiel: RAM
WIE	Arbeitsspeichertyp 2	Zeichenfolge	Typ der Speicherkarte, die im OT-Gerät installiert ist. Beispiele: RAM
AT	Arbeitsspeichertyp 3	Zeichenfolge	Typ der Speicherkarte, die im OT-Gerät installiert ist.

Spalten AU bis BD

Spalte	Erforderlicher Spaltenname	Typ	Beschreibung und Beispiel
AU	Modellnummer	Zeichenfolge	Modellnummer des Herstellers für das OT-Gerät. Beispiele: ThinkServer TD230, XPS 15z
AV	Modultyp	Zeichenfolge	Beschreibung der Funktion des Steuerungsmoduls, falls dieses Gerät eines ist. Beispiele: Eingabe, Ausgabe

Spalte	Erforderlicher Spaltenname	Typ	Beschreibung und Beispiel
AW	Name	Zeichenfolge	Hostname des OT-Geräts, normalerweise als Teil des FQDN. Beispiele: SPS1, Türkomponenten-HMI und Robot-Steuerungsmodul. i Hinweis: Für ein OT-Gerät müssen Sie einen Eintrag in mindestens einer dieser drei Tabellenspalten erstellen. Alle Werte in diesen Spalten müssen für die Tabelle eindeutig sein: ◦ MAC-Adresse 1 ◦ Name ◦ Seriennummer
AX	Betriebssystem	Zeichenfolge	Betriebssystem, das auf dem OT-Gerät installiert ist, falls vorhanden. Beispiele: Linux FeWo, Windows 10, Windows 2000, Mac OS 8. i Hinweis: Für ein OT-Gerät sollten Sie Einträge in den folgenden Tabellenspalten erstellen, auch wenn dies nicht erforderlich ist: ◦ Typ ◦ Wenn verfügbar, Betriebssystem ◦ Wenn verfügbar, Firmware-Version
AY	BS-Version	Zeichenfolge	Gemeldete Version des Betriebssystems, das (falls vorhanden) auf dem OT-Gerät installiert ist. Beispiele: 10.0, 13.5.2 i Hinweis: Für ein OT-Gerät sollten Sie Einträge in den folgenden Tabellenspalten erstellen, auch wenn dies nicht erforderlich ist: ◦ Typ ◦ os_version, falls verfügbar ◦ Wenn verfügbar, Firmware-Version
A-Z	OT-Stagingaufgabe	Zeichenfolge	Aufgaben erstellt, um ungültige Datensätze in der Bereitstellungstabelle zu korrigieren.
BA	Purdue-Ebene	Zeichenfolge	Zugewiesene Purdue-Ebene für das OT-Gerät. Durch das Zuweisen einer Purdue-Ebene wird sichergestellt, dass Discovery für die Funktion Operational Technology jedes Element ordnungsgemäß auf der richtigen ICS-Ebene findet und genaue Discovery -Ergebnisse erzeugt. Beispiele: 1, 2, 3
BB	Racknummer	Zeichenfolge	Rack, in dem das Steuerungsmodul installiert ist. Beispiele: 1, 2, 3

Spalte	Erforderlicher Spaltenname	Typ	Beschreibung und Beispiel
BC	Seriennummer	Zeichenfolge	Zugewiesene Seriennummer (falls vorhanden) für das OT-Gerät. Beispiele: SN545, SN998 i Hinweis: Für ein OT-Gerät müssen Sie einen Eintrag in mindestens einer dieser drei Tabellenspalten erstellen. Alle Werte in diesen Spalten müssen für die Tabelle eindeutig sein: ○ MAC-Adresse 1 ○ Name ○ Seriennummer
BD	Seriennummertyp	Zeichenfolge	Normalerweise auf den Wert „System“ festgelegt, es kann jedoch auch ein anderer Typ von Seriennummer sein. Beispiel: uuid

Spalten: BE bis BR

Spalte	Erforderlicher Spaltenname	Typ	Beschreibung und Beispiel
BE	Kurzbeschreibung	Zeichenfolge	Kurze Beschreibung des OT-Geräts. Beispiele: HMI für die Türlackierzelle, steuert den Türkomponenten-Robot.
BF	Site	Zeichenfolge	Die Anlagenmodelle beginnen auf Site-Ebene und enthalten eine detaillierte hierarchische Struktur, die jeden Industriestandort beschreibt. Weitere Informationen finden Sie unter Anlagenmodell nach ISA-95 .
BG	Slot-Nummer	Zeichenfolge	Gibt für ein Steuerungsmodul die Steckplätze an, die dieses Gerät im Gehäuse des Steuerungssystems belegt. Beispiele: 1, 2
BH	Datum der Softwareinstallation 1	Datum/ Uhrzeit	Datum, an dem die Anwendungssoftware auf dem OT-Gerät installiert wurde. Wenn mehrere Datumsangaben vorhanden sind, verwenden Sie mehrere Spalten. Verwenden Sie nur das UTC-Format für das Datum. Beispiel: JJJJ-MM-TT HH:MM:SS
BI	Datum der Softwareinstallation 2	Datum/ Uhrzeit	Datum, an dem die Anwendungssoftware auf dem OT-Gerät installiert wurde. Wenn mehrere Datumsangaben vorhanden sind, verwenden Sie mehrere Spalten. Verwenden Sie nur das UTC-Format für das Datum. Beispiel: JJJJ-MM-TT HH:MM:SS

Spalte	Erforderlicher Spaltenname	Typ	Beschreibung und Beispiel
BJ	Datum der Softwareinstallation 3	Datum/ Uhrzeit	Datum, an dem die Anwendungssoftware auf dem OT-Gerät installiert wurde. Wenn mehrere Datumsangaben vorhanden sind, verwenden Sie mehrere Spalten. Verwenden Sie nur das UTC-Format für das Datum. Beispiel: JJJJ-MM-TT HH:MM:SS.
BK	Software installiert 1	Zeichenfolge	Name der Anwendungssoftware, die auf dem OT-Gerät installiert ist, falls vorhanden. Wenn mehrere Namen vorhanden sind, verwenden Sie mehrere Spalten. Beispiel: Pop Art HMI Vision
BL	Software installiert 2	Zeichenfolge	Name der Anwendungssoftware, die auf dem OT-Gerät installiert ist, falls vorhanden.
BM	Software installiert 3	Zeichenfolge	Name der Anwendungssoftware, die auf dem OT-Gerät installiert ist, falls vorhanden.
BS	Softwareversion 1	Zeichenfolge	Gemeldete Version der Anwendungssoftware, falls vorhanden, die auf dem OT-Gerät installiert ist. Wenn mehrere Versionen vorhanden sind, verwenden Sie mehrere Spalten. Beispiel: v1.2 oder v2011 SP3 RF2 oder 4.54.32145
BO	Softwareversion 2	Zeichenfolge	Gemeldete Version der Anwendungssoftware, falls vorhanden, die auf dem OT-Gerät installiert ist. Beispiel: v1.2 oder v2011 SP3 RF2 oder 4.54.32145
BP	Softwareversion 3	Zeichenfolge	Gemeldete Version der Anwendungssoftware, falls vorhanden, die auf dem OT-Gerät installiert ist. Beispiel: v1.2 oder v2011 SP3 RF2 oder 4.54.32145
BQ	Status	Zeichenfolge	Status des OT-Geräts: – Keine Angabe – Kein zugewiesener Status. Abwesend OT-Gerät fehlt in Ihren Einrichtungen. In Wartung OT-Gerät wird gewartet und ist derzeit offline. Auf Lager OT-Gerät ist in Ihren Einrichtungen auf Lager. Installiert OT-Gerät ist in Ihren Einrichtungen installiert. Ausstehende Installation

Spalte	Erforderlicher Spaltenname	Typ	Beschreibung und Beispiel
			Die Installation des OT-Geräts steht in Ihren Einrichtungen aus. Ausstehende Reparatur Die Reparatur des OT-Geräts steht aus, ist jedoch noch nicht online. Deaktiviert OT-Gerät ist deaktiviert. Gestohlen OT-Gerät wurde gestohlen. i Hinweis: Die Werte in diesem Feld werden den Feldern Lebenszyklusphase und Status der Lebenszyklusphase im CI-Formular zugeordnet.
BR	Support-Gruppe	Zeichenfolge	Name der primären Supportgruppe für dieses OT-Gerät. Beispiele: Tür-Support, IT-Support des Unternehmens.

Spalten BS bis BW

Spalte	Erforderlicher Spaltenname	Typ	Beschreibung und Beispiel
BS	Umgewandelter Name	Zeichenfolge	Anwender dürfen diese Spalte nicht ausfüllen. Standardmäßig wird der transformierte Namenswert mit den Systemeigenschaften der transformierten Spalte gefüllt. Ein Anwender kann den umgewandelten Namen nicht bearbeiten. Informationen zu den Systemeigenschaften finden Sie unter Systemeigenschaften, die sich auf die Verarbeitung des Excel-Imports für SG-OT-Geräte auswirken.

Spalte	Erforderlicher Spaltenname	Typ	Beschreibung und Beispiel
Bluetooth	Typ	Zeichenfolge	Typ des OT-Geräts/ Konfigurationselements (CI). Beispiele: SPS, DCS i Hinweis: ○ Eine Liste und Erklärungen gültiger CI-Typen finden Sie unter Erweiterungsklassen für Operation Technology (OT) . ○ Für ein OT-Gerät sollten Sie Einträge in den folgenden Tabellenspalten erstellen, auch wenn dies nicht erforderlich ist: ▪ Typ ▪ os_version
BU	Validierungskommentare	Zeichenfolge	Anwender dürfen diese Spalte nicht ausfüllen. Standardmäßig werden Validierungskommentare ausgefüllt, nachdem die Validierungen für die Datensätze der Bereitstellungstabelle ausgeführt wurden, die aus Excel importiert werden. Validierungskommentare werden nicht aktualisiert, wenn Datensätze importiert werden.

Spalte	Erforderlicher Spaltenname	Typ	Beschreibung und Beispiel
			Der Anwender kann die Validierungskommentare nicht bearbeiten.
BV	Validierungsstatus	Zeichenfolge	Anwender dürfen diese Spalte nicht ausfüllen. Standardmäßig wird der Validierungsstatus ausgefüllt, wenn die Daten in die Bereitstellungstabelle importiert werden. Status des OT-Geräts: Ausstehende Validierung Standardstatus, wenn Datensätze in die Bereitstellungstabelle importiert werden. Ungültig Ein CI-Datensatz kann nicht eindeutig in CMDB erstellt werden. Teilweise gültig Einer der Werte „Umgewandelter Name“, „MAC-Adresse 1“ oder „Seriennummer“ hat keinen Wert. Alle anderen Felder (Korrelations-ID,

Spalte	Erforderlicher Spaltenname	Typ	Beschreibung und Beispiel
			übergeordnete ID des Steuerungsmoduls) enthalten Werte. Gültig Alle Bezeichner sind vorhanden und bereit für den Import. Importiert Der Import der Daten aus der Bereitstellungstabelle in die Importsatztable wurde abgeschlossen. Anwender kann den Validierungsstatus nicht bearbeiten.
BW	Lieferant	Zeichenfolge	Name des Lieferanten des OT-Geräts.

Spalten 1 bis 8

Spalte	Erforderlicher Spaltenname	Typ	Auswahlspalten, falls zutreffend	Beschreibung und Beispiel
1	Konfigurationsstatus der Sicherung	Auswahlliste	Sicherung aktiviert, Sicherung deaktiviert, Unbekannt, Nicht zutreffend, Geplant, Nicht geplant	Gibt an, ob das CI im Sicherungsservice oder auf der Appliance mit relevanten Richtlinien konfiguriert wurde. Beispiele: Sicherung aktiviert
2	Ausführungsmodus der Sicherung	Auswahlliste	Manuell, Automatisch, Manuell oder	Gibt an, ob die Sicherung so konfiguriert ist, dass sie regelmäßig

Spalte	Erforderlicher Spaltenname	Typ	Auswahlspalten, falls zutreffend	Beschreibung und Beispiel
			Automatisch, Unbekannt	automatisch ausgeführt wird, oder ob sie manuell bei Bedarf ausgeführt wird. Beispiele: Manuell, Automatisch
3	Sicherungsquellen-ID	Zeichenfolge		Bezeichner der Sicherungsservicequelle für ein Gerät, der das Gerät in externen oder internen Sicherungsservices identifiziert. Die Sicherungsquellen-ID kann host_id, vcenter_id, instance_id, db_id enthalten. Beispiele: AdvWrks2008R2Backup
4	Letzter Sicherungsversuch	glide_date_time		Datum und Uhrzeit des letzten Sicherungsversuchs für ein Gerät. Beispiele: 18.06.2024 09:53:37
5	Letzte erfolgreiche Sicherung	glide_date_time		Datum und Uhrzeit der letzten erfolgreichen Sicherung für ein Gerät. Beispiele: 18.06.2024 09:53:37
6	Tolerierter Datenverlust aufgrund von Ausfällen	glide_duration		Stellt die Zeit dar, die zwischen Sicherungen vergehen kann, und die Menge der verlorenen Daten. Beispiele: 90 12:00:00

Automatische Übersetzung

Spalte	Erforderlicher Spaltenname	Typ	Auswahlspalten, falls zutreffend	Beschreibung und Beispiel
7	Sicherung verwaltet von	Zeichenfolge		E-Mail-ID des Anwenders, der für die Verwaltung der Sicherung verantwortlich ist. Beispiele: firstname.lastname@example.co
8	Sicherung verwaltet von Gruppe	Zeichenfolge		Name der primären Supportgruppe, die für die Verwaltung der Sicherung verantwortlich ist. Beispiele: App Engine-Administratoren

2. Speichern Sie die Excel-Tabelle Microsoft Azure Event Hubs nach dem Ausfüllen an einem bekannten Ort, damit Sie sie beim Hochladen einfach aufrufen können.

Systemeigenschaften, die sich auf die Verarbeitung des Excel-Imports für SG-OT-Geräte auswirken

Der Excel-Importprozess für SG-OT-Geräte hängt von den folgenden Systemeigenschaften ab, um erfolgreich abgeschlossen zu werden.

sn_otsm_sgc.excel.fields.for.transformed.name

- Mit dieser Eigenschaft kann der Anwender die Felder zum Erstellen des transformierten Namens angeben.
- Der Feldwert oder die Spaltennamen müssen durch Kommas getrennt werden.

Dieser transformierte Name wird anstelle des Namensfelds direkt aus der Bereitstellungstabelle als Name des Configuration Item (CI) verwendet. Standardmäßig wird der Namensfeldwert selbst als transformierter Namenswert verwendet.

- Diese Eigenschaft gehört zum Bereich „sn_otsm_sgc“ und wird automatisch an diesen Eigenschaftsnamen angehängt.
- Erfordert die Rollen „admin“, „cmdb_ot_admin“ und „cmdb_inst_admin“ für Lese- und Schreibvorgänge.

sn_otsm_sgc.excel.transformed.name.delimiter

- Diese Eigenschaft gibt das Trennzeichen an, das verwendet werden soll, wenn der transformierte Name mit mehr als einem Feld- oder Spaltenwert berechnet wird, der in der Systemeigenschaft „**fields.for.transformed.name**“ angegeben ist.
- Wenn in der Eigenschaft „**fields.for.transformed.name**“ nur ein Spaltenname angegeben ist, wird das Trennzeichen nicht verwendet.
- Diese Eigenschaft gehört zum Bereich „**sn_otsm_sgc**“ und wird automatisch an diesen Eigenschaftsnamen angehängt.
- Erfordert die Rollen „admin“, „cmdb_ot_admin“ und „cmdb_inst_admin“ für Lese- und Schreibvorgänge.

sn_otsm_sgc.excel.fields.for.validation.state.change

- Mit dieser Eigenschaft können Sie eine durch Kommas getrennte Liste von Attributen bereitstellen, sodass der Validierungsstatus in **Validierung ausstehend** geändert wird. Der Standardwert ist **Leer**.

i Hinweis:

Bei Änderungen an den Bezeichnerfeldern, z. B. MAC-Adresse, Seriennummer, transformierter Name und Slotnummer (für OT-Steuerungsmodule), wird der Validierungsstatus in **Validierung ausstehend** geändert.

- Diese Eigenschaft gehört zum Bereich „sn_otsm_sgc“ und wird automatisch an diesen Eigenschaftsnamen angehängt.
- Erfordert die Rollen „admin“, „cmdb_ot_admin“ und „cmdb_inst_admin“ für Lese- und Schreibvorgänge.

sn_otsm_sgc.enable.cmdb.validations

- Diese Eigenschaft aktiviert CMDB -Validierungen für die Bereitstellungsgeräte. Bei Festlegung auf **True** werden Bereitstellungsgeräte für den Abgleich anhand vorhandener CMDB CIs validiert.
- Diese Eigenschaft gehört zum Bereich „sn_otsm_sgc“ und wird automatisch an diesen Eigenschaftsnamen angehängt.
- Erfordert die Rollen „admin“, „cmdb_ot_admin“ und „cmdb_inst_admin“ für Lese- und Schreibvorgänge.

Importieren Sie die Excel-Vorlage

Nachdem Sie die Importvorlage mit den neuen Daten aktualisiert haben, importieren Sie die Vorlage in Ihre Instanz, um zu validieren und fehlende, doppelte und ungültige Daten zu finden.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > OT-Manager > OT-Geräte importieren: Bereitstellungstabelle**.
2. Klicken Sie mit der rechten Maustaste auf den Spaltentitel, und wählen Sie **Importieren** aus dem Menü.

Insert new records or update existing records using an Excel template file. Click Upload to preview the data to be imported. [More Info](#)

< Import external data into SG OT Excel Staging

Do you want to insert or update data ? ☒ Insert ☐ Update

Do you want to create an Excel template to enter data ? ☒

Step 1: Create an Excel template file to enter data

Include all fields in the template? ☒

Create Excel template

Step 2: Upload the template file

Excel template file No file chosen

3. Wählen Sie **Einfügen** oder **Aktualisieren** als Importtyp aus.
4. Wählen Sie **Datei wählen aus**, und wählen Sie die Excel-Tabelle MicrosoftMicrosoft Azure Event Hubs aus.
5. Wählen Sie **„Hochladen“** aus, um die Excel-Tabelle MicrosoftMicrosoft Azure Event Hubs hochzuladen.
6. Wählen Sie auf der Seite „Upload-Fortschritt“ **Vorschau der importierten Daten** aus, um die importierten Daten zu überprüfen.
7. Wenn die Vorlage validiert wird und die importierte Vorschau Ihren Erwartungen entspricht, wählen Sie **Import abschließen**, um Daten in die Bereitstellungstabelle zu importieren.

Erstellen Sie ein OT-Gerät

Erstellen Sie ein OT-Gerät manuell in der Bereitstellungstabelle „OT-Geräte importieren“.

Vorbereitungen

Erforderliche Rolle: ot_staging_user, cmdb_ot_admin oder admin

Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > OT-Manager-Administrator > OT-Geräte importieren – Staging-Tabelle**.
2. Wählen Sie die Schaltfläche **Neu** aus.
3. Über **den Typ des Geräts?** Wählen Sie in der Liste den OT-Gerät-Typ aus.
Der von Ihnen ausgewählte Gerätetyp wird dem Formular automatisch hinzugefügt.

4. Füllen Sie im Formular „SG OT Excel-Bereitstellung – Neuer Datensatz“ die Felder nach Bedarf aus.

SG OT Excel-Bereitstellung – Formularfelder „Neuer Datensatz“.

Feld	Beschreibung
Anzeigename	Der Name des im Datensatz angezeigten OT-Geräts. i Hinweis: Sie können diesem Feld einen beliebigen Zeichenfolgenwert hinzufügen. Mehrere Geräte können denselben OT-Anzeigenamen haben. Dies dient dem leichteren Verständnis des OT-Geräts und unterscheidet sich von dem eindeutigen CI-Namen, der beim Importieren von OT-Geräten aus der Bereitstellungstabelle generiert wird.
Name	Eindeutiger generierter CI-Name.
Purdue-Ebene	Zugewiesene Purdue-Ebene. Die Ebenenbereiche sind 0–5. i Hinweis: Weitere Informationen zu den Purdue-Ebenen in Industrial Control Systems finden Sie unter https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lv1sec10/the-purdue-model-for-industrial-control-systems .
Gerät-Relevanz	Maß des relativen Risikos für den Standortprozess, wenn das Gerät ausfällt: ○ 1 – Sehr kritisch ○ 4 – Nicht kritisch
Korrelations-ID	Standort, zu dem das Gerät gehört.
Site	Die übergeordnete Entität der obersten Ebene oder der Industriestandort, an dem sich das Gerät befindet oder dem das Gerät zugewiesen ist.
Anlagenmodell-Entitätspfad	Pfad der Anlagenmodell-Entität, in dem sich das Gerät befindet.

5. **Wahlweise:** Fügen Sie in den folgenden zugehörigen Listen nach Bedarf zusätzliche Informationen hinzu.

- Zusätzliche Informationen
- Netzwerkadapter
- IP-Adresse
- Seriennummer
- BS-Information
- Steuerungssysteminformation

- Steuerungsmodulinformation
- Softwareinformationen
- Speichermodulinformation
- Informationen zum Sicherungsspeicher

6. Wählen Sie **OT-Gerät erstellen aus**.

Ergebnisse

Das OT-Gerät wird erstellt und der Bereitstellungstabelle hinzugefügt.

Validierungen verwalten

Durch die Validierung können Sie die importierten Daten in der Bereitstellungstabelle überprüfen und verwalten.

Auszuführende Validierungen:

- Fehlende Korrelations-ID (Korrelations-ID)
- Fehlende übergeordnete Korrelations-ID, wenn der Typ „Steuerungsmodul“ ist (übergeordnete ID des Steuerungsmoduls)
- Fehlende Seriennummer (Seriennummer)
- Fehlender transformierter Name (transformierter Name)
- Fehlende MAC-Adresse (Validierung wird für Spalte MAC-Adresse 1 ausgeführt)
- Fehlender Typ (Typ)
- Fehlende Racknummer (Racknummer)
- Fehlende Slotnummer (Slot-Nummer)
- Anlagenmodell-Entitätspfad ist nicht vorhanden (Anlagenmodell-Entitätspfad)
- Angegebener Name des Standorts ist ungültig (Name des Standorts).
- Duplikate für transformierten Namen validieren (transformierter Name)

i Hinweis:

Diese Validierung wird für Steuerungsmodule übersprungen.

- Duplikate für MAC-Adresse validieren (alle MAC-Adresse 1-Spalten überprüfen)
- Duplikate in Spalte „Seriennummer“ validieren (Seriennummer)
- Duplikate in Spalte „Korrelations-ID“ validieren (Korrelations-ID)
- Validiert Duplikate an Rack- und Steckplatznummern

i Hinweis:

Diese Validierung gilt nur für Steuerungsmodule.

- Validieren Sie „Hat Modul“ und „Übergeordnete ID des Steuerungsmoduls“.

i Hinweis:

Diese Validierung gilt nur für SPS und Steuerungsmodule.

- Ungültige Typen validieren: Vergleich mit der standardmäßigen Excel-Typ-zu-OT-Gerät-Typ-Zuordnung über die Implementierung des Erweiterungspunkts `sn_otsm_sgc.SGOTAssetImportExtensionPoint`.

Wenn Sie über zusätzliche Zuordnungen verfügen, erstellen Sie eine Erweiterungspunktimplementierung für den Erweiterungspunkt des Basissystems `sn_otsm_sgc.SGOTAssetImportExtensionPoint`.

Weitere Informationen zum Hinzufügen einer anwenderdefinierten Implementierung für die Geräteklassifizierung finden Sie unter [Fügen Sie eine anwenderdefinierte Implementierung für die Geräteklassifizierung hinzu](#).

Validierungen ausführen

Führen Sie Validierungen für Datensätze durch, um fehlende, doppelte und ungültige Daten zu finden.

Vorbereitungen

Erforderliche Rolle: `ot_staging_user`, `cmdb_ot_admin` oder `admin`

Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > OT-Manager > OT-Geräte importieren: Bereitstellungstabelle**.

2. Wählen Sie Validierungen ausführen aus, um Validierungen in der Bereitstellungstabelle auszulösen.

Validierungen werden für alle Datensätze im Hintergrund ausgeführt.

Die zum Validieren der Daten benötigte Zeit hängt von der Anzahl der in der Bereitstellungstabelle vorhandenen Datensätze ab.

3. Überprüfen Sie nach Abschluss der Validierung den Status des Datensatzes in der Spalte Validierungsstatus in der Bereitstellungstabelle.

4. Wenn der Status des Datensatzes teilweise gültig oder ungültig ist, gehen Sie wie folgt vor:

a. Überprüfen Sie den Datensatz auf fehlende Daten.

b. Nehmen Sie Korrekturen im Datensatz vor.

Der Datensatz kann in der Listenansicht der Bereitstellungstabelle und im Datensatz zur Ansicht bearbeitet werden.

c. Aktualisieren Sie den Datensatz.

d. Führen Sie die Validierungen aus.

5. Wenn die fehlenden Daten nicht verfügbar sind, gehen Sie wie folgt vor, um den Status für den jeweiligen Datensatz zu überschreiben und diesen Datensatz manuell als gültig festzulegen:

a. Wählen Sie den Datensatz aus, um das Formular zu öffnen.

b. Wählen Sie **Auf gültig festlegen**.

Hinweis:

Wenn ein Datensatz manuell als gültig festgelegt wird, kann dies zu Abgleichproblemen führen, und ein CI wird möglicherweise nicht erstellt.

Verwenden Sie OT-Bereitstellungsaufgaben, um ungültige Datensätze zu korrigieren

Korrigieren Sie ungültige Datensätze in der Tabelle „SG OT Excel-Bereitstellungen“ mithilfe von Bereitstellungsaufgaben für operative Technologie (OT). Die Verwendung von OT-Bereitstellungsaufgaben kann Ihnen dabei helfen, die ungültigen Datensätze nachzuverfolgen, die Sie korrigieren müssen.

Vorbereitungen

Erforderliche Rolle: cmdb_ot_admin, cmdb_ot_editor und ot_staging_user

Warum und wann dieser Vorgang ausgeführt wird

Sie können OT-Bereitstellungsaufgaben verwenden, um Ihre ungültigen Datensätze in der Tabelle „SG OT Excel-Bereitstellungen“ (sg_ot_excel_staging) zu korrigieren.

Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > OT-Manager-Administrator > OT-Geräte importieren – Staging-Tabelle**.
2. Wählen Sie im Header der Tabelle die Schaltfläche **Aufgaben erstellen**.
Die folgende Bestätigungsmeldung wird angezeigt.

ⓘ Staging task creation process for all the invalid records have started in the background. It may take few minutes to complete.
3. Warten Sie, bis der Stagingaufgaben-Erstellungsprozess abgeschlossen ist.
Nachdem die Erstellung der Stagingaufgabe abgeschlossen ist, wird die Spalte „OT-Stagingaufgabe“ in der Tabelle mit den OT-Stagingaufgaben gefüllt, die sich auf die ungültigen Stagingdatensätze beziehen.
4. Überprüfen und bearbeiten Sie den Stagingaufgaben-Datensatz.
 - a. Wählen Sie in der Spalte „OT-Stagingaufgabe“ einen Datensatz aus.
 - b. Füllen Sie im Formular „Staging-Aufgabendatensatz“ die Felder aus, falls zutreffend.

Datensatzformular für OT-Bereitstellungsaufgabe

Feld	Beschreibung
Status	Status der Bereitstellungsaufgabe. Der Status ändert sich und verfolgt die Bereitstellungsaufgaben durch mehrere Korrekturphasen.
Site	Standort, dem die Bereitstellungsaufgabe zugeordnet ist. Der Standard-Stagingaufgaben-Datensatz hat ein leeres Site-Feld. Alle ungültigen Bereitstellungsdatensätze mit leeren oder ungültigen Site-Feldern werden der Standard-Bereitstellungsaufgabe zugeordnet.  Hinweis: Wenn Sie das Feld Site in einem Bereitstellungsdatensatz ändern, wird der zugehörige Bereitstellungsaufgaben-Datensatz entfernt.
Beschreibung	Ausführliche Erklärung der Bereitstellungsaufgabe.
Geöffnet von	Benutzer, der den Stagingaufgaben-Datensatz erstellt hat.

Feld	Beschreibung
Zugewiesen an	Benutzer, der an der Bereitstellungsaufgabe arbeitet.
Zuweisungsgruppe	Zugewiesene Gruppe, die an der Bereitstellungsaufgabe arbeitet.

c. Wählen Sie **Aktualisieren**.

- 5. Wahlweise:** Zeigen Sie die Datensätze für OT-Bereitstellungsaufgaben an, die in der Tabelle SG OT Excel-Bereitstellungsaufgaben (sg_ot_excel_staging_task) erstellt wurden, indem Sie zu navigieren **Alle > Industrial Workspace-Administrator > OT-Manager-Administrator > OT-Geräte importieren – Staging-Aufgabentabelle**.

Ergebnisse

Der Stagingaufgaben-Datensatz wird jetzt erstellt und dem Benutzer zugewiesen, der für die Korrektur verantwortlich ist.

Planen Sie das Zeitintervall für den Import von Daten

Planen Sie das Zeitintervall, um die Daten aus der Bereitstellungstabelle in CMDB zu importieren.

Vorbereitungen

Erforderliche Rolle: admin oder cmdb_inst_admin

Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > OT-Manager > OT-Geräte importieren: Bereitstellungstabelle**.
2. Wählen Sie auf der Seite „SG OT Excel-Bereitstellung“ **Geplanter Import** aus.
3. Aktivieren Sie das Kontrollkästchen **Aktiv**, um das Zeitintervall für den Datenimport zu planen.
4. Wählen Sie **Jetzt ausführen aus**, um den Datensatz aus der Bereitstellungstabelle in CMDB zu importieren.

Der Status Validierung zeigt für erfolgreich importierte Daten den Status **Importiert** an.

In der Bereitstellungstabelle löscht die Tabellenbereinigung alle erfolgreich importierten Datensätze. Weitere Informationen zur Tabellenbereinigung finden Sie unter [Table cleaner](#).

Importieren Sie Ihre Excel-Tabelle Microsoft Azure Event Hubs mithilfe der Bereitstellungstabelle

Importieren Sie Ihre Excel-Tabelle Microsoft Azure Event Hubs mithilfe des einfachen Importierens in die Bereitstellungstabelle, um aus der Kalkulationstabelle die erforderlichen Daten in der Bereitstellungstabelle zu erstellen.

Vorbereitungen

Dieser Prozess erfordert das Plugin „IntegrationHub ETL“ (com. sn_int_studio).

Bevor Sie diesen Prozess ausführen, müssen Sie eine Excel-Tabelle Microsoft Azure Event Hubs ordnungsgemäß für den Import vorbereiten. Weitere Informationen finden Sie unter [Bereiten Sie Ihr Tool zur Überprüfung von OT-Arbeitsblatteinträgen vor dem Import für den Import von Service Graph Connector vor](#).

Wenn die Daten zum Import bereit sind, können Sie den Import in Configuration Management Database (CMDB) planen. Dieser Prozess erstellt eindeutige Datensätze in Configuration Management Database (CMDB) für die OT-Geräte, die in Ihrer Tabelle enthalten sind.

Erforderliche Rolle: cmdb_inst_admin, import_admin, import_scheduler, admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie den Prozess zum Extrahieren der Transformationslast (Extract Transform Load, ETL) in IntegrationHub ausführen, können Sie auch auf den eingebetteten Inhalt in Industriell Geführtes Setup verweisen, um zusätzliche Unterstützung zu erhalten.

Führen Sie die Validierungen in der Bereitstellungstabelle aus, um die Daten auf Duplikate und Inkonsistenzen zu prüfen.

Um auf Industriell Geführtes Setup zuzugreifen, navigieren Sie zu **Industrial Workspace-Administrator > Geführtes Setup**.

Prozedur

1. Navigieren zu **Alle > Konfiguration > IntegrationHub ETL**.
2. Wählen Sie die **CMDB-Anwendung: SG-OT Excel-Import ETL** aus.
3. Wählen Sie im Formular „Assistent für ETL-Transformationszuordnung“ **Quelldaten importieren und Grundlegende Details aus**.
4. Wählen Sie im Formular Grundlegende Informationen für die ETL-Transformationszuordnung angeben im Feld **Beispiel-Importsatz die Option Neuen Importsatz automatisch abrufen aus**.
5. Kehren Sie zum ETL-Formular IntegrationHub zurück.

Hinweis:

Die verbleibenden Schritte zum Erstellen einer -ETL-Transformationszuordnung werden automatisch abgeschlossen. Sie können jedoch einen bestimmten Schritt auswählen, um ihn zu überprüfen, bevor Sie den tatsächlichen Import durchführen. Wählen Sie beispielsweise **Daten vorbereiten und in der Vorschau anzeigen aus**, um die geschachtelte Datenstruktur und die Rohquelldaten anzuzeigen.

Hinweis:

Weitere Informationen finden Sie unter [ETL-Transformationszuordnung erstellen](#) .

6. Um den tatsächlichen Import einer Excel-Tabelle durchzuführen, wählen Sie **Integrationsergebnisse testen und zurücksetzen** aus.
7. Wählen Sie **Integration ausführen aus**.

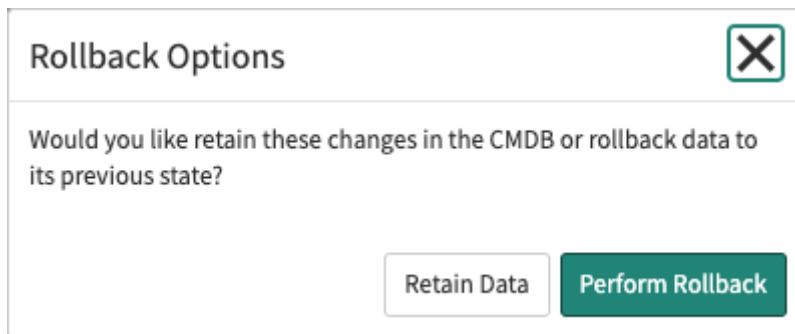
Hinweis:

Dieser Import testet 100 Datensätze. Um einen vollständigen Import von mehr als 100 Datensätzen auszuführen, müssen Sie den Import planen. Sie können den Import so planen, dass er nach einem regelmäßigen Zeitplan ausgeführt wird, indem Sie **Importzeitplan festlegen** auswählen.

Nach Abschluss des Datenimports wird das Formular „Integrationsergebnisse testen und zurücksetzen“ mit Importstatistiken angezeigt, einschließlich:

- Klassen zugeordnet
- Beziehungen zwischen Klassen
- Bei dieser Integrationsausführung erstellte neue Datensätze.
- Bei dieser Integrationsausführung aktualisierte Datensätze.

- Bei dieser Integrationsausführung erstellte Teildatensätze.
 - Bei dieser Integrationsausführung erstellte unvollständige Datensätze.
8. Verlassen Sie das Formular „Integrationsergebnisse testen und zurücksetzen“.
Das Dialogfeld „Rollback-Optionen“ wird angezeigt.



9. Wählen Sie **Daten beibehalten** aus, um die importierten Daten beizubehalten, oder wählen Sie **Rollback durchführen**, um die importierten Daten zurückzusetzen und den Microsoft Azure Event Hubs Excel-Import erneut zu versuchen.
10. So importieren Sie Ihre Tabellendaten offiziell in den Now Platform:
- Wählen Sie **Importzeitplan festlegen** aus.
 - Wählen Sie **Zeitplan festlegen** aus.
 - Wählen Sie in der Liste Geplante Datenimporte **SG-OT-Geräte Import mit Tabelle planen** aus.
 - Wählen Sie im Formular „Datenimport planen“ **die Option Jetzt ausführen** aus.

Nächste Maßnahme

Nachdem alle Schritte abgeschlossen sind, wählen Sie auf der Homepage des geführten Setups für SG-OT Geräteimport ETL **die Option Aktivieren** aus, um ETL zu aktivieren.

Fügen Sie in der Bereitstellungstabelle eine anwenderdefinierte Feldzuordnung für hinzu Service Graph

Fügen Sie der Bereitstellungstabelle ein anwenderdefiniertes Feld hinzu, und ordnen Sie das anwenderdefinierte Feld aus der Bereitstellungstabelle dem CI-Feld über Excel SGC zu.

Vorbereitungen

Informationen zum Konfigurieren des Formularlayouts finden Sie unter [Formularlayout konfigurieren](#) .

Informationen zum Erstellen eines anwenderdefinierten Felds in der Bereitstellungstabelle finden Sie unter [Feld in einer Tabelle hinzufügen und anpassen](#) .

Erforderliche Rollen:

- Administrator: Kann Änderungen in der Skripteinbindung vornehmen, Klassen- oder Feldzuordnungen hinzufügen und Änderungen in ETL vornehmen.
- cmdb_inst_admin: Kann nur neue Klassen- oder Feldzuordnungen hinzufügen und Änderungen in ETL vornehmen.

Prozedur

1. Nachdem in der Bereitstellungstabelle eine anwenderdefinierte Spalte erstellt wurde, navigieren Sie zu **Alle > Industrial Workspace-Administrator > OT-Manager > OT-Geräte importieren: Bereitstellungstabelle**.
2. Laden Sie die Excel-Vorlage herunter.
Weitere Informationen finden Sie unter [Excel-Vorlage herunterladen](#).

Wenn in der Bereitstellungstabelle Datensätze vorhanden sind, können Sie den Wert für die Spalte in den vorhandenen Datensätzen bearbeiten.
3. Bereiten Sie die Excel-Vorlage vor.
Weitere Informationen finden Sie unter [Tool zur Überprüfung von OT-Arbeitsblatteinträgen vor dem Import für den Import von Service Graph Connector vorbereiten](#).
4. Importieren Sie die Excel-Vorlage.
Weitere Informationen finden Sie unter [Excel-Vorlage importieren](#).
5. Navigieren zu **Alle > Industrial Workspace-Administrator > OT-Manager > OT-Geräte importieren – Skripteinbindungen** und wählen Sie die Skripteinbindung `SGOTAssetImportExcelConstants` aus.
6. Aktualisieren Sie im Skript den neuen Spaltennamen aus der Bereitstellungstabelle und den neuen ETL-Spaltennamen im Objekt `SGOTAssetImportExcelConstants.importSetColumnsVsStagingColumnsMap` im Format „<ETL Column Name> ”: “<Column Name from staging table> “.

In diesem Beispiel gibt „u_my_custom_field“ vor dem Doppelpunkt (:) den Namen der ETL-Spalte an (im ETL-Vorschau als Spalte angezeigt), und „u_my_custom_field“ hinter dem Doppelpunkt gibt den Namen der Spalte in der Bereitstellungstabelle an.

Stellen Sie sicher, dass am Ende der Zeile über der neuen Zeile ein Komma (,) hinzugefügt wird. In diesem Beispiel wird nach der Zeile „custom_fields“: „custom_fields“ ein Komma eingefügt.

```

SGOTAssetImportExcelConstants.importSetColumnsVsStagingColumnsMap = {
    // unique id used to uniquely identify the asset
    "id": "correlation_id",
    // Name of the asset
    "name": "transformed_name",
    // OperatingSystem of the asset
    //"operating_system": "os_version",
    // type of the asset.
    "type": "type",
    // if the asset has control module
    "has_module": "has_module",
    // id of the asset to which a control module belongs to (this is used in control module type asset).
    "control_module_parent_correlation_id": "control_module_parent_correlation_id",
    "ot_display_name": "display_name",
    "serial_number": "serial_number",
    "firmware_version": "firmware_version",
    "os_version": "os_version",
    "operating_system": "os",
    "assigned_to": "assigned_to",
    "manufacturer": "manufacturer",
    "model_number": "model_number",
    "serial_number_type": "serial_number_type",
    "purdue_level": "purdue_level",
    "asset_criticality": "asset_criticality",
    "short_description": "short_description",
    "vendor": "vendor",
    "equipment_model_entity_path": "equipment_model_entity_path",
    "first_discovered": "first_discovered",
    "hardware_version": "hardware_version",
    "status": "status",
    "backplane_name": "backplane_name",
    "backplane_id": "backplane_id",
    "slot_number": "slot_number",
    "rack_number": "rack_number",
    "module_type": "module_type",
    "device_type": "io_field_device_type",
    "support_group": "support_group",
    "site": "site",
    "ip_address": {
        "ip": "ip_address_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER
    },
    "mac_address": {
        "mac": "mac_address_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER
    },
    "memory": {
        "memory_card_serial": "memory_card_serial_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER,
        "memory_size": "memory_size_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER,
        "memory_type": "memory_type_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER
    },
    "software_installed": {
        "name": "software_installed_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER,
        "version": "software_version_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER,
        "install_date": "software_install_date_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER
    },
    // Do not change this. Key should match value of SGOTAssetImportExcelConstants.CUSTOM_FIELDS_COL_NAME_IN_IMPORT_SET
    "custom_fields": {
        "customfield": "customfield_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER
    }
}

```

7. Wählen Sie **Aktualisieren** aus, um Ihre Änderungen zu speichern.
8. Navigieren zu **Alle > Konfiguration > IntegrationHub ETL**.
9. Wählen Sie die **CMDB-Anwendung: SG-OT Excel-Import ETL** aus.
10. Wenn die Seite „Ungültige Zuordnungsdaten erkannt“ angezeigt wird, wählen Sie **Schließen** aus.
11. Wählen Sie im Assistenten für ETL-Transformationszuordnungen im Abschnitt Grundlegende Details angeben des geführten Setups **Quelldaten importieren und Grundlegende Details angeben aus**.

12. Wählen Sie im Feld **Beispiel-Importsatz** **Neuen Importsatz automatisch abrufen aus**.

13. Wählen Sie **Speichern**.

Das Banner „Grundlegende Informationen erfolgreich gespeichert“ wird angezeigt.

14. Wählen Sie **Als vollständig markieren** aus.

15. Wählen Sie auf der Seite „Assistent für ETL-Transformationszuordnung“ im Abschnitt Quelldaten für Zuordnung vorbereiten die Option **Vorschau anzeigen und Daten vorbereiten aus**.

Wenn die Spalte nicht sichtbar ist, wiederholen Sie die Schritte 11 bis 14.

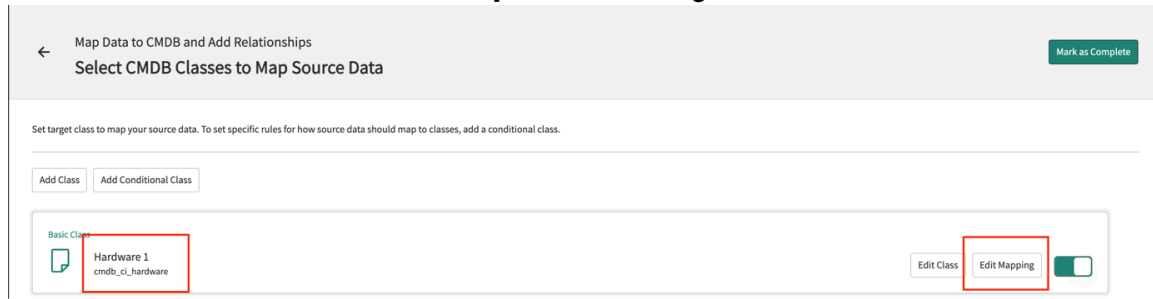
16. Wählen Sie **Als vollständig markieren** aus.

17. Wählen Sie auf der Seite „Assistent für ETL-Transformationszuordnung“ im Abschnitt „Daten zu CMDB zuordnen und Beziehungen hinzufügen“ die Option **CMDB-Klassen zur Zuordnung von Quelldaten** aus.

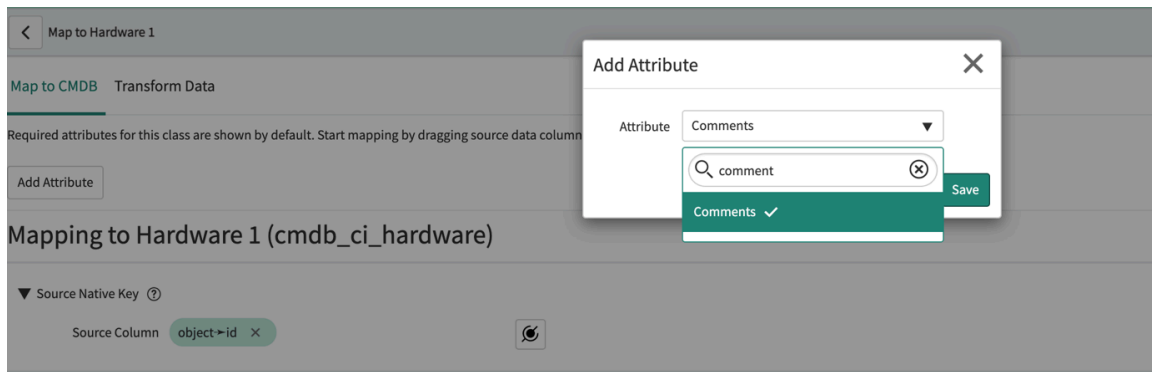
18. Ordnen Sie die Spalte der Zielklasse und dem Zielattribut zu.

Beispielsweise ist das Feld „Kommentare“ in der Klasse „Hardware“ *cmdb_ci_hardware* vorhanden. Nach der Zuordnung dieses Feldes wird auch das Feld „Kommentar“ in den untergeordneten Hardwareklassen aktualisiert, sofern der Wert für die Spalte „Kommentare“ in der Bereitstellungstabelle für diese Zeile nicht leer ist. Wenn Sie eine Zuordnung für ein neues Feld hinzufügen, das nicht vorhanden ist, oder für ein Feld, das nicht spezifisch für die Klasse „Hardware *cmdb_ci_hardware*“ ist, aber stattdessen ein Feld in der Klasse „Operative Technologie“ (*cmdb_ci_ot*) ist, fügen Sie die Feldzuordnung hinzu in der Stichprobe „Operative Technologien (OT) 1“.

- a. Fügen Sie der Klasse „Hardware 1“ eine Feldzuordnung hinzu.
- b. Wählen Sie für die Klasse Hardware 1 **die Option Zuordnung bearbeiten** aus.



19. Wählen Sie im angezeigten Dialogfeld „Attribut hinzufügen“ in der Liste „**Attribut**“ die Option **Kommentare** aus.



20. Wählen Sie **Speichern**.

Ein neues Feld mit dem Namen „Kommentare“ wird angezeigt. Möglicherweise müssen Sie einen Bildlauf durchführen, um das Feld anzuzeigen.

Map to Hardware 1
Last Saved: 2021-10-28 13:29:49

Map to CMDB Transform Data

Required attributes for this class are shown by default. Start mapping by dragging source data columns or transformed data columns to their CMDB class attributes

Add Attribute

Mapping to Hardware 1 (cmdb_ci_hardware)

Source Column	object → model_number_id_cleansed	
▼ Support group		
Source Column	object → support_group_sys_id	
▼ Manufacturer		
Source Column	object → manufacturer_sys_id_cleansed	
▼ First discovered		
Source Column	object → first_discovered_date_time_format	
▼ Class		
Source Column	object → asset_cmdb_class_sys_name	
▼ Comments		
Source Column		

21. Ziehen Sie die Datenpille aus dem Datenbereich in das Feld **Kommentarquellenspalte**.

now All Favorites History Workspaces IntegrationHub ETL

Map to Hardware 1
Last Saved: 2022-07-07 12:16:54

Successfully saved this mapping.

Map to CMDB Transform Data

Required attributes for this class are shown by default. Start mapping by dragging source data columns or transformed data columns to their CMDB class attributes

Add Attribute

Mapping to Hardware 1 (cmdb_ci_hardware)

From collection: object

Source Column	object → model_number_id_cleansed	
▼ Support group		
Source Column	object → support_group_sys_id	
▼ Manufacturer		
Source Column	object → manufacturer_sys_id_cleansed	
▼ First discovered		
Source Column	object → first_discovered_date_time_format	
▼ Class		
Source Column	object → asset_cmdb_class_sys_name	
▼ Comments		
Source Column	object → u_my_custom_field	

Data

serial_number_cleansed	SN0001
serial_number_snk	SN0001:066b81...
serial_number_type	system
serial_number_type_cleansed	system
serial_number_valid	true
sys_import_date_time_format	2022-07-07 06:4...
short_description	PLC with all the va...
site	Hyd Site
site_sys_id_computed	
slot_number	
status	installed
status_value	1
support_group	
support_group_sys_id	
type	plc
u_my_custom_field	My Custom value
vendor	Vendor E

Sie können auch das Quellspaltenymbol () auswählen, um das Datenzuordnungsfeld dafür auszuwählen. Die Quellspalte enthält die Datenpille.

Automatische Übersetzung

Map to Hardware 1
Last Saved: 2022-07-07 12:16:54

Map to CMDB Transform Data

Required attributes for this class are shown by default. Start mapping by dragging source data columns or transformed data columns to their CMDB class attributes

Add Attribute

Mapping to Hardware 1 (cmdb_ci_hardware)

From collection: object

Source Column	object.model_number_id_cleansed	
Support group	Source Column	object.support_group_sys_id
Manufacturer	Source Column	object.manufacturer_sys_id_cleansed
First discovered	Source Column	object.first_discovered_date_time_format
Class	Source Column	object.asset_cmdb_class_sys_name
Comments	Source Column	object.u.my_custom_field

22. Navigieren Sie zurück zu **CMDB-Klassen für die Zuordnung von Quelldaten** im Abschnitt „Daten zu CMDB zuordnen und Beziehungen hinzufügen“ auf der Seite „Assistent für ETL-Transformationszuordnung“.

Map to Hardware 1
Last Saved: 2021-10-28 13:40:03

Map to CMDB Transform Data

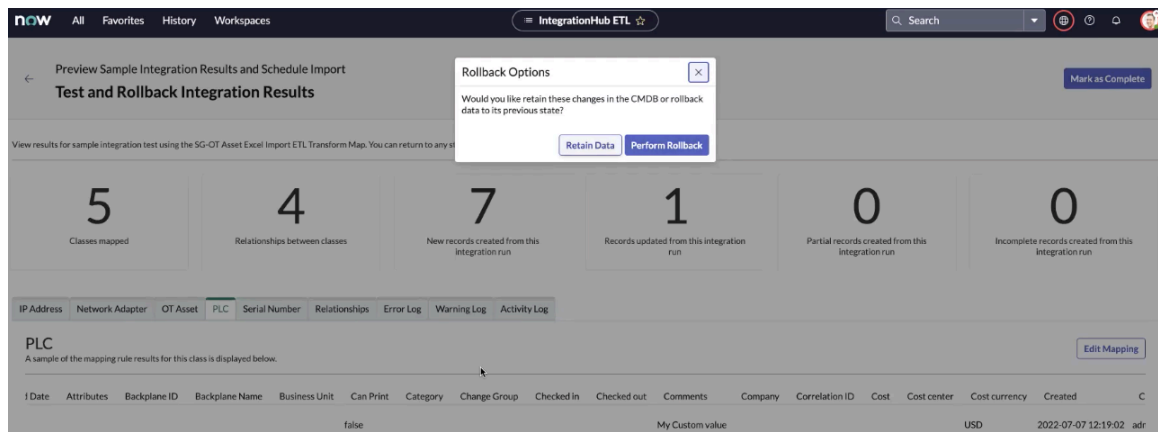
Required attributes for this class are shown by default. Start mapping by dragging source data columns or transformed data columns to their CMDB class attributes

Add Attribute

Mapping to Hardware 1 (cmdb_ci_hardware)

Source Native Key	Source Column	object.id
Source Recency Timestamp	Source Column	
Name	Source Column	object.name

23. Wählen Sie **Als vollständig markieren** aus.
24. Führen Sie diese Schritte aus, um die neuen Feldzuordnungen zu überprüfen.
- Navigieren Sie zur Startseite des Assistenten für ETL-Transformationszuordnungen.
 - Wählen Sie im Abschnitt Vorschau der Beispielintegrationsergebnisse anzeigen und Import planen des geführten Setups **die Option Integrationsergebnisse testen und zurücksetzen aus**.



g. Wenn ETL nicht aktiviert ist, wählen Sie **Aktivieren** aus.

Die neue Spaltenfeldzuordnung wurde erfolgreich hinzugefügt und verifiziert.

Fügen Sie eine anwenderdefinierte Implementierung für die Geräteklassifizierung hinzu

Passen Sie die Klassifizierung des Basissystems eines Geräts basierend auf Typ, os_version und Firmware_version an.

Vorbereitungen

Das Basissystem für den Erweiterungspunkt

`sn_otsm_sgc.SGOTAssetImportExtensionPoint` verwendet

das standardmäßige Implementierungsskript, das mit dem Namen

`sn_otsm_sgc.SGOTAssetImportUtil` ausgeliefert wird. Um eine anwenderdefinierte

Klassifizierung hinzuzufügen, erstellen Sie eine Implementierung für den Erweiterungspunkt im Bereich **Service Graph Connector für Operational Technology (Excel)**.

i Hinweis:

Der Benutzer darf nur eine Implementierung des Erweiterungspunkts haben. Wenn Sie anstelle des Standarderweiterungspunkts einen anwenderdefinierten Erweiterungspunkt implementieren und aktivieren, müssen Sie die Standardimplementierung deaktivieren.

Erforderliche Rolle: `cmdb_inst_admin`, `import_admin`, `import_scheduler`, `admin`

Prozedur

1. Navigieren zu **Alle > Systemerweiterungspunkt > Erweiterungspunkte mit Skript**.
2. Wählen Sie `sn_otsm_sgc.SGOTAssetImportExtensionPoint`.
3. Wählen Sie den zugehörigen Link **Implementierung erstellen aus**.
4. Geben Sie einen Namen für die Erweiterungspunkt-Implementierung ein.
5. Überprüfen Sie im Skriptfeld, ob das Klassenobjekt mit den folgenden beiden Funktionen ausgefüllt ist.
Stellen Sie sicher, dass das von zurückgegebene Ergebnis **`getAssetCMDBSysClassNameWithOtEntityTypeSysId`** Erweiterungspunkt folgt dem in den Kommentaren genannten Format. Jede Änderung des Formats der Ergebniszeichenfolge führt zu Importfehlern oder Unregelmäßigkeiten. Das Format muss sein `<cmdb class name> :::<ot entity type sys id>`.

Option	Bezeichnung
<code>getAssetCMDBSysClassNameWithOtEntityTypeSysId</code> <code>(/*string*/ type, /*string*/ osVersion, /*string*/ Firmware-Version)</code>	Implementieren Sie diese Methode, um den Sys-Klassennamen CMDB, zu dem das Gerät gehört, zusammen mit

Option	Bezeichnung
	der sys_id des OT-Entitätstyps zurückzugeben, die mit „:::“ verkettet ist. Für nicht klassifizierte Geräte wird der OT-Gerät-Typ auf ot_base festgelegt.
getComputerType(/*string*/ OperatingSystem)	Gibt den Sys-Klassennamen CMDB basierend auf dem übergebenen Betriebssystem zurück.

6. Nachdem Sie alle gewünschten Änderungen vorgenommen haben, wählen Sie **Aktualisieren** aus.
Die Implementierung für den Erweiterungspunkt wird erstellt.

Nächste Maßnahme

Öffnen Sie auf der Registerkarte „Implementierungen“ der zugehörigen Listen die Implementierung des Basissystem-Erweiterungspunkts, um sie zu deaktivieren.

Fügen Sie eine anwenderdefinierte Validierung für Geräte hinzu

Passen Sie die Validierung für Ihre OT-Geräte an.

Vorbereitungen

Das Basissystem für den Erweiterungspunkt

sn_otsm_sgc.SGOTAssetCustomValidationExtensionPoint verwendet das Standardimplementierungsskript **sn_otsm_sgc.SGOTExcelStagingAssetValidationProcessor**. Sie können eine anwenderdefinierte Validierung hinzufügen, indem Sie eine Implementierung für den Erweiterungspunkt im Bereich Service Graph Connector für Operational Technology (Excel) erstellen.

Erforderliche Rolle: cmdb_inst_admin, admin

Prozedur

1. Navigieren zu **Alle > Systemerweiterungspunkt > Skriptbasierte Erweiterungspunkte**.
2. Wählen Sie **sn_otsm_sgc.SGOTAssetCustomValidationExtensionPoint** aus.
3. Wählen Sie den zugehörigen Link **Implementierung erstellen aus**.
Eine Skripteinbindung wird erstellt, in der Sie Ihre anwenderdefinierte Validierung hinzufügen können.
4. Informationen zum Hinzufügen einer anwenderdefinierten Validierung finden Sie im folgenden

	A	B	C	D	E	F	G	H	I	J
	Custom Validation									
1	Default Validation	Invalid	Valid	Partially Valid	Invalid	Valid	Partially Valid		Implementation has different Name	Invalid state (Type)
2	Partially Valid	(Override - False)	(Override - False)	(Override - False)	(Override - True)	(Override - True)	(Override - True)	No Implementation created	(Override - True)	(Override - True)
3	(sn_otsm_sgc.enable.cmdb.validations - True)	Partially valid	Partially valid	Partially Valid	Invalid	Valid	Partially Valid	Partially Valid	Same as Custom validation state	Same as Default state
4	Invalid	Valid	Valid	Valid	Invalid	Valid	Partially valid	Valid	Same as Custom validation state	Same as Default state
5	(sn_otsm_sgc.enable.cmdb.validations - True)	invalid	invalid	invalid	invalid	Invalid	invalid	Invalid	Invalid	Same as Default state
6	Partially Valid	Partially valid	Partially valid	Partially Valid	Invalid	Valid	Partially Valid	Partially Valid	Same as Custom validation state	Same as Default state
7	(sn_otsm_sgc.enable.cmdb.validations - False)	Valid	Valid	Valid	Invalid	Valid	Partially valid	Valid	Same as Custom validation state	Same as Default state
8	Invalid	invalid	invalid	invalid	invalid	Invalid	invalid	Invalid	Invalid	Same as Default state
9	(sn_otsm_sgc.enable.cmdb.validations - False)	invalid	invalid	invalid	invalid	Invalid	invalid	Invalid	Invalid	Same as Default state

Validierungsszenario.

5. Wählen Sie **Aktualisieren**.

Testen Sie den Excel-Connector Service Graph

Die Problembehandlungsaktionen können helfen, häufige Probleme beim Importieren Ihrer Operational Technology -Geräte oder -Daten zu beheben. Greifen Sie auf das Systemprotokoll zu, um diese Fehler zu beheben.

Diese Protokolle können verwendet werden, um Probleme zu debuggen oder um festzustellen, ob die SGC-Schritte ordnungsgemäß ausgeführt wurden.

Problem	Lösung
Wenn beim Laden von Daten für das geführte ETL-Setup für SG-OT-Geräte-Excel-Import ein Problem auftritt	Versuchen Sie, die Daten in der Liste „Zugehörige Links“ zu laden. 1. Navigieren Sie zur Datenquelle SG-OT Excel-Import, und wählen Sie Testladen von 20 Datensätzen oder Alle Datensätze laden aus. 2. Kehren Sie zu ETL zurück, und versuchen Sie erneut, die Daten zu laden.
Wenn nach dem Ausführen des Tests des Connectors Service Graph im geführten ETL-Setup Einträge auf der Registerkarte „Teilnutzlast“ vorhanden sind	Aufgrund der folgenden Bedingungen: • Fehlende Werte für die Pflichtfelder eines Geräts. • Steuerungsmodule ohne zugeordnetes übergeordnetes Gerät: Stellen Sie sicher, dass der Typ des Felds „Übergeordnete ID des Geräts und des Steuerungsmoduls“ in der Bereitstellungstabelle ordnungsgemäß ausgefüllt ist.
Wenn nach dem Testlauf des Connectors Service Graph im geführten ETL-Setup Einträge auf der Registerkarte „Unvollständige Nutzlast“ vorhanden sind	Aufgrund der fehlenden Werte für Felder, die eindeutig zur Identifizierung eines Geräts verwendet werden.
Nachdem der einfache Import ausgeführt wurde, können Benutzer Datensätze anzeigen, die aus der aktuellen Ausführung importiert wurden. Wenn Validierungen ausgeführt werden, werden sie für alle Datensätze der Bereitstellungstabelle ausgeführt, nicht nur für Datensätze aus dem aktuellen Import.	Vor dem Ausführen der Validierungen muss der Anwender im Breadcrumb der Listenansicht der Bereitstellungstabelle auf ALLE klicken.
Wenn die Zeitstempelspalte in der Bereitstellungstabelle leer erscheint	Der Anwender muss das UTC-Format (JJJJ-MM-TT hh:mm:ss) verwenden, um Datum und Uhrzeit einzugeben.
Wenn die Validierungsstatusaktualisierung für Datensätze nach dem Klicken auf die Schaltfläche „Validierungen ausführen“ nicht sichtbar ist.	Der Anwender muss die Seite manuell aktualisieren.
Wenn der Benutzer die vorhandenen Daten der Datensätze in der Bereitstellungstabelle ändert, wird der Validierungsstatus nicht auf Validierung ausstehend festgelegt.	Der Validierungsstatus wird auf Validierung ausstehend festgelegt, wenn die folgenden Attribute geändert werden: • Bezeichnerfelder (MAC-Adresse (1–9)) • Seriennummer • Name • Korrelations-ID

Problem	Lösung
	• Typ • Übergeordnete Korrelations-ID des Steuerungsmoduls • Felder, die bei der Berechnung des transformierten Namens verwendet werden • Rack-Nummer • Steckplatznummer Weitere Informationen zu den Systemeigenschaften finden Sie unter Systemeigenschaften, die sich auf die Verarbeitung des Excel-Imports für SG-OT-Geräte auswirken.
Nachdem Datensätze in die Bereitstellungstabelle importiert wurden, werden die Aktualisierungen, die in den Systemeigenschaften im Zusammenhang mit der Berechnung des transformierten Namens vorgenommen werden, nicht in den Datensätzen der Bereitstellungstabelle widerspiegelt.	Ändern Sie die Systemeigenschaften, bevor Sie die Daten in die Bereitstellungstabelle importieren.
Wenn mehrere Fehlerbanner angezeigt werden, wenn Anwender einige Datensätze auswählen und auf Validierung ausführen klicken.	Die Validierungen werden für alle in der Bereitstellungstabelle verfügbaren Datensätze ausgeführt. Wählen Sie nicht den einzelnen Datensatz zur Validierung aus.
Wenn die doppelten Datensätze in CMDB vorhanden sind, wird sie von der Bereitstellungstabelle nicht als Duplikat erkannt.	Die Validierungen werden nur für die in der Bereitstellungstabelle verfügbaren Daten ausgeführt. Die Validierungen werden nicht für die verfügbaren Daten in CMDB ausgeführt.
Der Site-Name wird in der Tabellenkalkulation oder Bereitstellungstabelle bereitgestellt, aber nach dem Import der Tabellenkalkulation nicht in den OT-Geräten angezeigt.	Es werden nur die vorhandenen Site-Datensätze in der CMDB berücksichtigt. Der „entity_name“ für den Standort (Entität des Anlagenmodells nach ISA) muss mit dem Wert übereinstimmen, der in der Standortspalte in der Excel- oder Bereitstellungstabelle angegeben ist. Wenn „entity_name“ für den Standort nicht übereinstimmt, wird der Wert auf leer gesetzt.
Wenn Benutzer in der Datenquelle auf Alle Datensätze laden klicken, werden keine Datensätze in den Importsatz importiert.	In der Bereitstellungstabelle sind keine Datensätze verfügbar.

Problem	Lösung
	Die Datensätze sind in der Bereitstellungstabelle vorhanden, haben jedoch nicht den Status „Gültig“ oder „Teilweise gültig“. Greifen Sie auf alle Protokolle im Zusammenhang mit Excel SGC in zu Alle > Systemprotokolle > Systemprotokoll > Alle. Suchen Sie in der Spalte Nachricht nach der Zeichenfolge SGOTExcel.

Zeigen Sie Skripteinbindungen an, die vom Connector Service Graph verwendet werden

Zeigen Sie als Administrator die Skripteinbindungen im Zusammenhang mit dem Service Graph -Connector an.

Vorbereitungen

Zeigen Sie eine gefilterte Liste aller Skripts an, die vom Connector Service Graph verwendet werden.

Erforderliche Rolle: cmdb_ot_admin, cmdb_inst_admin oder admin

Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > OT-Manager > OT-Geräte importieren – Skripteinbindungen**.

Diese Liste zeigt die Datensätze, deren Namen mit SGOTAsset oder SGOTExcelStaging beginnen.

2. Zeigen Sie die Liste der Skripts an.

Greifen Sie auf die vom Service Graph Connector verwendeten Systemeigenschaften zu

Als Administrator können Sie Systemeigenschaften im Zusammenhang mit dem Service Graph Connector anzeigen.

Vorbereitungen

Zeigen Sie eine gefilterte Liste aller Skripts an, die vom Connector Service Graph verwendet werden.

Erforderliche Rolle: admin, cmdb_inst_admin oder cmdb_ot_admin

Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > OT-Manager-Administrator > OT-Geräte importieren – Systemeigenschaften**.

In der Liste werden Datensätze angezeigt, deren Namen mit **sn_otsm_sgc.excel** beginnen.

2. Zeigen Sie die Liste der Skripts an.

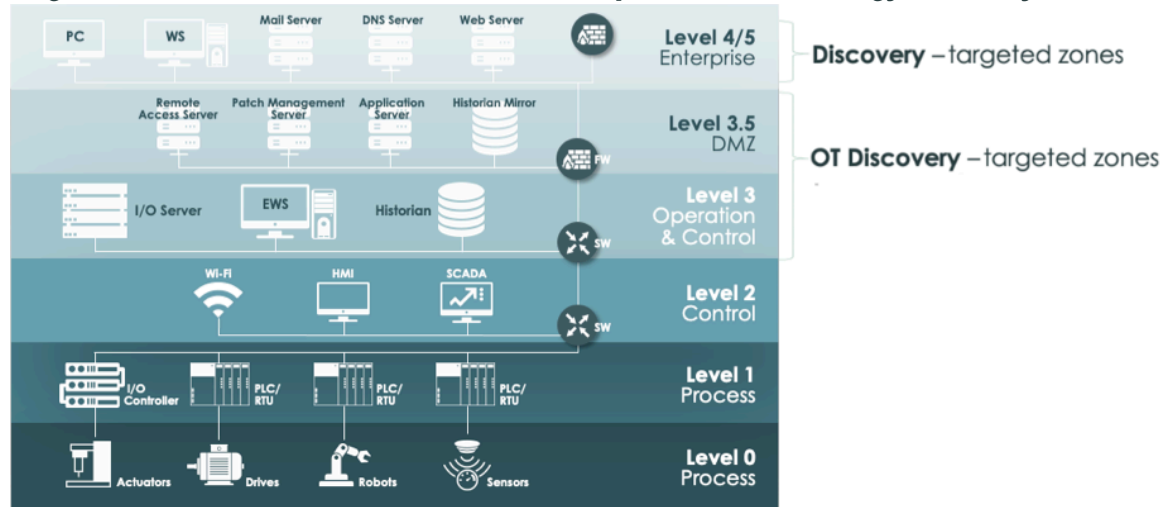
Discovery für Operational Technology

Sie können die Funktion Discovery für Operational Technology ausführen, um Geräte der IT-Klasse Operational Technology (OT) in festgelegten Purdue-Ebenen in Ihren ICS-Netzwerken (Industrial Control System) zu erkennen. Zu den IT-Klassenelementen gehören Switches, Router und Computer, die sowohl in Rechenzentren als auch in Ihren Werken vorhanden sind.

Ort, an dem die Standardverarbeitung Discovery stattfindet

Der Prozess Discovery für Operational Technology funktioniert ähnlich wie die standardmäßigen Discovery-Prozesse.

Angestrebte Purdue-Ebenen in Standard und Operational Technology Discovery



Die Standardverarbeitung von Discovery in Now Platform[®] erfolgt normalerweise auf den folgenden Purdue-Ebenen in Ihrem Unternehmen:

Verarbeitete Purdue-Ebenen

Purdue-Ebene	Beschreibung
4	Standortgeschäft und Logistik, z. B. alle Funktionen der Informationstechnologie (IT).
5	Unternehmensnetzwerk, in dem ERP-Funktionen (Enterprise Resource Planning) ausgeführt werden.

i Hinweis:

Weitere Informationen zu Purdue-Ebenen in Industrial Control Systems finden Sie unter https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lv1sec10/the-purdue-model-for-industrial-control-systems.

Wo und wie die Verarbeitung Discovery von für Operational Technology stattfindet

Im Gegensatz dazu kann die Verarbeitung Discovery von für Operational Technology in den folgenden Purdue-Ebenen erfolgen, je nachdem, was Sie beim Erstellen eines OT-Discovery-Zeitplans auswählen:

Verarbeitete Purdue-Ebenen

Purdue-Ebene	Beschreibung
3,5	Dewehrte Zone (DMZ) oder Dewehrte Industriezone (IDMZ) Ähnlich wie eine herkömmliche (IT) DMZ können Sie mit der OT-orientierten IDMZ Netzwerke mit unterschiedlichen Sicherheitsanforderungen sicher verbinden.

Verarbeitete Purdue-Ebenen (Fortsetzung)

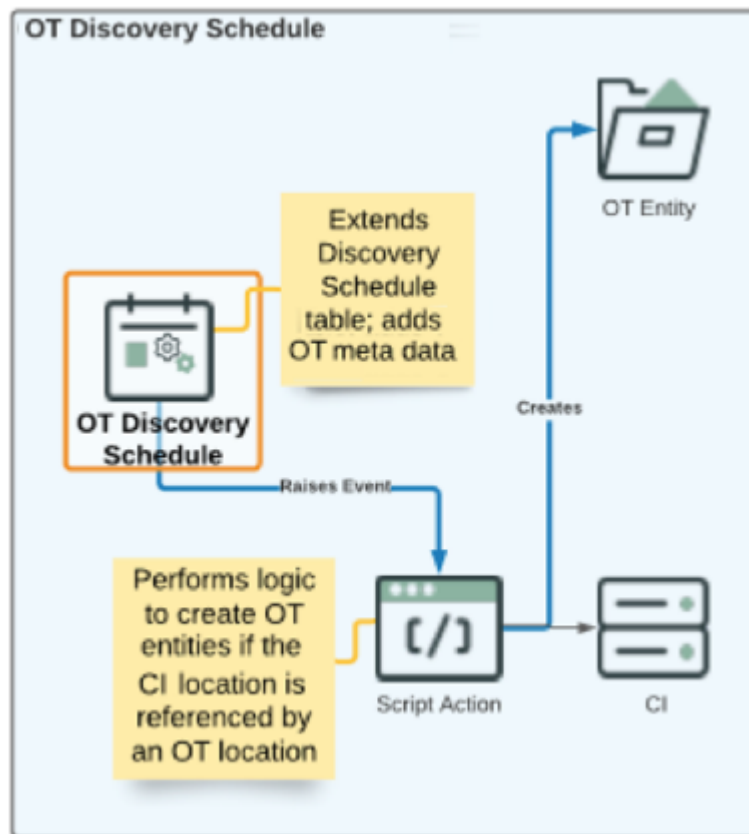
Purdue-Ebene	Beschreibung
3	Standortvorgänge, bei denen sich werks- oder standortweite Steuerungs- und Überwachungsfunktionen befinden.

Normalerweise führen Sie Discovery für Operational Technology in der DMZ (oder IDMZ, Purdue-Ebene 3.5) Ihrer ICS-Netzwerke aus. Auf dieser Purdue-Ebene sind normalerweise Computer und Server der IT- und OT-Klasse zu erkennen und zu verwalten.

i Hinweis:

Um zu vermeiden, dass Ihre Industrieabläufe unterbrochen werden, sollten Sie in Ihren ICS-Netzwerken keine Discovery -Prozesse für die Purdue-Ebenen 0 bis 2 ausführen.

Discovery für die Verarbeitung Operational Technology von [].



Wenn Sie einen OT-Erkennungszeitplan ausführen, wird die folgende Verarbeitung durchgeführt:

1. Durchläuft die zugewiesenen IP-Adressen und erkennt alle darin vorhandenen Hardwareelemente.
2. Wenn die Erkennung eines Konfigurationselements (Configuration Item, CI) abgeschlossen wird, wird intern ein Ereignis (`discovery.device.complete`) ausgelöst. Diese Logik überprüft, ob ein OT-Entitätsdatensatz (`cmdb_ot_entity`) dafür in Configuration Management Database (CMDB) vorhanden ist.
 - Wenn eines vorhanden ist und zugehörige Attribute für das erkannte Element geändert wurden, werden die OT-Entitäten aktualisiert, die sich auf dieses CI beziehen.
 - Wenn keiner vorhanden ist, wird einer dafür erstellt.

3. Zusätzlich zum Standortattribut werden auch die definierten Attribute aus dem OT-Erkennungszeitplan an das CI und an die zugehörigen OT-Entitätsdatensätze übertragen.
4. Außerdem werden OT-Entitätsdatensätze für die Anwendungen erstellt, die auf erkannten OT-Geräten installiert sind. Um die Anwendungen anzuzeigen, für die OT-Entitätsdatensätze über OT Discovery erstellt wurden, navigieren Sie zur Listenansicht Industrial Workspace, und öffnen Sie die Liste **der Anwendungen** unter **Operational Technology (OT)**.

Zugehörige Informationen

[Erweiterungsklassen für Operation Technology \(OT\)](#). 

[MID-Server](#) 

[Discovery](#) 

[Prozess-Flow der horizontalen Erkennung mit Probes und Sensoren](#) 

[Horizontale Erkennung planen](#) 

Zugehörige Links und ListenDiscovery für Operational Technology .

Discovery für Operational Technology enthält mehrere zugehörige Links und Listen.

Zugehörige Links

Verwandter Link	Beschreibung
Kurzbereiche	IP-Adressen und Adressbereiche, die gescannt werden sollen, wenn der OT-Erkennungszeitplan ausgeführt wird. Geben Sie IP-Adressen in mehreren Formaten (Netzwerk, Bereich oder Liste) in einer einzigen, durch Kommas getrennten Zeichenfolge ein. Der verwendete MID-Server muss eine Verbindung zu den angegebenen IP-Bereichen herstellen können. Weitere Informationen hierzu finden Sie unter Schnellen IP-Bereich für Discovery-Zeitplan erstellen  .
Discovery jetzt	Discovery für Operational Technology -Prozess sofort ausführen.
Punkt-Scan ausführen	Zugriff auf das Dialogfeld „Punktscan ausführen“. Weitere Informationen finden Sie unter Punktscan ausführen  .

Zugehörige Listen

Zugehörige Liste	Beschreibung
Discovery IP-Bereiche	Discovery Zu scannende und zu erkennende IP-Adressen und Adressbereiche. Wenn Sie einen einfachen CI-Scan (keine Verhaltensweisen) verwenden, verwenden Sie diese zugehörige Liste, um diese IP-Adressen zu definieren. Der verwendete MID-Server muss eine Verbindung zu den angegebenen IP-Bereichen herstellen können.  Hinweis: Um die Sicherheit zu verbessern, beschränken Sie den Bereich der Erkennungsziele, indem Sie unnötige Netzwerke und Geräte ausschließen.

Zugehörige Listen (Fortsetzung)

Zugehörige Liste	Beschreibung
Discovery Range Sets	Definition jedes Bereichssatzes, den der OT-Erkennungszeitplan mit einem oder mehreren Shazzam-Proben scannt.
Discovery Status	Verlauf der Ergebnisse der aktuellen und vergangenen Ausführungen des OT-Erkennungszeitplans.

Zugehörige Informationen

[MID-Server](#)

[Shazzam-Probe, Port-Probes und Protokolle](#)

[Erstellen Sie ein Shazzam-Probe](#)

Erstellen Sie einen Discovery-Zeitplan Operational Technology, und führen Sie den Prozess Discovery aus

Definieren Sie Discovery-Zeitpläne für Operational Technology (OT), die orchestrieren, wie und wann Discovery für eine OT-Funktion ausgeführt werden soll. Sie können auch eine sofortige Schnellausführung Discovery oder eine tatsächliche OT-Ausführung Discovery durchführen.

Vorbereitungen

Führen Sie die folgenden Aktionen aus, bevor Sie Discovery für Operational Technology ausführen:

- Installieren und konfigurieren Sie die Standardanwendung Discovery. Weitere Informationen finden Sie unter [Discovery-Setup](#).
- Installieren Sie das Plugin „CMDB CI Class Models“. Weitere Informationen finden Sie unter [Operational Technology Installation von Erweiterungsklassen für \(OT\)](#).
- Installieren Sie den MID-Server. Weitere Informationen finden Sie unter [MID-Server installieren](#).

Erforderliche Rolle: ot_discovery_admin

Prozedur

1. Navigieren zu **Alle > OT-Discovery > OT: Discovery-Zeitpläne**.
2. Führen Sie Schnell Discovery aus, oder wählen oder erstellen Sie einen OT-Erkennungszeitplan.
3. Füllen Sie im Formular die Felder OT Discovery-Zeitplan aus.
Die meisten Felder in diesem Formular sind mit dem Discovery-Standardformular identisch oder funktionieren auf die gleiche Weise. In diesem Thema werden nur Felder behandelt, die sich von der standardmäßigen Discovery-Zeitplanung unterscheiden. Weitere Informationen zu den verbleibenden Feldern finden Sie [unter Horizontal-Discovery planen](#).
4. Führen Sie den Prozess Discovery sofort aus, oder speichern Sie den OT-Erkennungszeitplan so, dass er zu den von Ihnen im Datensatz angegebenen Zeiten ausgeführt wird.

Ergebnisse

Wenn der Prozess Discovery für Operational Technology ausgeführt wird, wird ein Verlaufsdatensatz in der zugehörigen Liste „Status Discovery“ erstellt.

Bearbeiten oder zeigen Sie OT-Geräte nach dem Importieren oder der Discovery an

Verwenden Sie die Optionen im Menü Operational Technology (OT), um detaillierte Informationen für die OT-Geräte in Ihrem Unternehmen zu bearbeiten oder anzuzeigen.

Vorbereitungen

Importieren Sie Ihre Operational Technology -Gerätedaten auf eine der folgenden Arten:

- Verwenden Sie die Excel-Tabellenvorlage Microsoft Azure Event Hubs mit dem IntegrationHub Extract Transform Load (ETL), einem Operational Technology zertifizierten Service Graph Connector. Weitere Informationen finden Sie unter [Importieren Sie Ihre Excel-Tabelle Microsoft Azure Event Hubs mithilfe der Bereitstellungstabelle](#).
- Discovery für Operational Technology ausführen. Weitere Informationen finden Sie unter [Discovery für Operational Technology](#).
- Verwenden Sie einen Operational Technology -zertifizierten Service Graph Connector aus dem ServiceNow Store.

Erforderliche Rolle: cmdb_ot_viewer, cmdb_ot_editor, cmdb_ot_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Ihnen die Rolle cmdb_ot_viewer zugewiesen ist, können Sie OT-Geräte nur anzeigen. Wenn Ihnen die Rolle cmdb_ot_editor oder cmdb_ot_admin zugewiesen ist, können Sie OT-Gerät-Datensätze auf folgende Weise bearbeiten:

- Bearbeiten Sie OT-Gerät-Datensätze einzeln unter Now Platform.
- Massenbearbeiten Sie mehrere OT-Gerät-Datensätze aus der Listenansicht Industriell Arbeitsbereich.

Prozedur

1. Führen Sie die folgenden Schritte aus, um einen OT-Gerät-Datensatz Now Platform zu bearbeiten.

a. Navigieren zu **Alle > Operative Technologien (OT)** und wählen Sie eines der folgenden Menüelemente aus:

Alle OT-Geräte

Standardmäßig enthält diese Liste keine Steuerungsmodule.

Alle OT-Geräte nach IP-Adresse

Beachten Sie beim Anzeigen der Liste Alle OT-Geräte nach IP-Adresse Folgendes:

- Ein OT-Gerät mit mehreren IP-Adressen wird einmal pro zugewiesener IP-Adresse angezeigt.
- Wählen Sie den Namen des OT-Geräts aus, um den OT-Gerät-Datensatz zu öffnen. Wenn Sie die für den Datensatz angezeigte IP-Adresse auswählen, wird nur der Datensatz mit der IP-Adresse geöffnet.
- Sie **können** keinen neuen OT-Gerät-Datensatz aus dieser Liste erstellen.

OT-Steuerungssysteme

Standardmäßig enthält diese Liste keine Steuerungsmodule.

OT-Steuerungssysteme mit Modulen

Beachten Sie beim Anzeigen der Liste „OT-Steuerungssysteme mit Modulen“ Folgendes:

- In der Listenansicht werden alle Steuerungsmodule nach ihrem übergeordneten Steuerungssystem gruppiert angezeigt.
- Sie können keinen neuen OT-Gerät-Datensatz aus dieser Liste erstellen.

b. Wählen Sie in der Spalte **OT-Gerät** das OT-Gerät aus, das Sie bearbeiten möchten.

c. Füllen Sie die Felder des Formulars aus.

d. Klicken Sie auf **Aktualisieren**.

2. Um mehrere OT-Gerät-Datensätze Industriell Arbeitsbereichin einem Massenvorgang zu bearbeiten, führen Sie die folgenden Schritte aus.

a. Navigieren zu **Alle > Industrial Workspace**.

b. Öffnen Sie die Listenansicht (), und wählen Sie eine der folgenden Listen aus, die unter **Operational Technology (OT)** verfügbar sind.

- OT-Überwachungssysteme
- OT-Steuerungssysteme
- OT-Feldgeräte
- OT-Computer und -Server
- OT-Netzwerkgerät
- Industrielles IoT (IIoT)
- Nicht klassifizierte OT-Geräte

c. Aktivieren Sie das Kontrollkästchen neben jedem OT-Gerät, das Sie bearbeiten möchten.

Hinweis:

Sie können nur OT-Geräte mit demselben **Klassenfeld** massenbearbeiten. Sie können die Massenbearbeitungsfunktion für OT-Geräte mit anderen Klassen nicht verwenden.

d. Um die CI-Felder (Configuration Item, Konfigurationselement) zu bearbeiten, wählen Sie die Schaltfläche **Bearbeiten**, und bearbeiten Sie die Formularfelder nach Bedarf.



Hinweis:

Die maximale Anzahl von Datensätzen, für die Sie CI-Felder in einem Massenvorgang bearbeiten können, sind die auf einer einzelnen Seite angezeigten Datensätze.

e. Klicken Sie auf **Aktualisieren**.

- f. Um die OT-Gerät-Details zu bearbeiten, wählen Sie die Schaltfläche **OT-Details bearbeiten** aus, und bearbeiten Sie die Formularfelder nach Bedarf.

OT Supervisory Systems 24

Last refreshed 22m ago



Hinweis:

Die Massенbearbeitung von OT-Details ist ein Hintergrundauftrag, der einige Zeit in Anspruch nehmen kann. Wenn der Hintergrundauftrag ausgelastet ist, können Sie andere OT-Gerät-Datensätze nicht in einem Massenvorgang bearbeiten.

Zugehörige Elemente und zugehörige Listen für OT-Geräte

Die Menüoptionen Alle OT-Geräte, Alle OT-Geräte nach IP-Adresse und Alle OT-Geräte nach CI enthalten mehrere zugehörige Elemente und Listen.

Zugehörige Elemente

In diesem Abschnitt werden alle zugehörigen oder untergeordneten Elemente aufgelistet, die diesem OT-Gerät zugeordnet sind.

Hinweis:

Nicht alle OT-Geräte zeigen die folgenden zugehörigen Listen an. Für OT-Geräte in einer Klasse Operational Technology oder erweiterten Klasse werden die folgenden zugehörigen Listen angezeigt. Für OT-Geräte, die in einer anderen Hardwareklasse kategorisiert sind, z. B. Windows Server, muss ein Instanzadministrator dem Formular die zugehörigen Listen hinzufügen.

1. Um die zugehörigen Datensätze anzuzeigen, klicken Sie auf den Namen des zugehörigen Elements (z. B. Speichermodule).
2. Um eine CI-Beziehung (Configuration Item) für dieses OT-Gerät hinzuzufügen, klicken Sie auf das Symbol zum Hinzufügen von CI-Beziehungen (). Verwenden Sie das Suchfeld, um das CI-Element zu finden, für das Sie eine Beziehung erstellen möchten.
3. Um auf das Formular „Abhängigkeitsansicht“ zuzugreifen und eine bildliche Darstellung der OT-Gerät-Beziehungen anzuzeigen, klicken Sie auf das Symbol zum Anzeigen von Abhängigkeitsansichten ().
4. Um die Einstellungen zu ändern, die steuern, wie die zugehörigen Elemente angezeigt und gefiltert werden, klicken Sie auf das Einstellungssymbol ().

Zugehörige Listen für OT-Geräte

Zugehörige Liste	Beschreibung
IP-Adresse	Die IP-Adressen, IP-Versionen, Netzmasken, NIC-Nummern und Configuration Items, die dem OT-Gerät zugeordnet sind.
Netzwerkadapter	Die Namen, MAC-Adressen, IP-Adressen, Netzmasken, MAC-Hersteller und DHCP-fähige Indikatoren (Dynamic Host Configuration Protocol). Sie enthält Status der Netzwerkadapter, die dem OT-Gerät zugeordnet sind.
Seriennummern	Die Seriennummern, Gültigkeitsindikatoren und Seriennummerntypen, die dem OT-Gerät zugeordnet sind.
Anlagenmodell-Entitäten	Die Anlagenmodell-Entitäten, die vom OT-Gerät automatisiert werden.

Zugehörige Listen für OT-Geräte (Fortsetzung)

Zugehörige Liste	Beschreibung
OT-Steuerungsmodule	Die Steuerungsmodule, die dem OT-Gerät vom Typ OT-Steuerungssystem oder erweiterten Klassen (z. B. SPS) zugeordnet sind. Jedes OT-Steuerungsmodul, das eine Beziehung vom Typ „Eigentum von: Besitzt“ zum angezeigten OT-Steuerungssystem-Datensatz aufweist. Auf der Plattform können Benutzer ein OT-Steuerungsmodul erstellen. Je nach Feld Modultyp können Sie unter den folgenden Eingabe-/Ausgabewerten wählen: • Keine • Gebietsschema • Telearbeit • Verteilt
CMDB 360	Die zugehörigen 360-Daten CMDB in der Tabelle CMDB 360 [cmdb_multisource_data].
Speichermodule	Die Seriennummern, Gültigkeitsindikatoren und Seriennummertypen für die Speichermodule, die dem OT-Gerät zugeordnet sind.
Software installiert	Die Anwendungssoftware, die für das OT-Gerät installiert ist, falls vorhanden.
Angreifbare OT-Elemente	Die angreifbaren Elemente, die dem OT-Gerät zugeordnet sind.
OT-Incidents	Die OT-Incidents, die dem OT-Gerät zugeordnet sind.
OT-Change-Anforderungen	Die OT Change-Anforderungen, die dem OT-Gerät zugeordnet sind.
Externe Systemmetadaten	URL des Geräts im Quellsystem, in der Discovery-Quelle und auf aktualisierten Geräten, die dem CI zugeordnet sind. Die URL wird automatisch vom Quellsystem über den Service Graph Connector ausgefüllt.
OT-Protokolle	Dies gilt für die Protokollkonverterklasse. Protokolle, Beschreibung, Lieferant und Version, die der Protokollkonverterklasse zugeordnet sind.
Sicherungsinformationen	Das Sicherungsinformationsobjekt, das dem aktuellen CI zugeordnet ist.

Formular für Geräte der operativen Technologie

Verwenden Sie das Geräteformular für operative Technologie (OT), um die detaillierten Informationen für die OT-Geräte in Ihrem Unternehmen zu bearbeiten.

Formular für Geräte der operativen Technologie

Feld	Beschreibung
OT-Anzeigename	Der Name des im Datensatz angezeigten OT-Geräts. i Hinweis: Sie können diesem Feld einen beliebigen Zeichenfolgenwert hinzufügen. Mehrere Geräte können denselben OT-Anzeigenamen haben. Dies dient dem leichteren Verständnis des OT-Geräts und unterscheidet sich von dem eindeutigen CI-Namen, der beim Importieren von OT-Geräten aus der Bereitstellungstabelle generiert wird.
OT-Gerätetyp	Der Kategorietyt, als der das OT-Gerät klassifiziert ist. Der Gerätetyp ist auch die Funktion, die das Gerät im OT-Netzwerk spielt. Zum Beispiel: Ein IT-Gerät, z. B. ein Server, kann in ein OT-Gerät umgewandelt werden, und die Funktion, die es im Netzwerk ausübt, ist ein HMI. Daher ist seine Klasse „Server“ und sein Gerätetyp ist „HMI“. i Hinweis: In einigen Fällen gibt es OT-Geräte ohne OT-Funktion oder OT-Geräte, bei denen der Gerätetyp unbekannt ist. Wählen Sie für OT-Geräte ohne OT-Funktion Keine OT-Funktion aus. Wählen Sie für OT-Geräte, bei denen der Gerätetyp unbekannt ist, Unbekannt aus.
Gerät-Relevanz	Das Maß für das relative Risiko für den Standortprozess eines Gerätefehlers. Zum Beispiel: • 1 – Sehr kritisch • 4 – Nicht kritisch
Site	Die übergeordnete Entität der obersten Ebene oder der Industriestandort, an dem sich das Gerät befindet oder dem das Gerät zugewiesen ist.
Purdue-Ebene	Die zugewiesene Purdue-Ebene. Bereiche 0–5.

Formular für Geräte der operativen Technologie (Fortsetzung)

Feld	Beschreibung
	i Hinweis: Weitere Informationen zu Purdue-Ebenen in Industrial Control Systems finden Sie unter https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lv1sec10/the-purdue-model-for-industrial-control-systems .
Zone	Der Bereich innerhalb des Standorts, dem das Gerät zugewiesen ist.
Klasse	Der Name der zugewiesenen Klasse für das OT-Gerät. i Hinweis: Eine Liste und Erklärung von CI-Klassen finden Sie unter Erweiterungsklassen für Operation Technology (OT) .
Status	Status des OT-Geräts: – Keine Angabe – Kein zugewiesener Status. Abwesend OT-Gerät fehlt in Ihren Einrichtungen. In Wartung OT-Gerät wird gewartet und ist derzeit offline. Auf Lager OT-Gerät ist in Ihren Einrichtungen auf Lager. Installiert OT-Gerät ist in Ihren Einrichtungen installiert. Ausstehende Installation Die Installation des OT-Geräts steht in Ihren Einrichtungen aus. Ausstehende Reparatur Die Reparatur des OT-Geräts steht aus, ist jedoch noch nicht online. Deaktiviert OT-Gerät ist deaktiviert. Gestohlen OT-Gerät wurde gestohlen.

Formular für Geräte der operativen Technologie (Fortsetzung)

Feld	Beschreibung
Discovery Quelle	Die Quelle Discovery für die OT-Gerät-Daten. Beispiel: SG-OT Excel-Import, wenn Sie das OT-Gerät mit Microsoft Azure Event Hubs ETL aus einer IntegrationHub] Excel-Tabelle importiert haben. Weitere Informationen finden Sie unter Service Graph Connector für Operational Technology (Excel) .
Infrastrukturbeziehungen	Zeigt die Beziehung des OT-Geräts zu anderen OT-Geräten und den Anlagenmodell-Entitäten.
Servicebeziehungen	Zeigt die Beziehung des OT-Geräts zu den Anlagenmodell-Entitäten.
CI-Zeitleiste	Zeigt die Zeitleiste der OT-Incidents, den OT-Change und den Auditverlauf an, die dem OT-Gerät zugeordnet sind.
Die folgenden Felder gelten nur für die Klassendatensätze der speicherprogrammierbaren Steuerung (SPS):	
Schlüsselschalter	Die Modi des Schlüsselschalters: Remotemodus Sie können die Konfiguration der SPS ändern. Lokaler Modus Im Standardmodus können Sie die Konfiguration der SPS nicht ändern.
Schalterposition	Die Switch-Position der SPS hat die folgenden Positionen: • Ausführen • Programm • Telearbeit • Stoppen • Test Standardmäßig ist die Schalterposition auf Keine festgelegt. Wenn die Schalterposition auf Remote festgelegt ist, sind die Remote-Modi des Schalters aktiviert.
Schalter-Remotemodus	Der Remoteschalter der SPS besitzt die folgenden Modi: • Ausführen • Programm

Formular für Geräte der operativen Technologie (Fortsetzung)

Feld	Beschreibung
	• Test • Keine
Asset	Wenn Konfigurationselemente (CIs) in Configuration Management Database (CMDB) erstellt werden, werden Asset-Datensätze erstellt. Der Asset-Datensatz enthält die Modellkategorie des CI. Weitere Informationen zu den Modellkategorien für Operational Technology (OT) finden Sie unter Modellkategorien für Operational Technology. Führen Sie Folgendes aus, um die Modellkategorie für ein OT-Gerät anzuzeigen: 1. Navigieren zu Alle > Operative Technologien (OT) > Alle OT-Geräte. 2. Wählen Sie das OT-Gerät aus, für das Sie den Asset-Datensatz anzeigen möchten. 3. Wählen Sie neben dem Feld Asset das Symbol Vorschau auf diesen Datensatz anzeigen () aus. 4. Wählen Sie Datensatz öffnen.

Erstellen Sie das OT-Protokoll

Die OT-Protokolltabelle hilft Anwendern, die Informationen im Zusammenhang mit Protokollen wie Name, Version, ob es sich um ein lieferantenspezifisches Protokoll handelt oder nicht, zu erfassen. Die Protokolle sind das Kommunikationsmittel zwischen den verschiedenen Geräten, die mit dem Industrienetzwerk verbunden sind.

Vorbereitungen

Erforderliche Rolle: OT_admin und admin

Prozedur

1. Navigieren zu **Alle > Operative Technologien (OT) > OT-Protokolle**.
2. Klicken Sie auf der Seite „OT-Protokolle“ auf **Neu**.
3. Füllen Sie die Felder im Formular „OT-Protokoll“ aus.
4. Wenn das Protokoll ein lieferantenspezifisches Protokoll ist, aktivieren Sie die Checkbox **Lieferantenspezifisch**.
5. Klicken Sie auf **Absenden**.

Ordnen Sie OT-Protokolle Protokollkonverter-CIs zu

Ordnen Sie Operational Technology (OT)-Protokolle zu Protokollkonverter-Konfigurationselementen (CI) in Industriell Arbeitsbereich zu.

Vorbereitungen

Erforderliche Rolle: cmdb_ot_editor

Prozedur

1. Navigieren zu **Alle > Industrial Workspace** und öffnen Sie die Listenansicht Industriell Arbeitsbereich.
2. Wählen Sie in der Liste „**Alle OT-Geräte**“ einen Protokollkonverter-Datensatz aus.
3. Wählen Sie im Datensatz die Registerkarte **Zugehörige Datensätze** aus.
4. Wählen Sie die zugehörige Liste OT-Protokolle aus.
5. Wählen Sie **Hinzufügen**.
6. Wählen Sie die Protokolle aus, die Sie dem Protokollkonverter-Datensatz hinzufügen möchten, und klicken Sie auf **Hinzufügen**.
Die Protokolle werden der zugehörigen Liste hinzugefügt.
7. **Wahlweise:** Um Protokolldatensätze aus der zugehörigen Liste zu entfernen, wählen Sie die Datensätze aus, die Sie entfernen möchten, und klicken Sie auf **Entfernen**.

Konvertieren Sie ein IT-Hardwaregerät in ein OT-Gerät

Wenn Sie IT-Hardwaregeräte identifiziert haben, die zum OT-Netzwerk gehören, können Sie diese IT Configuration Items (CI) in OT-Geräte konvertieren.

Vorbereitungen

Erforderliche Rolle: cmdb_ot_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Diese Aufgabe gilt für alle IT-Hardwaregeräte.

Prozedur

1. Wählen Sie ein IT-CI aus.
Sie können beispielsweise zu navigieren **Alle > Konfiguration > Basiselemente > Computer**.
2. Wählen Sie das IT-Hardwaregerät aus, das Sie in ein OT-Gerät konvertieren möchten.
3. Wählen Sie im Modul „Zugehörige Links“ **die Option OT-Gerät-Details hinzufügen aus**.

Das Formular „OT-Gerät“ wird angezeigt.
4. Füllen Sie die Felder im Formular „OT-Gerät-Details“ aus.
5. Wählen Sie **Aktualisieren**.
6. Um das konvertierte OT-Gerät anzuzeigen, navigieren Sie zu **Alle > Operative Technologien (OT) > Alle OT-Geräte**.

Ergebnisse

Das ausgewählte IT-Hardwaregerät wurde in ein OT-Gerät konvertiert.

Alternativ können Sie mehrere IT-Hardwaregeräte auswählen und in einer Massenkonvertierung in OT-Geräte konvertieren. Weitere Informationen finden Sie unter [Konvertieren Sie IT-Hardware in einer Massenkonvertierung in OT-Geräte](#).

Konvertieren Sie IT-Hardware in einer Massenkonvertierung in OT-Geräte

Wählen Sie mehrere IT-Hardwaregeräte aus, und konvertieren Sie sie in einer Massenkonvertierung zu OT-Geräten, um Ihre Datensätze schneller und effizienter bearbeiten zu können.

Vorbereitungen

Erforderliche Rolle: cmdb_ot_admin oder admin

Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > Industrial Workspace**.
2. Navigieren Sie in Industriell Arbeitsbereich zur Liste Gesamte IT-Hardware.
3. **Wahlweise:** Wenn Sie die Liste Gesamte IT-Hardware filtern möchten, gehen Sie wie folgt vor:
 - Wählen Sie das Filter  in der oberen rechten Ecke der Liste.
 - Fügen Sie den Filter, den Sie auf die Liste anwenden möchten, hinzu.
 - Wählen Sie **Aktualisieren**.
4. Aktivieren Sie das Kontrollkästchen neben jedem IT-Hardwaregerät, das Sie konvertieren möchten.
Wenn Sie alle IT-Hardwaregeräte in der Liste auswählen möchten, aktivieren Sie das Kontrollkästchen neben der Spalte Name.
5. Wählen Sie die Schaltfläche **In OT-Geräte konvertieren**.
6. Füllen Sie die Felder des Formulars aus.

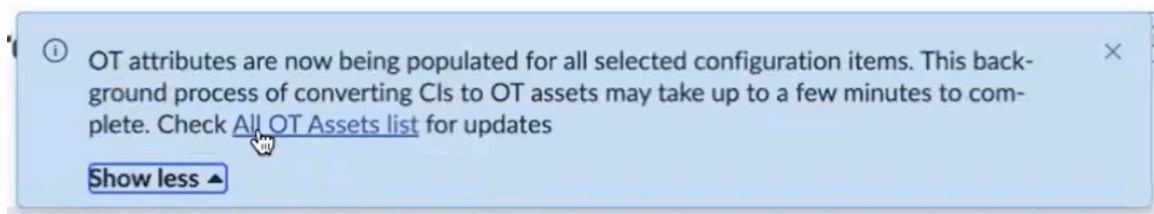
Formular „In OT-Geräte konvertieren“.

Feld	Beschreibung
OT-Gerätetyp	Der Kategoriety, als der das OT-Gerät klassifiziert ist. Der Gerätetyp ist auch die Funktion, die das Gerät im OT-Netzwerk spielt. Zum Beispiel: Ein IT-Gerät, z. B. ein Server, kann in ein OT-Gerät umgewandelt werden, und die Funktion, die es im Netzwerk ausübt, ist ein HMI. Daher ist seine Klasse „Server“ und sein Gerätetyp ist „HMI“. i Hinweis: In einigen Fällen gibt es OT-Geräte ohne OT-Funktion oder OT-Geräte, bei denen der Gerätetyp unbekannt ist. Wählen Sie für OT-Geräte ohne OT-Funktion Keine OT-Funktion aus. Wählen Sie für OT-Geräte, bei denen der Gerätetyp unbekannt ist, Unbekannt aus.
Gerät erelevanz	Maß des relativen Risikos für den Standortprozess, wenn das Gerät ausfällt: ◦ 1 – Sehr kritisch ◦ 4 – Nicht kritisch
Purdue-Ebene	Zugewiesene Purdue-Ebene. Die Ebenenbereiche sind 0–5.

Feld	Beschreibung
	 Hinweis: Weitere Informationen zu den Purdue-Ebenen in Industrial Control Systems finden Sie unter https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lv11sec10/the-purdue-model-for-industrial-control-systems .
Zone	Bereich innerhalb des Standorts, dem das Gerät zugewiesen ist.
Site	Übergeordnete Entität oder Industriestandort der obersten Ebene, an dem sich das Gerät befindet oder dem das Gerät zugewiesen ist.

7. Wählen Sie **Konvertieren** aus.

Das folgende Banner wird angezeigt, um Sie darüber zu informieren, dass der Prozess gestartet wurde. Um zu überprüfen, ob die Liste „Alle OT-Geräte“ aktualisiert wird, können Sie den Link im Banner auswählen.



Ergebnisse

Die ausgewählten IT-Hardwaregeräte wurden in OT-Geräte konvertiert.

Sie können auch die Funktion „Massenaktualisierungsregel für Neuzuweisung von IT zu OT“ verwenden, um eine geplante Aufgabe zu erstellen, die IT-Hardware automatisch in OT-Geräte konvertiert. Weitere Informationen finden Sie unter [Konvertieren Sie Ihre IT-Datensätze automatisch in OT-Geräte](#).

Konvertieren Sie Ihre OT-Geräte in einer Massенbearbeitung in IT-Hardwaregeräte

Bearbeiten Sie Ihre Operational Technology (OT)-Geräte in einem Massenvorgang, um die OT-Gerät-Details zu entfernen. Konvertieren Sie dann Ihre OT-Geräte in IT-Hardwaregeräte.

Vorbereitungen

Erforderliche Rolle: cmdb_ot_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie auf OT-Geräte stoßen, die keine OT-Funktion haben und als IT-Hardwaregeräte klassifiziert werden sollten, können Sie mehrere OT-Geräte in einer Massенbearbeitung auswählen und bearbeiten, um sie in IT-Hardwaregeräte zu konvertieren.

Prozedur

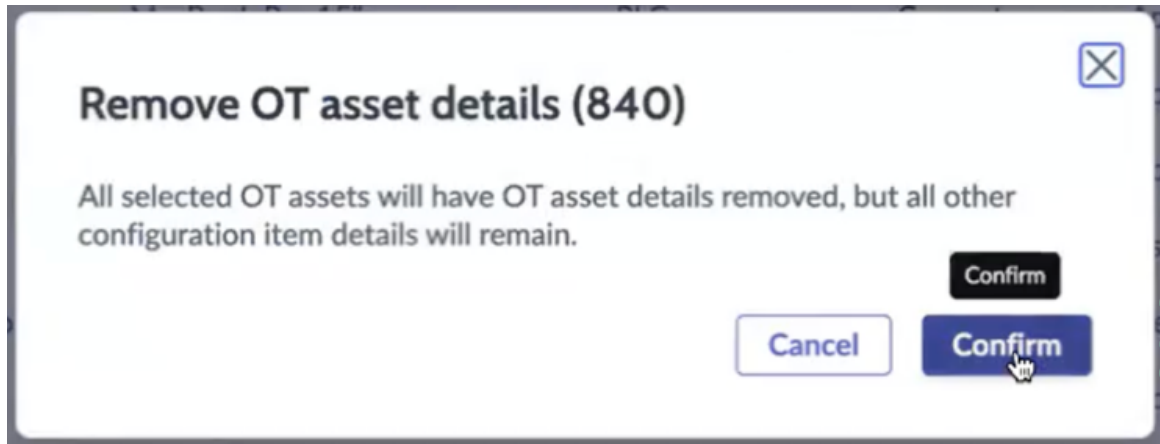
1. Navigieren zu **Alle > Industrial Workspace-Administrator > Industrieller Arbeitsbereich**.
2. Navigieren Sie zur Listenansicht Alle OT-Geräte in Industriell Arbeitsbereich.
3. Wählen Sie die OT-Geräte aus, die Sie in IT-Hardwaregeräte konvertieren möchten.
Wenn Sie alle OT-Geräte in der Liste auswählen möchten, aktivieren Sie das Kontrollkästchen neben der OT-Gerät-Spalte.

4. Wählen Sie die Schaltfläche **OT-Gerät-Details entfernen**.

Es wird ein Dialogfeld angezeigt, in dem Sie aufgefordert werden, zu bestätigen, dass Sie die OT-Gerät-Details entfernen, aber alle anderen Konfigurationselement-Details beibehalten möchten.

i Hinweis:

Keines der CI-Details, Netzwerkadapter oder IP-Adressen wird entfernt. Nur die OT-spezifischen Daten werden entfernt.



5. Wählen Sie **Bestätigen** aus.

Ergebnisse

Die OT-Gerät-Details werden aus den ausgewählten OT-Geräten entfernt, und die OT-Geräte werden in IT-Hardwaregeräte konvertiert. Sie können diese IT-Hardwaregeräte in der Listenansicht „IT-Hardware“ in Industrial Workspace anzeigen.

Ordnen Sie IP-Adressen OT-Geräten zu

Sie können die geplante SyncIPAddressToOT- Aufgabe verwenden, um die IP-Adressinformationen für alle verfügbaren OT-Geräte zu aktualisieren und zu synchronisieren. Die geplante SyncIPAddressToOT- Aufgabe ruft die IP-Adressinformationen aus der IP-Adresstabelle (cmdb_ci_ip_address) ab und fügt sie dem IP-Adressfeld des CI hinzu.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle > Systemdefinition > Geplante Aufgaben**.
2. Geben Sie auf der Seite „**Geplante Aufgaben**“ im **Suchfilter** SyncIPAddressToOT ein, und drücken Sie die Eingabetaste, um die geplante Aufgabe zu finden.
3. Wählen Sie SyncIPAddressToOTAus.
4. Wählen Sie auf der Seite Geplante SkriptausführungSyncIPAddressToOT **die Option Jetzt ausführen aus**.

Netzwerkangriffserkennungssystem-Appliances verwalten

Wenn Sie die Rolle cmdb_nids_admin oder admin innehaben, können Sie im Menü NIDS in Now Platform Metadatenattribute zu Klassendatensätzen des Netzwerkangriffserkennungssystems (Network Intrusion Detection System, NIDS) zuweisen.

Ein Netzwerkangriffserkennungssystem hilft bei der Verwaltung des Imports von IT- und OT-Geräten aus unterstützten Integrationen. Durch das Zuweisen von Metadaten wie Standort und NIDS-Netzwerktyp an NIDS-Datensätze können Sie zwischen erkannten OT- und IT-Geräten unterscheiden und die zugehörigen Metadaten automatisch den erstellten Datensätzen hinzufügen. Benutzer mit der Rolle `cmbd_nids_admin` oder `admin` können die Registerkarte **Zugewiesene NIDS-Metadaten** bearbeiten und die vom Benutzer vorgenommenen Änderungen im Aktivitätenstrom anzeigen.

Hinweis:

Die manuelle Erstellung für einen NIDS-Datensatz in der Tabelle ist in der Listenansicht oder der Formularansicht der Datensätze eingeschränkt.

Weitere Informationen zu den NIDS-Klassendatensätzen finden Sie unter [Netzwerkangriffserkennungssystem \(NIDS\) CI-Erweiterungsklasse](#) .

Wenn für einen NIDS-Datensatz das Feld Validiert auf wahr festgelegt ist und eines der folgenden Attribute des NIDS im NIDS-Formular geändert wird, wird eine Warnmeldung angezeigt.

- NIDS-Netzwerktyp
- NIDS-Quellenname
- NIDS-Quell-ID

Wenn der NIDS-Datensatz mit einer Beziehung vom Typ `detects::detected by` gelöscht wird, wird eine Warnmeldung angezeigt.

Das geführte Setup für Netzwerkangriffserkennungssysteme (NIDS) führt Sie durch die folgenden Schritte:

- Benutzer und Rollen für Benutzer konfigurieren, die noch keinen Account in einer Instanz haben
- NIDS-Datensätze aus Operational Technology (OT) zertifizierten Service Graph Connectors importieren, um festzulegen, ob NIDS-Geräte in OT- oder IT-Netzwerken ausgeführt werden
- NIDS werden validiert, damit erkannte Geräte importiert werden können. Weitere Informationen zum Validieren von NIDS finden Sie unter [Validieren Sie das NIDS](#).

Um auf das geführte Setup für NIDS zuzugreifen, navigieren Sie zu **Netzwerkangriffserkennungssystem (Network Intrusion Detection System, NIDS) > NIDS Geführtes Setup**.

Um eine Appliance als Manager für NIDS-Sensoren zuzuweisen, die Geräte erkennen, navigieren Sie zu **Netzwerkangriffserkennungssystem (Network Intrusion Detection System, NIDS) > Manager** um die entsprechenden Datensätze für „Verwaltungskonsolen“ oder „Zentralmanager“ zu bearbeiten.

- Überprüfen Sie die Liste „Sensoren“, um sicherzustellen, dass derzeit kein Gerät als Manager zugewiesen ist.
- Für alle Geräte, die nicht als Sensoren fungieren, **wird der Change-Manager auf true** festgelegt.

Informationen zur Skripteinbindung NIDSUtils, die vom NIDS zugewiesene Metadaten auf erkannte Geräte kopiert, finden Sie unter [Mit Operational Technology Manager installierte Skripteinbindungen](#).

Zugehörige Informationen

Netzwerkangriffserkennungssystem (Network Intrusion Detection System, NIDS) – CI-Erweiterungsklasse [\[7\]](#)

Mit Operational Technology Manager installierte Skripteinbindungen

Validieren Sie das NIDS

Validieren Sie NIDS, um die vom Sensor erkannten Geräte aus ETL zu importieren. Die Sensoren können die Validierung nur bestehen, wenn sie sich nicht im Lernmodus befinden, da solche Sensoren nicht für den Geräteimport geeignet sind.

Vorbereitungen

Es wird empfohlen, das Plugin Gemeinsames Servicedatenmodell zu installieren. Der Service Graph Connector wird an den Lebenszyklusdatenmodellen gemäß den Standards Configuration Management Database (CMDB) ausgerichtet. Weitere Informationen finden Sie unter [Implementing the CSDM framework in stages \[7\]](#).

Erforderliche Rolle: cmdb_nids_admin

Warum und wann dieser Vorgang ausgeführt wird

Die Felder „**Lebenszyklusphase**“ und „**Status der Lebenszyklusphase**“ werden verwendet, um den Lernmodus eines Sensors zu erfassen. Wenn das Feld Lebenszyklusphase auf **Funktionsfähig** und der Status der Lebenszyklusphase auf **Lernmodus** festgelegt ist, ist die Validierung nicht erfolgreich. Wenn das Feld Status der Lebenszyklusphase auf **In Gebrauch** festgelegt ist, ist die Validierung erfolgreich.

Prozedur

1. Navigieren zu **Alle > Netzwerk-IDS-Appliance (NIDS) > Sensoren**.
2. Wenn in der Liste Verwaltungskonsolen oder zentrale Manager vorhanden sind, führen Sie die folgenden Aktionen aus:
 - a. Klicken Sie auf „**Datensatz bearbeiten**“.
 - b. Wählen Sie auf der Registerkarte **NIDS-Administratorkonfiguration** die Option **Ist NIDS-Manager** aus, um die Spalte **Validiert** auf true festzulegen.
3. Stellen Sie im Abschnitt „NIDS-Administratorkonfiguration“ sicher, dass für den **Status der Lebenszyklusphase** nicht Lernmodus festgelegt ist. Andernfalls schlägt die Validierung fehl.
4. Wählen Sie den **NIDS-Netzwerktyp** aus.

Der Netzwerktyp muss basierend auf dem Standort des Sensors ausgewählt werden.

Hinweis:

Der Netzwerktyp OT erstellt den OT-Gerät-Datensatz. Der Netzwerktyp „IT“ erstellt die OT-Gerät-Datensätze nicht.

5. Überprüfen Sie auf der Registerkarte **Zugewiesene NIDS-Metadaten**, ob alle vom NIDS erkannten Geräte eingegeben wurden.

6. Klicken Sie auf **Validieren**.

i Hinweis:

Der Zonenwert wird durch die -ETL ausgefüllt. Wenn ein Zonenwert manuell in den NIDS-Datensatz eingegeben wird, wird er durch die Angaben in ETL überschrieben.

Wenn der NIDS-Datensatz nicht validiert ist, werden die Geräte, die vom Sensor erkannt wurden, nicht aus ETL importiert.

Nächste Maßnahme

Alternativ können Sie mehr als einen NIDS-Sensor durch eine Massenvvalidierung validieren. Weitere Informationen finden Sie unter [Validiert mehrere NIDS-Sensoren gleichzeitig](#).

Validiert mehrere NIDS-Sensoren gleichzeitig

Validieren Sie mehrere NIDS-Sensoren gleichzeitig durch eine Massenvvalidierung, um Ihre Datensätze schneller und effizienter bearbeiten zu können.

Vorbereitungen

Erforderliche Rolle: cmdb_nids_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Massenvvalidierung verwenden, um mehrere NIDS-Sensoren gleichzeitig zu validieren, anstatt jeden NIDS-Sensor einzeln zu validieren.

i Hinweis:

Überprüfen Sie die NIDS-Sensoren sorgfältig nach Discovery-Quelle, und gehen Sie bei der Massenvvalidierung mit Vorsicht vor.

Prozedur

1. Navigieren zu **Alle > Netzwerk-IDS-Appliance (NIDS) > Sensoren**.
2. Aktivieren Sie die Kontrollkästchen der Sensordatensätze, die Sie validieren möchten.
3. Wählen Sie die Schaltfläche **Sensoren validieren** aus.

Ergebnisse

Wenn die von Ihnen validierten Sensoren den **Lebenszyklusphasen-Status** In Gebrauch haben, wird eine Meldung angezeigt, dass die Validierung erfolgreich war.

Wenn die ausgewählten Sensoren den **Lebenszyklusphasenstatus** „Lernmodus“ haben oder die Spalte **Validiert** auf „wahr“ festgelegt ist, wird eine Fehlermeldung angezeigt, die Sie darüber informiert, dass mindestens ein Sensor im Lernmodus nicht validiert wurde oder bereits validiert wurde. Sie sollten in Betracht ziehen, die Spalte **„Status der Lebenszyklusphase“** in „In Gebrauch“ zu ändern, um mit der Massenvvalidierung fortzufahren.

Modellierung eines Operational Technology -Systemservice

Sie können einen Operational Technology (OT)-Systemservice modellieren, um andere Steuerungssysteme zu erstellen, z. B. ein verteiltes Steuerungssystem (Distributed Control System, DCS).

Ein OT-Systemservice bezieht sich auf eine Kategorie von Technologien und Systemen, die zur Verwaltung, Steuerung und Überwachung von physischen Prozessen, Maschinen und industriellen Vorgängen verwendet werden. OT-Systemservices werden normalerweise

in Sektoren wie Produktion, Energie, Versorgungsunternehmen und Transportwesen eingesetzt.

OT-Systemservices können Folgendes umfassen.

- Distributed Control Systems (DCS)
- SCADA (Supervisory Control and Data Acquisition)
- Industrielle Steuerungssysteme (ICS)
- Sicherheitsinstrumentensysteme (SIS)
- Manufacturing Execution Systems (Mes)
- Prozesssteuerungssysteme
- Transportmanagementsysteme
- Energiemanagementsysteme
- Gebäudemanagementsystem-Services (BMS)

Diese Systemservices stellen gemeinsam sicher, dass industrielle Prozesse effizient und sicher ablaufen.

DCS-Beispiel

Sie können OT-Systemservices modellieren, um andere Steuerungssysteme zu erstellen. Sie können beispielsweise ein verteiltes Steuerungssystem (Distributed Control System, DCS) und alle zugehörigen Komponenten (SPS, Steuerungsmodule, EWS, RTU, HMI, SCADA usw.) modellieren. Ein DCS ist eine Plattform für die automatisierte Steuerung und den Betrieb von Anlagen oder Industrieprozessen. Es koordiniert und überwacht die gesamte Anlage mit vielen unterschiedlichen Prozessen.

Ein DCS ist ein prozessorientiertes System, das eine geschlossene Schleifensteuerung verwendet. In der folgenden Tabelle werden die Komponenten eines DCS beschrieben.

DCS-Komponenten

Komponente	Beschreibung
Operator-Stationen	Im Herzstück des DCS zeigen Bediener den Prozess an und überwachen Alarmer und Warnungen.
Server, EWS, Historian	Datenerfassung und Datenaustausch für Hardwarekonfigurationen.
Controller, E/A-Module	Datenaustausch mit Servern.
Feldgeräte	Geräte wie Sender, Schalter, Aktuatoren und Schieber.

Ein DCS unterscheidet sich von einem zentralisierten Steuerungssystem, bei dem ein einzelner Controller an einem zentralen Ort die Steuerungsfunktion übernimmt. In einem DCS wird jedoch jedes Prozesselement, jede Maschine oder jede Gruppe von Maschinen von einer dedizierten Steuerung gesteuert.

Erstellen Sie einen Operational Technology -Systemservice

Erstellen Sie einen Operational Technology (OT)-Systemservice, um ein verteiltes Steuerungssystem (Distributed Control System, DCS) und alle zugehörigen Komponenten, z. B. Steuerungsmodule und Programmierlogiksteuerungen (PLCs), zu modellieren.

Warum und wann dieser Vorgang ausgeführt wird

Sie können einen OT-Systemservice an folgenden Stellen erstellen:

- Now Platform in der Liste **OT-Systeme**
- Industriell Industrial Workspace Listenansicht

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Wenn Sie einen OT-Systemservice für Now Platform erstellen möchten, führen Sie die folgenden Aktionen aus:
 - a. Navigieren zu **Alle > Operative Technologien (OT) > OT-Systeme**.
 - b. Wählen Sie **Neu**.
 - c. Füllen Sie die folgenden Felder des Formulars aus.

OT-Systemserviceformular

Feld	Beschreibung
Anzeigenname	Wird verwendet, um den Anzeigenamen des OT-Systemservice auszufüllen.
Name	Hostname des OT-Systemservice.
ISA-Entitätsstandort	ISA-Entitätsstandort, zu dem der OT-Systemservice gehört.
Hersteller	Name des Herstellers des OT-Systemservice.
Modellnummer	Modellnummer des Herstellers für den OT-Systemservice.
Kurzbeschreibung	Kurze Beschreibung des OT-Systemservice.
Details	
Eigentum von	Name des primären Besitzers des OT-Systemservice.
Verwaltet von	Name des primären Managers des OT-Systemservice.
Business-Relevanz	Maß dafür, wie kritisch oder wichtig der Systemservice ist. Beispiele: ▪ „Hoch“ oder „Sehr kritisch“. ▪ Mittel oder kritisch ▪ Niedrig oder Weniger kritisch ▪ Keine oder nicht kritisch
Supportgruppe	Name der primären Supportgruppe für den OT-Systemservice.
Verwaltet nach Gruppe	Name der Gruppe, die den OT-Systemservice verwaltet.

Feld	Beschreibung
Betriebsstatus	Status des Systemservice.

d. Wählen Sie **Absenden**.

2. Wenn Sie einen OT-Systemservice in der Listenansicht Industriell Arbeitsbereich erstellen möchten, führen Sie die folgenden Aktionen aus:

a. Navigieren zu **Alle > Industrial Workspace**.

b. Wählen Sie das Symbol Liste () aus.

c. Wählen Sie im Modul **Operational Technology (OT)** die Liste **OT-Systeme** aus.

d. Wählen Sie **Neu**.

e. Füllen Sie die folgenden Felder des Formulars aus.

OT-Systemserviceformular

Feld	Beschreibung
Anzeigename	Wird verwendet, um den Anzeigenamen des OT-Systemservice auszufüllen.
Name	Hostname des OT-Systemservice.
ISA-Entitätsstandort	ISA-Entitätsstandort, zu dem der OT-Systemservice gehört.
Hersteller	Name des Herstellers des OT-Systemservice.
Modellnummer	Modellnummer des Herstellers für den OT-Systemservice.
Kurzbeschreibung	Kurze Beschreibung des OT-Systemservice.
Details	
Eigentum von	Name des primären Besitzers des OT-Systemservice.
Verwaltet von	Name des primären Managers des OT-Systemservice.
Business-Relevanz	Maß dafür, wie kritisch oder wichtig der Systemservice ist. Beispiele: ▪ „Hoch“ oder „Sehr kritisch“. ▪ Mittel oder kritisch ▪ Niedrig oder Weniger kritisch ▪ Keine oder nicht kritisch
Supportgruppe	Name der primären Supportgruppe für den OT-Systemservice.
Verwaltet nach Gruppe	Name der Gruppe, die den OT-Systemservice verwaltet.
Betriebsstatus	Status des Systemservice.

f. Wählen Sie **Speichern**.

Nächste Maßnahme

Jetzt können Sie dem Systemservice OT-Geräte hinzufügen. Weitere Informationen finden Sie unter [Fügen Sie einem Operational Technology -Systemservice ein Gerät hinzu](#).

Fügen Sie einem Operational Technology -Systemservice ein Gerät hinzu

Fügen Sie einem OT-Systemservice ein Operational Technology (OT)-Gerät hinzu, um eine Beziehung zwischen der Anlagenmodell-Entität, zu der das Gerät gehört, und dem OT-Systemservice zu erstellen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle > Industrial Workspace**.
2. Wählen Sie das Symbol Liste () aus.
3. Wählen Sie im Modul **Operational Technology (OT)** die Liste **OT-Systeme** aus.
4. Wählen Sie den OT-Systemservice aus, dem Sie ein Gerät hinzufügen möchten.
5. Wählen Sie auf der Registerkarte **Zugehörige Datensätze** den zugehörigen Datensatz **Zugeordnete OT-Geräte** aus.
6. Wählen Sie **Hinzufügen**.
7. Aktivieren Sie das Kontrollkästchen neben einem oder mehreren OT-Geräten.
8. Nachdem Sie alle OT-Geräte ausgewählt haben, wählen Sie **Hinzufügen**.

Ergebnisse

Nachdem Sie die OT-Geräte hinzugefügt haben, werden die folgenden Beziehungen erstellt:

- Die Beziehung Depends on::Used by (Abhängig von::Verwendet von) zwischen dem ausgewählten Configuration Item (CI) und dem OT-Systemservice
- Die Beziehung „Verwaltet von::Verwaltet“ zwischen dem OT-Systemservice und der Anlagenmodell-Entität des CI.

Ordnen Sie einen Operational Technology -Systemservice einer Anlagenmodell-Entität zu

Ordnen Sie einen Operational Technology (OT)-Systemservice einer Entität im Anlagenmodell nach ISA zu, indem Sie eine geplante Aufgabe aktivieren. Wenn sich die Beziehung zwischen einem OT-Gerät und einer Anlagenmodell-Entität ändert, berechnet die geplante Aufgabe die Beziehung zwischen dem OT-Systemservice und der Anlagenmodell-Entität neu.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle > Systemdefinition > Geplante Aufgaben**.
2. Wählen Sie das Symbol zum Anzeigen/Ausblenden von Filtern ().
3. Fügen Sie den folgenden Filter hinzu.
[Name] [ist] [OT-Systeme zu ISA-Entitäten zuordnen]
4. Wählen Sie den **Datensatz der geplanten Aufgabe zum Zuordnen von OT-Systemen zu ISA-Entitäten** aus.

5. Aktivieren Sie das Kontrollkästchen neben dem Feld **Aktiv**.
6. Wählen Sie im Feld **Ausführen** die Option aus, die Ihren Anforderungen am besten entspricht.
7. Wählen Sie **Aktualisieren**.

Zeigen Sie die Abhängigkeitszuordnung für einen Operational Technology -Systemservice an

Zeigen Sie die Abhängigkeitszuordnung für einen Operational Technology (OT)-Systemservice an, um die grafische Darstellung der hierarchischen Struktur des ausgewählten OT-Systemservice und seiner Beziehung zu anderen Entitäten im Produktionsprozess anzuzeigen.

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Abhängigkeitszuordnung für einen OT-Systemservice an den folgenden Stellen anzeigen:

- Now Platform in einem OT-Systemservicedatensatz
- Industrial Workspace in einem OT-Systemservicedatensatz

Vorbereitungen

Erforderliche Rolle: cmdb_ot_editor

Prozedur

1. Wenn Sie die Abhängigkeitszuordnung für einen OT-Systemservice auf Now Platformanzeigen möchten, führen Sie die folgenden Aktionen aus:
 - a. Navigieren zu **Alle > Operative Technologien (OT) > OT-Systeme**.
 - b. Wählen Sie den OT-Systemservicedatensatz aus, für den Sie die OT-Abhängigkeitszuordnung anzeigen möchten.
 - c. Wählen Sie **OT-Abhängigkeitszuordnung anzeigen aus**.
2. Wenn Sie die Abhängigkeitszuordnung für einen OT-Systemservice in Industrial Workspaceanzeigen möchten, führen Sie die folgenden Aktionen aus:
 - a. Navigieren zu **Alle > Industrial Workspace**.
 - b. Wählen Sie das Symbol Liste () aus.
 - c. Wählen Sie im Modul **Operational Technology (OT)** die Liste **OT-Systeme** aus.
 - d. Wählen Sie den OT-Systemservicedatensatz aus, für den Sie die OT-Abhängigkeitszuordnung anzeigen möchten.
 - e. Wählen Sie **OT-Abhängigkeitszuordnung anzeigen aus**.

Konvertieren Sie Ihre IT-Datensätze automatisch in OT-Geräte

Erstellen Sie eine geplante Aufgabe, die Ihre IT-Hardware automatisch in Operational Technology-Geräte (OT) konvertiert, indem Sie die Funktion „Regelsatz für Massenaktualisierung für Neuzuweisung von IT zu OT“ verwenden. Diese geplante Aufgabe fügt der gesamten IT-Hardware, die Sie gleichzeitig konvertieren möchten, OT-Entitätsdetails hinzu.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Möglicherweise verfügen Sie über als IT-Hardware klassifizierte Konfigurationselemente (CIs), für die Sie OT-Entitätsdatensätze erstellen möchten. Befolgen Sie diese allgemeinen Richtlinien:

- Stellen Sie sicher, dass die von Ihnen verwendeten Felder den Filterkriterienbedingungen in den Schritten 3 bis 4 entsprechen. Stellen Sie sicher, dass der Datensatz 1 Million Datensätze nicht überschreitet, um Leistungsprobleme zu vermeiden.
- Erstellen Sie in den Schritten 3 bis 6 separate Definitionen für geplante Aufgaben für die einzelnen CI-Klassen. Auf diese Weise können Sie jede CI-Ebene filtern und die Standardwerte für die OT-Entität definieren.
- Verwenden Sie das Feld Klasse im Filter, um in Schritt 3 nur bestimmte CI-Klassen abzufragen.

i Hinweis:

In der Quelltable werden nur die Hardwareklasse und ihre erweiterten Klassen verwendet.

- Verwenden Sie die Schaltfläche **Vorschau**, um die Datensätze zu überprüfen, die in Schritt 4 zur weiteren Überprüfung ausgewählt wurden.
- Überprüfen Sie die Daten auf der Registerkarte **Standardkonfiguration für OT-Entitäten** in Schritt 5. Die OT-Entitätsdatensätze werden mit diesen Standardwerten erstellt.

Sie können die IT-Hardware auch manuell für OT-Geräte konvertieren. Weitere Informationen finden Sie unter [Konvertieren Sie IT-Hardware in einer Massенbearbeitung in OT-Geräte](#).

Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > OT-Manager-Administrator > Automatisierte IT-OT-Massenkonvertierung**.
2. Wählen Sie **Neu**.
3. Legen Sie auf der Registerkarte **Filterkriterien – OT-Geräte** die Quelltable und Filterkriterien fest, um die zu konvertierenden CIs zu identifizieren.

Wenn Sie beispielsweise die OT-Entitätsdetails für alle in das System importierten Computer mit dem Präfix „COMP“ hinzufügen möchten, wählen Sie die Quelltable **cmdb_ci_computer** aus, und fügen Sie die Filterkriterien **[Name] [beginnt mit] [COMP.]hinzu]**, **[Klasse] [ist] [Computer]** und **[OT-Gerät-Details] [ist**

The screenshot shows the 'Filter Criteria - OT Devices' configuration interface. The 'Table' dropdown is set to 'Computer [cmdb_ci_computer]'. Under 'Filter Criteria', there are three conditions: 'Name starts with COMP', 'Class is Computer', and 'OT device details is empty'. These are connected by 'AND' operators. A 'Preview' button is visible next to the filter criteria.

leer].

Sie können auch CMDB -Gruppen verwenden, um IT-CIs basierend auf zusätzlichen Informationen, z. B. „Software installiert“, zu gruppieren, damit Sie sie in OT-Geräte konvertieren können. Weitere Informationen finden Sie unter [Verwenden Sie CMDB -Gruppen, um IT-CIs OT-Kontext hinzuzufügen](#).

4. Überprüfen Sie die Anzahl der Datensätze, die aus der von Ihnen festgelegten Filterbedingung ausgewählt wurden, indem Sie die Schaltfläche **Vorschau** wählen.

Für diese Datensätze werden die OT-Entitätsdetails hinzugefügt, z. B. OT-Gerättyp und Geräterelevanz.

5. Füllen Sie die Felder auf der Registerkarte **Standardkonfiguration für OT-Entität aus.**

Die Felder in der folgenden Tabelle geben die Standardwerte an, die den OT-Entitätsdatensätzen oder den OT-bezogenen Metadaten hinzugefügt werden.

Formular „OT-Entität – Standardkonfiguration“.

Feld	Beschreibung
OT-Gerätetyp	Kategorietyt, als der das OT-Gerät klassifiziert ist. Der Gerätetyp ist auch die Funktion, die das Gerät im OT-Netzwerk spielt. Beispielsweise kann ein IT-Gerät, z. B. ein Server, in ein OT-Gerät konvertiert werden, und die Funktion, die es im Netzwerk ausübt, ist ein HMI. Seine Klasse ist „Server“, und sein Gerätetyp ist „HMI“. i Hinweis: In einigen Fällen haben OT-Geräte keine OT-Funktion, oder der Gerätetyp ist unbekannt. Wenn die OT-Geräte keine OT-Funktion haben, wählen Sie Keine OT-Funktion aus. Wenn die OT-Geräte einen unbekannten Gerätetyp haben, wählen Sie Unbekannt aus.
Geräterelevanz	Maß des relativen Risikos für den Standortprozess, wenn das Gerät ausfällt: ○ 1 – Sehr kritisch ○ 4 – Nicht kritisch
Purdue-Ebene	Zugewiesene Purdue-Ebene. Die Ebenenbereiche sind 0–5. i Hinweis: Weitere Informationen zu den Purdue-Ebenen in Industrial Control Systems finden Sie unter https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lv1sec10/the-purdue-model-for-industrial-control-systems .
Zone	Bereich innerhalb des Standorts, dem das Gerät zugewiesen ist.
Site	Übergeordnete Entität oder Industriestandort der obersten Ebene, an dem sich das Gerät befindet oder dem das Gerät zugewiesen ist.

6. Wählen Sie im Feld **Ausführen eine geplante Zeit für die Ausführung dieses Auftrags aus.**

7. Aktivieren Sie das Kontrollkästchen neben dem Feld **Aktiv.**

8. Wählen Sie **Absenden.**

Verwenden Sie CMDB -Gruppen, um IT-CIs OT-Kontext hinzuzufügen

Verwenden Sie Gruppen Configuration Management Database (CMDB), um IT Configuration Items (CIs) basierend auf zusätzlichen Informationen zu gruppieren, z. B. installierte Software. Anschließend können Sie den IT-CIs den Kontext Operational Technology (OT) hinzufügen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die Verwendung von CMDB -Gruppen ändert die Klasse des IT-CI nicht. Stattdessen werden dem IT-CI OT-Entitätsdatensätze hinzugefügt, die den OT-Kontext erfassen.

Hinweis:

Befolgen Sie diese allgemeinen Richtlinien:

1. Stellen Sie sicher, dass die Filterbedingungen in der CMDB-Gruppe jedes Mal einen eindeutigen Satz von CI-Datensätzen zurückgeben. Wenn beispielsweise eine Filterbedingung wie „**OT-Gerät-Details ist leer**“ hinzugefügt wird, wird sichergestellt, dass nur Datensätze ohne OT-Gerät-Details berücksichtigt werden.
2. Stellen Sie sicher, dass die indizierten Felder als Teil der Filterkriterienbedingungen verwendet werden. Stellen Sie sicher, dass der Datensatz 10.000 Datensätze nicht überschreitet, um Leistungsprobleme zu vermeiden.

Hinweis:

Die CMDB-Gruppen-API unterstützt das Abrufen von Datensätzen, das 10.000 oder den durch die folgenden Eigenschaften definierten Grenzwert überschreitet, nicht.

- glide.cmdb.query.max_results_limit
- glide.cmdb.group.max_ci_limit

Um dies zu beheben, müssen diese Eigenschaften angepasst werden, um größere Abfrageergebnisse zu ermöglichen, wenn die CMDB-Abfrage mehr Datensätze enthält, als die aktuellen Grenzwerte zulassen.

3. Stellen Sie sicher, dass pro CMDB-Gruppe ein Datensatz für die automatisierte Massenkonzertierung von IT in OT (sn_automated_it_ot_bulk_conversion) erstellt wird, um die Filterung auf Gruppenebene durchzuführen und die Standardwerte für die jeweiligen OT-Entitäten zu definieren.
4. Validieren Sie die Daten auf der Registerkarte **Standardkonfiguration für OT-Entität**. OT-Entitätsdatensätze werden mit diesen Standardwerten erstellt.

Prozedur

1. Definieren Sie eine Gruppe CMDB mit den erforderlichen Filterkriterien, die die richtigen IT-CIs identifiziert.
Weitere Informationen finden Sie unter [CMDB groups](#) .
2. Erstellen Sie einen Datensatz für die automatisierte Massenkonzertierung von IT in OT (sn_automated_it_ot_bulk_conversion), der der Gruppe CMDB zugeordnet ist.
Durch das Erstellen dieses Datensatzes wird IT-CIs OT-Kontext über die OT-Entitätsdetails hinzugefügt.

Weitere Informationen zum Erstellen eines Datensatzes für die automatisierte Massenkonzertierung von IT in OT finden Sie unter [Konvertieren Sie Ihre IT-Datensätze automatisch in OT-Geräte](#).

3. Führen Sie die folgenden Aktionen aus, um einen Datensatz in **sn_automated_it_ot_bulk_conversion_m2m_cmdb_group** zu erstellen.
 - a. Navigieren zu **Alle > Industrial Workspace-Administrator > OT-Manager-Administrator > Automatisierte IT-OT-Massenkonvertierung – CMDB-Gruppen verwenden**.
 - b. Wählen Sie **Neu**.
 - c. Wählen Sie im Feld **Automatisierte Massenkonzertierung von IT in OT** den in Schritt 2 erstellten Datensatz aus.
 - d. Wählen Sie im Feld **CMDB-Gruppe** den in Schritt 1 erstellten CMDB aus.
 - e. Wählen Sie **Absenden**.
Der Datensatz ordnet die Gruppe CMDB dem Datensatz „Automatisierte Massenkonzertierung von IT in OT“ zu.

Wenn Sie beispielsweise OT-Entitätsdetails für alle Computer hinzufügen möchten, auf denen eine bestimmte HISTORIAN-Software installiert ist, müssen Sie eine CMDB-Gruppe erstellen, die diesen Filterkriterien entspricht. Erstellen Sie dann eine geplante Aufgabe, und verknüpfen Sie sie mit der CMDB-Gruppe für Computer, auf denen HISTORIAN-Software installiert ist.

Operational Technology Manager-Referenz

Referenzthemen enthalten zusätzliche Informationen zur Anwendung Operational Technology Manager.

Mit Operational Technology Manager installierte Komponenten

Bei der Aktivierung der Anwendung Operational Technology Manager können verschiedene Arten von Komponenten installiert werden, einschließlich Anwenderrollen.

Hinweis:

In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter [Komponenten finden, die mit dieser Anwendung installiert wurden](#) .

Installierte Plugins

Plugin	Beschreibung
Industrial Core	Enthält die für das OT Service Graph Connector erforderlichen Klassenzuordnungen.

Installierte Rollen

Rolle	Beschreibung
Operational Technology Discovery -Administrator [ot_discovery_admin]	Kann den Prozess Discovery für den Prozess Operational Technology ausführen, aber nicht auf Configuration Management Database (CMDB) zugreifen, um die Configuration Items (CIs) und die zugehörigen Entitäten Operational Technology (OT) anzuzeigen, die aus erkannten Elementen erstellt wurden. Weitere Informationen finden Sie unter Erstellen Sie einen Discovery-Zeitplan Operational

Rolle	Beschreibung
	Technology , und führen Sie den Prozess Discovery aus.
Operational Technology Manager Betrachter [cmdb_ot_viewer]	Schreibgeschützter Zugriff auf Gerätedatensätze von Operational Technology (OT).
Operational Technology Manager -Editor [cmdb_ot_editor]	Erstellen, Lesen, Aktualisieren und Löschen von Zugriffsrechten für Erweiterungsklassen von Operation Technology (OT) ↗ .
Operational Technology Manager Administrator [cmdb_ot_admin]	Zugriffsrechte für Operational Technology (OT)-Gerätedatensätze erstellen, lesen, aktualisieren und löschen. Kann auch bestimmte Konfigurationen im OT-Entitätstyp bearbeiten und verwalten. Weitere Informationen finden Sie unter Erweiterungsklassen für Operation Technology (OT) ↗ .

Installierte Software für Operational Technology-Management

Die installierte Software für die Lösung Operational Technology-Management stammt von Discovery für Operational Technology (OT) oder von OT-zertifizierten Service Graph Connectors, die installierte Software unterstützen.

Übersicht über installierte Software

Die für ein CI installierte Software variiert je nachdem, ob Sie die Anwendung Software Asset Management (SAM) installiert haben. Die folgenden Tabellen werden erstellt, wenn SAM aktiviert wird:

- Software-Discovery-Modell [cmdb_sam_sw_discovery_model]
- Softwaremodell [cmdb_software_product_model]
- Softwareinstallation [cmdb_sam_sw_install]

Weitere Informationen dazu, wie sich die Tabellenstruktur für die Verwaltung von Softwareinstallationen bei aktiviertem SAM verhält, finden Sie unter [Discovery with Software Asset Management](#) [↗](#).

Sie können ein Computer-CI auch so konfigurieren, dass Daten Software Asset Management angezeigt werden. Weitere Informationen finden Sie unter [Configure a CI to display Software Asset Management data](#) [↗](#).

Zeigen Sie installierte Software für OT-Geräte an

Sie können die installierte Software für OT-Geräte im Industriell Arbeitsbereich an folgenden Stellen anzeigen:

- Liste **Auf OT-Geräte installierte Software**, indem Sie zu navigieren **Alle > Operative Technologien (OT) > Auf OT-Geräten installierte Software**.
- Liste „**Auf OT-Geräten installierte Software**“ in der Listenansicht Industriell Arbeitsbereich unter dem Modul „**Operative Technologie (OT)**“.
- Liste „**Software installiert**“ unter der Registerkarte „**Zugehörige Datensätze**“ in einem OT-Gerät-Datensatz.

Modellkategorien für Operational Technology

Wenn Konfigurationselemente (CIs) in CMDB erstellt werden, werden Asset-Datensätze erstellt. Der Asset-Datensatz enthält die Modellkategorie für das CI.

In der folgenden Tabelle werden die für Operational Technology (OT) verfügbaren Modellkategorien und ihre CI-Klasse beschrieben.

OT-Modellkategorien

Name	CI-Klasse
Industriell	N/V
Industriell Allgemein	Operative Technologien (OT) [cmdb_ci_ot]
Betriebsmittel	Betriebsmittel [cmdb_ci_oe]
OT-Steuerung	OT-Steuerungssystem [cmdb_ci_ot_control]
OT-Steuerung für 3D-Drucker	3D-Industriedrucker [cmdb_ci_ot_industrial_3d_printer]
OT-Steuerung (CNC).	CNC [cmdb_ci_ot_cnc]
OT-Steuerungs-DCS	DCS [cmdb_ci_ot_dcs]
OT-Steuerungs-DPU	DPU [cmdb_ci_ot_dpu]
OT-Steuerungs-IED	IED [cmdb_ci_ot_ied]
OT-Steuerungsmodul	OT-Steuerungsmodul [cmdb_ci_ot_control_module]
OT-Steuerungs-SPS	SPS [cmdb_ci_ot_plc]
OT-Steuerungs-RTU	RTU [cmdb_ci_ot_rtu]
OT-Steuerungs-SCADA	SCADA-Server [cmdb_ci_ot_scada_server]
OT-Steuerungsserver	OPC-Server [cmdb_ci_ot_opc_server]
OT-Feldaktuator	Industrieaktuator [cmdb_ci_ot_industrial_actuator]
OT-Feldgerät	OT-Feldgerät [cmdb_ci_ot_field_device]
OT-Feldlaufwerk	Industrielaufwerk [cmdb_ci_ot_industrial_drive]
OT-Feld-Robot	Industrierobot [cmdb_ci_ot_industrial_robot]
OT-Feldsensor	Industriesensor [cmdb_ci_ot_industrial_sensor]
OT-Aufsicht	OT-Überwachungssystem [cmdb_ci_ot_Supervisory]
OT-Aufsichts-EWS	EWS [cmdb_ci_ot_ews]
OT-Überwachungs-Historiker	Historian [cmdb_ci_ot_historian]
OT-Überwachungs-HMI	HMI [cmdb_ci_ot_hmi]
OT-Überwachungs-OPC	OPC-Client [cmdb_ci_ot_opc_client]
OT-Überwachungs-SCADA	cmdb_ci_ot_scada_client

APIs für die Konvertierung von IT in OT und OT in IT

Es gibt 2 APIs, die für die Verarbeitung von Aktualisierungs-Workflow-Szenarien für die Konvertierung von IT in Operational Technology (OT) und umgekehrt mit der Anwendung OT Asset-Management verwendet werden.

APIs, die in verwendet werden OT Asset-Management

Mit OT Asset-Management müssen Sie die Synchronisierung zwischen Asset und Configuration Item (CI) für OT-Assets aufrechterhalten. Die folgenden APIs werden für die Konvertierung von IT in OT und in der Anwendung OT Asset-Management verwendet.

i Hinweis:

Die IT CI-Klasse wird nicht geändert. Stattdessen wird ein OT-Entitätsdatensatz hinzugefügt, der den OT-Gerät-Kontext bereitstellt.

- Konvertieren Sie IT in eine OT-Asset-API
- Konvertieren Sie OT in IT-Asset-API

Konvertieren Sie IT in eine OT-Asset-API

Die API „IT in OT-Asset konvertieren“ wird in Aktualisierungs-Workflows verwendet, in denen ein OT-Configuration Item (CI) durch ein neues CI ersetzt wird. Diese API erstellt ein Replikat des vorherigen OT-Entitätsdatensatzes und ordnet sie dem neuen CI zu. Im vorherigen CI und im zugehörigen OT-Entitätsdatensatz treten keine Changes auf. Sowohl das neue CI als auch die vorherigen CI-Referenzen werden mit dieser API verwendet.

Konvertieren Sie OT in IT-Asset-API

Die API zum Konvertieren von OT in IT-Asset wird verwendet, wenn ein Asset ersetzt werden muss. Die API löscht den OT-Entitätsdatensatz des übergebenen CI.

Weitere Informationen zur Synchronisierung von Assets und Configuration Item (CI) für Operational Technology-Assets (OT) finden Sie unter [Asset and Configuration Item \(CI\) synchronization for Operational Technology \(OT\) assets](#) .

Weitere Informationen zu OT Asset-Management finden Sie unter [OT Asset Management](#) .

Zugehörige Informationen

Weitere Informationen zur Erweiterungsklasse des Netzwerkangriffserkennungssystems (Network Intrusion Detection System, NIDS), zu OT-Erweiterungsklassen und zu zugehörigen Anwendungen.

Übersicht über Erweiterungsklassen

Die Erweiterungsklassen helfen Ihnen zu verstehen, wie Operational Technology-Management mit Configuration Management Database (CMDB) funktioniert.

Network Intrusion Detection System (NIDS) CI extension class

Die Klasse des Netzwerkangriffserkennungssystems (Network Intrusion Detection System, NIDS) [cmdb_ci_nids] erstellt die Beziehungen zwischen passiven Netzwerküberwachungsgeräten und den Geräten im Netzwerk, die erkannt werden.

Operational Technology (OT) extension classes

Configuration Management Database (CMDB) aktualisiert Klassen für OT.

Zugehörige Anwendungen

CMDB CI Class Models

Die Store-App CMDB CI-Klassenmodelle fügt Klassenmodelle hinzu, die die Klassenhierarchie CMDB erweitern, einschließlich Klassenbeschreibungen, Identifizierungsregeln, Bezeichnereinträge und abhängige Beziehungen.

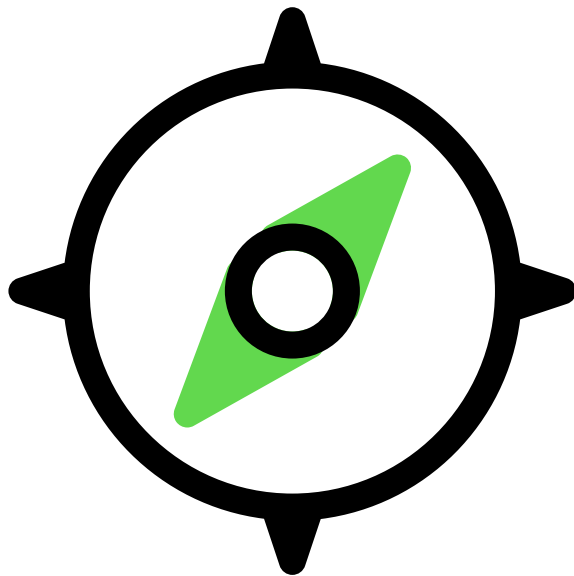
Prozessmanager Industrie

Verwenden Sie die Anwendung Prozessmanager Industrie, um die Datengrundlage des Anlagenmodells nach ISA-95 zu erstellen, die für die Lösung ServiceNow® Operational Technology erforderlich ist. Mit Prozessmanager Industrie können Sie Ihre eigene Version der Anlagenmodelle an jedem Ihrer Standorte erstellen.

Hinweis:

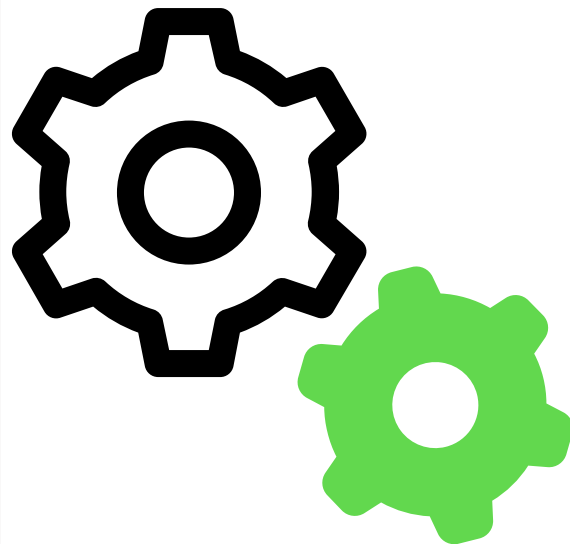
Der Manufacturing Process Manager wurde in Industrieprozessmanager für Vancouver umbenannt. Wenn Sie Version 1.0.9 und älter verwenden, heißt die Anwendung weiterhin Manufacturing Process Manager. Version 2.0 lautet die Anwendung Prozessmanager Industrie.

Untersuchen



Erfahren Sie, wie Hersteller den
verwenden Prozessmanager Industrie

Konfigurieren



Planen und konfigurieren
Sie Ihre -Implementierung

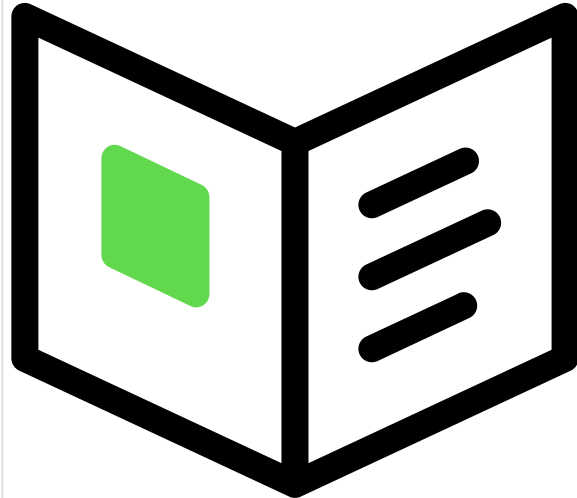
Automatische Übersetzung

Verwenden



Überprüfen Sie die Entitäten für Geräte und Anlagenmodell von Operational Technology

Referenz



Erhalten Sie Details zu zugehörigen Informationen und Anwendungen.

Automatische Übersetzung

Prozessmanager Industrie erkunden

Erfahren Sie mehr über gängige Begriffe, Akronyme und den Branchenstandard Anlagenmodell ISA-95, die in Prozessmanager Industrie verwendet werden.

Prozessmanager Industrie – Übersicht

Sehen Sie sich eine Übersicht über die Anwendung Prozessmanager Industrie an.

[https://player.vimeo.com/video/1044353688?](https://player.vimeo.com/video/1044353688?h=eba3593d47&badge=0&autopause=0&player_id=0&app_id=58479)

[h=eba3593d47&badge=0&autopause=0&player_id=0&app_id=58479](https://player.vimeo.com/video/1044353688?h=eba3593d47&badge=0&autopause=0&player_id=0&app_id=58479)

Prozessmanager Industrie gängige Terminologie

Bevor wir mit Prozessmanager Industrie beginnen, sehen wir uns einige gängige Begriffe und Akronyme an, die in diesem Inhalt verwendet werden.

Häufig verwendete Begriffe und Akronyme

Benennung	Akronym	Definition
Operational Technology	OT	Technologie, die für die industrielle Automatisierung zur Steuerung physischer Prozesse verwendet wird. i Hinweis: Operational Technology ist nicht das Internet der Dinge (IoT).

Häufig verwendete Begriffe und Akronyme (Fortsetzung)

Benennung	Akronym	Definition
Internationale Gesellschaft für Automatisierung	ISA	Organisation, die die Standards für Industrieunternehmen veröffentlicht, einschließlich des Anlagenmodells nach ISA-95.
Extrahieren, Transformieren, Laden	ETL	Allgemeiner Begriff, der verwendet wird, um Daten aus einem Quellsystem zu übernehmen, sie zu transformieren und dann in ein Zielsystem hochzuladen.

Anlagenmodell nach ISA-95

Das Anlagenmodell nach ISA-95 ist ein Branchenstandard, der eine Industrieanlage und die darin enthaltenen Produktionsgeräte darstellt. Sie können die Anlagenmodell-Entitäten in Ihren Einrichtungen beschreiben, indem Sie eine Anlagenmodell-Vorlage mit verschiedenen Ebenen und Ebenentypen definieren.

Mit dieser Vorlage können Sie die folgenden Aktionen ausführen:

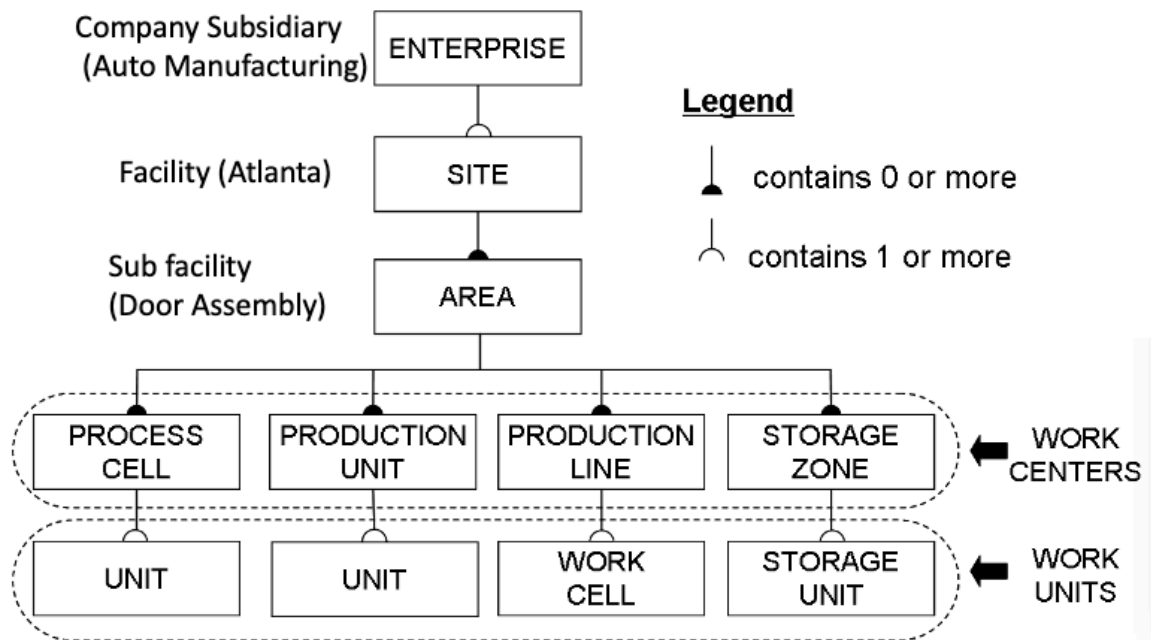
- Ordnen Sie Ihre Anlagenmodell-Entitäten zu. Mit dieser Zuordnung erstellen Sie eine hierarchische Struktur.
- Erstellen Sie mehrere Anlagenmodelle für mehrere Industriestandorte.
- Weisen Sie jedem Standort Benutzer zu, damit Sie deren Zugriff auf die Anlagenmodell-Informationen für bestimmte Standorte verwalten können. Beispielsweise können Sie festlegen, dass Benutzer in Atlanta nur auf die Informationen des Standorts Atlanta zugreifen können, nicht jedoch auf die Daten eines Standorts in Atlanta. Weitere Informationen finden Sie unter [Gewähren Sie Nicht-Administratoren Zugriff auf den Anlagenmodell-Standort, oder entfernen Sie ihn](#).

Die Anlagenmodelle beginnen auf Site-Ebene und enthalten eine detaillierte hierarchische Struktur, die jeden Industriestandort beschreibt. Um diese Daten in einer hierarchischen Sequenz zu strukturieren, wenden Sie eine Anlagenmodell-Vorlage an.

Die folgende Grafik ist ein Beispiel für die Standardvorlage ISA-95, die Sie erhalten, wenn Sie Prozessmanager Industrieeinstallieren. Diese Grafik zeigt eine Anlage in Atlanta, in der Autos hergestellt werden.

- Die untergeordneten Stockwerke unterhalb eines Standorts repräsentieren den Türkomponentenbereich, die zugehörigen untergeordneten Arbeitszentren und Arbeitseinheiten.
- Die Ebenen „Arbeitszentren“ und „Arbeitseinheit“ haben jeweils Ebenentypen. In diesem Modell gibt es vier verschiedene Ebenentypen für die Ebene „Arbeitszentrum“:
 - Prozesszelle
 - Produktionseinheit
 - Produktionslinie
 - Speicherzone

Beispiel für eine Anlagenmodell-Vorlage



Anlagenmodell-Vorlagen

Sie können Anlagenmodell-Vorlagen erstellen, die Sie verwenden, um ein Anlagenmodell zu charakterisieren oder die Daten zu strukturieren, die Ihre physische Industrieanlage beschreiben, indem Sie ähnliche Arten von Anlagenmodell-Entitäten gruppieren.

Eine Anlagenmodell-Vorlage besteht aus den folgenden Komponenten:

Anlagenmodell-Vorlage

Name und Beschreibung der Anlagenmodell-Vorlage.

Hierarchieebenen für Anlagenmodell-Vorlagen

Zugewiesene hierarchische Ebenen, die zum Sortieren und Strukturieren der Daten des Anlagenmodells verwendet werden.

Hierarchische Ebenentypen für Anlagenmodell-Vorlagen

Typen, die verschiedene Typen der Bereiche, Funktionen oder Produktionsprozesse innerhalb einer Hierarchieebene darstellen.

Weitere Informationen zu Anlagenvorlagen und ein grafisches Beispiel ihrer Struktur finden Sie unter [Anlagenmodell nach ISA-95](#) und [Anlagenmodell-Vorlagen definieren](#).

Prozessmanager Industrie konfigurieren

Konfigurieren Sie die Anwendung Prozessmanager Industrie, um die Anlagenmodell-Datengrundlage zu erstellen, die für die Lösung ServiceNow® Operational Technology erforderlich ist.

i Hinweis:

Wenn Sie über die Administratorrolle verfügen, können Sie das geführte Setup Industriell verwenden, um sich durch das Setup der Anwendung Prozessmanager Industrie führen zu lassen.

Um auf das geführte Setup zuzugreifen, navigieren Sie zu **Industrial Workspace-Administrator > Geführtes Setup**.

Aufgabe	Zweck
1. Installieren Sie Prozessmanager Industrie von ServiceNow Storeaus.	Installiert die Anwendung Prozessmanager Industrie und unterstützende Plugins.
2. Weisen Sie Prozessmanager Industrie Rollen zu.	Weist Rollen zu, um die für jeden Benutzer verfügbaren Aktionen zu steuern.
3. Füllen Sie eine Microsoft Azure Event Hubs Excel-Tabelle für Service Graph den Connector-Import aus.	Erstellt eine Excel-Tabelle Microsoft Azure Event Hubs und füllt sie mit Ihren vorhandenen Daten des Anlagenmodells nach ISA 95, um sie in Now Plattformhochzuladen.
4. Importieren Sie Ihre Excel-Tabelle.	Lädt Ihre vorhandenen Daten des Anlagenmodells nach ISA-95 in Configuration Management Database (CMDB)hoch.
5. Installieren Sie Service Graph-Connectors [service-graph], die von ServiceNow®-Partnern bereitgestellt werden, und importieren Sie die Anlagenmodell-Daten mithilfe der Integrationen.	Installiert ServiceNow Connectors, die von Partnern bereitgestellt werden, sobald sie in ServiceNow® Storeverfügbar sind, und importiert Anlagenmodell-Daten.
6. Gewähren Sie Benutzern mit nicht administrativen Rollen Zugriff auf den Anlagenmodell-Standort.	Weist Anwendern mit zugewiesenen Rollen „cldb_ot_isa_viewer“ oder „cldb_ot_isa_editor“ Zugriff auf den Standort zu oder entfernt ihn.
Optional: Automatisieren Sie die Zuordnung von OT-Geräten	Automatisiert die Zuordnung von OT-Geräten zum Produktionsprozess. i Hinweis: Zum Aktivieren der Zuordnungsfunktion sind die folgenden Plugins erforderlich: • Operational Technology Manager • Prozessmanager Industrie

Prozessmanager Industrie installieren

Wenn Sie über die erforderliche Berechtigung und die Administratorrolle verfügen, können Sie die Anwendung Prozessmanager Industrie und die zugehörigen Plugins installieren.

Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter [Rufen Sie eine Berechtigung für ab ServiceNow Produkt oder Anwendung](#).

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die folgenden Elemente werden mit Prozessmanager Industrie installiert:

- Plugins
- Anwendungsmenü, einschließlich Geführtes Setup
- Rollen
- Tabellen

Weitere Informationen zum Anzeigen der mit der Anwendung Prozessmanager Industrie installierten Komponenten finden Sie unter [Mit Prozessmanager Industrie installierte Komponenten](#).

i Hinweis:

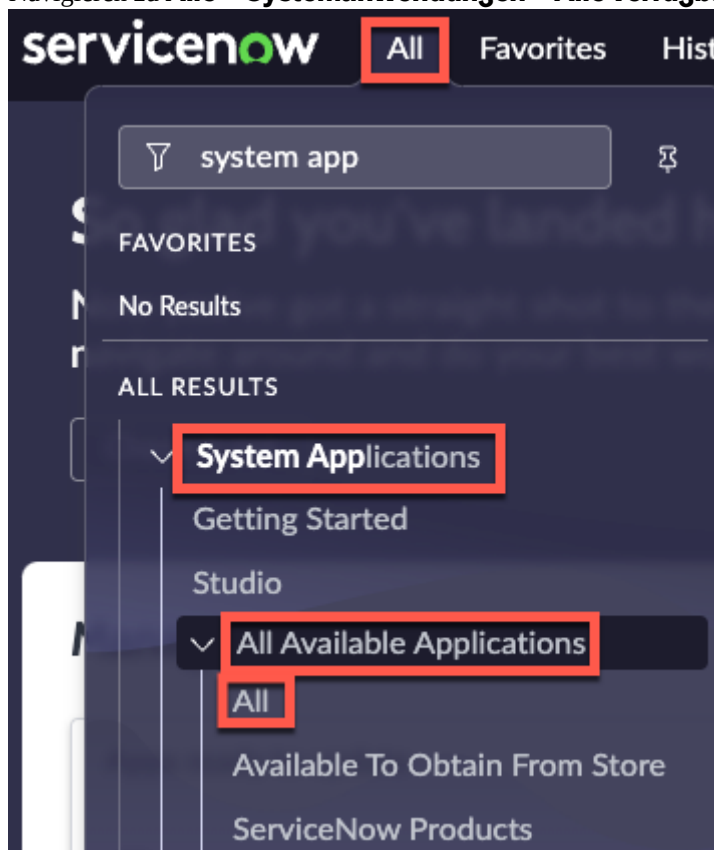
Beachten Sie für Operational Technology Service Management -Benutzer ohne Lizenz für Operational Technology -Transparenz Folgendes:

- Wenn Sie die neueste Version von Incident-Management für operative Technologie installiert haben, wird auch Prozessmanager Industrie installiert.
- Wenn Sie die neueste Version von Change-Management für operative Technologie installiert haben, wird auch Prozessmanager Industrie installiert.

Sie sollten ein Upgrade auf die neuesten Versionen durchführen, um Zugriff auf die Experience Operational Technology Service Management zu erhalten.

Prozedur

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



2. Suchen Sie die Anwendung Prozessmanager Industrie mithilfe der Filterkriterien und der Suchleiste.

Sie können nach der Anwendung anhand ihres Namens oder ihrer ID suchen. Wenn Sie die 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. Überprüfen Sie im Dialogfeld „Anwendungsinstallation“ die Anwendungsabhängigkeiten.

Abhängige Plugins und Anwendungen werden angezeigt, wenn sie installiert werden, derzeit installiert sind oder installiert werden müssen. Wenn Plugins oder Anwendungen installiert werden müssen, müssen Sie sie installieren, bevor Sie Prozessmanager Industrieeinstallieren können.

4. **Wahlweise:** Wenn Demodaten verfügbar sind und Sie diese installieren möchten, aktivieren Sie das Kontrollkästchen **Demodaten laden**.

Demodaten sind Beispieldatensätze, die Anwendungsfunktionen für die gängigen Anwendungsfälle veranschaulichen. Laden Sie die Demodaten, wenn Sie die Anwendung zum ersten Mal auf einer Entwicklungs- oder Testinstanz installieren.

i Wichtig:

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

5. Wählen Sie **Installieren** aus.

Administrator für den industriellen Arbeitsbereich Anwendungs Menü und im geführten Setup

Nachdem Sie die Anwendung und die zugehörigen Plugins installiert haben, können Sie über das Anwendungs Menü Administrator für den industriellen Arbeitsbereich auf die zugehörigen Funktionen Operational Technology Manager, Prozessmanager Industrie, Incident-Management für operative Technologie, Operational Technology Vulnerability Response, Change-Management für operative Technologie, Knowledge Management für operative Technologie und Anforderungsmanagement für operative Technologie zugreifen.

Administrator für den industriellen Arbeitsbereich Inhalte des Anwendungs Menüs

Um auf das Anwendungs Menü Administrator für den industriellen Arbeitsbereich zuzugreifen, geben Sie im Anwendungsnavigator Industrial Workspace Administrator ein. Die Lösung Operational Technology-Management besteht derzeit aus den folgenden Anwendungen und Funktionen:

- Operational Technology Manager
- Prozessmanager Industrie
- Operational Technology Vulnerability Response
- Incident-Management für operative Technologie
- Change-Management für operative Technologie
- Knowledge Management für operative Technologie
- Anforderungsmanagement für operative Technologie

i Hinweis:

Sie müssen zuerst die Anwendungen Operational Technology Manager oder Prozessmanager Industrie installieren, bevor Sie Incident-Management für operative Technologie und Change-Management für operative Technologie verwenden können.

Die Optionen, die im Anwendungsmenü Administrator für den industriellen Arbeitsbereich angezeigt werden, hängen davon ab, welche OT-Anwendungen installiert sind und welche Rollen dem Benutzer zugewiesen sind. Wenn Prozessmanager Industrie installiert ist, sind im Anwendungsmenü Administrator für den industriellen Arbeitsbereich die folgenden Funktionen verfügbar:

- Geführtes Setup
- Alle OT-Eigenschaften
- Systemeigenschaften des Arbeitsbereichs
- Konfiguration der OT-Fortschrittsbewertungsliste
- Attribute der OT-Fortschrittsbewertungsliste
- OT-Manager, das die folgenden Auswahlmöglichkeiten enthält:
 - OT-Manager-Administrator
 - Industrial Process Manager
 - OT-Incident-Administrator
 - Change-Management für operative Technologie

Weitere Informationen zur Anwendungsinstallation und zu den zugewiesenen Rollen finden Sie unter [Prozessmanager Industrie installieren](#) und [Weisen Sie Prozessmanager Industrie Anwenderrollen zu](#).

Administrator für den industriellen Arbeitsbereich Geführtes Setup

Wenn Sie über die Administratorrolle verfügen, können Sie das geführte Setup verwenden, um sich durch das Setup der Anwendung Prozessmanager Industrie führen zu lassen.

Um auf das geführte Setup zuzugreifen, navigieren Sie zu **Industrial Workspace-Administrator > Geführtes Setup**.

Die einzelnen Schritte, die im geführten Setup als entsperrt angezeigt werden, hängen davon ab, welche Anwendungen Sie in Ihrer Instanz installiert haben.

Wenn nur Prozessmanager Industrie installiert ist, sind die folgenden Setup-Funktionen gesperrt:

- Die Setup-Schritte Industrial Workspace.
- Die Setup-Schritte Operational Technology Manager.
- Alle Prozessmanager Industrie -Schritte, die von Operational Technology Manager abhängen.
- Die Setup-Schritte Operational Technology Vulnerability Response.
- Die Setup-Schritte Incident-Management für operative Technologie.
- Die Setup-Schritte Change-Management für operative Technologie.
- Die Setup-Schritte Knowledge Management für operative Technologie.
- Die Setup-Schritte Anforderungsmanagement für operative Technologie.

Weitere Informationen zu geführten Setups und ihrer Verwendung finden Sie unter [Geführtes Setup verwenden](#) .

Weisen Sie Prozessmanager Industrie Anwenderrollen zu

Weisen Sie Ihren Benutzern Rollen zu, damit Sie ihren Zugriff auf die Funktionen, Fähigkeiten und Daten in der Anwendung Prozessmanager Industrie steuern können.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Benutzer mit den in der folgenden Tabelle aufgeführten Rollen können die Anwendung Prozessmanager Industrie verwenden.

Rolle	Beschreibung
Anlagenmodell-Betrachter [cmdb_ot_isa_viewer]	Kann nur die zugewiesenen Datensätze der Tabelle „Anlagenmodell nach ISA [cmdb_ci_ot_isa_entity] anzeigen. Weitere Informationen finden Sie unter Prozessmanager Industrie mit Operational Technology Managerverwenden und Anlagenmodelle verwalten .
Anlagenmodell-Editor [cmdb_ot_isa_editor]	Kann die zugewiesenen Datensätze im Anlagenmodell nach ISA [cmdb_ci_ot_isa_entity] anzeigen und bearbeiten. Weitere Informationen finden Sie unter Prozessmanager Industrie mit Operational Technology Managerverwenden und Anlagenmodelle verwalten .
Anlagenmodell-Administrator [cmdb_ot_isa_admin]	Sie erben die Rolle „cmdb_ot_isa_editor“ und können außerdem die folgenden Aktionen ausführen: • Verwenden Sie das geführte Setup für Industriell, um Prozessmanager Industrie und Operational Technology Managereinzurichten. • Bearbeiten Sie die Tabelleneinträge Anlagenmodell-Vorlage [isa_entity_template], [isa_entity_level] und Anlagenentitätstyp [isa_entity_type]. Weitere Informationen finden Sie unter Administrator für den industriellen Arbeitsbereich Anwendungsmenü und im geführten Setup .
Anlagenmodell-Ausfallzeitplaner [sn_isa_schedule_admin]	Kann Zeitpläne für Anlagenentitäten erstellen, ändern und löschen. Kann Zeitpläne auch mit Anlagenentitäten verknüpfen.
Anlagenmodell-Betrachter – Alle [cmdb_ot_isa_viewer_all]	Kann alle Datensätze des Anlagenmodells nach ISA (cmdb_ci_ot_isa_entity) und die zugehörigen Anlagenmodell-Vorlagendatensätze (isa_entity_template, isa_entity_level, isa_entity_type) anzeigen.

Rolle	Beschreibung
	In cmdb_ot_admin enthaltene Rolle.
Erstaunlicher Administrator [sn_ot_amaking_admin]	Kann OT-Subnetzdatensätze (ot_subnet_mapping) für alle OT-Subnetz-Systemeigenschaften der Anlagenmodell-Entität erstellen, ändern und löschen.
Erstaunlicher Editor [sn_ot_amaking_write]	Kann OT-Subnetzdatensätze (ot_subnet_mapping) für alle Anlagenmodell-Entitäten erstellen, ändern und löschen, die dem Anwender zugeordnet sind.
Erstaunlicher Betrachter [sn_ot_amaking_read]	Kann OT-Subnetzdatensätze (ot_subnet_mapping) für alle Anlagenmodell-Entitäten anzeigen.

Prozedur

Weisen Sie Benutzern und Gruppen mit der Benutzerverwaltungsfunktion Now Platform Rollen zu.

Zeigen Sie OT-Systemeigenschaften an, und bearbeiten Sie sie

Zeigen Sie alle mit Operational Technology (OT) verbundenen Systemeigenschaften für verschiedene -Anwendungen an, und bearbeiten Sie sie.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Systemeigenschaften für die folgenden OT-Anwendungen im Modul **Alle OT-Eigenschaften** im Now Platform ändern.

- Discovery für Operational Technology
- Prozessmanager Industrie
- Anlagenmodell nach ISA
- Operational Technology Manager
- Incident-Management für operative Technologie
- Knowledge Management für operative Technologie
- Change-Management für operative Technologie
- Industrial Workspace Common

Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > Alle OT-Eigenschaften**.
2. Wählen Sie in der Tabelle „Systemeigenschaften“ die Anwendung aus, deren Systemeigenschaften Sie bearbeiten möchten.
3. Bearbeiten Sie die verfügbaren Systemeigenschaften nach Bedarf für die Anwendung oder Funktion.
4. Wählen Sie **Aktualisieren**.

Anlagenmodell-Vorlagen definieren

Erstellen Sie Vorlagen, die Sie den Anlagenmodell-Entitäten zuweisen können, die Sie in Now Platform erstellt haben. Sie können diese Vorlagen verwenden, um ein Anlagenmodell zu charakterisieren oder die Daten zu strukturieren, die Ihre physische Industrieanlage beschreiben, indem Sie ähnliche Arten von Anlagenmodell-Entitäten gruppieren.

Erstellt eine Anlagenmodell-Vorlage

Erstellen Sie einen Anlagenmodell-Vorlagendatensatz, der die Verwendung der Vorlage identifiziert und beschreibt. Nachdem Sie eine Anlagenmodell-Vorlage erstellt haben, können Sie hierarchische Ebenen und Typen dafür erstellen.

Vorbereitungen

Erforderliche Rolle: cmdb_ot_isa_admin

Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > Industrial Process Manager > Anlagenmodell-Vorlage**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular „Anlagenmodell-Vorlage“.

Feld	Beschreibung
Name	Name der Anlagenmodell-Vorlage.
Beschreibung	Beschreibung der Anlagenmodell-Vorlage.
Anwendung	Ausgewählter Anwendungsbereich. Global wird angezeigt, wenn dieser Bereich der globale Anwendungsbereich ist.

4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Erstellen Sie hierarchische Sortierebenen für die Anlagenmodell-Vorlage.

Erstellen Sie hierarchische Sortierebenen für eine Anlagenmodell-Vorlage

Hierarchieebenen für Ihre Anlagenmodell-Vorlage erstellen und zuweisen. Wenn Sie einem Anlagenmodell eine Anlagenmodell-Vorlage zuweisen, sortieren und strukturieren diese Ebenen die darin angezeigten Daten.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Sie können einer Anlagenmodell-Vorlage zu Sortierzwecken Ebenen zuweisen. Sie können der Ausrüstung beispielsweise Standort-, Bereichs-, Arbeitsplatz- und andere Ebenen zuweisen und die Sortierreihenfolge für jede festlegen.

Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > Industrial Process Manager > Anlagenmodell-Vorlage**.
2. Wählen Sie eine Anlagenmodell-Vorlage aus.
3. Klicken Sie in der zugehörigen Liste Vorlagenebenen auf **Neu**.
4. Füllen Sie die Felder des Formulars aus.

Formular „Vorlagenebene“

Feld	Beschreibung
Ebenenname	Name der Ebene, der Sie das Anlagenmodell zuweisen. Beispiele: Site Ein Industriestandort Bereich Ein Bereich an einem Industriestandort. Arbeitsplatz Ein Arbeitsplatz an einem Industriestandort.
Übergeordnet	Bezeichner für die Anlagenmodell-Vorlagenebene über dieser Ebene. Wenn Sie sie leer lassen, ist diese Ebene die oberste Ebene im Modell. Sie können beispielsweise die folgenden Aktionen ausführen: ○ Wenn Sie eine Standortebene erstellen, lassen Sie dieses Feld leer, wenn es sich um die oberste Ebene der Anlagenmodell-Hierarchie handelt, die kein übergeordnetes Element aufweist. ○ Wenn Sie eine Bereichsebene erstellen, die der Site-Ebene untergeordnet ist, wählen Sie Site als übergeordnetes Element aus. ○ Wenn Sie eine Arbeitsplatzebene erstellen und diese der Bereichsebene untergeordnet ist, wählen Sie „Bereich“ als übergeordnetes Element aus.
Anwendung	Ausgewählter Anwendungsbereich. Global wird angezeigt, wenn dieser Bereich der globale Anwendungsbereich ist.
Vorlage	Name der ausgewählten Anlagenmodell-Vorlage.
Reihenfolge	Zahl, die die Position der Ebene in der Anlagenmodell-Hierarchie zu Sortierzwecken angibt. Die kleinste eingegebene Zahl stellt die höchste hierarchische Ebene dar. Geben Sie beispielsweise 1 für Standort ein, wenn der

Feld	Beschreibung
	Standort die höchste Ebene in der Hierarchie für die Anlagenmodell-Vorlage darstellt.

5. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Erstellen Sie granulare Typen innerhalb der Hierarchieebene einer Anlagenmodell-Vorlage.

Erstellen Sie Ebenentypen für Anlagenmodelle

Erstellen Sie granulare Ebenentypen innerhalb jeder Anlagenmodell-Vorlagenebene, die Sie erstellt haben. Die Typen der granularen Ebene, die Sie innerhalb dieser Ebene erstellen, beschreiben die Art der darin enthaltenen Produktionsprozesse.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Sie können Typen erstellen, die die verschiedenen Arten von Standorten, Bereichen oder Funktionen innerhalb einer Ebene darstellen. In der Vorlage ISA 95 weist die Ebene „Arbeitszentrum“ beispielsweise die folgenden Ebenentypen auf:

- Produktionszelle
- Produktionseinheit
- Produktionszone
- Speicherzone

Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > Industrial Process Manager > Anlagenmodell-Vorlage**.
2. Wählen Sie eine Anlagenmodell-Vorlage aus.
3. Wählen Sie in der zugehörigen Liste Vorlagenebenen eine Anlagenmodell-Vorlagenebene aus.
4. Klicken Sie in der zugehörigen Liste Vorlagentypen auf **Neu**.
5. Füllen Sie die Felder des Formulars aus.

Formular „Vorlagenebenentyp“.

Feld	Beschreibung
Ebenentypname	Name des Ebenentyps, den Sie der ausgewählten Anlagenmodell-Vorlagenebene zuweisen. Sie weisen beispielsweise eine Produktionszelle zu, um einen Produktionszellentyp für eine Arbeitsplatzebene zu erstellen.
Ebenenname	Name der ausgewählten Anlagenmodell-Vorlagenebene.
Anwendung	Ausgewählter Anwendungsbereich. Global wird angezeigt, wenn dieser Bereich der globale Anwendungsbereich ist.

Feld	Beschreibung
Vorlage	Name der ausgewählten Anlagenmodell-Vorlage.

6. Klicken Sie auf **Absenden**.

Anlagenmodell-Daten werden importiert

Mit der Funktion für geplante Importe können Sie Ihre vorhandenen Anlagenmodell-Daten aus einer ausgefüllten Microsoft Azure Event Hubs Excel-Tabelle importieren. Sie können es verwenden, um Daten Ihres Anlagenmodells nach ISA-95 in Configuration Management Database (CMDB) zu importieren.

Sie müssen Prozessmanager Industrie installieren, bevor Sie Anlagenmodell-Daten importieren.

Für den Import der Anlagenmodell-Daten in Now Platform stehen mehrere Methoden zur Verfügung:

1. Wenn Sie die Tabelle zum Importieren der Daten verwenden, müssen Sie die Microsoft Excel-Tabelle mit Ihren vorhandenen Daten des Anlagenmodells nach ISA-95 füllen und den geplanten Import **von SG-Anlagenmodell mit Tabellenkalkulation** ausführen. Viele veraltete Datensatzsysteme enthalten Funktionen, mit denen Sie diese Daten in eine Excel-Tabelle exportieren können, ohne sie manuell ausfüllen zu müssen.
2. Mehrere ServiceNow -Partner entwickeln auch Integrationen für veraltete Datensatzsysteme von Drittanbietern, die Anlagenmodell-Daten speichern.
 - Sobald diese Integrationen verfügbar sind, können Sie sie unter ServiceNow Store finden, indem Sie nach Operational Technology zertifizierten Integrationen für Prozessmanager Industriesuchen.
 - Installieren Sie die Integrationen, die für Ihre Umgebung geeignet sind, und führen Sie sie nach Bedarf aus.

Mit diesen Importmethoden können Sie vorhandene Anlagenmodelle in Now Platform bei Bedarf mit den in Ihrer autorisierenden Quelle gespeicherten Daten aktualisieren. Für neu importierte Daten erstellt Now Platform automatisch CI-Klassendatensätze für Anlagenmodell-Entitäten in Configuration Management Database (CMDB).

Systemeigenschaften, die sich auf die Verarbeitung des Imports auswirken

Die folgenden Systemeigenschaften wirken sich darauf aus, wie Sie Ihre Excel-Tabelle Microsoft Azure Event Hubs mit Anlagenmodell-Daten füllen und wie der Prozess „Anlagenmodell importieren – ETL“ funktioniert.

sn_isa_model.cmdb_relationships_sync_levels

Bestimmt, wie viele Ebenen eines Anlagenmodells in Now Platform importiert werden können und dann in Configuration Management Database (CMDB) synchronisiert werden. Der Standardwert ist 8.

sn_isa_model.short_code_validation_max_length

Legt die maximale Länge für die Spalte Kurzwahl in Ihrer Tabelle fest. Der Standardwert ist 3.

sn_isa_model.user_search_matching_attribute

Entspricht den Benutzerdatenreferenzen, die aus der gefüllten Tabelle importiert werden, mit den entsprechenden Benutzerdatensätzen, die in der Tabelle „Systemanwender“ [sys_user] gespeichert sind. Standardmäßig wird die E-Mail-Adresse des Benutzers verwendet, da die E-Mail-Adresse für jeden Benutzerdatensatz eindeutig ist.

glide.scriptable.excel.max_file_size

Legt die maximale Größe einer Excel-Datei in Byte fest. Diese Eigenschaft ist global.

***i* Hinweis:**

Weitere Informationen zum Hinzufügen oder Erstellen von Systemeigenschaften zur Steuerung des Systemverhaltens finden Sie [unter Systemeigenschaft hinzufügen](#) .

Füllen Sie Ihre Excel-Tabelle MicrosoftMicrosoft Azure Event Hubs mit Anlagenmodell-Daten aus

Erstellen Sie eine Excel-Tabelle MicrosoftMicrosoft Azure Event Hubs, und füllen Sie sie mit Ihren vorhandenen Daten für das Anlagenmodell nach ISA aus. Die Positionierung Ihrer vorhandenen Daten in den richtigen Spalten ist entscheidend für den Erfolg Ihres Uploads.

Um eine Excel-Tabelle MicrosoftMicrosoft Azure Event Hubs zu erstellen, die Configuration Management Database (CMDB) in Now Plattformordnungsgemäß ausfüllt, führen Sie die folgenden Aktionen aus:

1. Bereiten Sie Ihre Tabelle für den Upload vor, indem Sie die Excel-Tabelle MicrosoftMicrosoft Azure Event Hubs verwenden, die an den Datenquellen-Datensatz angehängt ist. Um eine leere Vorlage zu finden, gehen Sie wie folgt vor:

- a. Navigieren zu **Anlagenmodell – ISA > Importieren von Geräten Modell: Datenquelle**
- b. Klicken Sie auf **Anlagenmodell importieren – Datenquelle – v2.xlsx**

***i* Hinweis:**

Alternativ können Sie zum Herunterladen der Tabelle „**Import Anlagenmodell – Datenquelle – v2.xlsx**“ die [Microsoft Excel-Tabellen lesen, die für den Artikel „Anlagenmodell nach ISA Excel Service Graph Connector“ \[KB0966600\] erforderlich sind](#),  in der Now Support Knowledge Base.

2. Laden Sie die angehängte Tabelle „Anlagenmodell importieren – Datenquelle – v2.xlsx“ herunter, um mehr über die Vorlage und ihre Arbeitsblätter zu erfahren:

***i* Hinweis:**

Wenn Sie ein ISA SGC-Benutzer sind, der ein Upgrade von v1 auf v2 durchführt, lesen Sie den Abschnitt „**Upgrade von v1 auf v2**“ weiter unten.

Anlagenmodell importieren – Datenquelle – v2.xlsx-Tabelle

Arbeitsblattname	Zweck
Leere Vorlage für Datenimport	Füllt Ihre Anlagenmodell-Daten für den Import aus. Detaillierte Beispiele finden Sie im Rest dieses Themas.
Beschreibungen der Datenspalte	Stellt Beschreibungen der Datenspalten in der Tabelle bereit, ähnlich den Informationen in diesem Thema.
Beispieldaten für Import	Stellt ein Beispiel für ein Anlagenmodell für den Import in die Tabelle bereit. Sie können diese Beispiele im Rest dieses Themas anzeigen.

3. Nachdem Sie die Excel-Tabelle MicrosoftMicrosoft Azure Event Hubs ausgefüllt haben, speichern Sie sie an einem bekannten Ort, damit Sie leicht darauf zugreifen können, wenn Sie die ETL-Funktion IntegrationHub ausführen.

***i* Hinweis:**

Spaltennamen können nicht geändert werden. Sie können zusätzliche Spalten hinzufügen, um zusätzliche Felder für die eindeutige Identifizierung von Besitzern zu unterstützen, wie in der Systemeigenschaft `sn_isa_model.user_search_matching_attribute` festgelegt.

Tabelle wird gefüllt

Beispieldaten für operative Technologie, Spalten A bis J

Sie können Daten von mehreren Sites in einer einzigen Tabelle importieren. Das Beispielfeld zeigt Daten für zwei Sites: ATL und CTL.

	A	B	C	D	E	F	G	H	I	J
1	Path	Short Code	Entity Name	Location	Assigned to	Support Group	Description	Process criticality	Company	Template
2	ATL	ATL	Atlanta Site	Atlanta Car Facility	fred.luddy@example.com	Atlanta Plant Support	the site in Atlanta where we make cars	1 - most critical	Demo Car Corp	ISA 95 Default Template
3	ATL-B64	B64	Building 64	Atlanta Building 64	fred.luddy@example.com	Atlanta Plant Support	the building with the number 64 on the side	1 - most critical	Demo Car Corp	ISA 95 Default Template
4	ATL-B42	B42	Building 42	Atlanta Building 42	fred.luddy@example.com	Atlanta Plant Support	similar to building 64 except with a 42 on the side	2 - somewhat critical	Demo Car Corp	ISA 95 Default Template
5	ATL-B64-MASS	MASS	Model M	Atlanta Building MASS	fred.luddy@example.com	Atlanta Plant Support	model S needs to be assembled somewhere	1 - most critical	Demo Car Corp	ISA 95 Default Template
6	ATL-B64-QASS	QASS	Model Q	Atlanta Building QASS	fred.luddy@example.com	Atlanta Plant Support	a place for the Q model to get assembled	1 - most critical	Demo Car Corp	ISA 95 Default Template
7	ATL-B64-MPROD	MPROD	Model MPROD	Atlanta Building MPROD	fred.luddy@example.com	Atlanta Plant Support	Model S also needs a production line	1 - most critical	Demo Car Corp	ISA 95 Default Template
8	ATL-B64-QPROD	QPROD	Model QPROD	Atlanta Building QPROD	fred.luddy@example.com	Atlanta Plant Support	Model Q production line	1 - most critical	Demo Car Corp	ISA 95 Default Template
9	ATL-B42-MQSTOR	MQSTOR	Model M and Q	Atlanta Building MQSTOR	fred.luddy@example.com	Atlanta Plant Support	storage for the models we built	2 - somewhat critical	Demo Car Corp	ISA 95 Default Template
10	ATL-B64-QPROD-C1	C1	Cell 1	Atlanta Building C1	fred.luddy@example.com	Atlanta Plant Support	Q prod assembly cell 1	1 - most critical	Demo Car Corp	ISA 95 Default Template
11	ATL-B64-QPROD-C2	C2	Cell 2	Atlanta Building C2	fred.luddy@example.com	Atlanta Plant Support	Q prod assembly cell 2	1 - most critical	Demo Car Corp	ISA 95 Default Template
12	ATL-B42-MQSTOR-Z1	Z1	Zone 1	Atlanta Building Z1	fred.luddy@example.com	Atlanta Plant Support	storage zone for MQ for transfer	2 - somewhat critical	Demo Car Corp	ISA 95 Default Template
13	ATL-B42-MQSTOR-Z6	Z6	Zone 2	Atlanta Building Z6	fred.luddy@example.com	Atlanta Plant Support	storage zone for MQ to just store the stuff	2 - somewhat critical	Demo Car Corp	ISA 95 Default Template
14	CTL	CTL	California Site	California Car Facility	fred.luddy@example.com	California Plant Support	the site in California where we make cars	1 - most critical	Demo Car Corp	ISA 95 Default Template
15	CTL-C64	C64	Building 64	California Building 64	fred.luddy@example.com	California Plant Support	the building with the number 64 on the side	1 - most critical	Demo Car Corp	ISA 95 Default Template

Spalten A bis J

Spalte	Name	Typ	Beschreibung	Erforderlich
A	Pfad	Zeichenfolge	Verkettung der Kurzwahlnummern dieser Entität und aller ihr übergeordneten Entitäten. Beispiel: ATL-B42-MQSTOR-Z1 ist die Verkettung dieser Kurzwahlen: • ATL-Kurzwahl für Standort Atlanta. • B42 Kurzwahlcode für Gebäude B42. • MQSTORE-Kurzwahlcode für die Modelle M und Q. • Kurzwahlcode Z1 für die Transferlagerzone Zone 1 für die Modelle M und Q.	Ja
B	Kurzwahlnummer	Zeichenfolge, nur alphanumerisch	Kurzbeschreibungscode für die Entität. Beispiele für Kurzwahlnummern finden Sie in der vorherigen Beschreibung der Pfadspalte. Die Kurzwahl darf die maximale Länge nicht überschreiten, die in der Systemeigenschaft <code>sn_isa_model.short_code_validation_max_length</code> festgelegt ist.	Nein
C	Entitätsname	Zeichenfolge	Langer Name der Entität. Zum Beispiel ein Name einer Stadt, eine Gebäudenummer oder eine Modellnummer.	Ja
D	Standort	Zeichenfolge	Standort der Entität. Zum Beispiel würden Sie Atlanta-Gebäude 64 für jedes der Anlagenmodelle auflisten, die sich dort befinden. Der CMN-Standortwert, der in Configuration Management Database (CMDB) im Now Plattformgespeichert ist und von als Referenz verwendet wird.	Nein

Spalten A bis J (Fortsetzung)

Spalte	Name	Typ	Beschreibung	Erforderlich
E	Zugewiesen an	Zeichenfolge	E-Mail-Adresse der zugewiesenen Person, die diesen Entitätsdatensatz besitzt und verwaltet. i Hinweis: Basierend auf den Einstellungen in der Systemeigenschaft <i>sn_isa_model.user_search_matching_attribute</i> können Sie zusätzliche Attribute verwenden.	Nein
F	Supportgruppe	Zeichenfolge	Name der Gruppe, die die Wartung und Verwaltung dieser Entität unterstützt.	Nein
G	Beschreibung	Zeichenfolge	Lange Beschreibung dieser Anlagenmodell-Entität und ihren Zweck.	Nein
H	Prozessrelevanz	Zeichenfolge	Maß dafür, wie kritisch oder wichtig die Entität für den industriellen Prozess ist. Beispiele lauten wie folgt: • 1 – sehr kritisch. • 2 – kritisch.	Nein
I	Unternehmen	Zeichenfolge	Name des Unternehmens, zu dem die Entität gehört. Der CMN-Standortwert, der in CMDB im Now Plattformgespeichert ist und von als Referenz verwendet wird.	Nein
J	Vorlage	Zeichenfolge	Die zum Importieren von Daten verwendete Vorlage. i Hinweis: Nach dem Import Ihrer Daten können Sie die Vorlage nicht mehr festlegen.	Ja

Upgrade von v1 auf v2

Wenn Sie ein ISA SGC-Benutzer sind, der ein Upgrade von v1 auf v2 durchführt, können Sie neue Entitäten des Anlagenmodells nach ISA importieren, die über einen eindeutigen Pfad verfügen, und vorhandene Entitäten des Anlagenmodells nach ISA, die bereits einen Pfadwert haben, mit einem Korrekturskript aktualisieren.

Importieren Sie Ihre Anlagenmodell-Daten mithilfe der Datenquelle und des geplanten Imports

Nachdem Sie Ihre Microsoft Excel-Tabelle mit Ihren Anlagenmodell-Daten abgeschlossen haben, importieren Sie sie mithilfe der Datenquelle und des geplanten Imports in Now Plattform.

Vorbereitungen

Bevor Sie diesen Prozess ausführen, müssen Sie eine Microsoft Excel-Tabelle für den Import vorbereiten. Weitere Informationen finden Sie unter [Füllen Sie Ihre Excel-Tabelle](#) [Microsoft Azure Event Hubs mit Anlagenmodell-Daten aus](#).

Erforderliche Rolle: cmdb_inst_admin, import_admin

Warum und wann dieser Vorgang ausgeführt wird

Durch Ausführen dieses Prozesses erstellen Sie eindeutige CI-Klassendatensätze für Anlagenmodell-Entitäten in Configuration Management Database (CMDB) für die Anlagenmodell-Datensätze, die in Ihrer Tabelle enthalten sind.

Prozedur

1. Navigieren zu **Alle > Anlagenmodell – ISA > Importieren von Geräten Modell: Datenquelle**.
2. Fügen Sie im Datenquellendatensatz „**SG-Anlagenmodell**“ die von Ihnen erstellte Microsoft Excel-Tabelle an:
 - a. Wählen Sie **Anhänge verwalten**.
 - b. Wählen Sie im Dialogfeld „Anhänge“ **Datei auswählen**.
 - c. Wählen Sie die von Ihnen erstellte Microsoft Excel-Tabelle aus, und schließen Sie dann das Dialogfeld „Anhänge“.
 - d. Wählen Sie nach dem Anhängen der Tabellenkalkulation den zugehörigen Link **„Alle Datensätze laden“** aus, um alle Datensätze aus der Tabellenkalkulation in die Importtabelle zu laden. Sobald der Vorgang abgeschlossen ist, sollte die folgende Bestätigungsmeldung mit dem Code für **den erfolgreichen** Abschluss angezeigt werden, wenn die Daten ohne Fehler geladen wurden.

Progress	
Name	ImportProcessor
State	Complete
Completion code	Success
Message	Processed: 25, inserts 0, updates 0, errors 0, empty and ignored 25, ignored errors 0 (0:00:00.087)

Next steps...

- [Import sets](#) Go to the import sets for this data load
- [Loaded data](#) Go to the newly imported data inside the staging table: sg_isa_entity_import
- [Run Robust Transform](#) Transform a loaded import set using a robust transform
- [Import log](#) View the import log

wurden.

- e. Wählen Sie in der Bestätigungsmeldung den zugehörigen Link **Run Robust Transform (Robuste Transformation ausführen)** aus.
- f. Wählen Sie **Umwandeln**. Wenn der Import erfolgreich ist, sollte die folgende Bestätigungsmeldung mit dem **Erfolgsabschlusscode** angezeigt

Progress

Name	Transforming: ISET0010001
State	Complete
Completion code	Success
Message	Transformation complete

Next steps...

[ISET0010001](#) Go to the import sets for this data load

[Transform history](#) Show the transform history, related errors and log

[Import log](#) View the import log

werden.

Gewähren Sie Nicht-Administratoren Zugriff auf den Anlagenmodell-Standort, oder entfernen Sie ihn

Gewähren Sie Nicht-Administratoren Zugriff auf den Anlagenmodell-Standort, oder entfernen Sie ihn. Sie können die Benutzerkriterien erstellen, um zu bestimmen, ob bestimmte Benutzer auf die Anlagenmodell-Entitäten für bestimmte Sites zugreifen können.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Verwenden Sie die Anwenderkriterien, um zu bestimmen, ob bestimmte Anwender Anlagenmodell-Entitäten für bestimmte Sites lesen oder bearbeiten können. Nachdem Sie einen Benutzerkriteriendatensatz erstellt haben, können Sie ihn einer Site zuweisen, um zu steuern, wer die Anlagenmodell-Entitäten lesen und bearbeiten kann. Sie können die OT-Rollen außerdem Anwendern oder Gruppen zuweisen, um ihnen den Zugriff auf OT-Geräte zu ermöglichen, die denselben Sites zugewiesen sind. Weitere Informationen finden Sie unter [Weisen Sie Operational Technology Manager Rollen zu](#).

i Hinweis:

Für Benutzer, die ein Upgrade auf Version 1.0.12 durchführen, wird der Site-Benutzerzugriff zu Benutzerkriterien und -gruppen migriert. Weitere Informationen finden Sie unter [Der Site-Benutzerzugriff wird auf Benutzerkriterien und -gruppen migriert](#).

Prozedur

1. Navigieren zu **Alle > Wissensmanagement > Administration > Anwenderkriterien**
2. Wählen Sie **Neu**.

3. Füllen Sie die Felder des Formulars aus.

Eine Beschreibung der Feldwerte finden Sie unter [Formular „Benutzerkriterien“](#).

Nächste Maßnahme

Nachdem Sie die Anwenderkriterien erstellt haben, können Sie sie einer Site zuweisen. Weitere Informationen zum Zuweisen des Zugriffs „Kann bearbeiten“ auf eine Site finden Sie unter [Weisen Sie die Anwenderkriterien für den Zugriff auf „Kann bearbeiten“ an eine Site zu](#). Weitere Informationen zum Hinzufügen der Berechtigung „Kann lesen“ zu einer Site finden Sie unter [Weisen Sie die Anwenderkriterien für den Zugriff „Kann lesen“ auf eine Site zu](#).

Weisen Sie die Anwenderkriterien für den Zugriff „Kann lesen“ auf eine Site zu

Weisen Sie die Anwenderkriterien einer Site zu, um zu definieren, welche Anwender die Anlagenmodell-Entitäten lesen oder anzeigen können, die zur ausgewählten Site gehören.

Vorbereitungen

Erforderliche Rolle: cmdb_ot_isa_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Anwenderkriterien für den Zugriff „Kann lesen“ an zwei Stellen zuweisen:

- Aus der Tabelle „Anlagenmodell-Entitätsansichtszugriff“.
- Über die zugehörige Liste „Kann Anlagenmodelle lesen“ in einem Standortdatensatz

Prozedur

1. Navigieren Sie entweder zur Tabelle oder zur zugehörigen Liste.
2. Erstellen Sie einen Datensatz, indem Sie **Neu**wählen.
3. Wählen Sie im Feld **Standort** den benötigten Anlagenmodell-Standortdatensatz aus.
4. Wählen Sie im Feld **Benutzerkriterien** die Anwenderkriterien aus, um zu definieren, welche Benutzer die Anlagenmodell-Entitäten der ausgewählten Site lesen oder anzeigen können.

** Hinweis:**

Wenn ein Benutzer über die Rolle „cmdb_ot_viewer“ verfügt, kann er auch die Operational Technology (OT)-Geräte anzeigen, die dem ausgewählten Standort zugewiesen sind.

Wenn ein Benutzer über die Rolle cmdb_ot_editor verfügt, kann er die OT-Geräte bearbeiten, die der ausgewählten Site zugewiesen sind.

5. Wählen Sie **Absenden**.

Weisen Sie die Anwenderkriterien für den Zugriff auf „Kann bearbeiten“ an eine Site zu

Weisen Sie die Anwenderkriterien einem Standort zu, um zu definieren, welche Anwender die Anlagenmodell-Entitäten bearbeiten können, die zum ausgewählten Standort gehören.

Vorbereitungen

Erforderliche Rolle: cmdb_ot_isa_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Anwenderkriterien für den Zugriff „Kann bearbeiten“ an zwei Stellen zuweisen:

- Über die Tabelle „Anlagenmodell-Entitätsbearbeitungszugriff“.
- Über die zugehörige Liste „Kann Anlagenmodelle bearbeiten“ in einem Standortdatensatz

Prozedur

1. Navigieren Sie zu einem der folgenden Speicherorte.
2. Erstellen Sie einen Datensatz, indem Sie **Neu**wählen.
3. Wählen Sie im Feld **Standort** den benötigten Anlagenmodell-Standortdatensatz aus.
4. Wählen Sie im Feld **Benutzerkriterien** die Anwenderkriterien aus, um zu definieren, welche Benutzer die Anlagenmodell-Entitäten des ausgewählten Standorts bearbeiten können.

Hinweis:

Wenn ein Benutzer über die Rolle „cmdb_ot_viewer“ verfügt, kann er auch die Operational Technology (OT)-Geräte anzeigen, die dem ausgewählten Standort zugewiesen sind.

Wenn ein Benutzer über die Rolle cmdb_ot_editor verfügt, kann er die OT-Geräte bearbeiten, die der ausgewählten Site zugewiesen sind.

5. Wählen Sie **Absenden**.

Entitätszeitplan für Anlagenmodelle verwalten

Sie können den Zeitplan für eine Anlagenmodell-Entität mit der Anwendung Prozessmanager Industrie verwalten. Mithilfe eines Zeitplans können Sie mehrere Wartungsaufgaben für eine Anlagenmodell-Entität nachverfolgen.

Übersicht über den Zeitplan für Anlagenmodell-Entitäten

Sie können Zeitpläne mit jeder Anlagenmodell-Entität verknüpfen. Wenn Sie über die Rolle „Anlagenmodell-Ausfallzeitplaner“ (sn_isa_schedule_admin) verfügen, können Sie die Zeitplaneinträge einer Anlagenmodell-Entität hinzufügen, ändern oder löschen und die folgenden Aufgaben ausführen:

- Verwaltet die Zeitpläne für die verschiedenen Anlagenmodell-Entitäten.
- Ordnen Sie diese Zeitpläne Anlagenmodell-Entitäten zu.
- Wählen Sie ein Zeitfenster aus einem Zeitplan aus, damit Sie an einem Incident oder einer Korrekturaufgabe für Operational Technology (OT) arbeiten können. Weitere Informationen finden Sie [unter Startzeit für eine OT-Korrekturaufgabe auswählen aus](#).

Beispiele

Angenommen, Sie möchten mehrere Zeitplaneinträge für den Zeitplan einer Anlagenmodell-Entität festlegen. Diese Einträge führen unterschiedliche Aufgaben aus und treten zu unterschiedlichen Zeiten auf. Sie können dazu Zeitplaneinträge im zugehörigen Link Zeitplaneinträge des vorhandenen Zeitplandatensatzes für die Anlagenmodell-Entität erstellen.

Wenn ein Zeitplan nicht mehr mit einer Anlagenmodell-Entität verknüpft sein soll, können Sie den Zeitplan mithilfe des zugehörigen Links Zeitpläne im Datensatz der Anlagenmodell-Entität trennen.

Wenn Sie vorhandene Zeitpläne für eine Anlagenmodell-Entität anzeigen möchten, können Sie dies im Anlagenmodell-Manager oder im Modul „Geplante Ausfallzeit“ auf der Plattform tun.

Erstellt einen Zeitplan für Anlagenmodell-Entitäten

Erstellen Sie mit der Anwendung Prozessmanager Industrie einen Zeitplan für Anlagenmodell-Entitäten. Mit diesen Zeitplänen können Sie problemlos mehrere Anlagenmodell-Entitäten verwalten.

Vorbereitungen

Erforderliche Rolle: sn_isa_schedule_admin

Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > Industrial Process Manager > Zeitpläne für Anlagenmodell-Entitäten**.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular „Zeitpläne für Anlagenmodell-Entitäten“.

Feld	Beschreibung
Name	Eindeutiger Name für den Zeitplan.
Zeitzone	Zeitzone für den Zeitplan. Wenn Sie Fließend auswählen, ist die Zeitzone relativ zu dem Prozess, der unter auf das Element zugreift. Wenn beispielsweise ein Ressourcenmanager in Amsterdam einen fließenden Zeitplan für 8:00 bis 17:00 Uhr festlegt, sieht ein Benutzer in San Candido (Kalifornien) den Zeitplan ebenfalls als 8:00 bis 17:00 Uhr. Wenn Sie einen Zeitplan in einer Zeitzone definieren, sehen Benutzer in anderen Zeitzonen den Zeitplan in ihrer jeweiligen Zeitzone.
Typ	Textbezeichnung, die den Zweck des Zeitplans beschreibt.
Beschreibung	Beschreibung des Zeitplans.

4. Wählen Sie **Absenden**.

Nächste Maßnahme

Jetzt können Sie die Einträge für einen Zeitplan für Anlagenmodell-Entitäten erstellen. Weitere Informationen finden Sie unter [Erstellen Sie einen Zeitplaneintrag](#).

Erstellen Sie einen Zeitplaneintrag

Erstellen Sie einen Zeitplaneintrag für einen vorhandenen Zeitplan für Anlagenmodell-Entitäten in der Anwendung Prozessmanager Industrie. Sie können mehr als einen Eintrag für einen Zeitplan erstellen. Zeitplaneinträge ermöglichen die Ausführung mehrerer Wartungsaufgaben für eine Anlagenmodell-Entität.

Vorbereitungen

Erforderliche Rolle: sn_isa_schedule_admin

Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > Industrial Process Manager > Zeitpläne für Anlagenmodell-Entitäten**.
2. Wählen Sie einen vorhandenen Zeitplandatensatz für eine Anlagenmodell-Entität aus.
3. Wählen Sie die Registerkarte **Zeitplaneinträge**.
4. Wählen Sie **Neu**.
5. Füllen Sie die Felder des Formulars aus.

Formular „Zeitplaneinträge“.

Feld	Beschreibung
Name	Eindeutiger Name für den Zeitplaneintrag.
Typ	Bezeichnung, die den Zweck des Zeitplans beschreibt.
Zeigen als	Option, die angibt, wie der Zeitplaneintrag in Kalenderanwendungen angezeigt werden soll.
Wiederholen	Wiederholungsintervall für den Zeitplaneintrag, falls vorhanden. Wenn Sie ein Wiederholungsintervall auswählen, werden andere Felder angezeigt, sodass Sie das Wiederholungsintervall genauer spezifizieren können.
Wiederholen alle	Wiederholungshäufigkeit planen – wöchentlich, monatlich oder jährlich. Dieses Feld wird nur angezeigt, wenn Täglich , Wöchentlich , Monatlich oder Jährlich im Feld Wiederholungen ausgewählt ist.
Wiederholung an	Wochentage, an denen sich ein wöchentlicher Zeitplan wiederholt. Dieses Feld wird nur angezeigt, wenn Wöchentlich im Feld Wiederholungen ausgewählt wird.
Monatlicher Typ	Monatliche Wiederholungshäufigkeit des Zeitplans. Dieses Feld wird nur angezeigt, wenn Monatlich im Feld Wiederholungen ausgewählt wird. Verfügbare Optionen: ○ An einem bestimmten Tag des Monats wiederholen. ○ An einem bestimmten Tag in einer bestimmten Woche des Monats wiederholen. ○ Wiederholen Sie dies am letzten Tag des Monats. ○ An einem bestimmten Wochentag in der letzten Woche des Monats wiederholen.

Feld	Beschreibung
Jährlicher Typ	Jährliche Wiederholungshäufigkeit des Zeitplans. Dieses Feld wird nur angezeigt, wenn Jährlich im Feld Wiederholungen ausgewählt wird. Verfügbare Optionen: ○ An einem bestimmten Tag des Jahres wiederholen. ○ An einem fließenden Tag wiederholen.
Fließende Woche	Woche des Monats, in der sich ein fließender jährlicher Zeitplan wiederholt. Dieses Feld wird nur angezeigt, wenn Fließend im Feld Jährlich ausgewählt ist.
Fließender Tag	Wochentag, an dem sich ein fließender jährlicher Zeitplan wiederholt. Dieses Feld wird nur angezeigt, wenn Fließend im Feld Jährlich ausgewählt ist.
Monat	Monat, in dem sich ein jährlicher fließender Zeitplan wiederholt. Dieses Feld wird nur angezeigt, wenn Fließend im Feld Jährlich ausgewählt ist.
Wiederholen bis	Enddatum der Wiederholung. Wenn Sie dieses Feld leer lassen, wird der Zeitplan auf unbestimmte Zeit wiederholt.

6. Wählen Sie **Absenden**.

Ergebnisse

Ihr Zeitplaneintrag wird erstellt und Sie können ihn jetzt nach Bedarf bearbeiten und aktualisieren.

Ordnen Sie einer Anlagenmodell-Entität einen Zeitplan zu

Erstellen Sie einen oder mehrere Wartungszeitpläne für eine Anlagenmodell-Entität, bearbeiten Sie einen vorhandenen Zeitplan, oder löschen Sie Zeitpläne mit der Anwendung Prozessmanager Industrie.

Vorbereitungen

Erforderliche Rolle: sn_isa_schedule_admin

Prozedur

1. Navigieren zu **Alle > Anlagenmodell – ISA > Anlagenmodell-Entitäten**.
2. Wählen Sie die Anlagenmodell-Entität aus, die Sie einem Zeitplan zuordnen möchten.
3. Wählen Sie die **Registerkarte** Zeitpläne.
4. **Wahlweise:** Um einen neuen Zeitplan für die ausgewählte Anlagenmodell-Entität hinzuzufügen, gehen Sie wie folgt vor:
 - Wählen Sie **Neu**.
 - Füllen Sie das Formular aus, und wählen Sie **Absendenaus**.
5. **Wahlweise:** Gehen Sie wie folgt vor, um einen Zeitplan für die ausgewählte Anlagenmodell-Entität zu löschen:

- Wählen Sie den Zeitplan aus, den Sie löschen möchten.
- Wählen Sie **Löschen**.

6. Wahlweise: Um einen Zeitplan für die ausgewählte Anlagenmodell-Entität zu bearbeiten, gehen Sie wie folgt vor:

- Wählen Sie den Zeitplan aus, den Sie bearbeiten möchten.
- Fügen Sie Ihre Änderungen hinzu, und wählen Sie **Aktualisierenaus**.

Ergebnisse

Der Wartungsplan wird erstellt, gelöscht oder bearbeitet. Je nachdem, welche Schritte Sie ausgeführt haben, kann ein berechtigter Anwender den neuen Zeitplan sehen, den gelöschten Zeitplan nicht mehr sehen oder die bearbeitete Version des Zeitplans anzeigen.

Fügen Sie einer Anlagenmodell-Entität einen Zeitplan hinzu

Hängen Sie mit der Anwendung Prozessmanager Industrie einen vorhandenen Zeitplan an eine Anlagenmodell-Entität an. Durch das Anhängen eines Zeitplans an eine Anlagenmodell-Entität werden der Zeitplan und seine Einträge auf diese Entität angewendet.

Vorbereitungen

Erforderliche Rolle: sn_isa_schedule_admin

Prozedur

1. Navigieren zu **Alle > Anlagenmodell – ISA > Anlagenmodell-Entitäten**.
2. Wählen Sie einen Anlagenmodell-Entitätsdatensatz aus.
3. Wählen Sie die **Registerkarte** Zeitpläne.
4. Wählen Sie **Bearbeiten**.
5. Wählen Sie in der Liste Sammlung den Zeitplan aus, den Sie an die Anlagenmodell-Entität anhängen möchten.
6. Verschieben Sie den ausgewählten Zeitplan mithilfe der mittleren Pfeile in die Liste Zeitpläne.
7. Wählen Sie **Speichern**.

Ergebnisse

Der angehängte Zeitplan wird jetzt auf die Anlagenmodell-Entität angewendet. Sie können den angehängten Zeitplan im Datensatz der Anlagenmodell-Entität anzeigen und verwalten.

Trennen Sie einen Zeitplan von einer Anlagenmodell-Entität

Trennen Sie einen vorhandenen Zeitplan mit der Anwendung Prozessmanager Industrie von einer Anlagenmodell-Entität. Wenn ein Zeitplan für eine Anlagenmodell-Entität nicht mehr gilt, können Sie ihn problemlos entfernen, sodass er für diese Entität nicht mehr angezeigt wird.

Vorbereitungen

Erforderliche Rolle: sn_isa_schedule_admin

Prozedur

1. Navigieren zu **Alle > Anlagenmodell – ISA > Anlagenmodell-Entitäten**.
2. Wählen Sie einen Anlagenmodell-Entitätsdatensatz aus.
3. Wählen Sie die **Registerkarte** Zeitpläne.
4. Wählen Sie **Bearbeiten**.

5. Wählen Sie in der Liste der Zeitpläne den Zeitplan aus, den Sie von der Anlagenmodell-Entität trennen möchten.
6. Verschieben Sie den ausgewählten Zeitplan mithilfe der mittleren Pfeile in die Liste Sammlung.
7. Wählen Sie **Speichern**.

Zeigen Sie einen Zeitplan für die Anlagenmodell-Entität an

Zeigen Sie einen Zeitplan für eine vorhandene Anlagenmodell-Entität in der Anwendung Prozessmanager Industrie an.

Vorbereitungen

Erforderliche Rolle: cmdb_ot_isa_viewer

Warum und wann dieser Vorgang ausgeführt wird

Je nachdem, wo Sie arbeiten, können Sie Zeitpläne für Anlagenmodell-Entitäten an zwei Stellen anzeigen:

- Anlagenmodell-Manager
- Modul „Geplante Ausfallzeit“ auf der Plattform

Prozedur

1. Um die Zeitpläne für Anlagenmodell-Entitäten im Anlagenmodell-Manager anzuzeigen, gehen Sie wie folgt vor:
 - a. Navigieren Sie zum **Anlagenmodell-Manager**.
 - b. Wählen Sie einen Anlagenmodell-Entitätsdatensatz aus.
 - c. Wählen Sie **Zeitpläne anzeigen** aus.
 - d. Zeigen Sie die Ausfallzeitfenster für diese Anlagenmodell-Entität an.
2. Um die Zeitpläne für Anlagenmodell-Entitäten im Modul „Geplante Ausfallzeiten“ anzuzeigen, gehen Sie wie folgt vor:
 - a. Navigieren zu **Alle > Industrial Workspace-Administrator > Industrial Process Manager > Geplante Ausfallzeit**.
 - b. Zeigen Sie die Zuordnung der Zeitpläne und Anlagenmodell-Entitäten an.

Fügen Sie einen untergeordneten Zeitplan hinzu

Fügen Sie einem vorhandenen Zeitplan für Anlagenmodell-Entitäten mit der Anwendung Prozessmanager Industrie einen untergeordneten Zeitplan hinzu. Wenn Sie Anpassungen am untergeordneten Zeitplan vornehmen, gilt dies auch für den übergeordneten Zeitplan. Beispielsweise können Sie die geplante Zeit an einem bestimmten Tag verlängern oder Feiertage aus einem Zeitplan entfernen.

Vorbereitungen

Erforderliche Rolle: sn_isa_schedule_admin

Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > Industrial Process Manager > Zeitpläne für Anlagenmodell-Entitäten**.
2. Wählen Sie einen Datensatz für einen vorhandenen Zeitplan für Anlagenmodell-Entitäten aus.
3. Wählen Sie die Registerkarte **Untergeordnete Zeitpläne**.

4. Wählen Sie **Bearbeiten**.

5. Wählen Sie den gewünschten Zeitplan in der Liste Sammlung aus.

6. Verschieben Sie den ausgewählten Zeitplan mithilfe der mittleren Pfeile in die Liste „Untergeordnete Zeitpläne“.

7. Wählen Sie **Speichern**.

Ergebnisse

Der ausgewählte untergeordnete Zeitplan gilt jetzt für den übergeordneten Zeitplan.

Prozessmanager Industrie mit Operational Technology Managerverwenden

Nachdem Sie alle erforderlichen Einrichtungsaufgaben abgeschlossen haben (einschließlich des Imports von Anlagenmodellen), können Sie die Funktionen Operational Technology Manager und Prozessmanager Industrie im Menü Administrator für den industriellen Arbeitsbereich verwenden. Zu diesen Funktionen gehören der Anlagenmodell-Manager und der Industrie-Arbeitsbereich.

Die folgende Grafik zeigt einige häufige Fragen, die gewerbliche Mitarbeiter zu betrieblichen Problemen in einem Unternehmen stellen, und die Funktionen Now Platform, mit denen Sie diese Fragen beantworten können. Diese Funktionen helfen Ihren Mitarbeitern, Datenbeziehungen in Ihren Industrieanlagen zu visualisieren.

Fragen von Industriepersonal zu betrieblichen Problemen



Betty, eine Konfigurationsmanagerin, arbeitet auf Unternehmensebene und möchte wissen, wo sich die OT-Geräte im Unternehmen befinden. Um diese Frage zu beantworten, kann ein Konfigurationsmanager die Funktionen Operational Technology Manager im Menü Administrator für den industriellen Arbeitsbereich verwenden. Weitere Informationen finden Sie unter [Administrator für den industriellen Arbeitsbereich Anwendungsmenü und im geführten Setup](#).

Devnesh, ein OT-Ingenieur, arbeitet auf Site-Ebene und möchte wissen, wie OT-Geräte bestimmten Produktionsprozessen zugeordnet werden. Eine Frage könnte beispielsweise lauten: „Welche HMIs und SPS steuern diesen bestimmten Teil der industriellen Verarbeitung? Um diese Frage zu beantworten, kann ein OT-Manager auf Site-Ebene die Funktionen Prozessmanager Industrie im Menü Administrator für den industriellen Arbeitsbereich verwenden.

Anlagenmodelle verwalten

Mit dem Anlagenmodell-Manager können Sie Daten des Anlagenmodells nach ISA-95 überprüfen und verwalten. Sie können damit importierte Anlagenmodell-Daten überprüfen oder manuell ein Anlagenmodell erstellen.

Ein Anlagenmodell ordnet die operativen Elemente einer bestimmten Einrichtung zu. Zum Beispiel eine Industrieanlage in Atlanta, in der Materialien gelagert und zur Produktion von Autos verwendet werden. Mit dem Anlagenmodell-Manager können Sie ausgewählte Anlagenmodell-Entitäten für bestimmte Industriestandorte anzeigen und die folgenden Aufgaben ausführen:

- Zeigen Sie eine grafische Darstellung der Hierarchie eines Anlagenmodells und ihrer Beziehung zu anderen Entitäten an.
- Zeigen Sie vor- oder nachgelagerte Produktionsprozesse an oder ordnen Sie sie zu.
- Überprüfen Sie die untergeordneten Entitäten.
- Überprüfen oder ordnen Sie zusätzliche OT-Geräte der ausgewählten Anlagenmodell-Entität zu

Hinweis:

Benutzer mit der zugewiesenen Rolle „cmdb_ot_isa_admin“ können Anlagenmodell-Entitäten für jeden Standort anzeigen. Benutzer mit zugewiesenen Rollen cmdb_ot_isa_editor oder cmdb_ot_isa_viewer können jedoch nur auf Websites zugreifen, auf die ein Administrator bestimmten Benutzern Zugriff gewährt hat. Weitere Informationen zum Gewähren des Website-Zugriffs finden Sie unter [Gewähren Sie Nicht-Administratoren Zugriff auf den Anlagenmodell-Standort, oder entfernen Sie ihn](#).

Überprüfen und aktualisieren Sie die Anlagenmodell-Details

Überprüfen und aktualisieren Sie die Details für ein Anlagenmodell, das Sie in Now Platform importiert haben, um sicherzustellen, dass die Informationen korrekt sind. Sie können auch manuell eine neue Anlagenmodell-Entität erstellen und ihr dann Details hinzufügen.

Vorbereitungen

Importieren Sie Anlagenmodell-Daten in Now Platform. Weitere Informationen finden Sie unter [Anlagenmodell-Daten werden importiert](#).

Erforderliche Rolle: cmdb_ot_isa_viewer, cmdb_ot_isa_editor, cmdb_ot_isa_admin.

Warum und wann dieser Vorgang ausgeführt wird

Wenn Ihnen die Rolle cmdb_ot_isa_viewer zugewiesen ist, können Sie nur Anlagenmodell-Entitäten anzeigen. Wenn Ihnen eine der anderen cmdb_ot_isa-Rollen zugewiesen ist, können Sie auch Anlagenmodell-Entitäten bearbeiten.

Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > Industrial Process Manager > Anlagenmodell-Manager**.
2. Wählen Sie im Feld **Anlagenmodell-Ansicht für** den Standort aus, für den Sie die Anlagenmodell-Informationen anzeigen möchten.
Sie können nach einer Website suchen, indem Sie den Namen der Website oder ihren Kurzwahlcode eingeben.
3. Überprüfen Sie eine vorhandene Anlagenmodell-Entität, oder erstellen Sie eine.
4. Überprüfen und aktualisieren Sie die Felder im Formular.

Formular „Anlagenmodelldetails“.

Feld	Beschreibung
Einheitsname	Name der Anlagenmodell-Entität i Hinweis: Sie können das Feld Entitätsname aktualisieren, nachdem die Anlagenmodell-Entität erstellt wurde. Durch das Aktualisieren dieses Felds werden auch die Strukturkomponente und der Standortfilter aktualisiert. Weitere Informationen finden Sie unter Aktualisiert den Entitätsnamen oder das übergeordnete Element einer Anlagenmodell-Entität.
Übergeordnet	Name der Entität (falls vorhanden), die dieser Anlagenmodell-Entität übergeordnet ist. Dieses Feld ist für die übergeordnete Entität der obersten Ebene, die kein übergeordnetes Element hat, leer. Die übergeordnete Entität der obersten Ebene wird als Site bezeichnet. i Hinweis: Sie können das Feld Übergeordnet aktualisieren, nachdem die Anlagenmodell-Entität erstellt wurde. Durch das Aktualisieren dieses Felds werden auch die Strukturkomponente und der Standortfilter aktualisiert. Weitere Informationen finden Sie unter Aktualisiert den Entitätsnamen oder das übergeordnete Element einer Anlagenmodell-Entität.
Vorlage	Anlagenmodell-Vorlage, die einer manuell erstellten Anlagenmodell-Entität zugewiesen ist. i Hinweis: Sie können eine Anlagenmodell-Vorlage keinem Anlagenmodell zuweisen, das Sie mit IntegrationHub ETL oder einer Drittanbieterintegration in Now Platform[®] importiert haben.
Ebene	Hierarchieebene, die von der ausgewählten Anlagenmodell-Vorlage zum Sortieren und Strukturieren von Daten zugewiesen wird. Beispiele lauten wie folgt: Site

Feld	Beschreibung
	Industriestandort. Bereich Bereich an einem Industriestandort. Arbeitsplatz Arbeitsplatz an einem Industriestandort. Suchen Sie nach einer Geräteebe- ne, und wählen Sie sie aus, um sie der Anlagenmodell-Entität zuzuweisen. Weitere Informationen finden Sie unter Erstellen Sie hierarchische Sortierebenen für eine Anlagenmodell- Vorlage.
Typ	Name des Ebenentyps, der der Anlagenmodell- Vorlagenebene zugewiesen ist. Zum Beispiel Materialkomponentengruppe oder Produktionszelle für eine Arbeitsplatzebene. Weitere Informationen finden Sie unter Erstellen Sie Ebenentypen für Anlagenmodelle .
Kurzbeschreibung	Kurzbeschreibung dieser Anlagenmodell-Entität und ihres Zwecks.
Kurzwahlnummer	Kurzwahlcode, der dieser Anlagenmodell-Entität zugewiesen ist.
Pfad	Verkettung der Kurzwahlnummern dieser Anlagenmodell-Entität und aller ihr übergeordneten Entitäten. Beispiel: ATL-B42-MQSTOR-Z1 ist die Verkettung der folgenden Kurzwahlen: ○ ATL-Kurzwahl für Standort Atlanta. ○ B42 Kurzwahlcode für Gebäude B42. ○ MQSTORE-Kurzwahlcode für die Modelle M und Q. ○ Kurzwahlcode Z1 für die Transferlagerzone Zone 1 für die Modelle M und Q.
Standort	Standort der Anlagenmodell-Entität. Zum Beispiel wäre Atlanta-Gebäude 64 der Standort für jedes zugeordnete Anlagenmodell, das sich dort befindet. Suchen Sie nach dem Standort, der der Anlagenmodell-Entität zugewiesen werden soll, und wählen Sie ihn aus.
Unternehmen	Name des Unternehmens, das der Anlagenmodell- Entität zugeordnet ist. Suchen Sie nach einem Unternehmen, und wählen Sie es aus, um es der Entität zuzuweisen.
Zugewiesen an	Zugewiesener Benutzer, der diese Anlagenmodell- Entität bedient und bearbeitet. Suchen Sie nach dem

Feld	Beschreibung
	Anwender, der der Entität zugewiesen werden soll, und wählen Sie ihn aus.
Verwaltet von	Name der zugewiesenen Person, die diesen Entitätsdatensatz besitzt und für die Verwaltung verantwortlich ist. Suchen Sie nach dem Benutzer, der der Anlagenmodell-Entität zugewiesen werden soll, und wählen Sie ihn aus.
Prozessrelevanz	Maß dafür, wie kritisch oder wichtig die Anlagenmodell-Entität für den industriellen Prozess ist. Wählen Sie die Prozessrelevanz für die Entität aus. Zum Beispiel: 1 – sehr kritisch. 2 – kritisch.
Supportgruppe	Name der Gruppe, die diese Anlagenmodell-Entität unterstützt. Suchen Sie nach der Benutzergruppe, die der Anlagenmodell-Entität zugewiesen werden soll, und wählen Sie sie aus.
Verwaltet nach Gruppe	Name der zugewiesenen Gruppe, die diesen Entitätsdatensatz besitzt und für die Verwaltung verantwortlich ist. Suchen Sie nach der Benutzergruppe, die der Entität zugewiesen werden soll, und wählen Sie sie aus.
Unternehmen	Name des Unternehmens, zu dem die Anlagenmodell-Entität gehört. Der Wert „core_company“ wird in CMDB in Now Platform als Referenz gespeichert.
Betriebsstatus	Aktueller Betriebsstatus der Anlagenmodell-Entität: Operativ Entität, die im Produktionsprozess vollständig funktionsfähig ist. Nicht funktionsfähig Entität, die im Produktionsprozess nicht funktionsfähig ist.

5. Überprüfen Sie die zugehörigen Anlagenmodell-Daten auf den Registerkarten der zugehörigen Liste wie folgt:

Aufgabe	Beschreibung
Zeigen Sie die Hierarchie des Anlagenmodells an	Weitere Informationen finden Sie unter Zeigen Sie die Hierarchie des Anlagenmodells an .
Ordnen Sie die vorgelagerten Produktionsprozesse für die Anlagenmodell-Entität zu.	a. Klicken Sie auf Vorgelagerter Prozess. b. Weitere Informationen finden Sie unter Ordnen Sie die vorgelagerten Produktionsprozesse für die ausgewählte Anlagenmodell-Entität zu.

Aufgabe	Beschreibung
Ordnen Sie die nachgelagerten Produktionsprozesse für die Anlagenmodell-Entität zu.	a. Klicken Sie auf Nachgelagerter Prozess. b. Weitere Informationen finden Sie unter Ordnen Sie die nachgelagerten Produktionsprozesse für die ausgewählte Anlagenmodell-Entität zu.
Zeigen Sie die untergeordneten Entitäten für die Anlagenmodell-Entität an.	a. Klicken Sie auf Untergeordnete Entitäten. b. Weitere Informationen finden Sie unter Überprüfen Sie die untergeordneten Entitäten für die Anlagenmodell-Entität.
Zeigen Sie die OT-Geräte an, die der aktuellen Anlagenmodell-Entität und ihren untergeordneten Entitäten zugeordnet sind.	a. Klicken Sie auf Zugeordnete OT-Geräte. b. Weitere Informationen finden Sie unter Fügen Sie OT-Geräte hinzu, die der ausgewählten Anlagenmodell-Entität zugeordnet sind. ? Hinweis: Standardmäßig können OT-Steuerungsmodule in dieser Liste nicht angezeigt werden.

6. Wenn Sie mit der Überprüfung und Aktualisierung der Anlagenmodell-Details fertig sind, führen Sie eine der folgenden Aktionen aus.

Nächste Maßnahme

Um das Rollup für OT-Daten anzuzeigen, die der Anlagenmodell-Entität und ihren untergeordneten Entitäten zugeordnet sind, können Sie die folgenden zugehörigen Listen im Anlagenmodell-Entitätsdatensatz verwenden. Die Rollup-Ansicht stellt die OT-Geräte, OT-Incidents, OT-Changes usw. dar, die die gesamte Hierarchie einer Anlagenmodell-Entität automatisieren.

- Zugeordnete OT-Geräte
- OT-Incidents
- OT-Change-Anforderungen
- Angreifbare Elemente
- Korrekturaufgaben

Erstellen Sie eine Entität für ein neues Anlagenmodell

Erstellen Sie eine Entität für ein neues Anlagenmodell. Führen Sie diese Aufgabe aus, wenn Sie eine neue Anlagenmodell-Entität manuell direkt in Now Platform erstellen möchten, anstatt die Anlagenmodell-Daten aus einer externen Quelle zu importieren.

Vorbereitungen

Erforderliche Rolle: `cmdb_ot_isa_editor`, `cmdb_ot_isa_admin`.

Warum und wann dieser Vorgang ausgeführt wird

Benutzer mit der zugewiesenen Rolle „`cmdb_ot_isa_admin`“ können Anlagenmodell-Entitäten für jeden Standort anzeigen. Benutzer mit der zugewiesenen Rolle `cmdb_ot_isa_editor` können jedoch nur auf die Websites zugreifen, auf die ein Administrator bestimmten

Benutzern Zugriff gewährt hat. Weitere Informationen zum Gewähren des Website-Zugriffs finden Sie unter [Gewähren Sie Nicht-Administratoren Zugriff auf den Anlagenmodell-Standort, oder entfernen Sie ihn](#).

Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > Industrial Process Manager > Anlagenmodell-Manager**.
2. Wählen Sie im Feld **Anlagenmodell-Ansicht für** den Standort aus, für den Sie die Anlagenmodell-Informationen anzeigen möchten.
Sie können nach einer Website suchen, indem Sie den Namen der Website oder ihren Kurzwahlcode eingeben.
3. Wählen Sie **Neue Entität erstellen aus**.
4. Suchen Sie im Fenster **Neue Entität erstellen** nach der übergeordneten Entität, und wählen Sie sie aus.

Hinweis:

Sie können die übergeordnete Entität nach Kurzwahl oder Name suchen.

5. Füllen Sie die Felder des Formulars aus.

Formular zum Erstellen einer neuen Entität

Feld	Beschreibung
Übergeordnet	Name der Entität, die dieser Entität übergeordnet ist, falls vorhanden. Das aktuell ausgewählte Anlagenmodell wird als übergeordnete Entität angezeigt. Um das übergeordnete Element zu ändern, suchen und wählen Sie die Entität, die der von Ihnen erstellten Entität übergeordnet ist.
Einheitsname	Name der Anlagenmodell-Entität
Kurzwahlnummer	Kurzwahlcode, der dieser Entität zugewiesen ist.
Entitätstyp	Name des Ebenentyps, der der Anlagenmodell-Vorlagenebene zugewiesen ist. Zum Beispiel Materialkomponentengruppe oder Produktionszelle für eine Arbeitsplatzebene. Suchen Sie nach einem Entitätstyp, und wählen Sie ihn aus. Weitere Informationen finden Sie unter Erstellen Sie Ebenentypen für Anlagenmodelle .

6. Wählen Sie **Speichern**.
7. Geben Sie im Detailformular die verbleibenden Details für die neue Anlagenmodell-Entität ein.
Weitere Informationen finden Sie unter [Überprüfen und aktualisieren Sie die Anlagenmodell-Details](#).

Zeigen Sie die Hierarchie des Anlagenmodells an

Zeigen Sie eine grafische Darstellung der hierarchischen Struktur der ausgewählten Anlagenmodell-Entität und ihrer Beziehungen zu anderen Entitäten im Produktionsprozess an.

Vorbereitungen

Erforderliche Rolle: cmdb_ot_isa_editor, cmdb_ot_isa_admin.

Warum und wann dieser Vorgang ausgeführt wird

Benutzer mit der zugewiesenen Rolle „cmdb_ot_isa_admin“ können Anlagenmodell-Entitäten für jeden Standort anzeigen. Benutzer mit zugewiesenen Rollen cmdb_ot_isa_editor oder cmdb_ot_isa_viewer können jedoch nur auf Websites zugreifen, auf die ein Administrator bestimmten Benutzern Zugriff gewährt hat. Weitere Informationen zum Gewähren des Website-Zugriffs finden Sie unter [Gewähren Sie Nicht-Administratoren Zugriff auf den Anlagenmodell-Standort, oder entfernen Sie ihn](#).

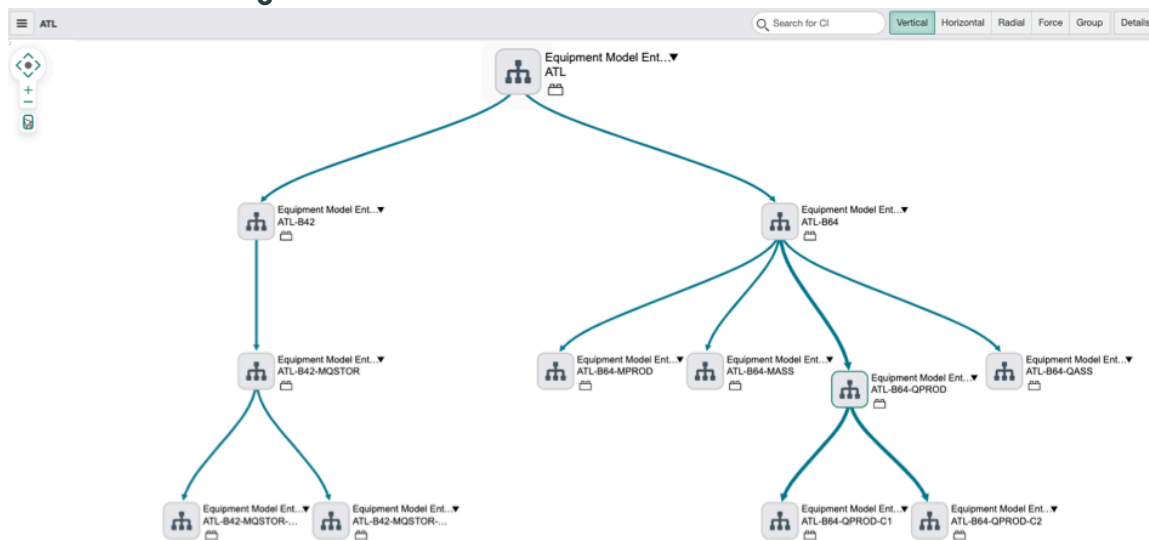
Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > Industrial Process Manager > Anlagenmodell-Manager**.
2. Wählen Sie im Feld **Anlagenmodell-Ansicht für** den Standort aus, für den Sie Anlagenmodell-Informationen anzeigen möchten.
Sie können nach einer Website suchen, indem Sie den Namen der Website oder ihren Kurzwahlcode eingeben.
3. Klicken Sie im Auswahlbereich auf die Anlagenmodell-Entität, für die Sie eine grafische Darstellung ihrer Hierarchie und der Beziehung zu anderen Entitäten anzeigen möchten.
Klicken Sie beispielsweise auf die Site-Entität der obersten Ebene, um eine Darstellung der gesamten Site anzuzeigen.
4. Um die hierarchische Struktur für die Anlagenmodell-Entität anzuzeigen, klicken Sie auf **Hierarchie anzeigen**.

Ergebnisse

Die folgende grafische Darstellung wird für die ausgewählte Anlagenmodell-Entität angezeigt. Das aktuell ausgewählte Anlagenmodell wird als übergeordnete Entität in der Hierarchie angezeigt.

Hierarchie der Anlagenmodell-Entität



Zeigen Sie die OT-Gerätezuordnung des Anlagenmodells an

Zeigen Sie die grafische Darstellung der ausgewählten Anlagenmodell-Entität und ihre Beziehung zu anderen Operational Technology (OT)-Geräten im Produktionsprozess an.

Vorbereitungen

Erforderliche Rolle: cmdb_ot_isa_editor, cmdb_ot_isa_admin.

Warum und wann dieser Vorgang ausgeführt wird

Benutzer mit der zugewiesenen Rolle „cmdb_ot_isa_admin“ können Anlagenmodell-Entitäten für jeden Standort anzeigen. Benutzer mit zugewiesenen Rollen cmdb_ot_isa_editor oder cmdb_ot_isa_viewer können jedoch nur auf Websites zugreifen, auf die ein Administrator bestimmten Benutzern Zugriff gewährt hat. Weitere Informationen zum Gewähren des Website-Zugriffs finden Sie unter [Gewähren Sie Nicht-Administratoren Zugriff auf den Anlagenmodell-Standort, oder entfernen Sie ihn](#).

Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > Industrial Process Manager > Anlagenmodell-Manager**.
2. Wählen Sie im Feld **Anlagenmodus-Ansicht für** den Standort aus, für den Sie Anlagenmodell-Informationen anzeigen möchten.
Sie können nach einer Website suchen, indem Sie den Namen der Website oder ihren Kurzwahlcode eingeben.
3. Wählen Sie im Auswahlbereich die Anlagenmodell-Entität aus, deren Beziehung Sie zu anderen Geräten grafisch darstellen möchten.
Wählen Sie beispielsweise die Standortentität der obersten Ebene aus, um eine Darstellung des gesamten Standorts anzuzeigen.
4. Um die Beziehungen der Anlagenmodell-Entität zu Geräten anzuzeigen, wählen Sie **OT-Gerätezuordnung anzeigen** aus.

Zeigen Sie die OT-Abhängigkeitszuordnung des Anlagenmodells an

Zeigen Sie die grafische Darstellung der hierarchischen Struktur der ausgewählten Anlagenmodell-Entität und ihre Beziehung zu anderen Entitäten und Geräten im Produktionsprozess an.

Vorbereitungen

Erforderliche Rolle: cmdb_ot_isa_editor, cmdb_ot_isa_admin.

Warum und wann dieser Vorgang ausgeführt wird

Benutzer mit der zugewiesenen Rolle „cmdb_ot_isa_admin“ können Anlagenmodell-Entitäten für jeden Standort anzeigen. Benutzer mit zugewiesenen Rollen cmdb_ot_isa_editor oder cmdb_ot_isa_viewer können jedoch nur auf Websites zugreifen, auf die ein Administrator bestimmten Benutzern Zugriff gewährt hat. Weitere Informationen zum Gewähren des Website-Zugriffs finden Sie unter [Gewähren Sie Nicht-Administratoren Zugriff auf den Anlagenmodell-Standort, oder entfernen Sie ihn](#).

Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > Industrial Process Manager > Anlagenmodell-Manager**.
2. Wählen Sie im Feld **Anlagenmodus-Ansicht für** den Standort aus, für den Sie Anlagenmodell-Informationen anzeigen möchten.

Sie können nach einer Website suchen, indem Sie den Namen der Website oder ihren Kurzwahlcode eingeben.

3. Wählen Sie im Auswahlbereich die Anlagenmodell-Entität aus, für die Sie eine grafische Darstellung ihrer Hierarchie und ihrer Beziehung zu anderen Geräten und Entitäten anzeigen möchten.
Wählen Sie beispielsweise die Standortentität der obersten Ebene aus, um eine Darstellung des gesamten Standorts anzuzeigen.
4. Um die hierarchische Beziehungsstruktur der Anlagenmodell-Entität zu anderen Geräten und Entitäten anzuzeigen, wählen Sie **OT-Abhängigkeitszuordnung anzeigen** aus.

Ordnen Sie die vorgelagerten Produktionsprozesse für die ausgewählte Anlagenmodell-Entität zu

Verwenden Sie den Upstream-Prozess, um Upstream-Produktionsprozesse für die ausgewählte Anlagenmodell-Entität zu überprüfen. Sie können auch einen neuen vorgelagerten Produktionsprozess für die Anlagenmodell-Entität erstellen und zuordnen.

Vorbereitungen

Erforderliche Rolle: cmdb_ot_isa_editor, cmdb_ot_isa_viewer, cmdb_ot_isa_admin

Warum und wann dieser Vorgang ausgeführt wird

Benutzer mit der zugewiesenen Rolle „cmdb_ot_isa_admin“ können Anlagenmodell-Entitäten für jeden Standort anzeigen. Benutzer mit der zugewiesenen Rolle cmdb_ot_isa_editor können jedoch nur auf die Websites zugreifen, auf die ein Administrator bestimmten Benutzern Zugriff gewährt hat. Weitere Informationen zum Gewähren des Website-Zugriffs finden Sie unter [Gewähren Sie Nicht-Administratoren Zugriff auf den Anlagenmodell-Standort, oder entfernen Sie ihn](#).

Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > Industrial Process Manager > Anlagenmodell-Manager**.
2. Wählen Sie im Feld **Anlagenmodell-Ansicht für** den Standort aus, für den Sie Anlagenmodell-Informationen anzeigen möchten.
Sie können nach einer Website suchen, indem Sie den Namen der Website oder ihren Kurzwahlcode eingeben.
3. Erweitern Sie im Auswahlbereich die Anlagenmodell-Hierarchie, und klicken Sie dann auf die Entität, die Sie anzeigen möchten.
4. Klicken Sie auf **Vorgelagerter Prozess**, um die vorgelagerten Produktionsprozesse für die Anlagenmodell-Entität anzuzeigen.
5. Überprüfen Sie die vorgelagerten Produktionsprozesse für das Anlagenmodell, oder ordnen Sie ein neues zu.
6. Klicken Sie auf **Absenden**.

Ordnen Sie die nachgelagerten Produktionsprozesse für die ausgewählte Anlagenmodell-Entität zu

Verwenden Sie den Downstream-Prozess, um die Downstream-Produktionsprozesse für die ausgewählte Anlagenmodell-Entität zu überprüfen. Sie können auch einen neuen nachgelagerten Produktionsprozess für die Anlagenmodell-Entität erstellen und zuordnen.

Vorbereitungen

Erforderliche Rolle: cmdb_ot_isa_editor, cmdb_ot_isa_viewer, cmdb_ot_isa_admin

Warum und wann dieser Vorgang ausgeführt wird

Benutzer mit der zugewiesenen Rolle „cldb_ot_isa_admin“ können Anlagenmodell-Entitäten für jeden Standort anzeigen. Benutzer mit der zugewiesenen Rolle cldb_ot_isa_editor können jedoch nur auf die Websites zugreifen, auf die ein Administrator bestimmten Benutzern Zugriff gewährt hat. Weitere Informationen zum Gewähren des Website-Zugriffs finden Sie unter [Gewähren Sie Nicht-Administratoren Zugriff auf den Anlagenmodell-Standort, oder entfernen Sie ihn](#).

Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > Industrial Process Manager > Anlagenmodell-Manager**.
2. Wählen Sie im Feld **Anlagenmodell-Ansicht für** den Standort aus, für den Sie die Anlagenmodell-Informationen anzeigen möchten.
Sie können nach einer Website suchen, indem Sie den Namen der Website oder ihren Kurzwahlcode eingeben.
3. Erweitern Sie im Auswahlbereich die Anlagenmodell-Hierarchie, und klicken Sie dann auf die Entität, die Sie anzeigen möchten.
4. Um die nachgelagerten Produktionsprozesse für die Anlagenmodell-Entität anzuzeigen, klicken Sie auf **Nachgelagerter Prozess**.
5. Überprüfen Sie die nachgelagerten Produktionsprozesse für das Anlagenmodell, oder ordnen Sie ein neues zu.
6. Klicken Sie auf **Absenden**.

Überprüfen Sie die untergeordneten Entitäten für die Anlagenmodell-Entität

Überprüfen Sie die untergeordneten Entitäten, die der ausgewählten Anlagenmodell-Entität zugeordnet sind. Sie können die Beziehungen der zugeordneten Entitäten überprüfen, die einer Entität einer höheren Ebene untergeordnet sind.

Vorbereitungen

Erforderliche Rolle: cldb_ot_isa_editor, cldb_ot_isa_admin.

Warum und wann dieser Vorgang ausgeführt wird

Benutzer mit der zugewiesenen Rolle „cldb_ot_isa_admin“ können Anlagenmodell-Entitäten für jeden Standort anzeigen. Benutzer mit der zugewiesenen Rolle cldb_ot_isa_editor können jedoch nur auf die Websites zugreifen, auf die ein Administrator bestimmten Benutzern Zugriff gewährt hat. Weitere Informationen zum Gewähren des Website-Zugriffs finden Sie unter [Gewähren Sie Nicht-Administratoren Zugriff auf den Anlagenmodell-Standort, oder entfernen Sie ihn](#).

Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > Industrial Process Manager > Anlagenmodell-Manager**.
2. Wählen Sie im Feld **Anlagenmodell-Ansicht für** den Standort aus, für den Sie die Anlagenmodell-Informationen anzeigen möchten.
Sie können nach einer Website suchen, indem Sie den Namen der Website oder ihren Kurzwahlcode eingeben.
3. Erweitern Sie im Auswahlbereich die Anlagenmodell-Hierarchie, und klicken Sie dann auf die Entität, die Sie anzeigen möchten.

4. Um die untergeordneten Entitäten für die Anlagenmodell-Entität anzuzeigen, klicken Sie auf **Untergeordnete Entitäten**.
5. Um eine neue untergeordnete Entität zu erstellen, klicken Sie auf die Schaltfläche **Neue Entität erstellen** und füllen Sie die Details im Formular „Neue Entität erstellen“ aus.
Weitere Informationen finden Sie unter [Erstellen Sie eine Entität für ein neues Anlagenmodell](#).

Fügen Sie OT-Geräte hinzu, die der ausgewählten Anlagenmodell-Entität zugeordnet sind

Verwenden Sie OT-Geräte, um die OT-Geräte zu überprüfen, die der ausgewählten Anlagenmodell-Entität und ihren untergeordneten Entitäten zugeordnet sind. Sie können auch andere OT-Geräte auswählen und der ausgewählten Anlagenmodell-Entität zuordnen.

Vorbereitungen

Um der ausgewählten Anlagenmodell-Entität zusätzliche OT-Geräte zuzuordnen, müssen die Anwendungen Operational Technology Manager und Prozessmanager Industrie installiert sein.

Erforderliche Rolle: Um OT-Geräte hinzuzufügen, muss der angemeldete Anwender eine Kombination der folgenden zugewiesenen Rollen aufweisen:

- Rolle cmdb_ot_viewer, cmdb_ot_editor oder cmdb_ot_admin
- Rolle cmdb_ot_isa_editor oder cmdb_ot_isa_admin

Hinweis:

Weitere Informationen zum Zuweisen von -Benutzerrollen finden Sie unter [Weisen Sie Prozessmanager Industrie Anwenderrollen zu](#).

Warum und wann dieser Vorgang ausgeführt wird

Benutzer mit der zugewiesenen Rolle „cmdb_ot_isa_admin“ können Anlagenmodell-Entitäten für jeden Standort anzeigen. Benutzer mit zugewiesenen Rollen cmdb_ot_isa_editor oder cmdb_ot_isa_viewer können jedoch nur auf Websites zugreifen, auf die ein Administrator bestimmten Benutzern Zugriff gewährt hat. Weitere Informationen zum Gewähren des Website-Zugriffs finden Sie unter [Gewähren Sie Nicht-Administratoren Zugriff auf den Anlagenmodell-Standort, oder entfernen Sie ihn](#).

Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > Industrial Process Manager > Anlagenmodell-Manager**.
Sie können nach einer Website suchen, indem Sie den Namen der Website oder ihren Kurzwahlcode eingeben.
2. Wählen Sie im Feld **Anlagenmodell-Ansicht für** den Standort aus, für den Sie Anlagenmodell-Informationen anzeigen möchten.
3. Erweitern Sie im Auswahlbereich die Anlagenmodell-Hierarchie, und klicken Sie dann auf die Entität, die Sie anzeigen möchten.
4. Um die zugeordneten OT-Geräte für die Anlagenmodell-Entität und ihre untergeordneten Entitäten anzuzeigen, klicken Sie auf **Zugeordnete OT-Geräte**.
5. Überprüfen Sie die OT-Geräte, die der ausgewählten Anlagenmodell-Entität zugeordnet sind, oder die zusätzlichen OT-Geräte, die der ausgewählten Anlagenmodell-Entität zugeordnet sind.
6. Klicken Sie auf **Speichern**.

Aktualisiert den Entitätsnamen oder das übergeordnete Element einer Anlagenmodell-Entität

Aktualisieren Sie die Felder „Entitätsname“ oder „Übergeordnet“ in einem Anlagenmodell-Entitätsdatensatz nach Bedarf, um Ihre Anlagenmodell-Informationen auf dem neuesten Stand zu halten.

Vorbereitungen

Erforderliche Rolle: cmdb_ot_isa_editor

Prozedur

1. Navigieren zu **Alle > Industrial Workspace**.
2. Wählen Sie die Schaltfläche Anlagenmodell () aus.
Alternativ können Sie zu navigieren **Alle > Industrial Workspace-Administrator > Industrial Process Manager > Anlagenmodell-Manager**.
3. Wählen Sie den Datensatz der Anlagenmodell-Entität aus, den Sie aktualisieren möchten.
4. Aktualisieren Sie das Feld **Entitätsname** oder das Feld **Übergeordnet** nach Bedarf.
5. Wählen Sie **Speichern**.

Ergebnisse

Wenn Sie die Felder **Entitätsname** oder **Übergeordnet** aktualisieren, werden die Felder auch in der Baumkomponente im Anlagenmodell-Manager und im Standortfilter auf der Zielseite Operational Technology (OT) in Industriell Arbeitsbereich aktualisiert.

Massenbearbeitung der Zuweisungsgruppe Operational Technology Vulnerability Response einer Site

Verwenden Sie die Massenbearbeitungsfunktion, um das Zuweisungsgruppenfeld Operational Technology Vulnerability Response (OT VR) in mehreren Standortdatensätzen gleichzeitig zu aktualisieren.

Vorbereitungen

Erforderliche Rolle: cmdb_ot_isa_admin

Prozedur

1. Navigieren zu **Alle > Industrial Workspace**.
2. Öffnen Sie die Listenansicht ()
3. Wählen Sie im Modul **Prozessmanager Industrie** die Liste Sites aus.
4. Aktivieren Sie das Kontrollkästchen neben jeder OT-Site, die Sie bearbeiten möchten.
5. Wählen Sie die Schaltfläche **Bearbeiten**.
6. Fügen Sie im **Feld OT VR-Zuweisungsgruppe** die Zuweisungsgruppe Operational Technology Vulnerability Response für die ausgewählten Sites hinzu.
7. Wählen Sie **Aktualisieren**.

Ergebnisse

Das Feld „**OT VR-Zuweisungsgruppe**“ wird für jeden ausgewählten Standort aktualisiert.

Suchen Sie nach einer Anlagenmodell-Entität

Suchen Sie in Industrial Workspace nach einer Anlagenmodell-Entität, um sie schneller und effizienter zu finden.

Vorbereitungen

Erforderliche Rolle: cmdb_ot_isa_editor

Prozedur

1. Navigieren zu **Alle > Industrial Workspace**.
2. Wählen Sie das Symbol Anlagenmodell-Manager ()
3. Suchen Sie in der **Suchleiste** nach der Anlagenmodell-Entität, die Sie anzeigen möchten.

Automatisierte Zuordnung von OT-Geräten zum Anlagenmodell

Automatisieren Sie die Zuordnung von OT-Geräten zum Produktionsprozess. ☑

Wenn OT-Manager auf Schwachstellen stoßen oder Workflows mit OT-Geräten verwalten müssen, ist der Kontext der Verbindung des OT-Geräts mit dem von ihm automatisierten Produktionsprozess entscheidend für die Priorisierung der Arbeit. Die automatische Zuordnung von OT-Geräten zu Entitäten des Anlagenmodells nach ISA ermöglicht die Ansicht von Gerät-zu-Prozess-Beziehungen.

Hinweis:

Pro Standort wird nur ein Subnetzbereich unterstützt. Zwei verschiedene Sites können dasselbe Subnetz haben. Beispiel: 192.168.101.0/24. Mehrere Subnetze desselben Bereichs werden jedoch **nicht** für dieselbe Site unterstützt. Es wird empfohlen, in diesem Szenario die manuelle Zuordnung zu verwenden.

Hauptvorteile

- Laden Sie OT-Subnetze aus autorisierten Quellen (z. B. NetDB oder Firewalls) als Datensätze in einer Instanz ServiceNow hoch, und speichern Sie sie.
- Automatisieren Sie die Zuweisung von OT-Geräten zur ISA-Entität mithilfe von IP-Adressen und OT-Subnetz
- Minimieren Sie Probleme bei der Wiederverwendung privater IP-Adressbereiche über mehrere Sites hinweg

Industrielle Netzwerke verwenden Subnetze, um den privaten IP-Adressraum durch ein einzelnes Subnetz zu teilen, das häufig an einem Teil des Produktionsprozesses oder der Anlagenmodell-Entität ausgerichtet ist. Beispiel: Eine Canning-Linie wird in einem 192.168.101.0/24-Netzwerk ausgeführt, in dem alle Geräte vom Integrator konfiguriert wurden. Die von den Steuerungssystemen oder OT-Geräten verwendeten IPs sind häufig in der Automatisierungssoftware fest codiert, die für den Betrieb der Anlage verwendet wird. Wenn das Subnetz der Canning Line am Standort Atlanta zugeordnet ist, kann ein Manager der Canning Line automatisch eine erkannte SPS mit der IP 192.168.101.66 zuordnen.

Die Zuordnungsfunktion bezieht jedes Subnetz auf eine Anlagenmodell-Entität, sodass Sie OT-Geräte automatisch den Subnetzen zuordnen können, die der Anlagenmodell-Entität zugeordnet sind, basierend auf der IP-Adresse, die beim Import aus einer zertifizierten OT-Integration oder ServiceNow® [Discovery für OT](#) gemeldet wurde.

Ein Systemadministrator kann OT-Subnetz-zuordnungsdatensätze importieren. Ein ISA-Administrator kann über einen Flow für geplante Aufgaben automatisch Zuordnungen von Subnetzen zu Anlagenmodell-Entitäten erstellen. Ein ISA-Editor kann bei Bedarf manuell Zuordnungen eines einzelnen OT-Geräts erstellen.

Personae der Funktion „Automatisierte Zuordnung“

Die automatisierte Zuordnungsfunktion richtet sich an die folgenden Personas.

Personas für die automatisierte Zuordnung

Persona	Beschreibung
Systemadministrator	Der Systemadministrator führt diese Aufgaben aus: • Importiert Daten in die Tabelle „OT-Subnetz zur Anlagenmodell-Entitätszuordnung“. • Aktiviert, plant oder löst den geplanten Flow für die OT-Subnetzzuordnung manuell aus
ISA-Administrator	Der ISA-Administrator löst die UI-Aktion Alle OT-Geräte zuordnen manuell in der Listenansicht der OT-Subnetzzuordnung aus.
ISA-Editor	Der ISA-Editor führt diese Aufgaben aus: • Erstellt und aktualisiert manuell OT-Subnetzzuordnungseinträge für bestimmte Sites • Ordnet einzelne OT-Geräte einer Anlagenmodell-Entität aus einem OT-Gerät-Datensatz zu • Ordnet einer Anlagenmodell-Entität mehrere OT-Geräte aus einem OT-Subnetzzuordnungsdatensatz zu

Plugins

Zum Aktivieren der Zuordnungsfunktion sind die folgenden Plugins erforderlich:

- [Operational Technology Manager](#)
- [Prozessmanager Industrie](#)

Wenn die erforderlichen Plugins installiert sind, kann ein ISA-Administrator über das Anwendungsmenü Prozessmanager Industrie auf die Funktion zur Subnetzzuordnung zugreifen.

Workflow für die automatisierte Zuordnungsfunktion

Prozessmanager Industrie enthält einen automatisierten Flow für die automatisierte Zuordnungsfunktion.

Diese Funktion enthält vordefinierte Flows, mit denen Sie die Zuweisung von OT-Geräten zu Anlagenmodell-Entitäten planen können.

Mit [Flow Designer](#) können Sie den vordefinierten Flow für Ihre Geschäftsanforderungen überprüfen und konfigurieren.

Für diese Funktion verfügbarer Flow

In der folgenden Tabelle ist der vordefinierte Flow aufgeführt, der mit Prozessmanager Industrie verfügbar ist, wenn er mit Operational Technology Manager installiert wird.

Anwendung	Flow
Prozessmanager Industrie bei Installation mit Operational Technology Manager	Flow für OT-Gerät-Zuordnung

Allgemeine Anwendungsfälle für die automatisierte Zuordnungsfunktion

Die folgenden Anwendungsfälle gelten normalerweise für die automatisierte Zuordnungsfunktion:

- Ein OT-Manager verfügt über vorhandene OT-Geräte und möchte bei Bedarf einzelne OT-Geräte zuordnen.
- Ein OT-Administrator möchte neu erkannte OT-Geräte mit gültigen IP-Adressen automatisch einer Anlagenmodell-Entität zuordnen.

Im Folgenden finden Sie einen typischen Workflow für die automatisierte Zuordnungsfunktion.

- Ein Systemadministrator importiert OT-Subnetzdaten mithilfe von [Einfaches Importieren](#) aus einer Excel-Tabelle in die OT-Subnetz-Zuordnungstabelle.
- Entweder überprüft der Experience-Administrator die importierten Datensätze und ordnet OT-Subnetzzuordnungsdatensätze einer Site und/oder der Anlagenmodell-Entität innerhalb dieser Site zu (ordnet sie zu).
- Der AWS-Administrator aktiviert oder löst den geplanten Flow aus, um OT-Geräte für alle Sites in einer Instanz automatisch zuzuordnen.
- Der Erstaunliche Editor kann die Datensätze aktualisieren, die zu den Sites gehören, für die er Bearbeitungszugriff hat.

Konfigurieren Sie die automatisierte Zuordnung von OT-Geräten mithilfe des geführten Setups

Verwenden Sie das geführte Setup Prozessmanager Industrie, um OT-Geräte automatisch der Entität des Anlagenmodells nach ISA zuzuordnen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie über die Administratorrolle verfügen, können Sie das geführte Setup Prozessmanager Industrie verwenden, um sich durch die Zuordnung von OT-Geräten zur Entität des Anlagenmodells nach ISA führen zu lassen. Sie können OT-Geräte für die Sites zuordnen, auf die Sie Zugriff haben.

Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > Geführtes Setup**.
2. Wählen Sie **Erste Schritte** für die Anwendung Prozessmanager Industrie aus.
3. Wählen Sie die Aufgabe **OT-Geräte automatisch zuordnen** aus.
4. Wählen Sie die folgenden Aufgabenregisterkarten aus, und wählen Sie dann **Konfigurieren** aus, um die Konfigurationsaufgaben abzuschließen.

Zugehörige Informationen

[Guided Setup](#) 

[Automatisierte Zuordnung von OT-Geräten zum Anlagenmodell](#)

Ordnen Sie alle OT-Geräte automatisch einer Anlagenmodell-Entität zu

Ein AWS-Administrator kann die automatisierte Zuordnung aller OT-Geräte zur entsprechenden Entität des Anlagenmodells nach ISA auslösen.

Vorbereitungen

Die folgenden Plugins müssen installiert sein:

- [Operational Technology Manager](#)
- [Prozessmanager Industrie](#)

Erforderliche Rolle: sn_ot_amaking_admin

Prozedur

1. Navigieren zu **Industrial Workspace-Administrator** > **Industrial Process Manager** > **OT-Subnetzzuordnung**.
2. Wählen Sie **Alle OT-Geräte zuordnen** aus, um den Flow zum Zuordnen von OT-Geräten auszuführen.

Ergebnisse

OT-Geräte werden automatisch den Anlagenmodell-Entitäten zugeordnet, die in allen aktiven OT-Subnetzzuordnungsdatensätzen aufgeführt sind. Nachdem die Zuordnung ausgelöst wurde, können Sie die Zuordnungsergebnisse anzeigen, indem Sie den in der Informationsnachricht in der Listenansicht verfügbaren Link auswählen.

Hinweis:

Die Subnetzzuordnung unterstützt auch Discovery erstellte Configuration Items (CIs) für Anlagenmodelle nach ISA.

Ordnen Sie alle OT-Geräte in einem Subnetz zu

Ein OT-Administrator kann die automatisierte Zuordnung aller OT-Geräte in einem ausgewählten Subnetz auslösen.

Vorbereitungen

Die folgenden Plugins müssen installiert sein:

- [Operational Technology Manager](#)
- [Prozessmanager Industrie](#)

Erforderliche Rolle: sn_ot_amaking_write

Prozedur

1. Navigieren zu **Industrial Workspace-Administrator** > **Industrial Process Manager** > **OT-Subnetzzuordnung**.
2. Öffnen Sie in der Liste „OT-Subnetzzuordnung“ den Datensatz der OT-Subnetzzuordnung, dessen Geräte Sie zuordnen möchten.

Hinweis:

Die Subnetzzuordnung unterstützt auch Discovery erstellte Configuration Items (CIs) für Anlagenmodelle nach ISA.

3. Stellen Sie sicher, dass die Felder Standort und Anlagenmodell-Entität korrekt ausgefüllt sind.
4. Wählen Sie die UI-Aktion „**OT-Geräte in diesem Subnetz zuordnen**“ aus, um automatisch alle OT-Geräte in dieser Site mit IP-Adressen im ausgewählten OT-Subnetz zuzuordnen.

Ergebnisse

Wenn in der ausgewählten Site OT-Geräte mit IP-Adressen vorhanden sind, die in den ausgewählten IP-Bereich fallen, werden alle Geräte in der Site für das OT-Subnetz zugeordnet. Nachdem die Zuordnung ausgelöst wurde, können Sie die Zuordnungsergebnisse anzeigen, indem Sie den in der Informationsnachricht in der Listenansicht verfügbaren Link auswählen.

Zeigen Sie OT-Geräte an, die keiner Site zugewiesen sind

Zeigen Sie die Liste der Operational Technology (OT-)Geräte an, die keiner Site zugewiesen sind.

Vorbereitungen

Die folgenden Plugins müssen installiert sein:

- [Operational Technology Manager](#)
- [Prozessmanager Industrie](#)

Erforderliche Rolle: cmdb_ot_isa_editor und cmdb_ot_editor

Warum und wann dieser Vorgang ausgeführt wird

Im Rahmen der OT-Gerät-Zuordnung müssen Sie das Gerät einer Site zuweisen, bevor Sie es einer Anlagenmodell-Entität zuordnen. Dazu können Sie eine Liste aller OT-Geräte anzeigen, die keiner Site zugewiesen sind.

Prozedur

1. Navigieren zu **Alle > Operative Technologien (OT) > OT-Geräte ohne Standortzuweisung**.
2. Um ein Gerät einer Site einzeln zuzuweisen, wählen Sie den Gerätedatensatz aus, und aktualisieren Sie das Feld **Site**.
3. Führen Sie die folgenden Schritte aus, um eine Massенbearbeitung durchzuführen, die **Site**-Spalte zu aktualisieren und mehrere Geräte derselben Site zuzuweisen.
 - a. Aktivieren Sie die Kontrollkästchen neben jedem OT-Gerät, das Sie einer Site zuweisen möchten.
 - b. Klicken Sie im Header **der Site** -Spalte auf die Schaltfläche Spaltenoptionen, und wählen Sie **Update Selected (Ausgewählte aktualisieren)** aus.
 - c. Aktualisieren Sie das Feld **Site**.
 - d. Wählen Sie **Aktualisieren**.

Nächste Maßnahme

Die OT-Geräte sind einer Site zugewiesen, aber keiner Anlagenmodell-Entität zugeordnet. Sie können eine Liste der nicht zugeordneten OT-Geräte anzeigen, um die Gerätezuordnung abzuschließen. Weitere Informationen finden Sie unter [Zeigen Sie nicht zugeordnete OT-Geräte an](#).

Zeigen Sie nicht zugeordnete OT-Geräte an

Zeigen Sie eine Liste von Geräten Operational Technology (OT) mit IP-Adressen an, die keiner Anlagenmodell-Entität zugeordnet sind.

Vorbereitungen

Die folgenden Plugins müssen installiert sein:

- [Operational Technology Manager](#)
- [Prozessmanager Industrie](#)

Erforderliche Rolle: cmdb_ot_isa_editor und cmdb_ot_editor

Prozedur

1. Navigieren zu **Alle > Industrial Workspace**.

2. Wählen Sie in der Listenansicht Industriell Arbeitsbereich im Modul **Operational Technology (OT)** die Liste **Nicht zugeordnete OT-Geräte** aus.

Diese Liste zeigt die OT-Gerät-Datensätze mit IP-Adressen und anderen Feldern, mit denen Sie sie Anlagenmodell-Entitäten für den zugewiesenen Standort zuordnen können.

3. **Wahlweise:** Wählen Sie im Header der **Site**-Spalte die Schaltfläche Filter und dann **Group by Site (Nach Standort gruppieren)** aus.

Mit diesem Filter können Sie die nicht zugeordneten OT-Geräte nach Site organisieren und können hilfreich sein, wenn Sie mehrere Sites verwalten.

Nächste Maßnahme

Jetzt können Sie die OT-Geräte Anlagenmodell-Entitäten zuordnen. Weitere Informationen finden Sie unter [Ordnen Sie ein einzelnes OT-Gerät einer Anlagenmodell-Entität zu](#).

Ordnen Sie ein einzelnes OT-Gerät einer Anlagenmodell-Entität zu

Führen Sie bei Bedarf eine Zuordnung eines OT-Geräts zur Entität des Anlagenmodells nach ISA für die Sites durch, auf die Sie Zugriff haben.

Vorbereitungen

Die folgenden Plugins müssen installiert sein:

- [Operational Technology Manager](#)
- [Prozessmanager Industrie](#)

Erforderliche Rolle: sn_ot_amaking_write und cmdb_ot_viewer

Prozedur

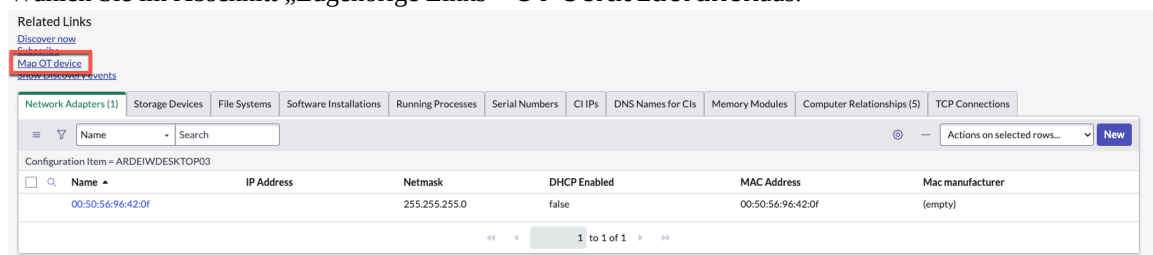
1. Navigieren zu **Alle > Operative Technologien (OT) > Alle OT-Geräte**.

2. Wählen Sie in der Spalte **OT-Gerät** das OT-Gerät aus, das Sie zuordnen möchten.

i Hinweis:

Die Subnetzzuordnung unterstützt auch Discovery erstellte Configuration Items (CIs) für Anlagenmodelle nach ISA.

3. Wählen Sie im Abschnitt „Zugehörige Links“ **OT-Gerät zuordnen** aus.



Ergebnisse

Wenn ein aktives OT-Subnetz vorhanden ist, das der IP-Adresse und dem Standort des ausgewählten Geräts entspricht, wird das Gerät zugeordnet.

Konfigurieren Sie den geplanten Flow für die OT-Subnetzzuordnung

Konfigurieren Sie den OT-Gerät-Zuordnungs-Flow, um OT-Geräte automatisch Sites und Anlagenmodell-Entitäten zuzuordnen.

Vorbereitungen

Die folgenden Plugins müssen installiert sein:

- [Operational Technology Manager](#)
- [Prozessmanager Industrie](#)

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Der OT-Gerät-Zuordnungs-Flow kann so eingestellt werden, dass er auf Zeitplanbasis ausgeführt wird, um OT-Geräte für alle aktiven OT-Subnetzzuordnungsdatensätze automatisch zuzuordnen.

Prozedur

1. Navigieren zu **Industrial Workspace-Administrator** > **Industrial Process Manager** > **Geplanter Flow für OT-Subnetzzuordnung**.
2. **Wahlweise:** Site-Zuordnung aktivieren:
 - a. Öffnen Sie den Abschnitt Flow-Variablen festlegen.
 - b. Aktivieren Sie das Kontrollkästchen neben **Automatische Site-Zuweisung ausführen**, und wählen Sie **Speichern** aus.
3. Um den Flow so zu planen, dass er regelmäßig ausgeführt wird, wählen Sie den Link im Abschnitt Auslöser, um das Intervall zu definieren.
4. Wählen Sie im Header **Aktivieren** aus, um die geplante Ausführung des OT-Gerät-Zuordnungs-Flows zu aktivieren.
Nach der Aktivierung kann dieser Flow zeitplanbasiert ausgeführt werden, um OT-Geräte für alle aktiven OT-Subnetzzuordnungsdatensätze in einer Instanz automatisch zuzuordnen.

Hinweis:

Die Subnetzzuordnung unterstützt auch Discovery erstellte Configuration Items (CIs) für Anlagenmodelle nach ISA.

Zeigen Sie OT-Subnetzzuordnungen an

Zeigen Sie alle zugeordneten OT-Subnetze an, die einer Anlagenmodell-Entität zugewiesen sind.

Vorbereitungen

Erforderliche Rollen:

- sn_ot_amaking_write, cmdb_ot_isa_editor und cmdb_ot_viewer oder
- sn_ot_amaking_admin, cmdb_ot_isa_editor und cmdb_ot_viewer

Prozedur

1. Navigieren Sie mit einer der folgenden Optionen zum Anlagenmodell-Manager:
 - Navigieren zu **Alle > Industrial Workspace-Administrator > Industrial Process Manager > Anlagenmodell-Manager**.
 - Navigieren zu **Alle > Industrial Workspace**. Wählen Sie das Symbol Anlagenmodell ().
2. Wählen Sie in der Ansicht Anlagenmodell den Standort aus, oder erweitern Sie die Anlagenmodell-Hierarchie, um die Entität auszuwählen, für die Sie Zuordnungen anzeigen möchten.
3. Wählen Sie im Entitätsformular die **Registerkarte Zugeordnete OT-Subnetze** zugehörige Liste aus. Die zugeordneten OT-Subnetze werden als aktiv oder inaktiv angezeigt. Nur aktive OT-Subnetze werden in den geplanten Flow aufgenommen. Weitere Informationen finden Sie unter [Konfigurieren Sie den geplanten Flow für die OT-Subnetzzuordnung](#).
4. **Wahlweise:** Um die OT-Subnetze anzuzeigen, die für die Zuordnung auf OT-Gerät-Ebene verwendet werden, wählen Sie die zugehörige Liste **OT-Subnetze** in einem OT-Gerät-Datensatz aus.

Nächste Maßnahme

[Erstellen Sie einen neuen Datensatz für die OT-Subnetzzuordnung](#)

Erstellen Sie einen neuen Datensatz für die OT-Subnetzzuordnung

Erstellen Sie eine neue OT-Subnetzzuordnung, die einer Anlagenmodell-Entität zugeordnet werden soll.

Vorbereitungen

Erforderliche Rolle: sn_ot_amaking_write oder sn_ot_amaking_admin

Hinweis:

Beim Erstellen neuer OT-Subnetzzuordnungsdatensätze sind die neuen Datensätze standardmäßig inaktiv. Um Datensätze automatisch zuzuordnen, wenn der OT-Gerät-Zuordnungs-Flow ausgelöst wird, müssen OT-Subnetz-Zuordnungsdatensätze aktiv sein.

Prozedur

1. Navigieren zu **Industrial Workspace-Administrator > Industrial Process Manager > Anlagenmodell-Entitäten**.
2. Wählen Sie den Standort oder die Anlagenmodell-Entität aus, für die Sie eine neue Zuordnung erstellen möchten.

Hinweis:

Die Subnetzzuordnung unterstützt auch Discovery erstellte Configuration Items (CIs) für Anlagenmodelle nach ISA.

3. Wählen Sie die zugehörige Liste **Zugeordnete OT-Subnetze** und dann **Neu** aus.
4. Füllen Sie die Felder des Formulars aus.

Formular „OT-Subnetz für die Zuordnung von Anlagenmodell-Entitäten“.

Feld	Beschreibung
Name	Zonen- oder VLAN-Name für das Subnetz.

Feld	Beschreibung
Site	Wählen Sie in der Suche die ISA-Site aus der Liste der verfügbaren Sites aus, wenn sie noch nicht ausgefüllt ist.
Typ	Wählen Sie den Subnetztyp aus diesen Optionen aus: • IP-Bereich – eine Teilmenge von IP-Adressen in einem Subnetz • IP-Netzwerk: Das gesamte Subnetz in CIDR-Schreibweise
IP-Startadresse	Start-IP für den IP-Bereich Dieses Feld ist sichtbar, wenn der Typ auf IP-Bereich festgelegt ist.
IP-Endadresse	Endende IP für den IP-Bereich Dieses Feld ist sichtbar, wenn der Typ auf IP-Bereich festgelegt ist.
Quellenname	Name der Quelle, z. B. NetDB oder Firewall.
Firewall-Name	Name der Firewall, die die Zone verwaltet, falls zutreffend.
Beschreibung	Beschreibung für die Subnetzzuordnung.
Aktiv	Wählen Sie Aktiv aus, um das Subnetz in die automatisierte Zuordnung einzubeziehen, wenn der geplante Flow für die OT-Subnetzzuordnung ausgeführt wird.
Anlagenmodell-Entität	Wählen Sie in der Suche die Anlagenmodell-Entität aus der Liste der verfügbaren Entitäten aus, wenn sie noch nicht ausgefüllt ist.
Subnetz	Geben Sie die Subnetzadresse (CIDR-Format) ein. Dieses Feld ist sichtbar, wenn der Typ auf IP-Netzwerk festgelegt ist.
Standort	Fügen Sie dem Subnetzdatensatz einen Standort hinzu, um den Standort in den zugeordneten OT-Geräten automatisch hinzuzufügen oder zu aktualisieren.  Hinweis: Der Standort wird basierend auf der Systemeigenschaft <code>sn_otsm.subnet_mapping.location_auto_update</code> zugeordnet. Weitere Informationen zu Systemeigenschaften, die für die OT-Subnetzzuordnung verwendet werden, finden Sie unter Systemeigenschaften, die von der OT-Subnetzzuordnungsfunktion verwendet werden .
Schnittstellenname	Name für die Firewall-Schnittstelle, falls zutreffend.

Feld	Beschreibung
VLAN-ID	Geben Sie ggf. die VLAN-ID an.

5. Wählen Sie **Absenden**.

Alle zugeordneten OT-Geräte anzeigen

Zeigen Sie eine Liste aller Operational Technology (OT-)Geräte an, die einer Anlagenmodell-Entität zugeordnet sind.

Vorbereitungen

Erforderliche Rolle: sn_ot_amaking_write oder sn_ot_amaking_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie einen übergeordneten Datensatz in der CI-Beziehungstabelle öffnen, können Sie die zugehörige Liste Zugeordnete OT-Geräte anzeigen. Die zugehörige Liste ist eine Rollup-Ansicht, die alle Geräte anzeigt, die untergeordneten Entitäten des Anlagenmodells nach ISA zugeordnet sind, nachdem Sie die übergeordnete Entität des Anlagenmodells nach ISA geöffnet haben. Sie enthält die Datensätze, die eine Zuordnung zwischen einer Anlagenmodell-Entität und einem Gerät darstellen.

Prozedur

1. Führen Sie die folgenden Aktionen aus, um die zugeordneten OT-Geräte in Industrial Workspace anzuzeigen.

- a. Navigieren Sie zum Industrial Workspace.
- b. Wählen Sie das Symbol Anlagenmodell ().
- c. Öffnen Sie die Anlagenmodell-Entität, für die Sie die zugeordneten Geräte anzeigen möchten.
- d. Wählen Sie die Registerkarte **Zugeordnete OT-Geräte**.

Hinweis:

Die Spalte „**Zugeordnete Anlagenmodell-Entität**“ gibt die Anlagenmodell-Entität an, der das Gerät zugeordnet ist. Sie können ein Gerät mehreren Anlagenmodell-Entitäten zuordnen.

2. Um die zugeordneten OT-Geräte auf Now Plattform anzuzeigen, navigieren Sie zu **Alle > Industrial Workspace-Administrator > Industrial Process Manager > Zugeordnete OT-Geräte**.

Diese Liste enthält alle Geräte, die verschiedenen Anlagenmodell-Entitäten zugeordnet sind. Die Beziehung **Automatisiert durch :: Automatisiert** CI wird auf die über- und untergeordneten Entitäten angewendet.

In dieser Liste können Sie die **Spalte Zugeordnete Anlagenmodell-Entität** verwenden, um die Anlagenmodell-Entität zu identifizieren, der das Gerät zugeordnet ist. Weitere Informationen zum Hinzufügen einer Spalte zu einer Liste finden Sie unter [Personalize a list](#) .

Systemeigenschaften, die von der OT-Subnetzzuordnungsfunktion verwendet werden

Ein Advanced-Administrator kann die Systemeigenschaften anzeigen und konfigurieren, die die OT-Subnetzzuordnungsfunktion unterstützen.

Anwender mit der Rolle „Erstaunlicher Administrator“ können auf die Einstellungen für die OT-Subnetzzuordnung zugreifen, indem sie zu navigieren **Industrial Workspace-Administrator > Industrial Process Manager > Eigenschaften der OT-Subnetzzuordnung**.

Systemeigenschaften für die OT-Subnetzzuordnung

Eigenschaft	Beschreibung
<code>sn_otsm.map_all_ot_assets.all_discovery_sources</code>	Steuern Sie die Zuordnung von OT-Geräten für alle Discovery-Quellen. OT-Geräte für alle Discovery-Quellen zuordnen. Wenn diese Option aktiviert ist, werden die folgenden spezifischen Discovery-Quellen überschrieben. Der Standardwert ist „Ja“ (wahr). Standardwert: true
<code>sn_otsm.map_all_ot_assets.discovery_sources</code>	OT-Geräte für angegebene Discovery-Quellen zuordnen (kommagetrenntes Format). Gilt nur, wenn oben „OT-Geräte für alle Discovery-Quellen zuordnen“ deaktiviert ist.
<code>sn_otsm.subnet_mapping.auto_assign_ot_devices</code>	Wenn die OT-Subnetzmappingmodule automatisch Anlagenmodell-Entitäten basierend auf der Beziehung „Eigentümer von::Eigentum von“ zu. Der Standardwert ist „Ja“ (wahr).
<code>sn_otsm.subnet_mapping.location_auto_update</code>	Überprüfen Sie den Standort eines OT-Geräts mit dem Standort des Subnetzes. Wenn diese Option aktiviert ist, hat der Standort des Subnetzes Vorrang vor dem Standort des OT-Geräts, wenn es dem Subnetz zugeordnet wird. Der Standardwert ist „Ja“.

Komponenten der automatisierten Zuordnung, die installiert werden, wenn Prozessmanager Industrie und Operational Technology Manager installiert werden

Bei der Aktivierung von Prozessmanager Industrie werden verschiedene Arten von Komponenten für die automatisierte Zuordnung installiert, wenn auch Operational Technology Manager aktiv ist, einschließlich Tabellen, Systemeigenschaften und geplanten Flows.

Diese Komponenten für die automatisierte Zuordnung werden mit installiert oder sind verfügbar, wenn Prozessmanager Industrie mit Operational Technology Manager installiert wird.

Tabellen

Tabelle	Beschreibung
Zuordnung von OT-Subnetz zu Anlagenmodell-Entität <code>ot_subnet_mapping</code>	Speichert die Zuordnungen von OT-Subnetz zu Anlagenmodell-Entitäten.

Eigenschaften

Eigenschaft	Beschreibung
<code>sn_otsm.map_all_ot_assets.all_discovery_sources</code>	Steuern Sie die Zuordnung von OT-Geräten für alle Discovery-Quellen. Standardwert: true

Eigenschaften (Fortsetzung)

Eigenschaft	Beschreibung
sn_otsm.map_all_ot_assets.discovery_sources	OT-Geräte für angegebene Discovery-Quellen zuordnen (kommagetrenntes Format).
sn_otsm.subnet_mapping.auto_assign_ot_control_modules	Weist alle OT-Steuerungsmodule automatisch Anlagenmodell-Entitäten basierend auf der Beziehung „Eigentümer von::Eigentum von“ zu. Der Standardwert ist „Ja“ (wahr).
sn_otsm.subnet_mapping.location_auto_update	Überschreiben Sie den Standort eines OT-Geräts mit dem Standort des Subnetzes. Wenn diese Option aktiviert ist, hat der Standort des Subnetzes Vorrang vor dem Standort des OT-Geräts, wenn es dem Subnetz zugeordnet wird. Der Standardwert ist „Ja“.

Flow Designer-Flows

Anwendung	Flow
Integration von Operational Technology Manager in Prozessmanager Industrie	Flow für OT-Gerät-Zuordnung

Prozessmanager Industrie-Referenz

Referenzthemen enthalten zusätzliche Informationen zur Anwendung Prozessmanager Industrie.

Mit Prozessmanager Industrie installierte Komponenten

Bei der Aktivierung der Anwendung Prozessmanager Industrie können verschiedene Arten von Komponenten installiert werden, einschließlich Anwenderrollen.

** Hinweis:**

In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter [Komponenten finden, die mit dieser Anwendung installiert wurden](#) .

Installierte Rollen

Rolle	Beschreibung
Anlagenmodell-Betrachter [cmdb_ot_isa_viewer]	Kann nur die zugewiesenen Datensätze der Tabelle „Anlagenmodell nach ISA [cmdb_ci_ot_isa_entity] anzeigen. Weitere Informationen finden Sie unter Prozessmanager Industrie mit Operational Technology Manager verwenden und Anlagenmodelle verwalten .
Anlagenmodell-Editor [cmdb_ot_isa_editor]	Kann die zugewiesenen Datensätze im Anlagenmodell nach ISA [cmdb_ci_ot_isa_entity] anzeigen und bearbeiten. Weitere Informationen finden Sie unter Prozessmanager Industrie mit Operational

Rolle	Beschreibung
	Technology Manager verwenden und Anlagenmodelle verwalten.
Anlagenmodell-Administrator [cmdb_ot_isa_admin]	Sie erben die Rolle „cmdb_ot_isa_editor“ und können außerdem die folgenden Aktionen ausführen: • Verwenden Sie das geführte Setup für Industriell, um Prozessmanager Industrie und Operational Technology Managereinzurichten. • Bearbeiten Sie die Tabelleneinträge Anlagenmodell-Vorlage [isa_entity_template], [isa_entity_level] und Anlagenentitätstyp [isa_entity_type]. Weitere Informationen finden Sie unter Administrator für den industriellen Arbeitsbereich Anwendungsmenü und im geführten Setup.
ISA-Site-Viewer [cmdb_ot_isa_bypass_qbr]	Kann alle Sites in der OT-Fortschrittsbewertungsliste anzeigen.
Anlagenmodell-Ausfallzeitplaner [sn_isa_schedule_admin]	Kann Zeitpläne für Anlagenentitäten erstellen, ändern und löschen. Kann Zeitpläne auch mit Anlagenentitäten verknüpfen.
Anlagenmodell-Betrachter – Alle [cmdb_ot_isa_viewer_all]	Kann alle Datensätze des Anlagenmodells nach ISA (cmdb_ci_ot_isa_entity) und die zugehörigen Anlagenmodell-Vorlagendatensätze (isa_entity_template, isa_entity_level, isa_entity_type) anzeigen. In cmdb_ot_admin enthaltene Rolle.
Erstaunlicher Administrator [sn_ot_amaking_admin]	Kann OT-Subnetzdatensätze (ot_subnet_mapping) für alle OT-Subnetz-Systemeigenschaften der Anlagenmodell-Entität erstellen, ändern und löschen.
Erstaunlicher Editor [sn_ot_amaking_write]	Kann OT-Subnetzdatensätze (ot_subnet_mapping) für alle Anlagenmodell-Entitäten erstellen, ändern und löschen, die dem Anwender zugeordnet sind.
Erstaunlicher Betrachter [sn_ot_amaking_read]	Kann OT-Subnetzdatensätze (ot_subnet_mapping) für alle Anlagenmodell-Entitäten anzeigen.

Der Site-Benutzerzugriff wird auf Benutzerkriterien und -gruppen migriert

Wenn Sie ein Upgrade auf Version 1.0.12 des Anlagenmodells nach ISA durchführen, beginnt die Migration vom Site-Benutzerzugriff zu Benutzerkriterien und -gruppen automatisch.

Die folgenden Änderungen treten auf, wenn Sie ein Upgrade auf Version 1.0.12 des Anlagenmodells nach ISA durchführen.

- Verbesserte Zugriffssteuerung auf Site-Ebene für, die Benutzerkriterien verwendet, um den Benutzerzugriff auf Lese- oder Schreibebene für Anlagenmodell-Entitäten zu definieren. Durch die zusätzliche Zuweisung der Rollen OT-Betrachter (cmdb_ot_viewer) oder OT-Editor (cmdb_ot_editor) können Sie auch über Anzeige- oder Bearbeitungszugriff auf OT-Geräte an den entsprechend zugewiesenen Sites verfügen.

- Wenn Sie ein Upgrade auf Version 1.0.12 des Anlagenmodells nach ISA durchführen, werden vorhandene Site-Benutzerdatensätze zu einem verbesserten Zugriffssteuerungsmodell migriert, bei dem Benutzerkriterien verwendet werden, um die gleichen Zugriffsberechtigungen beizubehalten. Für jede Site mit ISA-Entitäts-Site-Benutzer-Datensätzen werden die folgenden Änderungen vorgenommen.
 - Für Benutzer mit Betrachter-Zugriff:
 - Ein neuer Anwenderkriteriendatensatz mit dem Namen **Anwenderkriterien lesen für** wird erstellt <site name> Standort [vom System generiert]
 - Eine neue Anwendergruppe mit allen Site-Anwendern dieser Site wird erstellt und trägt den Namen **„Gruppe lesen für“**. <site name> Standort [vom System generiert]
 - In der neuen Tabelle „Anlagenmodell-Entitätsansichtszugriff“ (isa_entity_m2m_user_criteria_can_view) wird ein neuer Datensatz mit den neuen Anwenderkriterien und der neuen Anwendergruppe erstellt.
 - Für Benutzer mit Editor-Zugriff:
 - Ein neuer Anwenderkriteriendatensatz mit dem Namen **Anwenderkriterien bearbeiten für** wird erstellt <site name> Standort [vom System generiert]
 - Eine neue Anwendergruppe mit allen Site-Anwendern dieser Site wird erstellt und trägt den Namen **Gruppe bearbeiten für** <site name> Standort [vom System generiert]
 - In der neuen Tabelle „Anlagenmodell-Entitätsbearbeitungszugriff“ (isa_entity_m2m_user_criteria_can_edit) wird ein neuer Datensatz mit den neuen Anwenderkriterien und der neuen Anwendergruppe erstellt.
- Das Anwendungsmenü „Site-Anwender“ und die zugehörige Liste „Site-Anwender“ im Datensatz „Anlagenmodell-Entität“ für eine Site werden entfernt.
- Alle Site-Anwender-Datensätze (isa_entity_site_user) werden auf inaktiv gesetzt.
- Die Anwendungsmenüelemente **„Site-Anwender – Kann lesen“** und **„Site-Anwender – Kann bearbeiten“** werden zu Now Platform hinzugefügt.
- Die zugehörigen Listen **„Kann Anlagenmodelle lesen“** und **„Kann Anlagenmodelle bearbeiten“** werden dem Anlagenmodell-Entitätsdatensatz für einen Standort hinzugefügt.

Formular „Benutzerkriterien“

Sie können das Formular „Benutzerkriterien“ verwenden, um zu bestimmen, ob bestimmte Benutzer auf die Anlagenmodell-Entitäten für bestimmte Sites zugreifen können.

In der folgenden Tabelle werden die Felder des Formulars „Anwenderkriterien“ beschrieben.

Formular „Benutzerkriterien“

Feld	Beschreibung
Name	Name der Benutzerkriterien.
Kurzbeschreibung	Kurze Beschreibung der Anwenderkriterien für den Zugriff auf die Anlagenmodell-Entitäten der Site.
Anwender	Benutzer, die auf die Anlagenmodell-Entitäten der Site zugreifen können, wenn Sie die Anwenderkriterien anwenden. Wählen Sie die Benutzer aus, die auf die Entitäten zugreifen können, indem Sie das Symbol zum Entsperren von Benutzern

Formular „Benutzerkriterien“ (Fortsetzung)

Feld	Beschreibung
	() wählen. Fügen Sie sich selbst als Benutzer hinzu, indem Sie das Symbol „Mich hinzufügen“ () wählen.
Gruppen	Gruppen, die auf die Anlagenmodell-Entitäten der Site zugreifen können, wenn Sie die Anwenderkriterien anwenden. Wählen Sie die Gruppen aus, indem Sie das Symbol zum Entsperren von Gruppen () wählen.
Rollen	Rollen, die auf die Anlagenmodell-Entitäten der Site zugreifen können, wenn Sie die Anwenderkriterien anwenden. Wählen Sie die Gruppen aus, indem Sie das Symbol zum Entsperren von Gruppen () wählen.
Erweitert	Option zum Erstellen eines Skripts für die Benutzerkriterien
Anwendung	Feld, das automatisch auf Globalfestgelegt wird.
Aktiv	Option, über die die Benutzerkriterien verfügbar gemacht werden können
Unternehmen	Unternehmen, die auf die Anlagenmodell-Entitäten der Site zugreifen können, wenn Sie die Anwenderkriterien anwenden. Wählen Sie die Unternehmen aus, indem Sie das Symbol zum Entsperren von Unternehmen () wählen.
Standorte	Standorte, die auf die Anlagenmodell-Entitäten der Site zugreifen können, wenn Sie die Anwenderkriterien anwenden. Wählen Sie die Standorte aus, indem Sie das Symbol zum Entsperren von Standorten () wählen.
Abteilungen	Abteilungen, die auf die Anlagenmodell-Entitäten der Site zugreifen können, wenn Sie die Anwenderkriterien anwenden. Wählen Sie die Abteilungen aus, indem Sie das Symbol zum Entsperren von Abteilungen () wählen.
Alle abgleichen	Option, um jede Bedingung obligatorisch zu machen, wenn die Anwenderkriterien angewendet werden. Die Bedingungen werden in den vorherigen Feldern festgelegt, z. B. in den Feldern Standort , Abteilung .

Systemeigenschaften für das Anlagenmodell nach ISA

Aktivieren Sie die Systemeigenschaften für das Anlagenmodell nach ISA nach Bedarf.

Sie können auf die Systemeigenschaften für das Anlagenmodell nach ISA zugreifen, indem Sie zu navigieren **Alle > Industrial Workspace-Administrator > Alle OT-Eigenschaften**.

Weitere Informationen zum Anzeigen und Bearbeiten der OT-Systemeigenschaften finden Sie unter [Zeigen Sie OT-Systemeigenschaften an, und bearbeiten Sie sie](#).

In der folgenden Tabelle werden die Systemeigenschaften für das Anlagenmodell nach ISA beschrieben.

Systemeigenschaften des Anlagenmodells nach ISA

Systemeigenschaft	Beschreibung	Typ
sn_isa_model.cmdb_relationships_sync	Anzahl der Ebenen von CMDB Beziehungen, die synchronisiert werden.	Ganzzahl
sn_isa_model.short_code_validation	Die maximale Länge für die Kurzwahlvalidierung.	Ganzzahl
sn_isa_model.user_search_matching	Die Spalte in der Benutzertabelle [sys_user], die einem Benutzer im System entspricht. Standardmäßig wird die Spalte E-Mail in der Benutzertabelle verwendet.	Zeichenfolge

Vordefinierte Filter für Prozessmanager Industrie

Die Anwendung **Prozessmanager Industrie** verwendet vordefinierte Filter, sodass Sie die Abhängigkeitszuordnungen für Anlagenmodelle anzeigen können, indem Sie die verfügbaren UI-Aktionen in **Industriell Arbeitsbereich** auswählen.

Die folgenden vordefinierten Filter sind für **Prozessmanager Industrie** verfügbar.

Anlagenmodell nach ISA – Hierarchieprozess

Die hierarchische Struktur der ausgewählten Anlagenmodell-Entität und ihre Beziehungen zu anderen Entitäten im Produktionsprozess.

Anlagenmodell nach ISA – OT-Abhängigkeitszuordnung

Die hierarchische Struktur der ausgewählten Anlagenmodell-Entität und ihre Beziehung zu anderen Entitäten und Operational Technology (OT-Geräten im Produktionsprozess).

Anlagenmodell nach ISA – OT-Gerätezuordnung

Die grafische Darstellung der ausgewählten Anlagenmodell-Entität und ihre Beziehung zu anderen OT-Geräten im Produktionsprozess.

Anlagenmodell nach ISA – Prozess

Die grafische Darstellung der ausgewählten Anlagenmodell-Entität und ihre Beziehung zum Produktionsprozess.

Sie können die Abhängigkeitszuordnungen des Anlagenmodells mit den beschriebenen vordefinierten Filtern anzeigen, indem Sie zum **Industrial Workspace** navigieren und die Anlagenmodell-Ansicht öffnen. Anschließend können Sie die Anlagenmodell-Entität auswählen, für die Sie eine Abhängigkeitszuordnung anzeigen möchten. Wenn Sie den -Datensatz öffnen, werden die folgenden UI-Aktionen angezeigt, aus denen Sie auswählen können:

- OT-Abhängigkeitszuordnung anzeigen

i Hinweis:

Sie können die OT-Abhängigkeitszuordnung auch in einem OT-Gerät-Datensatz anzeigen, indem Sie im Datensatzheader **Karte anzeigen** auswählen.

- OT-Gerätezuordnung anzeigen
- Hierarchie anzeigen
- Prozess anzeigen

Sie können auch die vordefinierten Filter nach Bedarf für Ihre Organisation aktualisieren. Weitere Informationen finden Sie unter [Ändern Sie vordefinierte Filter](#).

Ändern Sie vordefinierte Filter

Ändern Sie die vordefinierten Filter für die Anwendung Anlagenmodell nach ISA nach Bedarf für Ihre Organisation.

Vorbereitungen

Erforderliche Rolle: `ecmdb_admin`

Prozedur

1. Navigieren zu **Alle > Abhängigkeitsansichten > Vordefinierte Filter**.
2. Wenden Sie den Filter **[Anwendung] [ist] [Anlagenmodell nach ISA] an**.
3. Wählen Sie den vordefinierten Filterdatensatz aus, den Sie bearbeiten möchten.
4. Ändern Sie die zugehörigen Listen Konfigurationstypen, CI-Filter und Beziehungstypen nach Bedarf. Weitere Informationen zum Ändern dieser zugehörigen Listen finden Sie unter [Create a predefined filter](#).
5. Wählen Sie **Aktualisieren**.

Standort vs. Standort

Die Attribute „site“ und „location“ haben unterschiedliche Verwendungszwecke für Operational Technology (OT).

Site

Ein Standort ist Teil der Entität im Anlagenmodell nach ISA und beschreibt einen Industriestandort, an dem der Produktionsprozess stattfindet. Standorte sind logisch und können zum Definieren eines Anlagenmodells verwendet werden. Dieses Anlagenmodell können Sie dann für die Zugriffssteuerung verwenden. Weitere Informationen zur Zugriffssteuerung finden Sie unter [Gewähren Sie Nicht-Administratoren Zugriff auf den Anlagenmodell-Standort, oder entfernen Sie ihn](#).

Sites können einen Standort haben, werden jedoch nicht als Standort betrachtet. Jedes OT-Gerät kann einen Standort haben und einer Anlagenmodell-Entitätsstandort zugewiesen werden.

Standort

Standort bezieht sich auf den in der Tabelle „**Standorte**“ (`cmn_location`) gespeicherten Wert. Es handelt sich um den physischen Standort eines Anlagenmodells oder Geräts. Wenn beispielsweise eines Ihrer Anlagenmodelle zum Standort Atlanta gehört und sich in Atlanta, GA befindet, geben Sie als Standort **Atlanta, GA** an.

Zugehörige Informationen

Weitere Informationen zur Erweiterungsklasse des Netzwerkangriffserkennungssystems (Network Intrusion Detection System, NIDS), zu OT-Erweiterungsklassen und zu zugehörigen Anwendungen.

Übersicht über Erweiterungsklassen

Die Erweiterungsklassen helfen Ihnen zu verstehen, wie Operational Technology-Management mit Configuration Management Database (CMDB) funktioniert.

Network Intrusion Detection System (NIDS) CI extension class

Die Klasse des Netzwerkangriffserkennungssystems (Network Intrusion Detection System, NIDS) [cmdb_ci_nids] erstellt die Beziehungen zwischen passiven Netzwerküberwachungsgeräten und den Geräten im Netzwerk, die erkannt werden.

Operational Technology (OT) extension classes

Configuration Management Database (CMDB) aktualisiert Klassen für OT.

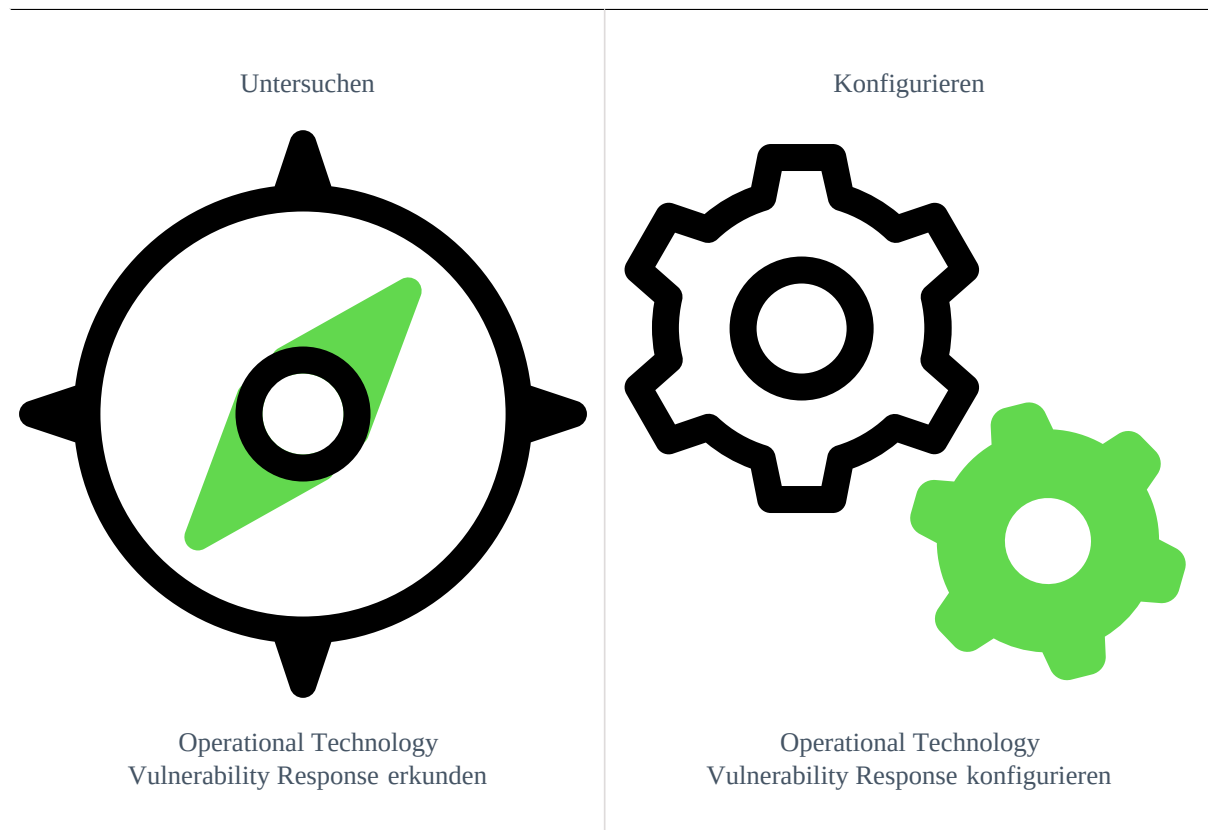
Zugehörige Anwendungen

Operational Technology Manager

Mit der Anwendung Operational Technology Manager können Sie OT-Gerät-Daten aus mehreren Quellen zusammenfassen, um die grundlegenden Datenbeziehungen aufzubauen, die in der Lösung Industriell verwendet werden.

Operational Technology Vulnerability Response

Operational Technology Vulnerability Response ermöglicht die effektive Priorisierung und Behebung von OT-Gerät-Schwachstellen auf Site-Ebene. Durch die Nutzung der CMDB-Beziehungen von OT-Geräten können angreifbare Geräte oder Elemente basierend auf der Relevanz des von ihnen automatisierten Produktionsprozesses priorisiert werden.

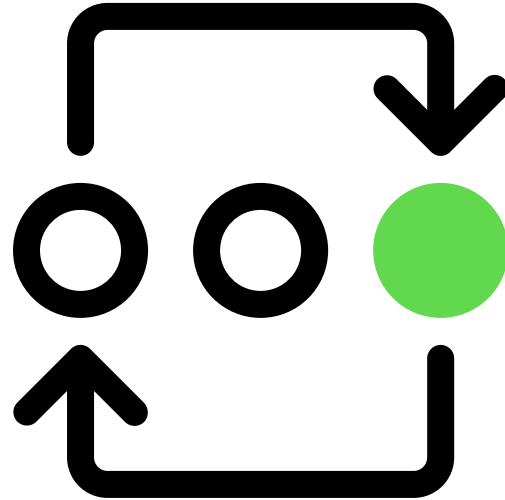


Verwenden



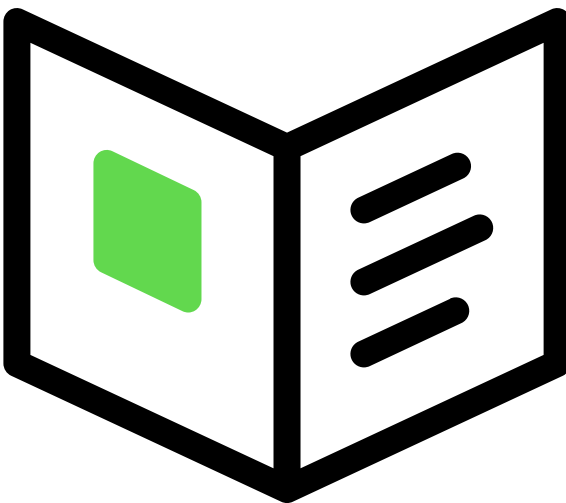
Operational Technology
Vulnerability Response verwenden

integrieren



Erweitern Sie Operational Technology
Vulnerability Response durch die
Integration mit anderen Anwendungen

Referenz



Erhalten Sie Details zu zugehörigen
Informationen und Anwendungen.

Automatische Übersetzung

Operational Technology Vulnerability Response erkunden

Verwenden Sie Operational Technology Vulnerability Response als integrierte Lösung für den industriellen Produktionsprozess.

Operational Technology Vulnerability Response – Übersicht

[https://player.vimeo.com/video/1020858131?](https://player.vimeo.com/video/1020858131?h=c90c2ff89a&badge=0&autoplay=0&player_id=0&app_id=58479)

[h=c90c2ff89a&badge=0&autoplay=0&player_id=0&app_id=58479](https://player.vimeo.com/video/1020858131?h=c90c2ff89a&badge=0&autoplay=0&player_id=0&app_id=58479)

Als OT-Ingenieur oder OT-Schwachstellenmanager können Sie Operational Technology Vulnerability Response mit Antworten auf folgende Fragen finden, z. B.:

- Was sind meine OT-Geräte-Schwachstellen? 
- Wie kann ich die Nachbesserung von Schwachstellen mit OT-spezifischem Risiko priorisieren?
- Welche Fortschritte machen wir bei der Behebung von OT-Schwachstellen?

Status von Korrekturaufgaben und angreifbaren Elementen

Angreifbare Elemente (VITs) und ihre Korrekturaufgaben können aufgrund komplexer Anwendungsfälle unterschiedliche Status aufweisen. Weitere Informationen zu Korrekturaufgaben und Status angreifbarer Elemente sowie zu deren Workflow finden Sie unter [Vulnerability Response remediation task and vulnerable item states](#) .

Schlüsselfunktionen

Mit Operational Technology Vulnerability Response können Sie die folgenden wichtigen Funktionen verwenden.

- Das Dashboard Operational Technology Vulnerability Response (PA) verfolgt das Volumen, die Leistung und den Fortschritt von OT-VITs von der ersten Analyse und Erkennung bis zur Eindämmung oder Behebung.
- Das Dashboard Operational Technology (OT) Rollup für Schwachstellenrisiken enthält die Risikopunktzahl der OT-Geräte auf jeder Ebene des Anlagenmodells.

Operational Technology Vulnerability Solution Management

Ab Version Xanadu ist Operational Technology (OT) Vulnerability Solution Management eine Funktion, die in der Anwendung Operational Technology Vulnerability Response verfügbar ist.

Sicherheits- und IT-Teams wenden häufig viel Zeit und Arbeit auf, um Schwachstellenergebnisse zu recherchieren und die effektivsten Lösungen für ihre Umgebung zu identifizieren. In großen Organisationen ist die Übertragung von Schwachstellenergebnissen in Korrekturaufgaben aufgrund des Umfangs und der Komplexität der Schwachstellen ein manueller, langwieriger und fehleranfälliger Prozess.

OT Vulnerability Solution Management korreliert automatisch die Schwachstellenergebnisse in Ihrer Umgebung mit möglichen Lösungen, die sie beheben. Sie können die Korrekturaktionen identifizieren, die für Ihre Schwachstellen gelten, und sie nach dem Schweregrad des Schwachstellenrisikos priorisieren. Außerdem können Sie das Risiko von Schwachstellen, die nicht sofort gepatcht werden können, mindern, indem Sie Ausgleichssteuerungen für OT verwenden. Weitere Informationen finden Sie unter [Verwenden Sie Ausgleichssteuerungen für Operational Technology](#).

Die OT-Funktion Vulnerability Solution Management basiert auf der in der Anwendung Vulnerability Response verfügbaren Funktion. Weitere Informationen zur Verwaltung von Schwachstellenlösungen finden Sie unter [Vulnerability Solution Management](#) .

OT Vulnerability Solution Management unterstützt das generische Format für die Integration von Solution Intelligence. Das generische Framework für die Integration von Solution Intelligence erfasst Daten in verschiedenen Dateiformaten von Lösungsanbietern. Diese

Formate beschleunigen den Austausch und die Verarbeitung von Informationen. Es verbessert auch die Freigabe kritischer sicherheitsbezogener Informationen in einem standardisierten Berichterstellungsformat. Das unterstützte Dateiformat ist Common Security Advisory Framework (CSAF), ein Open-Source-Standard, der JSON-basierte strukturierte, maschinenlesbare Sicherheitswarnhinweise bereitstellt. Wichtige Lieferanten wie Cybersecurity & Infrastructure Security Agency (CISA), SIEMENS, HITAMI, SCHNEID Electric und andere unterstützen das CSAF-Format.

Das von CSAF unterstützte Lösungsmanagement umfasst die folgenden Schlüsselfunktionen:

- Konfiguration über den Setup-Assistenten. Weitere Informationen finden Sie unter [Configure vulnerability solution providers](#) .
- Unterstützung für den Import von CSAF-Daten über Dateiimport. Weitere Informationen finden Sie unter [Import Common Security Advisory Framework data through file import](#) .
- Unterstützung für den Import von CSAF-Daten über die CSAF-URL. Weitere Informationen finden Sie unter [Import Common Security Advisory Framework \(CSAF\) data through CSAF URL](#) . Mit OT Vulnerability Solution Management können Sie CSAF-Daten importieren aus:
 - Einzelne Lieferanten, die das CSAF-Format unterstützen und über einen CSAF-URL-ROLIE-Feed verfügen. Sie können den vom Lieferanten bereitgestellten CSAF-URL-ROLIE-Feed verwenden, um die CSAF-Daten zu importieren. Zum Beispiel der URL-ROLIE-Feed von Windows.
 - CSAF-Aggregatoren oder vertrauenswürdige Anbieter über einen URL-Import, der den ROLIE-Feed unterstützt. Sie können CSAF-Daten mehrerer Lieferanten von einem vertrauenswürdigen Anbieter importieren. CISA ist beispielsweise ein vertrauenswürdiger Anbieter, und Sie können CSAF-Daten mehrerer Lieferanten aus den CSAF-Hinweisen für Industrial Control System (ICS) importieren, die sich im [GitHub CSAF-Repository von CISA](#)  befinden. Diese Schwachstellenlösungen werden basierend auf Common Vulnerabilities and Exposures (CVE) automatisch den richtigen Lieferanten und angreifbaren Elementen (VITs) zugeordnet. Die Verwendung eines vertrauenswürdigen Anbieters reduziert den Zeit- und Arbeitsaufwand für den Import von CSAF-Daten aus den CSAF-URLs einzelner Lieferanten.
- Unterstützung für den Import von CSAF-Daten über Hinweise oder mithilfe der APIs. Weitere Informationen finden Sie unter [Import Common Security Advisory Framework data from advisories](#) .

Hinweis:

Navigieren zu **Alle > Vulnerability Response > Lösungen > Alle** um die Liste der Lösungen anzuzeigen, die Sie mit den oben genannten Methoden importiert haben.

Das Plugin Vulnerability Response übernimmt die Aktualisierung der Metrikstatus der erstellten Lösung.

Zugehörige Informationen

[Zeigen Sie Lösungen eines angreifbaren Elements im an Industrial Workspace](#)

Operational Technology Vulnerability Response konfigurieren

Konfigurieren Sie Zuweisungsregeln für Operational Technology (OT), Korrekturziele, Risikorechner und Risiko-Rollup-Berechnung. Konfigurieren Sie dann Integrationen, um Datensätze für angreifbare Elemente zu erstellen.

Hinweis:

Wenn Sie über die Rolle `sn_vul.vulnerability_admin` verfügen, können Sie sich anhand des Industriell Geführten Setups durch das Setup der Anwendung Operational Technology Vulnerability Response führen lassen.

Um auf das geführte Setup zuzugreifen, navigieren Sie zu **Industrial Workspace-Administrator > Geführtes Setup**.

Aufgabe	Zweck
1. Installieren Sie Operational Technology Vulnerability Response von ServiceNow Storeaus.	Installieren Sie die Anwendung Operational Technology Vulnerability Response.
2. Weisen Sie Administratoren oder Benutzergruppen bei Bedarf Rollen zu.	Weist Rollen zu, um die für jeden Benutzer verfügbaren Aktionen zu steuern.
3. Weisen Sie dem Besitzer der OT-Schwachstellenkorrektur Rollen zu.	Weist Rollen zu, um die Aktionen zu steuern, die für den Besitzer der OT-Schwachstellenkorrektur verfügbar sind.
4. Erstellen Sie Zuweisungsgruppen, und weisen Sie Benutzer Sites und Gruppen zu. 1. Erstellen Sie für jeden Standort im Anlagenmodell-Manager eine Operational Technology Vulnerability Response -Standortzuweisungsgruppe. 2. Weisen Sie Sites Anwender zu, die bereits über die Rolle „ <code>cmdb_ot_isa_viewer</code> “ oder „ <code>cmdb_ot_isa_editor</code> “ verfügen. 3. Fügen Sie der Zuweisungsgruppe für ihre Site Benutzer hinzu.	• Ermöglicht Anwendern von OT-Korrekturbesitzern, nur angreifbare Elemente für ihre Site anzuzeigen. • Ermöglicht Benutzern das Anzeigen der angreifbaren Elemente für die Sites, denen sie zugewiesen sind.
5. Konfigurieren Sie die OT-Korrekturzielregeln.	• Weist angreifbare OT-Elemente Gruppen auf Site-Ebene oder Gruppen basierend auf der Klassifizierung zu. • Definiert den erwarteten Zeitrahmen für die Korrektur angreifbarer Elemente.
6. Laden Sie die Demodatensätze für die Anwendung Operational Technology Vulnerability Response .	Berechnet das Korrekturziel für angreifbare OT-Elemente.
7. Konfigurieren Sie OT-Risikorechner.	Bestimmt, welche OT-Risikofaktoren bei der Berechnung des Risikos eines angreifbaren Elements auf einem OT-Gerät verwendet werden sollen.
8. Konfigurieren Sie den Rollup-Rechner für OT-Risiken.	Berechnet die Risikopunktzahl der OT-Geräte auf jeder Ebene für die Anlagenmodell-Entität.
9. Installieren Sie Operational Technology Zertifizierte Integrationen für die Anwendung Operational Technology Vulnerability Response , die für Ihre Umgebung geeignet sind.	Integriert zertifizierte Drittanbieteranwendungen, die die Funktionalität des OT-Schwachstellenmanagements verbessern.

Operational Technology Vulnerability Response installieren

Mit der Administratorrolle können Sie die Anwendung Operational Technology Vulnerability Response installieren. Diese Anwendung enthält Demodaten und installiert die zugehörigen Store-Anwendungen und Plugins, falls sie nicht bereits installiert sind.

Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter [Rufen Sie eine Berechtigung für ab ServiceNow Produkt oder Anwendung](#) .
- Wenn die Anwendung Plugins oder weitere Anwendungen aus dem ServiceNow Store erfordert, installieren Sie diese zuerst, falls dies noch nicht geschehen ist.
- Operational Technology Vulnerability Response erfordert die folgenden Plugins. Stellen Sie sicher, dass diese Plugins aktiviert sind, bevor Sie Operational Technology Vulnerability Response installieren.

Benötigte ServiceNow-Plugins

Vulnerability Response (sn_vul)

Die Anwendung ServiceNow® Vulnerability Response importiert und gruppiert angreifbare Elemente automatisch gemäß Gruppenregeln, sodass Sie Schwachstellen beheben können. Weitere Informationen finden Sie unter [Vulnerability Response installieren](#) .

Prozessmanager Industrie (sn_otsm)

Erstellt die Datengrundlage des Anlagenmodells nach ISA-95, die für die Lösung ServiceNow® Industriell erforderlich ist. Weitere Informationen finden Sie unter [Prozessmanager Industrie installieren](#).

Operational Technology Manager

Die Anwendung Operational Technology Manager erstellt die grundlegenden Daten und Beziehungen, die es Ihrem Unternehmen ermöglichen, die Lösung ServiceNow® Industriell zu verwenden. Operational Technology Manager unterstützt die Verwendung der Anwendungen Configuration Management Database (CMDB), Service Graph Connectors und Discovery in Now Platform. Weitere Informationen finden Sie unter [Operational Technology Manager \(OTM\) konfigurieren](#).

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die folgenden Elemente werden mit der Installation der Anwendung Operational Technology Vulnerability Response installiert:

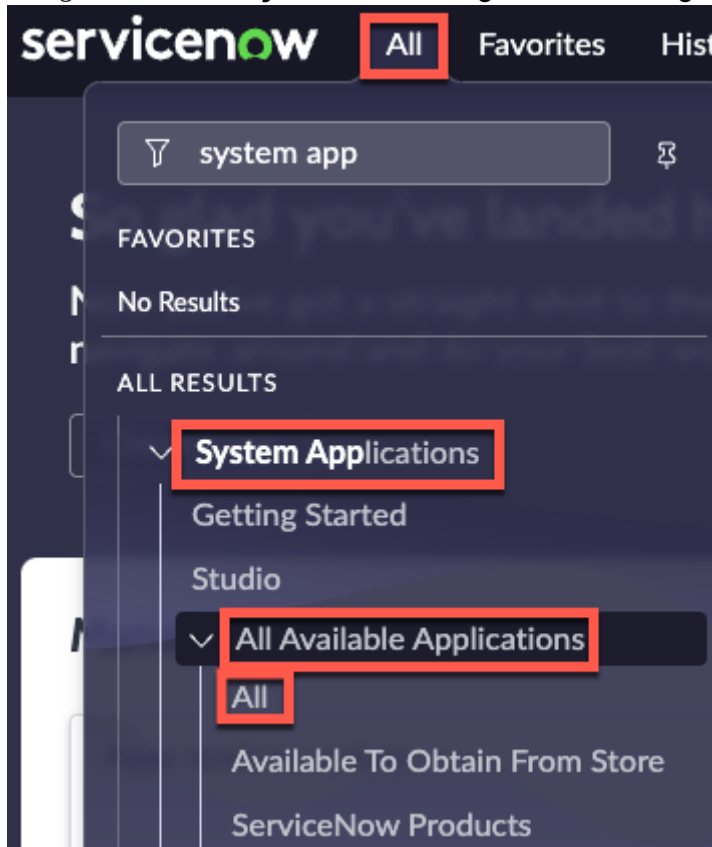
- Plugins
- Store-Anwendungen
- Rollen
- Business-Regeln

Weitere Informationen zum Anzeigen der mit einer Anwendung installierten Komponenten finden Sie unter:

- Mit Operational Technology Vulnerability Response installierte Komponenten
- Suchen Sie mit einer Anwendung installierte Komponenten [↗](#).

Prozedur

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



2. Suchen Sie die Anwendung Operational Technology Vulnerability Response 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**.
Demodaten sind Beispieldatensätze, die Anwendungsfunktionen für die gängigen Anwendungsfälle veranschaulichen. Laden Sie die Demodaten, 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.

Weisen Sie Operational Technology Vulnerability Response Rollen zu

Weisen Sie Ihren Benutzern Rollen zu, damit Sie ihren Zugriff auf die Funktionen, Fähigkeiten und Daten in der Anwendung Operational Technology Vulnerability Response steuern können.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Benutzer mit den in den folgenden Tabellen aufgeführten Rollen können die Anwendung Operational Technology Vulnerability Response verwenden.

Weisen Sie Administratoren oder Anwendergruppen nach Bedarf Rollen zu.

Weisen Sie Administratoren oder Administratorgruppen Rollen zu

Rolle	Beschreibung
OT VR-Integrationsbetrachter [sn_otvr.integration_viewer]	Kann OT VR-Integrationsdatensätze anzeigen.
OT VR-Integrationsadministrator [sn_otvr.integration_admin]	Kann OT VR-Integrationsdatensätze anzeigen und bearbeiten.
Besitzer der OT-Schwachstellenkorrektur [sn_otvr.remediation_owner]	Kann Korrekturaufgaben erstellen. Kann auch vorhandene Korrekturaufgaben für angreifbare Elemente planen.

Prozedur

Weisen Sie Benutzern und Gruppen mit der Benutzerverwaltungsfunktion Now Platform Rollen zu.

Nächste Maßnahme

[Erstellt eine Site-Zuweisungsgruppe.](#)

Erstellt eine Site-Zuweisungsgruppe

Erstellen Sie eine Zuweisungsgruppe Operational Technology Vulnerability Response pro Standort im Anlagenmodell-Manager. Dadurch können OT-Korrekturbesitzer nur angreifbare Elemente für ihre Site anzeigen.

Vorbereitungen

Erstellen Sie eine Zuweisungsgruppe Operational Technology Vulnerability Response, vorzugsweise mit demselben Namen wie der Standort, auf den sie sich bezieht. Wenn sich Ihr Standort beispielsweise in Mailand befindet, nennen Sie die Gruppe „Mailand OT VR-Zuweisungsgruppe“.

Erforderliche Rolle: cmdb_ot_isa_admin

Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > Industrial Process Manager > Sites**.
2. Wählen Sie einen Site-Datensatz aus.
Der Site-Datensatz ist eine übergeordnete Anlagenmodell-Entität, die selbst kein übergeordnetes Element hat.
3. Wählen Sie im Feld **OT VR-Zuweisungsgruppe** das Suchsymbol, um vorhandene Benutzergruppen anzuzeigen.
4. Wählen Sie die entsprechende Zuweisungsgruppe aus.
 - Wenn die gewünschte Gruppe vorhanden ist, wählen Sie sie in der Liste aus.
 - Wenn die gewünschte Gruppe nicht vorhanden ist, wählen Sie **Neu**, um die Gruppe zu erstellen, und wählen Sie dann **Absenden aus**.
5. Kehren Sie zum Site-Datensatz zurück, und wählen Sie **Aktualisieren** aus.
Die neue OT VR-Zuweisungsgruppe wird erstellt.

Nächste Maßnahme

Weisen Sie Sites Benutzer zu

Weisen Sie Sites Benutzer zu

Wenn Sie dies noch nicht während der Konfiguration von Prozessmanager Industriegetan haben, weisen Sie Sites Anwender zu, die bereits über die Rolle „cmdb_ot_isa_viewer“ oder „cmdb_ot_isa_editor“ verfügen.

Vorbereitungen

Wenn sich OT-Geräte in der CMDB befinden, kann der Standortzugriff so konfiguriert werden, dass die Sichtbarkeit von OT-Geräten auf Anwender mit der Rolle „cmdb_ot_viewer“, „cmdb_ot_editor“ oder „cmdb_ot_admin“ und der Rolle „cmdb_ot_isa_viewer“ oder „cmdb_ot_isa_editor“ beschränkt wird.

Erforderliche Rolle: cmdb_ot_isa_admin

Prozedur

1. Wählen Sie im Formular „Anlagenmodell-Entitäten“ eine übergeordnete Anlagenmodell-Entität aus.
Informationen zu Anlagenmodellen finden Sie unter [Anlagenmodelle verwalten](#).
2. Wählen Sie auf der Registerkarte Site-Anwender **Neu**.
3. Füllen Sie im Formular „Benutzer von ISA-Entitätsstandorten“ die Felder aus.
4. Wählen Sie **Absenden**.
Der Benutzer ist der Site zugewiesen.

Nächste Maßnahme

Weisen Sie Anwender Zuweisungsgruppen zu

Weisen Sie Anwender Zuweisungsgruppen zu

Fügen Sie Anwender zu Zuweisungsgruppen hinzu, damit diese die angreifbaren Elemente für den ihnen zugewiesenen Standort sehen können.

Vorbereitungen

Damit Anwender die angreifbaren Elemente für die Sites anzeigen können, denen Sie sie zugewiesen haben, fügen Sie der OT VR-Zuweisungsgruppe für die Site Anwender hinzu.

Wenn angreifbare OT-Elemente erstellt werden, ist die Sichtbarkeit beschränkt auf:

- Benutzer mit der Rolle „Besitzer der VR-Korrektur“ (sn_vul.remediation_owner).
- Mitgliedschaft in der Zuweisungsgruppe Operational Technology Vulnerability Response, die der Site zugeordnet ist, zu der das OT-Gerät gehört

Erforderliche Rolle: Administrator

Prozedur

1. Öffnen Sie die Gruppe, die der Zuweisungsgruppe Operational Technology Vulnerability Response für den Standort entspricht.
2. Wählen Sie **Bearbeiten** auf der Registerkarte Gruppenmitglieder.
3. Fügen Sie die Anwender aus der Liste Sammlung in der Liste Gruppenmitglieder hinzu.
4. Wählen Sie **Speichern**.
Benutzer werden der Gruppe zugewiesen und können die angreifbaren Elemente für den zugewiesenen Standort anzeigen. Weitere Informationen zu Administrationsaufgaben, z. B. das Hinzufügen von Benutzern zu Gruppen, finden Sie unter [User administration](#) .

Nächste Maßnahme

[Weisen Sie angreifbare Elemente Gruppen zu.](#)

Weisen Sie angreifbare Elemente Gruppen zu

Konfigurieren Sie Zuweisungsregeln für OT-Schwachstellen.

Vorbereitungen

Angreifbare OT-Elemente können abhängig von Ihrer Nachbesserungsstrategie Gruppen auf Site-Ebene oder basierend auf der Klassifizierung zugewiesen werden.

Erforderliche Rolle: sn_vul.manage_assignment_rules oder sn_vul.vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn angreifbare Elemente importiert werden, werden sie basierend auf den Zuweisungsregeln für Schwachstellen der entsprechenden Gruppe zugewiesen. Operational Technology Vulnerability Response wird mit einer OT-Schwachstellen-Zuweisungsregel geliefert, **der Zuweisungsregel für Operational Technology (OT)**, die OT-Datensätze zu angreifbaren Elementen (OT VIT) der entsprechenden OT VR-Zuweisungsgruppe basierend auf ihrem Standort zuweist. Wenn es zu keiner Site gehört oder wenn für die Site keine Gruppe angegeben ist, wird die Regel der OT VR-Standardzuweisungsgruppe zugewiesen.

Weitere Informationen zum Erstellen von Vulnerability Response-Zuweisungsregeln finden Sie unter [Vulnerability Response-Zuweisungsregeln erstellen oder bearbeiten](#) .

Prozedur

1. Wählen Sie in der Liste „Zuweisungsregeln für Schwachstellen“ **die Option Zuweisungsregel für operative Technologie (OT)** aus.
2. Konfigurieren Sie dies basierend auf Ihrer Nachbesserungsstrategie:

- Wenn Ihre Nachbesserungsstrategie darin besteht, der Site alle angreifbaren OT-Elemente zuzuweisen, legen Sie die Ausführungsreihenfolge der OT VR-Zuweisungsregel auf einen niedrigeren Wert als für alle anderen Regeln fest.
 - Wenn Ihre Strategie darin besteht, die Zuweisung nach Klasse und dann an Sites für alle anderen Klassen vorzunehmen, legen Sie die Ausführungsreihenfolge der OT VR-Zuweisungsregel so fest, dass sie größer ist als die aller klassenbasierten Regeln.
3. Sobald die Ausführungsreihenfolge aktualisiert wurde, legen Sie den Status für „OT VR-Zuweisungsregel aktiv“ auf **true** fest.

Nächste Maßnahme

Konfigurieren Sie die OT-Korrekturzielregeln.

Konfigurieren Sie die Regeln für OT-Korrekturaufgaben

Aktualisieren Sie für Korrekturaufgaben, die in Industriell Arbeitsbereicherstellt werden, die vorhandenen Korrekturaufgabenregeln, um zu verhindern, dass importierte angreifbare Elemente automatisch OT-Geräte hinzufügen.

Vorbereitungen

Erforderliche Rolle: sn_vul.manage_group_rules oder sn_vul.vulnerability_admin

Wenn angreifbare Elemente importiert werden, können sie basierend auf den konfigurierten Regeln für Korrekturaufgaben zu Korrekturaufgaben hinzugefügt werden. Wenn Sie Vulnerability Response sowohl für IT- als auch für OT-Netzwerke verwenden, müssen Sie eine Konfiguration ändern, wenn Sie Schwachstellenelemente zur Korrektur in IT- und OT-Netzwerken unterschiedlich gruppieren. Operational Technology Vulnerability Response stellt einen Beispieldatensatz für eine Korrekturaufgabenregel bereit, der mit Demodaten geladen wird, um zu demonstrieren, wie OT-Netzwerkschwachstellen von der automatischen Gruppierung ausgeschlossen werden.

Konfigurieren Sie neue oder vorhandene Korrekturaufgabenregeln basierend auf Ihrer Nachbesserungsstrategie:

- Wenn Ihre Nachbesserungsstrategie darin besteht, automatisch Korrekturaufgaben nur für Schwachstellen in Ihrer IT-Umgebung zu erstellen, fügen Sie jeder vorhandenen Regel für Korrekturaufgaben die folgende Bedingung hinzu, um OT-Schwachstellen auszuschließen:
 - Konfigurationselement. OT-Gerät-Details = **ist leer**
- Wenn Ihre Nachbesserungsstrategie darin besteht, automatisch Korrekturaufgaben für alle angreifbaren OT-Elemente zu erstellen, erstellen Sie eine entsprechende Regel.

Beispiel, das mit OT VR-Demodaten geliefert wird: Regel für Korrekturaufgaben – Schwachstelle (OT ausschließen)

The screenshot shows the configuration interface for a Remediation Task Rule named 'Vulnerability (exclude OT)'. The rule is currently inactive. The description states that this rule is necessary to avoid including OT assets in remediation tasks by adding an 'AND' clause where 'Configuration Item - OT asset details' is empty. The condition is set to 'All of these conditions must be met', with two criteria: 'Active' is 'true' and 'Configuration Item - OT asset details' is 'empty'. The 'Group by' section allows grouping by 'Vulnerable Item' using the 'Assignment group' field. The 'Assignment' section shows tasks can be assigned by 'Group by field' to the 'Assignment group'.

Prozedur

1. Navigieren zu **Vulnerability Response > Administration > Regeln für Korrekturaufgaben**.
2. Wählen Sie den Namen der Regel aus, die Sie aktualisieren möchten.
 - Definieren Sie die Regeln so, dass alle angreifbaren Elemente in einer Gruppe vom selben Team, der gleichen Korrekturaktion und dem gleichen Zeitrahmen behoben werden. Beispiel: Nach angreifbarem Element gruppieren: „Zuweisungsgruppe“, „Schwachstelle“ und CI „Verwendet für“ (z. B. Produktion, Bereitstellung, Entwicklung), wenn diese Umgebungen unterschiedliche Wartungsfenster haben.
 - Weitere Informationen zu Regeln für Korrekturaufgaben finden Sie unter [Vulnerability Response-Arbeitsbereiche](#).
 - Weitere Informationen zu Korrekturaufgaben finden Sie [unter IT-Korrektur-Arbeitsbereich erkunden](#).

Konfigurieren Sie die OT-Korrekturzielregeln

Konfigurieren Sie Korrekturzielregeln für angreifbare OT-Elemente.

Um das Zieldatum der Korrektur für angreifbare OT-Elemente zu berechnen, laden Sie die Demodatensätze für die Anwendung Operational Technology Vulnerability Response, und konfigurieren Sie die Korrekturzielregeln.

Erforderliche Rolle: sn_vul.manage_remediation_target_rules oder sn_vul.vulnerability_admin

OT-Korrekturziele können aufgrund der seltenen Möglichkeiten zur Durchführung von Wartungsarbeiten in einer industriellen Umgebung unterschiedlich sein. Korrekturzielregeln werden in der Reihenfolge vom kleinsten Ziel zum größten Ziel angewendet.

Für OT-Geräte-Schwachstellen, für die keine Wartungsfenster im gleichen Zeitrahmen wie andere Schwachstellen verfügbar sind, ist möglicherweise ein anderes Zieldatum für die Nachbesserung erforderlich. Um zu demonstrieren, wie die Zieldaten für die Korrektur in

dieser Situation konfiguriert werden, werden zwei Demodatensätze bereitgestellt, um zu demonstrieren, wie dies für kritische Risikobewertungen verwaltet werden kann:

- Regel für die Einstufung kritischer Risiken (nur OT): Diese Regel verwendet die Bedingung **„Konfigurationselement.OT-Gerät-Details ist nicht leer UND Risikobewertung = 1 – Kritisch“**. Aktualisieren Sie das Ziel (Tage), und aktivieren Sie den Datensatz.
- Regel für die Einstufung kritischer Risiken (OT ausschließen): Um ein kürzeres Ziel nur auf Nicht-OT-Elemente vom Typ „Kritisches Risiko“ anzuwenden, müssen Sie zuerst OT-Geräte herausfiltern. Diese Regel verwendet die Bedingung **Konfigurationselement.OT-Gerät-Details ist leer UND Risikobewertung = 1 – Kritisch**. Aktualisieren Sie das Ziel (Tage), deaktivieren Sie alle vorhandenen Regeln für kritische Ziele, und aktivieren Sie diese Regel an ihrer Stelle.

Hinweis:

Beide Regeln müssen aktiviert sein, damit alle OT-Schwachstellen mit kritischem Risiko von der Nicht-OT-Korrekturzielregel ausgeschlossen werden.

Weitere Informationen zum Erstellen von Vulnerability Response-Zuweisungsregeln finden Sie unter:

- [Korrekturzielregeln für Vulnerability Response](#)
- [Erstellen oder bearbeiten Sie Vulnerability Response-Korrekturzielregeln](#)

[Konfigurieren Sie Risikorechner](#)

Konfigurieren Sie Risikorechner

Bestimmen Sie, welche OT-Risikofaktoren bei der Berechnung des Risikos eines angreifbaren Elements für ein OT-Gerät verwendet werden sollen.

Vorbereitungen

In Operational Technology können zusätzliche Faktoren die OT-Gerät-Relevanz, die Purdue-Ebene und die Relevanz des Produktionsprozesses umfassen, den das OT-Gerät automatisiert.

Erforderliche Rolle: sn_vul.manage_risk_score_configuration oder sn_vul.vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird

Informationen zu diesem Schritt finden Sie im Standardrisiko-Rechner mit OT-Schwachstellen-Rechner, der in den Demodaten der Anwendung Operational Technology Vulnerability Response enthalten ist. Der Standardrisikorechner mit OT wird verwendet, wenn das Risiko für angreifbare OT- und Nicht-OT-Elemente unterschiedlich berechnet werden muss.

Hinweis:

Da jeweils nur ein Schwachstellen-Rechner aktiv sein kann, wird die bereitgestellte Standardrisikoregel (nicht OT) als Beispiel für die Berechnung des Risikos für alle angreifbaren Nicht-OT-Elemente verwendet.

Weitere Informationen finden Sie unter [Felder und Gewichtungen für die Risikoregel definieren](#).

Um die Risikopunktzahl für angreifbare OT-Elemente festzulegen, passen Sie die Gewichtungen für die Risikoregeldatensätze der OT-Standardrisikoregel in den Demodaten an. Weitere Felder, die für OT in den Demodaten verfügbar sind, sind:

- Anlagenmodell-Entitätsrelevanz: Verwenden Sie die Servicegeschäfts-Relevanzregel.
- OT-Gerät-Relevanz: Verwenden Sie die Geräterelevanzregel für OT-Gerätedetails.
- Purdue-Ebene: Verwenden Sie das Feld Purdue-Ebene „OT-Gerät-Details des Konfigurationselements“.

Prozedur

1. Navigieren Sie zu **Schwachstellen-Rechner**.
2. Wählen Sie in der Liste „Schwachstellen-Rechner“ **Standardrisiko-Rechner mit OT** aus.
3. Öffnen Sie in der Liste Regeln des Schwachstellen-Rechners die Risikoregel, die Sie bearbeiten möchten. Wählen Sie beispielsweise **OT-Standardrisikoregel** aus.
4. Wählen Sie auf der Seite „Regel für Schwachstellenrisiko“ im Abschnitt „Kriterien des Risikorechners“ ein Risikoregelfeld aus.
5. Aktualisieren Sie im Datensatz des Felds „Risikoregel“ die Gewichtung oder den Gewichtungsprozentsatz für jedes Kriterium entsprechend seiner Bedeutung für die Berechnung der Gesamtrisikopunktzahl.
6. Wählen Sie **Aktualisieren**.

Nächste Maßnahme

Um die Risikopunktzahl für alle anderen angreifbaren Elemente festzulegen, kopieren Sie die vorhandenen Risikoregeln in den Standardrisiko-Rechner mit OT, und legen Sie die Ausführungsreihenfolge nach der OT-Standardrisikoregel fest.

Konfigurieren Sie den Rechner für das Rollup des OT-Schwachstellenrisikos

Verwenden Sie den Rollup-Rechner für OT-Schwachstellenrisiko, um die Risikopunktzahl der OT-Geräte auf jeder Ebene des Anlagenmodells zu berechnen. Die Gesamtrisikopunktzahl wird für die übergeordnete Anlagenmodell-Entität zusammengefasst.

Vorbereitungen

- Risikopunktzahl für alle Anlagenmodell-Entitäten berechnen, indem die geplante Aufgabe ausgeführt wird.

Hinweis:

Die Berechnung der Risikopunktzahl für alle Anlagenmodell-Entitäten gilt nur für die nachfolgende Ausführung der täglichen geplanten Aufgabe.

- Überprüfen Sie, ob die Spalte Serviceausfüllungsinstanz in der Liste Anlagenmodell-Entitäten auf **OTDynamicManualServicePopulator** festgelegt ist, indem Sie zu navigieren **Alle > Anlagenmodell – ISA > Anlagenmodell-Entitäten**. Wenn andere Werte festgelegt sind, müssen Sie die bedarfsgesteuerte Aufgabe *Update ISA entity service populator* ausführen:
 - Navigieren zu **Alle > Systemdefinition > Geplante Aufgaben**.
 - Wählen Sie den Auftrag *Update ISA entity service populator* aus.
 - Wählen Sie **Jetzt ausführen**.

i Hinweis:

Wenn die Spalte Serviceausfüllungsinstanz in der Liste Anlagenmodell-Entitäten nicht angezeigt wird, können Sie sie hinzufügen, indem Sie die Liste personalisieren. Weitere Informationen finden Sie unter [Personalize a list](#) .

- Erforderliche Rolle: sn_vul.vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird

Informationen zu diesem Schritt finden Sie unter Schwachstellen-Rollup-Rechner mit OT-Schwachstellen-Rechner, die im Lieferumfang der Demodaten der Anwendung Operational Technology Vulnerability Response enthalten sind.

Weitere Informationen finden Sie unter [Vulnerability Response-Rollup-Rechner](#) .

Um die Risikopunktzahl für die Anlagenmodell-Entität zu berechnen, richten Sie die Gewichtungen für diese Felder ein:

- Maximale Risikopunktzahl der angreifbaren Elemente (VITs), die der Anlagenmodell-Entität zugeordnet sind.
- Durchschnittliche Risikopunktzahl der VITs, die der Anlagenmodell-Entität zugeordnet sind.
- Anzahl der angreifbaren Elemente pro Anlagenmodell-Entität.

Prozedur

1. Navigieren zu **Alle > Vulnerability Response > Administration > Rechner für Schwachstellen-Rollup**.
2. Wählen Sie in der Liste „Rechner für Schwachstellen-Rollup“ **Anlagenmodell-Entitäts-Rollup** aus.
3. Aktualisieren Sie bei Bedarf im Abschnitt Rollup-Gewichtungen die Gewichtung für jedes Kriterium.
4. Wählen Sie **Aktualisieren**.

Nächste Maßnahme

Jetzt können Sie das auf einer Ebene zugeordnete Risiko für Ihre Anlagenmodell-Entitäten berechnen.

1. Risiko-Rollup für alle Anlagenmodell-Entitäten berechnen:
 - a. Navigieren zu **Alle > Industrial Workspace-Administrator > Geführtes Setup**.
 - b. Wählen Sie **Operational Technology Vulnerability Response** aus.
 - c. Wählen Sie im Abschnitt „Risiko-Rollup-Berechnung“ die Aufgabe Risiko-Rollup-Konfiguration aus.
 - d. Wählen Sie **Konfigurieren**.
 - e. Befolgen Sie die im geführten Setup beschriebenen Schritte.
2. Konfigurieren Sie die geplante Aufgabe *Risk Rollup for VITs by Equipment Model Entity*:
 - a. Navigieren zu **Alle > Industrial Workspace-Administrator > Geführtes Setup**.
 - b. Wählen Sie **Operational Technology Vulnerability Response** aus.
 - c. Wählen Sie im Abschnitt „Berechnung des Risiko-Rollups“ die Aufgabe Täglicher Zeitplan für die Aufgabe des Risiko-Rollups aus.
 - d. Wählen Sie **Konfigurieren**.

- e. Befolgen Sie die im geführten Setup beschriebenen Schritte.

i Hinweis:

Standardmäßig ist die Aufgabe auf „täglich ausgeführt“ festgelegt. Sie können dies an Ihre Geschäftsanforderungen anpassen, indem Sie die Felder **Ausführen**, **Zeitzone** und **Zeit** bearbeiten.

3. Konfigurieren Sie die Entitäten für das Rollup der Risikopunktzahl:

- a. Navigieren zu **Alle > Industrial Workspace-Administrator > Geführtes Setup**.
- b. Wählen Sie **Operational Technology Vulnerability Response** aus.
- c. Wählen Sie im Abschnitt „Risiko-Rollup-Berechnung“ die Aufgabe Alle Entitäten für Rollup-Auftrag für Risikopunktzahlen festlegen aus.
- d. Wählen Sie **Konfigurieren**.
- e. Befolgen Sie die im geführten Setup beschriebenen Schritte.

4. Um zu vermeiden, dass für Korrekturaufgaben die falsche Risikopunktzahl und Bewertung angezeigt wird, ändern Sie das Feld **Tabelle im Datensatz „OT-Geräte ohne zugewiesene Sites“ :**

- a. Navigieren zu **Alle > Systemdefinition > Skripts – Hintergrund**.
- b. **Fügen Sie im Feld Skript** ausführen das folgende Skript hinzu.

```
var gr = new GlideRecord('sn_vul_rollup');

gr.get('sys_id','24973dc4939e42900b1566f4548918eb');

gr.table = 'sn_ot_metric';

gr.update();
```

- c. Wählen Sie **Skript ausführen** aus.
- d. Um den Wert des Felds **Tabelle** im Datensatz „OT-Geräte ohne zugewiesene Sites“ zu überprüfen und die geplante Aufgabe auszuführen, navigieren Sie zu **Alle > Vulnerability Response > Administration > Rechner für Schwachstellen-Rollup**.
- e. Wählen Sie den Datensatz „OT-Geräte ohne zugewiesene Sites“ aus.
- f. Stellen Sie sicher, dass das Feld **Tabelle** auf **OT-Metrik [sn_ot_metric]** festgelegt ist.
- g. Führen Sie die geplante Aufgabe aus.

Nach dem Ausführen des Auftrags werden die richtigen VIT-Risikopunktzahlen und Bewertungen für die Korrekturaufgaben zusammengefasst.

Installieren Sie zertifizierte Vulnerability Response Integrationen

Integrieren Sie zertifizierte Drittanbieteranwendungen, die die Funktionalität des OT-Schwachstellenmanagements verbessern.

Suchen Sie in ServiceNow® Store nach Operational Technology Zertifizierten Integrationen für die Anwendung Operational Technology Vulnerability Response, und installieren Sie die für Ihre Umgebung zutreffenden.

Operational Technology Vulnerability Response Integrationen

Die Anwendung Operational Technology Vulnerability Response unterstützt Drittanbieterintegrationen.

Die folgenden Drittanbieterintegrationen werden derzeit unterstützt.

- Vulnerability Response für Microsoft Defender for IoT (lokale Verwaltungskonsole)
- Vulnerability Response Integration mit Claroty CTD

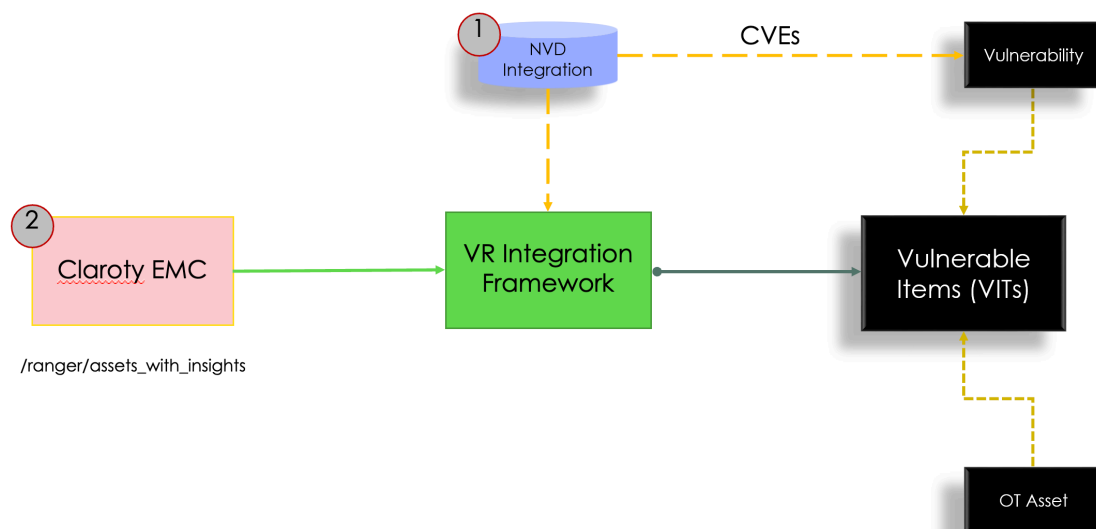
Vulnerability Response Integration mit Claroty CTD

Die Vulnerability Response Integration with Claroty Continuous Threat Detection (CTD) verwendet aus Claroty CTD importierte Schwachstellendaten, um risikobasierte Aktionen innerhalb des Produktionsprozesses zu ermöglichen.

Verwenden Sie diese Vulnerability Response -Integration mit der Anwendung ServiceNow® Operational Technology Vulnerability Response, um im Produktionsprozess verwendete Schwachstellen nachzuverfolgen, zu priorisieren und zu beheben.

Die folgende Abbildung zeigt den Prozess für die Integration von Vulnerability Response mit Claroty CTD.

Prozess für die Integration von Vulnerability Response mit Claroty CTD



Bevor Sie die Vulnerability Response -Integration mit Claroty CTD ausführen, müssen Sie die Integration der National Vulnerability Database (NVD) ausführen. Die NVD-Integration ruft veröffentlichte Common Vulnerabilities and Exposures (CVE) aus dem NVD ab und trägt sie in ServiceNow ein. Wenn Sie dann die Anwendung Vulnerability Response Integration with Claroty CTD ausführen, identifiziert die Anwendung die Schwachstellen für jedes Gerät und erstellt angreifbare Elemente (VITs).

Jede VIT hat eine Beziehung zu einem OT-Gerät (Operational Technology) oder einem Configuration Item (CI) und der erkannten Schwachstelle. Das Vulnerability Integration Framework stellt eine Verbindung mit der Claroty Enterprise Management Console (EMC) her und ruft die Schwachstellen für alle OT-Geräte ab.

i Hinweis:

Die Claroty CTD EMC Platform Insights-API hat eine Beschränkung von 10 CVEs. Daher werden ServiceNow von Claroty nur 10 CVEs bereitgestellt. Für die xDome-Plattform gilt diese Einschränkung jedoch nicht.

Schlüsselfunktionen

- Importieren Sie allgemeine Schwachstellen und Risiken (CVEs), die Operational Technology (OT)-Geräten zugeordnet sind, aus Claroty CTD. Erstellen Sie angreifbare Elemente (VITs), um eine einheitliche Ansicht der Schwachstellendaten für OT-Geräte und ihrer Auswirkungen auf den Produktionsprozess bereitzustellen.
- Führen Sie Importe neu erkannter Schwachstellen automatisch nach Ihrem eigenen Zeitplan aus.
- Verwenden Sie Zuweisungsregeln, um VITs automatisch zur Korrektur an lokale Teams vor Ort weiterzuleiten, die risikobasierte Aktionen durchführen können.

Installieren Sie Vulnerability Response Integration with Claroty CTD

Ich installiere die Vulnerability Response Integration with Claroty CTD (sn_clarotyctdvr). Die Anwendung enthält die mit Installationen verbundenen ServiceNow® Store -Anwendungen und -Plugins, falls sie nicht bereits installiert sind.

Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter [Rufen Sie eine Berechtigung für ab ServiceNow Produkt oder Anwendung](#) .
- Überprüfen Sie die Anwendungsliste [Vulnerability Response Integration with Claroty CTD](#)  in ServiceNow Store auf Informationen zu Abhängigkeiten, Lizenzierungs- oder Abonnementanforderungen sowie zur Releasekompatibilität.
- Vulnerability Response Die Integration mit Claroty CTD erfordert die folgenden ServiceNow Store -Anwendungen. Stellen Sie sicher, dass diese Anwendungen installiert sind, bevor Sie die Vulnerability Response Integration with Claroty CTD installieren.

Store-App „CMDB CI Class Models“

Diese Integration verwendet Operational Technology [Erweiterungsklassen](#)  die Teil der Anwendung CMDB CI Class Models sind. Weitere Informationen finden Sie unter [CMDB CI Class Models](#) .

Service Graph Connector Integration for Claroty CTD

Diese Integration verwendet die Anwendung Operational Technology Manager, um den Import von Sites, von den einzelnen Sites erkannten Geräten, Verbindungen (oder Basissystemen) und installierten Programmen in Configuration Management Database (CMDB) zu automatisieren. Informationen zur Installation von Service Graph Connector Integration for Claroty CTD finden Sie unter [Installieren Sie Vulnerability Response Integration with Claroty CTD](#).

Erforderliche Rolle: Administrator

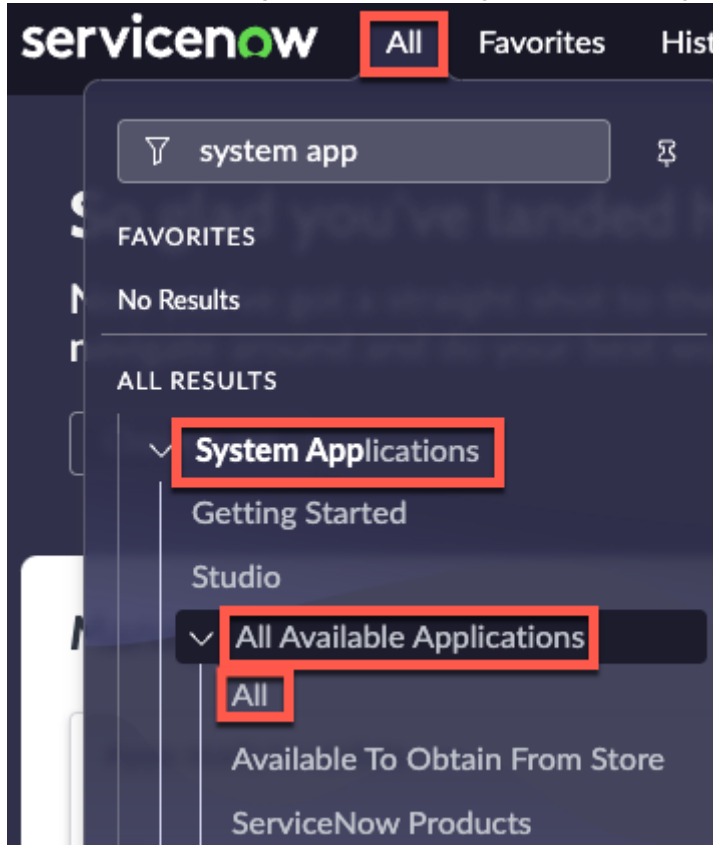
Warum und wann dieser Vorgang ausgeführt wird

Die folgenden Elemente werden mit Vulnerability Response Integration with Claroty CTD installiert:

- Vulnerability Response-Plugin
- Vulnerability Response Integration with NVD

Prozedur

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



2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach der Anwendung Vulnerability Response Integration with Claroty CTD (sn_clarotyctdvr).

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

In der Liste neben der Schaltfläche **Installieren** werden die für Sie verfügbaren Versionen angezeigt.

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. Wählen Sie **Installieren** aus.

Weisen Sie Vulnerability Response Integration mit Claroty CTD-Rollen zu

Weisen Sie Ihren Anwendern Rollen zu, damit Sie ihren Zugriff auf die Funktionen, Fähigkeiten und Daten in der Anwendung Vulnerability Response Integration with the Claroty CTD steuern können.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Wenn Ihnen die in der folgenden Tabelle aufgeführten Rollen zugewiesen sind, können Sie die Anwendung Vulnerability Response Integration with Claroty CTD verwenden.

Weisen Sie Administratoren oder Anwendergruppen nach Bedarf Rollen zu.

Weitere Informationen zu den Rollen, die für die Anwendung Vulnerability Response Integration with Claroty CTD verfügbar sind, finden Sie unter [Vulnerability Response Integration mit Claroty CTD-Rollen](#).

Prozedur

Weisen Sie Benutzern oder Gruppen mit der Benutzerverwaltungsfunktion Now Platform Rollen zu.

Vulnerability Response Integration mit Claroty CTD-Rollen

Rollen steuern den Zugriff auf Funktionen und Fähigkeiten in der Vulnerability Response Integration with Claroty CTD.

In der folgenden Tabelle werden die Rollen und Berechtigungen für die Vulnerability Response Integration with Claroty CTD beschrieben.

Vulnerability Response Integration mit Claroty CTD-Rollen

Rolle	Beschreibung
OT VR-Integrationsbetrachter [sn_otvr.integration_viewer]	Kann OT VR-Integrationsdatensätze anzeigen.
OT VR-Integrationsadministrator [sn_otvr.integration_admin]	Kann die OT VR-Integration konfigurieren und ausführen.
MID-Server [mid_server]	Kann ein MID-Serverkonfigurieren.

Erforderliche Berechtigungen in Claroty CTD

Überprüfen Sie, ob für die folgenden Anwenderberechtigungen der **Anzeigezugriff** in Claroty CTD aktiviert ist, um Daten von Claroty CTD bis ServiceNow zu erfassen:

- Sichtbarkeit
- Ermittlung
- Bedrohungserkennung
- Risiko und Schwachstellen

Integration der US-Schwachstellendatenbank (National Vulnerability Database) ausführen

Führen Sie die Integration der National Vulnerability Database (NVD) aus, um Daten aus dem NVD-Produkt des National Institute of Standards and Technology (NIST) zu importieren. Durch das Ausführen der NVD-Integration können Sie den Schweregrad und die Details der in Ihrer Umgebung gefundenen allgemeinen Schwachstellen und Risiken (Common Vulnerabilities and Exposures, CVEs) bestimmen.

Vorbereitungen

Bevor Sie die NIST NVD-Integration in Ihrer Instanz von ausführen, müssen die Installations- und Konfigurationsschritte abgeschlossen werden. Durch das Abschließen der

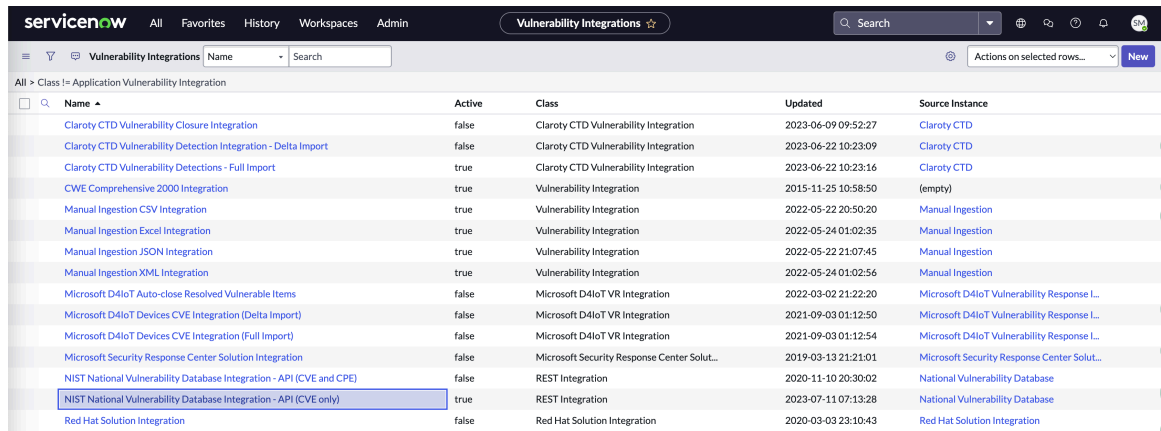
Installation und Konfiguration wird sichergestellt, dass das NVD-Produkt ordnungsgemäß in die Anwendung Operational Technology Vulnerability Response integriert wird.

Informationen zur Installation des NVD-Plugins finden Sie unter [Install the Vulnerability Response Integration with the NIST National Vulnerability Database](#) .

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle > Vulnerability Response > Administration > Integrationen**.
2. Wählen Sie den Datensatz NIST NVD integration – API (nur CVE) aus.



Name	Active	Class	Updated	Source Instance
Clarity CTD Vulnerability Closure Integration	false	Clarity CTD Vulnerability Integration	2023-06-09 09:52:27	Clarity CTD
Clarity CTD Vulnerability Detection Integration - Delta Import	false	Clarity CTD Vulnerability Integration	2023-06-22 10:23:09	Clarity CTD
Clarity CTD Vulnerability Detections - Full Import	true	Clarity CTD Vulnerability Integration	2023-06-22 10:23:16	Clarity CTD
CWE Comprehensive 2000 Integration	true	Vulnerability Integration	2015-11-25 10:58:50	(empty)
Manual Ingestion CSV Integration	true	Vulnerability Integration	2022-05-22 20:50:20	Manual Ingestion
Manual Ingestion Excel Integration	true	Vulnerability Integration	2022-05-24 01:02:35	Manual Ingestion
Manual Ingestion JSON Integration	true	Vulnerability Integration	2022-05-22 21:07:45	Manual Ingestion
Manual Ingestion XML Integration	true	Vulnerability Integration	2022-05-24 01:02:56	Manual Ingestion
Microsoft D4IoT Auto-close Resolved Vulnerable Items	false	Microsoft D4IoT VR Integration	2022-03-02 21:22:20	Microsoft D4IoT Vulnerability Response L...
Microsoft D4IoT Devices CVE Integration (Delta Import)	false	Microsoft D4IoT VR Integration	2021-09-03 01:12:50	Microsoft D4IoT Vulnerability Response L...
Microsoft D4IoT Devices CVE Integration (Full Import)	false	Microsoft D4IoT VR Integration	2021-09-03 01:12:54	Microsoft D4IoT Vulnerability Response L...
Microsoft Security Response Center Solution Integration	false	Microsoft Security Response Center Solut...	2019-03-13 21:21:01	Microsoft Security Response Center Solut...
NIST National Vulnerability Database Integration - API (CVE and CPE)	false	REST Integration	2020-11-10 20:30:02	National Vulnerability Database
NIST National Vulnerability Database Integration - API (CVE only)	true	REST Integration	2023-07-11 07:13:28	National Vulnerability Database
Red Hat Solution Integration	false	Red Hat Solution Integration	2020-03-03 23:10:43	Red Hat Solution Integration

3. Legen Sie den Wert im Feld **Importieren seit** auf **NULL** fest.

4. Wählen Sie **Jetzt ausführen**.

Konfigurieren Sie die Vulnerability Response -Integration mit Clarity CTD

Konfigurieren Sie die Vulnerability Response -Integration mit Clarity CTD, um mit dem Importieren von Daten zu beginnen.

Verwenden Sie die Clarity CTD-Schwachstellenintegration Geführtes Setup, um die Konfiguration abzuschließen.

Um auf die Integration von Clarity CTD Vulnerability Geführtes Setup zuzugreifen, navigieren Sie zu **Clarity CTD – Schwachstellenintegration > Administrator > Setup**.

Stellen Sie eine Verbindung mit Clarity CTD her

Stellen Sie eine Verbindung mit Clarity CTD her, um mit dem Setup der Schwachstellenintegration zu beginnen.

Vorbereitungen

Ändern Sie vor dem Durchführen des Setups den Anwendungsbereich in **Vulnerability Response Integration with Clarity CTD**, indem Sie in der Navigationsleiste das Globussymbol () auswählen.

Erforderliche Rolle: Administrator

Automatische Übersetzung

Prozedur

1. Navigieren zu **Alle > Claroty CTD – Schwachstellenintegration > Administrator > Setup**.
2. Wählen Sie im Abschnitt „Mit Claroty CTD verbinden“ die Aufgabe **Verbindungen einrichten** aus.
3. Wählen Sie auf der Aufgabenseite „Verbindungen einrichten“ **Konfigurieren** aus.
Die Seite „Claroty CTD-Verbindungsmanager“ wird geöffnet.
4. Füllen Sie die folgenden Felder des Formulars aus.

Stellen Sie eine Verbindung mit dem Claroty CTD-Formular her

Feld	Beschreibung
Claroty EMC URL	URL der Claroty CTD Enterprise Management Console (EMC).
CVSS-Mindestpunktzahl	Gegebenenfalls können Sie filtern, welche Schwachstellen importiert werden basierend auf ihrer Punktzahl im Common Vulnerability Bewertungssystem (CVSS). Dies ist ein Filter, der größer als oder gleich ist. Wenn Sie also „9,0“ eingeben, importiert die Integration Schwachstellen mit einer CVSS-Punktzahl von 9,0 bis 10,0.
Anwendername	Claroty-Account-Anwendername.
Passwort	Claroty-Account-Passwort.
MID-Server	Wenn Ihre Claroty EMC lokal ist, ist möglicherweise ein MID-Server erforderlich. Wenn ja, wählen Sie hier ein MID-Server aus.

5. Wählen Sie **Aktualisieren**.
6. Wählen Sie **Verbindung testen**.

Wenn der Verbindungstest erfolgreich ist, wird die Ausgabemeldung „Ergebnisse 200“ angezeigt. Bei einem nicht erfolgreichen Verbindungsversuch werden der Fehlercode und die von Claroty empfangene Nachricht angezeigt.

Aktivieren Sie die Delta-Import-Integration

Aktivieren Sie die Delta-Import-Integration, um Schwachstellen aus Claroty CTD zu importieren.

Vorbereitungen

Führen Sie vor dem Planen des Imports von Claroty CTD-Datensätzen die NVD-Integration aus, um Probleme zu beheben. Weitere Informationen finden Sie unter [Integration der US-Schwachstellendatenbank \(National Vulnerability Database\) ausführen](#).

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die Delta-Import-Integration importiert Schwachstellen aus Claroty CTD aus der letzten erfolgreichen Integrationsausführung. Standardmäßig importiert die erste Ausführung die Daten der letzten 90 Tage. Das Löschen des Felds **Startzeit** führt zu einem vollständigen Import.

Prozedur

1. Navigieren zu **Alle > Claroty CTD – Schwachstellenintegration > Administrator > Setup**.
2. Wählen Sie im Abschnitt Geplante Integrationsaufgaben konfigurieren die Aufgabe **Delta-Importintegration aktivieren aus**.
3. Wählen Sie **Konfigurieren**.
4. Stellen Sie sicher, dass der Delta-Import-Integrationsdatensatz auf **Aktiv** festgelegt ist.
5. Stellen Sie sicher, dass das Feld **Ausführen** auf **Bei Bedarf** festgelegt ist.
6. **Wahlweise:** Löschen Sie zum Ausführen eines vollständigen Imports das Feld **Startzeit**.
7. Wählen Sie **Aktualisieren**.

Führen Sie die Schwachstellenintegration nach dem Service Graph Connector aus

Führen Sie die Claroty CTD Vulnerability-Integration aus, nachdem Sie Service Graph Connector für Claroty CTD ausgeführt haben. Durch Ausführung der Vulnerability Integration unmittelbar nach dem Ausführen von Service Graph Connector wird sichergestellt, dass die aktuellsten CMDB Informationen aus Claroty CTD übernommen werden.

Vorbereitungen

Service Graph Connector Integration for Claroty CTD muss konfiguriert und aktiv sein, um die Vulnerability Response -Integration nach dem Service Graph -Connector auszuführen.

Führen Sie vor dem Planen des Imports von Claroty CTD-Datensätzen die NVD-Integration aus, um Probleme zu beheben. Weitere Informationen finden Sie unter [Integration der US-Schwachstellendatenbank \(National Vulnerability Database\) ausführen](#).

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle > Claroty CTD – Schwachstellenintegration > Administrator > Setup**.
2. Wählen Sie in der Aufgabe Geplante Integrationsaufgaben konfigurieren die **Registrierkarte Nach Service Graph Connector** ausführen.
3. Wählen Sie **Konfigurieren**.
4. Aktivieren Sie den Datensatz Nach SGC ausführen – Integration von Claroty CTD Vulnerability Detection – Delta-Import, indem Sie die Option **Aktiv** auswählen.
5. Stellen Sie sicher, dass das Feld **Ausführen** auf **Nach übergeordneten Ausführungen** festgelegt ist.
6. Stellen Sie sicher, dass das **Feld** Übergeordnet auf **Geplanter Import von SG-OT Claroty CTD-Assets** festgelegt ist.
7. Wählen Sie **Aktualisieren**.

Integration des automatischen Abschlusses aktivieren

Aktivieren Sie die Integration zum automatischen Schließen, um die entsprechenden ServiceNow Schwachstellenerkennungen zu schließen.

Vorbereitungen

Führen Sie vor dem Planen des Imports von Claroty CTD-Datensätzen die NVD-Integration aus, um Probleme zu beheben. Weitere Informationen finden Sie unter [Integration der US-Schwachstellendatenbank \(National Vulnerability Database\) ausführen](#).

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Für die Vulnerability Response-Integration mit Claroty CTD sind zwei Abschlussintegrationsaufträge verfügbar:

- Claroty CTD – Integration zum Abschluss gelöster Schwachstellen
- Claroty CTD – Integration zum vollständigen Schließen von Schwachstellen

Die Claroty CTD – Integration zum Schließen gelöster Schwachstellen sucht nach angreifbaren Elementen (VITs), die in ServiceNow Configuration Management Database (CMDB) als **Gelöst** markiert wurden. Anschließend fragt es Claroty CTD für diese VITs ab und schließt sie basierend auf der von Claroty CTD erhaltenen Antwort.

Die Claroty CTD Integration zum vollständigen Schließen von Schwachstellen sucht nach allen VITs unabhängig von ihrem Status (Gelöst oder nicht) in ServiceNow CMDB. Anschließend fragt sie in Claroty CTD alle VITs ab und schließt diejenigen, die keinen entsprechenden CVE-Eintrag in Claroty CTD haben.

Prozedur

1. Navigieren zu **Alle > Claroty CTD – Schwachstellenintegration > Administrator > Setup**.
2. Wählen Sie in der Aufgabe Geplante Integrationsaufgaben konfigurieren die Registerkarte **Integration für automatischen Abschluss aktivieren**.
3. Wählen Sie **Konfigurieren**.

Hinweis:

Die Integration des automatischen Abschlusses ist so vorkonfiguriert, dass sie nach dem Delta-Import ausgeführt wird, sodass keine Zeitplanung erforderlich ist.

4. Stellen Sie sicher, dass das Feld **Ausführen** auf **Bei Bedarf** festgelegt ist.
5. Stellen Sie sicher, dass der Datensatz auf **Aktiv** festgelegt ist.
6. Wählen Sie **Aktualisieren**.

Konfigurieren Sie die vollständige Importintegration aus Claroty CTD

Konfigurieren Sie die vollständige Importintegration, um den gesamten Schwachstellenbestand eines Geräts aus Claroty CTD zu importieren.

Vorbereitungen

Führen Sie vor dem Planen des Imports von Claroty CTD-Datensätzen die NVD-Integration aus, um Probleme zu beheben. Weitere Informationen finden Sie unter [Integration der US-Schwachstellendatenbank \(National Vulnerability Database\) ausführen](#).

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die Integration „Claroty CTD Vulnerability Detections – Vollständiger Import“ importiert den gesamten Schwachstellenbestand eines Geräts aus Claroty CTD ohne Rücksicht auf ein bestimmtes Datum. Diese Integration ist nützlich, wenn mit den täglichen Delta-Importen nicht alle erforderlichen Schwachstellendaten importiert wurden.

i Hinweis:

Die Integration „Vollständiger Import“ berücksichtigt die Konfiguration der minimalen CVSS-Punktzahl. Wenn Sie die Integration so konfiguriert haben, dass nur CVSS 9.0 und höher importiert wird, importiert der vollständige Import nur CVSS 9.0 und höher.

Prozedur

1. Navigieren zu **Alle > Claroty CTD – Schwachstellenintegration > Administrator > Setup**.
2. Wählen Sie in der Aufgabe Geplante Integrationsaufgaben konfigurieren die Registerkarte **Integration für vollständige Importe konfigurieren aus**.
3. Wählen Sie **Konfigurieren**.
4. Stellen Sie sicher, dass das Feld **Ausführen** auf **Bei Bedarf** festgelegt ist.
5. Stellen Sie sicher, dass der Datensatz auf **Aktiv** festgelegt ist.
6. Wählen Sie **Aktualisieren**.

Legen Sie die Systemeigenschaften fest

Legen Sie die Systemeigenschaften für die Vulnerability Response Integration with Claroty CTD fest, damit Sie die Eigenschaften nach Bedarf aktivieren können.

Vorbereitungen

Ändern Sie vor dem Setup den Anwendungsbereich in **Vulnerability Response Integration with Claroty CTD**, indem Sie in der Navigationsleiste das Globussymbol () auswählen.

Erforderliche Rolle: sn_otvr.integration_admin

Prozedur

1. Navigieren zu **Alle > Claroty CTD – Schwachstellenintegration > Administrator > Eigenschaften**
2. Aktualisieren Sie die Systemeigenschaftsdatsätze nach Bedarf für Ihre Organisation.
Weitere Informationen zu den für die Anwendung Vulnerability Response Integration with Claroty CTD installierten Systemeigenschaften finden Sie unter [Eigenschaften, die für die Vulnerability Response Integration with Claroty CTD installiert sind](#).
3. Wählen Sie **Aktualisieren** aus, und speichern Sie Ihre Änderungen.

Eigenschaften, die für die Vulnerability Response Integration with Claroty CTD installiert sind

Sie können Systemeigenschaften für die Anwendung Vulnerability Response Integration with Claroty CTD aktivieren.

Um auf die Systemeigenschaften Vulnerability Response von Integration with Claroty CTD zuzugreifen, navigieren Sie zu **Alle > Claroty CTD – Schwachstellenintegration > Administrator > Eigenschaften**.

Systemeigenschaften

Name	Beschreibung	Typ	Standardwert
sn_clarotycdv.api_token	Teilungsschlüssel des Claroty CTD-API-Tokens. Der Standardwert	Ganzzahl	480

Systemeigenschaften (Fortsetzung)

Name	Beschreibung	Typ	Standardwert
	ist 480 Minuten (8 Stunden).		
sn_clarotyctdvr.api_token_timeout	Identifiziert den Zugriff auf die API.	Zeichenfolge	{"customer_name":"","first_name":"Service für API","id":1,"last_name":null,"mail":null,"password":"test"}
sn_clarotyctdvr.auto_close_vulnerabilities	Warnungen Schwachstellenerkennungen aus Claroty CTD automatisch schließen.	wahr, falsch	falsch
sn_clarotyctdvr.auto_close_vulnerabilities_after_days	Warnungen von Claroty CTD werden nach einer festgelegten Anzahl von Tagen seit „Zuletzt gefunden“ automatisch geschlossen.	Ganzzahl	90.0
sn_clarotyctdvr.default_api_pagination_size	Anzahl der Datensätze, die pro Seite aus der Claroty CTD-API abgerufen werden sollen.	Ganzzahl	500
sn_clarotyctdvr.detection_import_start_time_in_buffer	Beim Importieren von Daten aus der Claroty CTD-API wird vor der „Startzeit“ ein Puffer mit einer bestimmten Anzahl von Stunden hinzugefügt. Dadurch wird sichergestellt, dass im Delta-Import keine Datensätze übersehen werden.	Ganzzahl	4
sn_clarotyctdvr.integration_start_time_in_buffer	Beim Importieren der ersten Ausführung der Integration Daten aus einer Anzahl von Tagen in der Vergangenheit.	Ganzzahl	90.0
sn_clarotyctdvr.require_validation	Eingabe des CI muss mit CMDB übereinstimmen, um Schwachstellen-Erkennungen zu erstellen.	wahr, falsch	wahr

Automatische Übersetzung

Datenzuordnung für die Vulnerability Response Integration mit Claroty CTD

In diesem Abschnitt wird angegeben, wie Felder aus der Claroty CTD-API Feldern in den Tabellen ServiceNow zugeordnet werden.

Zuordnung von Schwachstellen-Erkennungsdaten

Claroty CTD-Feld	ServiceNow Feld	Notizen
	Quelle	Immer auf Claroty CTD festgelegt.
Identified_on	Zuerst gefunden	
Last_updated	Zuletzt gefunden	
Status	Status	Der Status 0 bedeutet Offen . Ein Status von 2 bedeutet Geschlossen/Behoben .
Resource_id	Konfigurationselement	Das Configuration Item (CI) wird durch eine CI-Suchregel festgelegt, die die Tabelle „sys_object_source“ nach der Ressourcen-ID durchsucht. Beispiel: 33,1.

Datenzuordnung des Schwachstelleneintrags

Schwachstelleneinträge werden nur erstellt, wenn in der Tabelle „National Vulnerability Database Eintrag“ [sn_vul_nvd_entry] kein vorhandener Common Vulnerabilities and Exposures-Datensatz (CVE) gefunden wird. Wenn die Claroty CTD-Integration ein CVE erstellen muss, ordnet sie die folgenden in der Tabelle aufgeführten Quellfelder zu.

Claroty CTD-Feld	ServiceNow Feld	Notizen
Cve_id	ID	Beispiel: CVW-2017-17562
Titel	Zusammenfassung	Die Integration fügt der Zusammenfassung [Claroty] hinzu, sodass die von Claroty aufgefüllten NVD-CVEs sichtbar sind. Beispiel: [Claroty] Schwachstelle bei der Authentifizierungsumgehung in SIPROTEC.
CVSS	V3_base_score	
Veröffentlicht	Date_published	
Geändert	Last_modified	

Fehler für die Vulnerability Response Integration mit Claroty CTD

Während der Arbeit mit der Vulnerability Response Integration with Claroty CTD können Fehler auftreten, die eine Problembehandlung erfordern.

Vulnerability Detection Integration (Datenabruf)

Fehlermeldung	Mögliche Ursache
Eine Claroty CTD-Integration kann ohne eine Kombination aus Anwendername und Passwort nicht ausgeführt werden.	In der Integrationskonfiguration ist kein Anwendername oder Passwort vorhanden.
Die Integration kann ohne angegebene REST-Nachricht und REST-Methode nicht ausgeführt werden.	Im Datensatz der Claroty CTD-Integration sind die Felder „REST-Nachricht“ oder „REST-Methode“ nicht ausgefüllt.
Die Integration kann ohne angegebene Claroty CTD-Server-URL nicht ausgeführt werden.	In der Integrationskonfiguration ist keine URL vorhanden.
Die Integration kann ohne angegebenen Pfad der Erkennungs-API-Ressource nicht ausgeführt werden.	In der Integrationskonfiguration ist der Parameter „detection_api_resource_path“ nicht ausgefüllt. Der Standardwert ist /ranger/assets_with_insights.
Ungültiger Antwortcode {Antwortcode} von Claroty CTD erhalten.	Die Antwort von der Claroty-API war ungültig. Beispielsweise wird die Nachricht Ungültiger Antwortcode 401 von Claroty CTD empfangen. Dieser ungültige Antwortcode bedeutet, dass Sie nicht autorisiert sind und dass die Anmeldeinformationen (Anwendername/Passwort) wahrscheinlich ungültig sind.
Die Eigenschaft „count_total“ kann nicht aus JSON-Daten gelesen werden.	Der für die Paginierung verwendete „count_total“ war in der API-Antwort nicht vorhanden. Dies bedeutet wahrscheinlich, dass eine ungültige Nutzlast von Claroty CTD empfangen wurde. Stellen Sie sicher, dass die Claroty CTD-Instanz über den MID-Server erreichbar ist, und überprüfen Sie die Datei response.json des Datenquellenanhangs, um sicherzustellen, dass „count_total“ vorhanden ist.

Vulnerability Detection Integration (Datenverarbeitung)

Fehlermeldung	Mögliche Ursache
Fehler beim Schreiben des Anhangs.	Das System konnte die Antwortdaten nicht an die Datenquelle anhängen. Wenden Sie sich an Ihren Administrator, um weitere Unterstützung zu erhalten. Eine häufige Ursache für diesen Fehler ist, dass dem MID-Server-Benutzer die Rolle „sn_vul.vr_import_admin“ fehlt.
Anhangsinhalt ist null: Anhang sys_id = {sys_id}.	Der Inhalt des Anhangs „Datenquelle“ ist NULL. Dies kann auf ein Problem mit der Claroty-API selbst oder auf ein Problem in ServiceNow hinweisen. Wenden Sie sich an Ihren Administrator, um weitere Unterstützung zu erhalten.

Fehlermeldung	Mögliche Ursache
Anhang mit sys_id {sys_id} konnte nicht gefunden werden.	Datenquellenanhang wurde nicht gefunden. Führen Sie die gleichen Schritte für den vorhergehenden Fehler aus.

Integration des automatischen Abschlusses von Schwachstellen (Datenabruf)

Fehlermeldung	Mögliche Ursache
Eine Claroty CTD-Integration kann ohne eine Kombination aus Anwendername und Passwort nicht ausgeführt werden.	In der Integrationskonfiguration ist kein Anwendername oder Passwort vorhanden.
Die Integration kann ohne angegebene REST-Nachricht und REST-Methode nicht ausgeführt werden.	Im Datensatz der Claroty CTD-Integration sind die Felder „REST-Nachricht“ oder „REST-Methode“ nicht ausgefüllt.
Die Integration kann ohne angegebene Claroty CTD-Server-URL nicht ausgeführt werden.	In der Integrationskonfiguration ist keine URL vorhanden.
Die Integration kann ohne angegebenen Pfad der Erkennungs-API-Ressource nicht ausgeführt werden.	In der Integrationskonfiguration ist der Parameter „detection_api_resource_path“ nicht ausgefüllt. Der Standardwert ist /ranger/assets_with_insights.
Ungültiger Antwortcode {Antwortcode} von Claroty CTD erhalten.	Die Antwort von der Claroty-API war ungültig. Beispielsweise wird die Nachricht Ungültiger Antwortcode 401 von Claroty CTD empfangen. Dieser ungültige Antwortcode bedeutet, dass Sie nicht autorisiert sind und dass die Anmeldeinformationen (Anwendername/Passwort) wahrscheinlich ungültig sind.
Die Eigenschaft „count_total“ kann nicht aus JSON-Daten gelesen werden.	Der für die Paginierung verwendete „count_total“ war in der API-Antwort nicht vorhanden. Dies bedeutet wahrscheinlich, dass eine ungültige Nutzlast von Claroty CTD empfangen wurde. Stellen Sie sicher, dass die Claroty CTD-Instanz über den MID-Server erreichbar ist, und überprüfen Sie die Datei response.json des Datenquellenanhangs, um sicherzustellen, dass „count_total“ vorhanden ist.
Fehler beim Analysieren des Arrays „objects“ aus dem Antworttext.	„Wahrscheinlich“ bedeutet, dass eine ungültige Nutzlast von Claroty CTD empfangen wurde. Stellen Sie sicher, dass die Claroty CTD-Instanz erreichbar ist, und überprüfen Sie die ausgehenden HTTP-Protokolle, um zu sehen, ob eine gültige Antwort eingegangen ist.

Integration des automatischen Abschlusses von Schwachstellen (Datenverarbeitung)

Fehlermeldung	Mögliche Ursache
Fehler beim Analysieren der Datenwörterbuch-JSON.	Die Nutzlast aus dem Datenquellenanhang war ungültiges JSON. Wahrscheinlich tritt vor diesem Fehler ein anderer Fehler auf. Stellen Sie sicher, dass die Claroty CTD-Instanz erreichbar ist, und überprüfen Sie die ausgehenden HTTP-Protokolle, um zu sehen, ob eine gültige Antwort eingegangen ist.

Vulnerability Response Integration mit Microsoft Defender for IoT (Azure)

Die Integration von Vulnerability Response mit Microsoft Defender for IoT (Azure) verwendet aus Microsoft Defender for IoT (Azure) importierte Daten, um risikobasierte Aktionen mit dem Produktionsprozesskontext zu ermöglichen.

Verwenden Sie die Integration Vulnerability Response von mit der Anwendung ServiceNow® Operational Technology Vulnerability Response, um Schwachstellen auf Geräten, die im Produktionsprozess verwendet werden, nachzuverfolgen, zu priorisieren und zu beheben.

Schlüsselfunktionen

- Importieren Sie CVEs, die OT-Geräten zugeordnet sind, aus Microsoft Defender for IoT (Azure), und erstellen Sie angreifbare Elemente (VITs), um eine einheitliche Ansicht der Schwachstellendaten für OT-Geräte mit Produktionsprozesskontext bereitzustellen.
- Importieren Sie Schwachstellen automatisch nach Ihrem eigenen Zeitplan.
- Mithilfe von Zuweisungsregeln können VITs automatisch zur Korrektur an lokale standortbasierte Teams weitergeleitet werden, um risikobasierte Maßnahmen zu ergreifen.

Vulnerability Response für Microsoft Defender for IoT installieren (Azure)

Mit der Administratorrolle können Sie Vulnerability Response für Microsoft Defender for IoT (Azure) installieren. Die Anwendung enthält zugehörige Installationen ServiceNow® Store, Anwendungen und Plugins, falls sie nicht bereits installiert sind.

Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter [Rufen Sie eine Berechtigung für ab ServiceNow Produkt oder Anwendung](#) .
- Überprüfung des folgenden Elements: [Vulnerability Response für Microsoft Defender for IoT \(Azure\)](#)  Anwendungsliste in ServiceNow Store, um Informationen zu Abhängigkeiten, Lizenzierungs- oder Abonnementanforderungen und Releasekompatibilität zu erhalten.
- Vulnerability Response für Microsoft Defender for IoT (Azure) erfordert die folgenden ServiceNow Store -Anwendungen. Stellen Sie sicher, dass diese Anwendungen installiert sind, bevor Sie die Integration Vulnerability Response mit Microsoft Defender for IoT installieren.

Store-App „CMDB CI Class Models“

Diese Integration verwendet Operational Technology [Erweiterungsklassen](#) die Teil der Anwendung CMDB CI Class Models sind. Weitere Informationen finden Sie unter [CMDB CI Class Models](#).

Service Graph Connector Microsoft Defender for IoT (Azure)

Diese Integration verwendet die Anwendung Operational Technology Manager, um den Import von Sensorgeräten, OT-Geräten und Netzwerkverbindungen zu automatisieren. Informationen zur Installation von Service Graph finden Sie unter [Service Graph Connector für Microsoft Defender for IoT \(Azure\)](#).

Erforderliche Rolle: Administrator

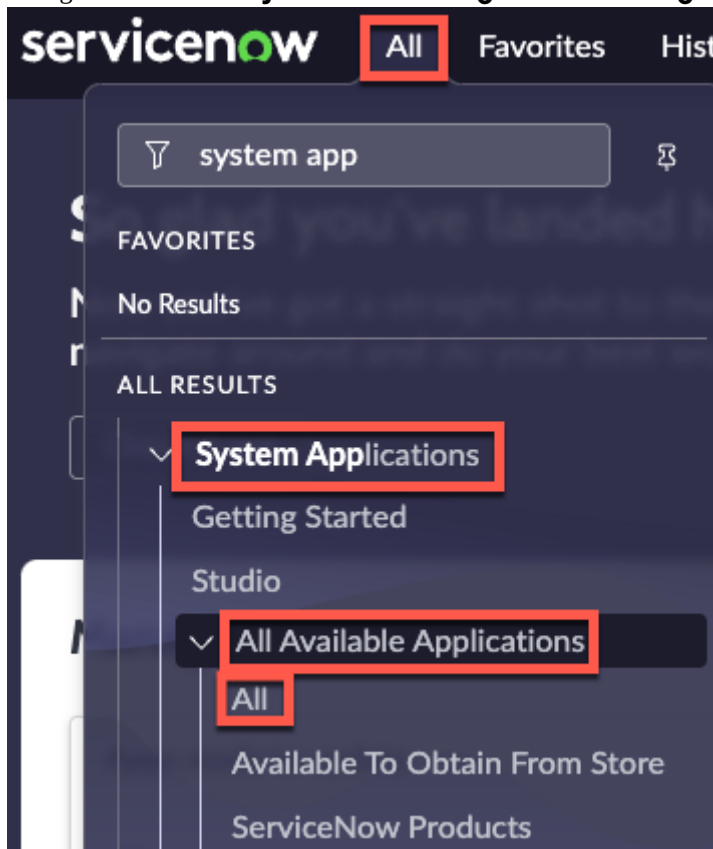
Warum und wann dieser Vorgang ausgeführt wird

Die folgenden Elemente werden mit Vulnerability Response für Microsoft Defender for IoT (Azure) installiert:

- Vulnerability Response-Plugin
- Vulnerability Response Integration with NVD

Prozedur

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



2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach Vulnerability Response Integration for Microsoft Defender for IoT (Azure).

Sie können nach der Anwendung anhand ihres Namens oder der Anwendungsbereich-ID suchen. Wenn Sie die Anwendung nicht finden können, müssen Sie möglicherweise Anwendungen synchronisieren oder sie von ServiceNow Store anfordern und Ihre -Instanz berechtigen.

In der Liste neben der Schaltfläche **Installieren** werden die für Sie verfügbaren Versionen angezeigt.

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. Wählen Sie **Installieren** aus.

Navigieren Sie zu Geführtes Setup für die Vulnerability Response Integration mit Microsoft Defender for IoT (Azure).

Navigieren Sie nach der Installation der Vulnerability Response Integration mit Microsoft Defender for IoT (Azure) zu Geführtes Setup, um Sie durch die Konfiguration der Anwendung führen zu lassen.

Vorbereitungen

Ändern Sie den Anwendungsbereich in Vulnerability Response Integration with Microsoft Defender for IoT (Azure), indem Sie in der Navigationsleiste das Globussymbol () auswählen.

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle > Azure D4IoT-Schwachstellen-Integration > Administrator > Geführtes Setup**.
2. Wählen Sie **Erste Schritte** aus.

Stellen Sie eine Verbindung mit Microsoft Defender for IoT (Azure) her.

Stellen Sie eine Verbindung mit Microsoft Defender for IoT (Azure) her, um mit dem Setup der Schwachstellenintegration zu beginnen.

Vorbereitungen

Überprüfen Sie, ob die Berechtigung „**Sicherheitsleser**“ für Microsoft Defender for IoT Azure aktiviert ist, die die folgenden Benutzeraktionen bereitstellt:

- Laden Sie die Endpunktdetails des Sensors herunter
- Zeigen Sie Werte auf der Seite Sites und Sensoren an
- Zeigen Sie den Azure-Gerätebestand an
- Zeigen Sie Azure-Arbeitsmappen an
- Zeigen Sie Defender for IoT-Einstellungen an
- Laden Sie OT-Bedrohungsentelligenz-Pakete herunter

Weitere Informationen finden Sie unter [Azure-Anwenderrollen und -Berechtigungen für Defender for IoT](#)  .

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle > Azure D4IoT-Schwachstellen-Integration > Administrator > Geführtes Setup**.
2. Wählen Sie im Abschnitt „Verbindung mit Microsoft Defender for IoT (Azure) herstellen“ die Aufgabe **Verbindungen einrichten** aus.
3. Wählen Sie auf der Aufgabenseite „Verbindungen einrichten“ **Konfigurieren** aus.
Die Seite „Mit Microsoft Azure Defender for IoT verbinden“ wird geöffnet.
4. Füllen Sie die folgenden Felder des Formulars aus.

Stellen Sie eine Verbindung mit dem Microsoft Azure Defender for IoT-Formular her

Feld	Beschreibung
OAuth-Token-URL	Die OAuth 2.0-Token-URL für „login.microsoftonline.com“. Beispiel: <a href="https://login.microsoftonline.com/<your tenant id>/oauth2/v2.0/token">https://login.microsoftonline.com/<your tenant id>/oauth2/v2.0/token .
OAuth-Client-ID	Ihre Client-ID.
OAuth-Client-Geheimnis	Ihr Clientgeheimnis.
Größenbeschränkung für Seite	Die maximale Anzahl von Datensätzen, die für jede Seite mit Daten abgerufen werden sollen. Der Standardwert ist 500.
CVSS-Mindestpunktzahl	Nur Schwachstellen mit einer CVSS-Punktzahl von diesem oder einem höheren Wert werden importiert. Der Standardwert für alle Schwachstellen ist 0,0.
Wird nach dem Import von Service Graph Connector ausgeführt	Dies ist ein empfohlenes Feld, das den Import von Schwachstellen unmittelbar nach Abschluss des Imports von Geräten in Service Graph Connector für Microsoft Defender for IoT (Azure) ausführt. Dies stellt die beste Wahrscheinlichkeit sicher, dass eingehende Schwachstellendaten mit CMDBabgeglichen werden. Am häufigsten ist der Wert Geplanter Import von SG-OT Microsoft Azure D4IoT-Geräten. Wenn Sie dieses Feld auswählen, lassen Sie die geplante Aufgabe „Azure D4IoT – Integration der Schwachstellenerkennung – vollständiger Import“ auf Ausführung bei Bedarf festgelegt. Dadurch wird sichergestellt, dass der Service Graph Connector-Geräteimport ihn als untergeordneten Auftrag ausführen kann, sobald der Geräteimport abgeschlossen ist.
Tägliche Importzeit	Wenn Sie das Feld Nach Service Graph Connector-Import ausführen nicht verwenden,

Feld	Beschreibung
	können Sie mit diesem Feld die tägliche Importzeit der Integration festlegen.
	 Hinweis: Wenn Sie für das Feld Nach Service Graph Connector-Import ausführen einen geplanten Import ausgewählt haben, ist dieses Feld nicht verfügbar.

5. Wählen Sie **Aktualisieren**.

6. Wählen Sie **Verbindung testen**.

Wenn der Verbindungstest erfolgreich ist, wird die Ausgabemeldung „Ergebnisse 200“ angezeigt. Bei einem nicht erfolgreichen Verbindungsversuch werden der Fehlercode und die von Microsoft Defender for IoT (Azure) empfangene Nachricht angezeigt.

Integration der US-Schwachstellendatenbank (National Vulnerability Database) ausführen

Führen Sie die Integration der National Vulnerability Database (NVD) aus, um Daten aus dem NVD-Produkt des National Institute of Standards and Technology (NIST) zu importieren. Durch das Ausführen der NVD-Integration erhalten Sie die grundlegenden CVEs-Daten (Common Vulnerabilities and Exposures), auf die von den Microsoft Defender for IoT (Azure)-Schwachstellen verwiesen wird, um den Schweregrad und die Details von Schwachstellen in Ihrer Umgebung zu bestimmen.

Vorbereitungen

Bevor Sie die NIST NVD-Integration auf Ihrer Instanz ausführen, müssen die Installations- und Konfigurationsschritte für die Integration abgeschlossen werden. Durch das Abschließen der Installation und Konfiguration wird sichergestellt, dass das NVD-Produkt ordnungsgemäß in die Anwendung Operational Technology Vulnerability Response integriert wird.

Informationen zur Installation des NVD-Plugins finden Sie unter [Install the Vulnerability Response Integration with the NIST National Vulnerability Database](#) .

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle > Azure D4IoT-Schwachstellen-Integration > Administrator > Geführtes Setup**.
2. Wählen Sie im Abschnitt **Integration konfigurieren** neben der Aufgabe **CVE-Einträge aus National Vulnerability Database (NVD) importieren** die Option **Konfigurieren aus**.
3. Je nachdem, was aktiv ist, wählen Sie entweder den Datensatz „NIST NVD integration – API (nur CVE)“ oder den Datensatz „NIST National Vulnerability Database Integration – API“ (CVE und CPE) aus.

Hinweis:

Der Datensatz „NIST NVD integration – API (nur CVE)“ ist standardmäßig standardmäßig aktiv.

Name	Active	Class	Updated	Source Instance
Claroty CTD Vulnerability Closure Integration	false	Claroty CTD Vulnerability Integration	2023-06-09 09:52:27	Claroty CTD
Claroty CTD Vulnerability Detection Integration - Delta Import	false	Claroty CTD Vulnerability Integration	2023-06-22 10:23:09	Claroty CTD
Claroty CTD Vulnerability Detections - Full Import	true	Claroty CTD Vulnerability Integration	2023-06-22 10:23:16	Claroty CTD
CWE Comprehensive 2000 Integration	true	Vulnerability Integration	2015-11-25 10:58:50	(empty)
Manual Ingestion CSV Integration	true	Vulnerability Integration	2022-05-22 20:50:20	Manual Ingestion
Manual Ingestion Excel Integration	true	Vulnerability Integration	2022-05-24 01:02:35	Manual Ingestion
Manual Ingestion JSON Integration	true	Vulnerability Integration	2022-05-22 21:07:45	Manual Ingestion
Manual Ingestion XML Integration	true	Vulnerability Integration	2022-05-24 01:02:56	Manual Ingestion
Microsoft D4IoT Auto-close Resolved Vulnerable Items	false	Microsoft D4IoT VR Integration	2022-03-02 21:22:20	Microsoft D4IoT Vulnerability Response L...
Microsoft D4IoT Devices CVE Integration (Delta Import)	false	Microsoft D4IoT VR Integration	2021-09-03 01:12:50	Microsoft D4IoT Vulnerability Response L...
Microsoft D4IoT Devices CVE Integration (Full Import)	false	Microsoft D4IoT VR Integration	2021-09-03 01:12:54	Microsoft D4IoT Vulnerability Response L...
Microsoft Security Response Center Solution Integration	false	Microsoft Security Response Center Solut...	2019-03-13 21:21:01	Microsoft Security Response Center Solut...
NIST National Vulnerability Database Integration - API (CVE and CPE)	false	REST Integration	2020-11-10 20:30:02	National Vulnerability Database
NIST National Vulnerability Database Integration - API (CVE only)	true	REST Integration	2023-07-11 07:13:28	National Vulnerability Database
Red Hat Solution Integration	false	Red Hat Solution Integration	2020-03-03 23:10:43	Red Hat Solution Integration

4. Um den Datensatz zu bearbeiten, legen Sie den **Anwendungsbereich** mithilfe des Globussymbols () auf **Vulnerability Response Integration with NVD** fest.

5. Legen Sie im Feld **Importieren seit** auf der Registerkarte **Integrationsdetails** den Wert auf ein Datum in der Vergangenheit fest.

Hinweis:

Dies ist erforderlich, damit ein vollständiger Import des NVD erfolgt. Das empfohlene Datum ist 1999-01-01 00:00:00.

6. Wählen Sie **Speichern**.

7. Wählen Sie **Jetzt ausführen**.

Konfigurieren Sie geplante Integrationsaufgaben

Aktivieren Sie die geplanten Aufgaben, die Schwachstellendaten importieren.

Vorbereitungen

Führen Sie vor dem Planen des Imports von Microsoft Defender for IoT (Azure)-Datensätzen die NVD-Integration aus, um etwaige Probleme zu beheben. Weitere Informationen finden Sie unter [Integration der US-Schwachstellendatenbank \(National Vulnerability Database\) ausführen](#).

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle > Azure D4IoT-Schwachstellen-Integration > Administrator > Geführtes Setup**.

2. Wählen Sie im Abschnitt **Integration konfigurieren** neben der Aufgabe **Geplante Integrationsaufgaben Verify and Activate Integration (Geplante Aufgaben für Integration verifizieren und aktivieren)** die Option **Konfigurieren aus**.

3. Wählen Sie die Aufgabe **Azure D4IoT – Integration zur Schwachstellenerkennung – Vollständiger Import** aus.

Dieser Auftrag importiert Schwachstellenerkennungen aus Microsoft Defender for IoT (Azure).

4. Aktivieren Sie das Kontrollkästchen neben dem Feld **Aktiv**.

Sie können den Zeitplan auch anpassen, wenn weitere Änderungen erforderlich sind. Wenn Sie die Schwachstellen-Integration in der Aufgabe „**Verbindungen einrichten**“ auf **Nach Import von Service Graph Connector ausführen** konfiguriert haben, sollten Sie die Ausführung dieser Aufgabe **bei**

Bedarffestlegen. Weitere Informationen zur Aufgabe „**Verbindungen einrichten**“ finden Sie unter [Stellen Sie eine Verbindung mit Microsoft Defender for IoT \(Azure\) her.](#).

5. Wählen Sie Aktualisieren.

6. Wählen Sie den Auftrag Azure D4IoT – Integration zum Schließen von Schwachstellen aus.
Azure D4IoT – Integration zum Schließen von Schwachstellen ist ein Erkennungsauftrag, der bestimmt, welche Erkennungen aus Microsoft Defender for IoT (Azure) gelöscht wurden, und sie dann in ServiceNowschließt.

7. Aktivieren Sie das Kontrollkästchen neben dem Feld Aktiv.
 Es wird empfohlen, das Feld **Ausführen** auf **Bei Bedarf** zu belassen.

8. Wählen Sie Aktualisieren.

Automatisches Schließen veralteter Erkennungen aktivieren

Konfigurieren Sie die Systemeigenschaften, die beim Prozess für das automatische Schließen veralteter Erkennungen verwendet werden, um Schwachstellen, die sich nicht mehr in Ihrer Umgebung befinden, automatisch zu schließen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle > Azure D4IoT-Schwachstellen-Integration > Administrator > Geführtes Setup**.
2. Wählen Sie im Abschnitt **Veraltete Erkennungen automatisch schließen (optional)** die Aufgabe **Veraltete Erkennungen automatisch schließen aus**.
3. Wählen Sie **Konfigurieren**.
4. Auf der Seite **mit den Eigenschaften für das automatische Schließen von Azure D4IoT VR** im Feld **Veraltete Erkennungen von Microsoft Azure Defender for IoT automatisch schließen?** Feld wählen Sie **Ja**.
5. Geben Sie im Feld „**Erkennungen von Microsoft Azure Defender for IoT werden nach (Wert) Tagen seit der Aktualisierung automatisch geschlossen**“ die Anzahl der Tage ein, die gewartet werden soll, bis die Erkennungen automatisch geschlossen werden.
 Der Standardwert ist 90.
6. Wählen Sie **Speichern**.

Aktivieren Sie den Auftrag Veraltete Erkennungen automatisch schließen

Aktivieren Sie die geplante Aufgabe, um veraltete Erkennungen in regelmäßigen Abständen automatisch zu schließen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle > Azure D4IoT-Schwachstellen-Integration > Administrator > Geführtes Setup**.
2. Wählen Sie im Abschnitt **Veraltete Erkennungen automatisch schließen (optional)** die Aufgabe **Geplante Aufgabe zum automatischen Schließen veralteter Erkennungen aktivieren**.
3. Wählen Sie **Konfigurieren**.

4. Aktivieren Sie das Kontrollkästchen neben dem Feld **Aktiv**.

5. **Wahlweise:** Wählen Sie im Feld **Ausführen** die Option aus, die Ihren Anforderungen entspricht. Standardmäßig ist das Feld auf **Bei Bedarf** festgelegt. Sie können dies jedoch entsprechend Ihren Anforderungen ändern. Sie können beispielsweise **Täglich** auswählen und im angezeigten Feld **Zeit** Stunde und Minute des Tages auswählen.

6. Wählen Sie **Speichern**.

Unterstützung für die Vulnerability Response Integration mit Microsoft Defender for IoT (Azure)

In diesem Abschnitt finden Sie Fragen zur Datenzuordnung und Fehlerbehandlung.

Datenzuordnung

In den folgenden Tabellen werden die Datenzuordnungsfelder beschrieben, die für die Erkennung von Schwachstellen und Einträge in der National Vulnerability Database (NVD) in der Anwendung Microsoft Defender for IoT (Azure) verwendet werden. Außerdem wird angegeben, ob ein entsprechender Eintrag verwendet wird, nachdem die Daten in ServiceNow CMDB importiert wurden.

Erkennung von Schwachstellen

Feld „Microsoft Defender for IoT (Azure)“	ServiceNow Feld
N/V	Quelle Hinweis: Legen Sie dieses Feld immer auf Microsoft Azure Defender for IoT fest.
name	discovery_key
N/V	status Hinweis: Dieses Feld ist standardmäßig auf 0 festgelegt, was offen bedeutet.

NVD-Einträge

Feld „Microsoft Defender for IoT (Azure)“	ServiceNow Feld
Eigenschaften/Schwachstellen-ID	id
	Quelle Hinweis: Dieses Feld ist standardmäßig auf NVD festgelegt.
Eigenschaften/Beschreibung	Zusammenfassung
Eigenschaften/Punktzahl	Punktzahl
Eigenschaften/Exploittype	Exploit vorhanden

NVD-Einträge (Fortsetzung)

Feld „Microsoft Defender for IoT (Azure)“	ServiceNow Feld
	Wenn die API-Daten angeben, dass ein Exploit vorhanden ist, setzt die Integration dieses Feld auf Ja .
Eigenschaften/Exploittyp	public_exploit Wenn die API-Daten angeben, dass ein Exploit vorhanden ist, setzt die Integration dieses Feld auf Ja .

Configuration Item (CI)-Suche

Die CI-Suche wird mit der **deviceid** von Microsoft Defender for IoT (Azure) durchgeführt. In der Tabelle „sys_object_source“, die mit Service Graph Connector gefüllt wird, wird nach der übereinstimmenden Geräte-ID gesucht. Wenn eine Übereinstimmung gefunden wird, werden die Erkennung und das angreifbare Element mit diesem CI verknüpft.

i Hinweis:

Standardmäßig ist zum Einfügen von Schwachstellenerkennungen eine CI-Übereinstimmung erforderlich. Dies trägt dazu bei, nicht klassifizierte Hardware-CIs in CMDB zu minimieren. Um dieses Verhalten zu ändern, können Sie die Systemeigenschaft **sn_msft4iotazvr.require_ci_match** auf den Wert **false** festlegen. Wenn Sie die Eigenschaft auf „false“ festlegen, können nicht klassifizierte Hardware-CIs erstellt werden, wenn keine CI-Übereinstimmung gefunden wird.

Fehlerbehandlung

Die Integration ist so konzipiert, dass sie weitgehend vorkonfiguriert ist, sodass Sie nur Ihre Azure-Mandanten-ID, Client-ID und Ihren geheimen Clientschlüssel eingeben müssen. Protokollnachrichten aus der Anwendung können in den Systemprotokollen aus der Quelle **sn_msft4iotazvr** angezeigt werden. Zusätzliche relevante Protokollnachrichten können auch aus der Quelle **„sn_vul“** angezeigt werden.

Wenn die Integrationsausführung fehlschlägt, wird der Fehler im Feld **Hinweise** zur Integrationsausführung angezeigt. Der Status wird auf **Abgeschlossen** mit dem Substatus **Fehlgeschlagen** festgelegt.

Die Tabelle „Importwarteschlange“ (sn_vul_ds_import_q_entry) enthält alle ausstehenden Transformationsanforderungen. Sie können diese Tabelle filtern, um nur Elemente anzuzeigen, die den **Status „In Verarbeitung“** haben, um anzuzeigen, was derzeit transformiert wird.

In den folgenden Tabellen werden die Fehlermeldungen und möglichen Ursachen während des Datenabrufs und der Datenverarbeitung beschrieben.

Vulnerability Detection Integration (Datenabruf)

Fehlermeldung	Mögliche Ursache
Die Integration kann ohne angegebene REST-Nachricht und REST-Methode nicht ausgeführt werden	Im Datensatz der Erkennungsintegrationsaufgabe werden die Felder „ REST-Nachricht “ oder „ REST-Methode “ nicht ausgefüllt.
Die Integration kann ohne angegebene Microsoft Defender for IoT (Azure) oauth_client_id nicht ausgeführt werden	In der Integrationsinstanz ist die OAuth-Client-ID nicht ausgefüllt.
Die Integration kann ohne Angabe von Microsoft Defender for IoT (Azure) oauth_client_secret nicht ausgeführt werden	In der Integrationsinstanz ist das OAuth-Clientgeheimnis nicht ausgefüllt.
Die Integration kann ohne angegebenen Pfad der Erkennungs-API-Ressource nicht ausgeführt werden	In der Integrationsinstanz ist der Pfad der Erkennungs-API-Ressource nicht ausgefüllt. Der Standardwert ist <code>https://management.azure.com/providers/Microsoft.ResourceGraph/resources</code>
Die Integration mit der angegebenen API-Version kann nicht ausgeführt werden	In der Integrationsinstanz ist die API-Version nicht ausgefüllt. Der Standardwert ist 01.03.2021.
Ungültiger Antwortcode {Antwortcode} von Microsoft Defender for IoT (Azure) erhalten	Die Antwort von der Microsoft-API ist ungültig. Beispielsweise bedeutet der ungültige Antwortcode 401, der von Microsoft Defender for IoT (Azure) empfangen wurde, Nicht autorisiert . Die Anmeldeinformationen oder das OAuth-Token sind wahrscheinlich ungültig.
Fehler beim Analysieren des JSON-Antworttexts	Die empfangene JSON-Antwort ist ungültig, wenn sie nicht analysiert werden kann. Dies bedeutet, dass keine Daten empfangen wurden. Stellen Sie sicher, dass die Anmeldeinformationen korrekt sind und keine anderen Fehler auftreten.
Fehler beim Schreiben des Anhangs	Das System konnte die Antwortdaten nicht an die Datenquelle anhängen. Wahrscheinlich müssen Sie sich für weitere Problembehandlungen an Ihren Systemadministrator wenden. Eine häufige Ursache für diesen Fehler ist, dass dem MID-Server oder der Ausführung als Benutzer die Rolle „sn_vul.vr_import_admin“ fehlt.

Vulnerability Detection Integration (Datenabruf) (Fortsetzung)

Fehlermeldung	Mögliche Ursache
Anhangsinhalt ist NULL: Anhang sys_id = {sys_id}	Der Inhalt des Anhangs „Datenquelle“ ist NULL. Dies kann auf ein Problem mit der Microsoft-API selbst oder auf ein Problem in ServiceNow hinweisen. Wenden Sie sich für weitere Problembehandlungen an den Systemadministrator.
Anhang mit sys_id {sys_id} konnte nicht gefunden werden	Datenquellenanhang wurde nicht gefunden. Dies kann auf ein Problem mit der Microsoft-API selbst oder auf ein Problem in ServiceNow hinweisen. Wenden Sie sich für weitere Problembehandlungen an den Systemadministrator.

Vulnerability Detection Integration (Datenverarbeitung)

Fehlermeldung	Mögliche Ursache
Eine Erkennung ohne Schwachstellen-ID kann nicht erstellt werden	Für den Datensatz war keine Schwachstellen-ID vorhanden. Dies wird höchstwahrscheinlich durch ein Problem mit der Microsoft-API verursacht.

Vulnerability Response für Microsoft Defender for IoT (lokale Verwaltungskonsole)

Vulnerability Response für Microsoft Defender for IoT (lokale Managementkonsole) verwendet Daten, die aus Microsoft Defender for IoT (lokale Managementkonsole) importiert wurden, um risikobasierte Aktionen mit dem Produktionsprozesskontext zu ermöglichen.

Verwenden Sie die Anwendung Vulnerability Response für Microsoft Defender for IoT (lokale Managementkonsole), um Schwachstellen auf Geräten, die im Produktionsprozess verwendet werden, nachzuverfolgen, zu priorisieren und zu beheben.

Schlüsselfunktionen

- Importieren Sie CVEs, die OT-Geräten zugeordnet sind, aus Microsoft Defender for IoT (lokale Verwaltungskonsole), und erstellen Sie angreifbare Elemente (VITs), um eine einheitliche Ansicht der Schwachstellendaten für OT-Geräte mit Produktionsprozesskontext bereitzustellen.
- Führen Sie Importe neu erkannter Schwachstellen automatisch nach Ihrem eigenen Zeitplan aus.
- Die Verwendung von Zuweisungsregeln für VITs kann automatisch zur Korrektur an lokale Teams vor Ort weitergeleitet werden, um risikobasierte Maßnahmen zu ergreifen.

Vulnerability Response für Microsoft Defender for IoT installieren (lokale Verwaltungskonsole)

Mit der Administratorrolle können Sie Vulnerability Response für Microsoft Defender for IoT (lokale Verwaltungskonsole) installieren. Die Anwendung enthält zugehörige Installationen ServiceNow® Store, Anwendungen und Plugins, falls sie nicht bereits installiert sind.

Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter [Rufen Sie eine Berechtigung für ab ServiceNow Produkt oder Anwendung](#) .
- Überprüfung des folgenden Elements: [Vulnerability Response für Microsoft Defender for IoT \(lokale Verwaltungskonsole\)](#)  Anwendungsliste in ServiceNow Store, um Informationen zu Abhängigkeiten, Lizenzierungs- oder Abonnementanforderungen und Releasekompatibilität zu erhalten.
- Vulnerability Response für Microsoft Defender for IoT (lokale Verwaltungskonsole) erfordert die folgenden ServiceNow Store -Anwendungen. Stellen Sie sicher, dass diese Anwendungen installiert sind, bevor Sie die Integration Vulnerability Response mit Microsoft Defender for IoT installieren.

Store-App „CMDB CI Class Models“

Diese Integration verwendet Operational Technology [Erweiterungsklassen](#)  die Teil der Anwendung CMDB CI Class Models sind. Weitere Informationen finden Sie unter [CMDB CI Class Models](#) .

Service Graph Connector Microsoft Defender for IoT (lokal)

Diese Integration verwendet die Anwendung Operational Technology Manager, um den Import von Sensorgeräten, OT-Geräten und Netzwerkverbindungen zu automatisieren. Informationen zur Installation von Service Graph finden Sie unter [Service Graph Connector für Microsoft Defender for IoT \(lokale Verwaltungskonsole\)](#).

Erforderliche Rolle: Administrator

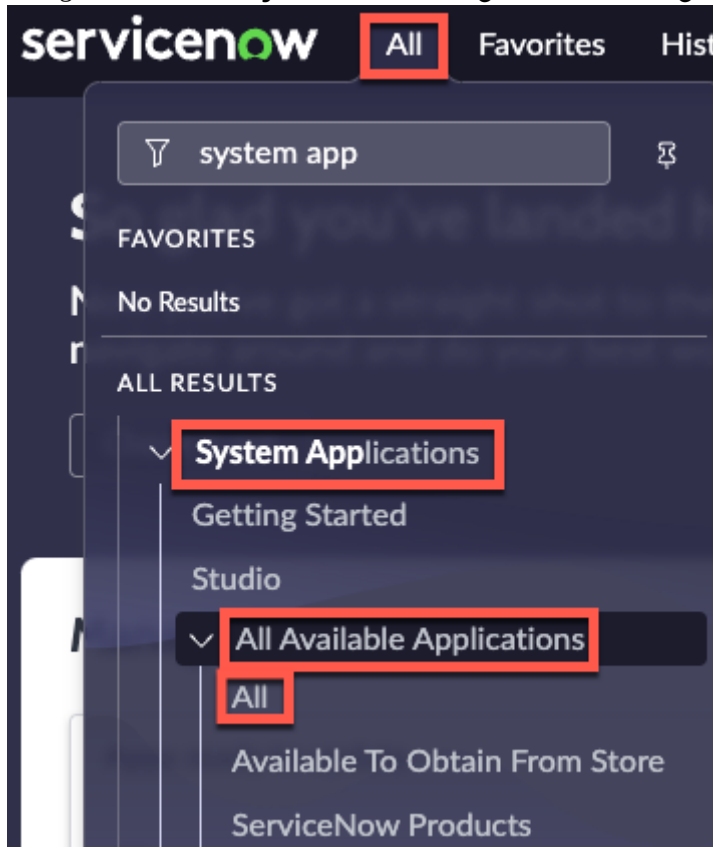
Warum und wann dieser Vorgang ausgeführt wird

Die folgenden Elemente werden mit Vulnerability Response für Microsoft Defender for IoT (lokale Managementkonsole) installiert:

- Vulnerability Response-Plugin
- Vulnerability Response Integration with NVD

Prozedur

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



2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach Vulnerability Response für Microsoft Defender for IoT (lokale Verwaltungskonsole).

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

In der Liste neben der Schaltfläche **Installieren** werden die für Sie verfügbaren Versionen angezeigt.

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. Wählen Sie **Installieren** aus.

Weisen Sie Vulnerability Response für die Rollen Microsoft Defender for IoT (lokale Verwaltungskonsole) zu

Weisen Sie Ihren Anwendern Rollen zu, damit Sie ihren Zugriff auf die Funktionen, Fähigkeiten und Daten in der Anwendung Vulnerability Response für Microsoft Defender for IoT (lokale Verwaltungskonsole) steuern können.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Benutzer mit den in den folgenden Tabellen aufgeführten Rollen können die Anwendung Vulnerability Response für Microsoft Defender for IoT (lokale Verwaltungskonsole) verwenden.

Weisen Sie Administratoren oder Anwendergruppen nach Bedarf Rollen zu.

Vulnerability Response für Microsoft Defender for IoT (lokale Verwaltungskonsole) Rollen

Rolle	Beschreibung
OT VR-Integrationsbetrachter [sn_otvr.integration_viewer]	Kann OT VR-Integrationsdatensätze anzeigen.
OT VR-Integrationsadministrator [sn_otvr.integration_admin]	Kann OT VR-Integration konfigurieren und ausführen.
MID-Server [mid_server]	Kann MID-Serverkonfigurieren.

Prozedur

Weisen Sie Benutzern und Gruppen mit der Benutzerverwaltungsfunktion Now Platform Rollen zu.

Integration der US-Schwachstellendatenbank (National Vulnerability Database) ausführen

Führen Sie die Integration der National Vulnerability Database (NVD) aus, um Daten aus dem NVD-Produkt des National Institute of Standards and Technology (NIST) zu importieren. Durch das Ausführen der NVD-Integration können Sie den Schweregrad und die Details der in Ihrer Umgebung gefundenen allgemeinen Schwachstellen und Risiken (Common Vulnerabilities and Exposures, CVEs) bestimmen.

Vorbereitungen

Bevor Sie die NIST NVD-Integration in Ihrer Instanz von ausführen, müssen die Installations- und Konfigurationsschritte abgeschlossen werden. Durch das Abschließen der Installation und Konfiguration wird sichergestellt, dass das NVD-Produkt ordnungsgemäß in die Anwendung Operational Technology Vulnerability Response integriert wird.

Informationen zur Installation des NVD-Plugins finden Sie unter [Install the Vulnerability Response Integration with the NIST National Vulnerability Database](#) .

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle > Vulnerability Response > Administration > Integrationen**.
2. Wählen Sie den Datensatz NIST NVD integration – API (nur CVE) aus.

Vulnerability Integrations					
Name	Active	Class	Updated	Source Instance	
Claroty CTD Vulnerability Closure Integration	false	Claroty CTD Vulnerability Integration	2023-06-09 09:52:27	Claroty CTD	
Claroty CTD Vulnerability Detection Integration - Delta Import	false	Claroty CTD Vulnerability Integration	2023-06-22 10:23:09	Claroty CTD	
Claroty CTD Vulnerability Detections - Full Import	true	Claroty CTD Vulnerability Integration	2023-06-22 10:23:16	Claroty CTD	
CWE Comprehensive 2000 Integration	true	Vulnerability Integration	2015-11-25 10:58:50	(empty)	
Manual Ingestion CSV Integration	true	Vulnerability Integration	2022-05-22 20:50:20	Manual Ingestion	
Manual Ingestion Excel Integration	true	Vulnerability Integration	2022-05-24 01:02:35	Manual Ingestion	
Manual Ingestion JSON Integration	true	Vulnerability Integration	2022-05-22 21:07:45	Manual Ingestion	
Manual Ingestion XML Integration	true	Vulnerability Integration	2022-05-24 01:02:56	Manual Ingestion	
Microsoft D4IoT Auto-close Resolved Vulnerable Items	false	Microsoft D4IoT VR Integration	2022-03-02 21:22:20	Microsoft D4IoT Vulnerability Response L...	
Microsoft D4IoT Devices CVE Integration (Delta Import)	false	Microsoft D4IoT VR Integration	2021-09-03 01:12:50	Microsoft D4IoT Vulnerability Response L...	
Microsoft D4IoT Devices CVE Integration (Full Import)	false	Microsoft D4IoT VR Integration	2021-09-03 01:12:54	Microsoft D4IoT Vulnerability Response L...	
Microsoft Security Response Center Solution Integration	false	Microsoft Security Response Center Solut...	2019-03-13 21:21:01	Microsoft Security Response Center Solut...	
NIST National Vulnerability Database Integration - API (CVE and CPE)	false	REST Integration	2020-11-10 20:30:02	National Vulnerability Database	
NIST National Vulnerability Database Integration - API (CVE only)	true	REST Integration	2023-07-11 07:13:28	National Vulnerability Database	
Red Hat Solution Integration	false	Red Hat Solution Integration	2020-03-03 23:10:43	Red Hat Solution Integration	

3. Legen Sie den Wert im Feld **Importieren seit** auf **NULL** fest.

4. Wählen Sie **Jetzt ausführen**.

Vulnerability Response für Microsoft Defender for IoT konfigurieren (lokale Verwaltungskonsole)

Konfigurieren Sie den -Datensatz für die Integration Vulnerability Response für Microsoft Defender for IoT (lokale Verwaltungskonsole).

Vorbereitungen

Verwenden Sie das geführte Setup für Vulnerability Response für Microsoft Defender for IoT (lokale Verwaltungskonsole), um die Konfiguration abzuschließen. Um auf das geführte Setup zuzugreifen, navigieren Sie zu **MSFT D4IoT Schwachstellenintegration > Administration > Geführtes Setup**.

Erforderliche Rolle: sn_otvr.integration_admin und mid_server

Prozedur

1. Navigieren zu **Alle > MSFT D4IoT Schwachstellenintegration > Administration > Konfigurationen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular aus.
Eine Beschreibung der Feldwerte finden Sie unter [Microsoft Defender for IoT Formular „VR-Konfiguration“](#).
4. Klicken Sie auf **Anmeldeinformationen speichern und überprüfen**.

Microsoft Defender for IoT Formular „VR-Konfiguration“.

Verwenden Sie das Formular Microsoft Defender for IoT VR-Konfiguration, um die Anwendung Vulnerability Response für Microsoft Defender for IoT (lokale Verwaltungskonsole) zu konfigurieren.

Microsoft Defender for IoT Formular „VR-Konfiguration“.

Feld	Beschreibung
Name	Der Name der Konfiguration.
Integrationsinstanz	Die Instanz für die Konfiguration.

Microsoft Defender for IoT Formular „VR-Konfiguration“. (Fortsetzung)

Feld	Beschreibung
	Die verfügbare Standardintegrationsinstanz ist die Instanz Microsoft Defender for IoT Vulnerability Response.
Endpunkt-URL	Die URL der Microsoft Defender for IoT -Verwaltungskonsole. Beispiel: https://10.10.0.222/external/v3/integration/devicecve
MID-Server	MID-Server, der für die Integration verwendet wird.
API Key	Das für den Zugriff auf die Central Manager-APIs erforderliche Token. Informationen zum Erstellen eines API-Schlüssels in der -Verwaltungskonsole Microsoft Defender for IoT finden Sie unter https://docs.microsoft.com/en-us/azure/defender-for-iot/organizations/references-work-with-defender-for-iot-apis .
Seitengröße	Die Anzahl der Geräte pro Seite in der API-Antwort Microsoft Azure Event Hubs Die Standardseitengröße beträgt 50.
CVSS v2-Bewertung	Schwachstellen mit einer Punktzahl, die größer oder gleich der konfigurierten CVSS V2-Punktzahl ist, werden für den Import von CVEs und die Erstellung von Datensätzen für angreifbare Elemente (VIT) berücksichtigt. Der Standardwert ist 0.
Gelöste VIs automatisch schließen	Wenn der VIT-Datensatz auf „Gelöst“ festgelegt ist, kann er automatisch geschlossen werden, wenn das CVE in der API-Antwort von Microsoft Defender for IoT für dieses OT-Gerät nicht mehr angezeigt wird.
Wartezeit in Tagen bis zur erneuten Öffnung eines gelösten VI	Wenn eine VIT behoben ist, kann es eine Weile dauern, bis Microsoft Defender for IoT bestätigt, dass die Schwachstelle basierend auf der Kommunikation des OT-Geräts im Netzwerk behoben ist. Definieren Sie die Anzahl der Tage, die gewartet werden soll, bevor das gelöste VIT erneut geöffnet wird, wenn das NIDS es nicht als geschlossen bestätigen kann.

Konfigurieren Sie Importzeitpläne

Konfigurieren Sie die Importzeitpläne für den Zugriff auf die Datensätze Microsoft Defender for IoT.

Vorbereitungen

Führen Sie vor dem Planen des Imports von Microsoft Defender for IoT -Datensätzen die NVD-Integration aus, um Probleme zu beheben. Weitere Informationen finden Sie unter [Integration der US-Schwachstellendatenbank \(National Vulnerability Database\) ausführen](#).

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle > MSFT D4IoT Schwachstellenintegration > Administration > Integrationen**.

2. Wählen Sie in der Liste der Datensätze Ihren Datensatz aus:

- Der Zeitplan für den **vollständigen Import** importiert alle Schwachstellen für alle OT-Geräte.

Hinweis:

Eine häufige Ausführung des vollständigen Importzeitplans wird nicht empfohlen, da die Anzahl der Datensätze hoch sein kann.

- Der **Delta-Import**- Zeitplan kann standardmäßig so konfiguriert werden, dass er nach der Integration von Microsoft Azure Event Hubs Service Graph Connections ausgeführt wird. Weitere Informationen finden Sie unter [Konfigurieren Sie die System-ID der OT-Integration Vulnerability Response ..](#)
- Verwenden Sie den Zeitplan **Import gelöster VITs automatisch schließen**, wenn die Schwachstelle im OT-Gerät behoben ist. Die angreifbaren Elemente (VITs) werden basierend auf der Bestätigung vom Scanner automatisch geschlossen.

Wenn sich der Bereich nicht in der richtigen Anwendung befindet, wird oben auf der Seite die Meldung Klicken Sie hier, um diesen Datensatz zu bearbeiten angezeigt.

3. Klicken Sie **hier**, um den Datensatz zu bearbeiten.

4. Aktivieren Sie das Kontrollkästchen **Aktiv**, um **Aktiv** in **wahr** zu ändern.

5. Wählen Sie nach Bedarf in der Dropdown-Liste **Zeitplan** aus.

6. Klicken Sie auf **Jetzt ausführen**.

Konfigurieren Sie die System-ID der OT-Integration Vulnerability Response .

Konfigurieren Sie die System-ID für den vollständigen Import von Integrationsdatensätzen nach der Integration von Microsoft Azure Event Hubs SGC Connections.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Diese Konfiguration wird dringend empfohlen, um sicherzustellen, dass sich alle OT-Geräte in der CMDB befinden, für die möglicherweise Schwachstellen gemeldet wurden.

Prozedur

1. Navigieren zu **Alle > Service Graph Connector Microsoft D4 IoT > Eigenschaften**.

Wenn der Bereich auf die falsche Anwendung festgelegt ist, wird oben auf der Seite die Meldung Klicken Sie hier, um diesen Datensatz zu bearbeiten angezeigt.

① This record is in the [Service Graph Connector Integration with Microsoft Azure Defender for IoT application](#), but [Global](#) is the current application. To edit this record click [here](#).

Microsoft Defender for IoT Integration Properties

Integration Configurations

The following system properties are used to configure the Microsoft Defender for IoT integration.

Sensor API resource path. Default value is "/external/v3/integration/sensors". ②

Device API resource path. Default value is "/external/v3/integration/devices". ②

Connection API resource path. Default value is "/external/v3/integration/connections". ②

(Optional) Override Connection Alias record sys_id used to connect the integration. Default value is empty. ②

The number of device records to fetch in a paginated REST call to the Microsoft Defender for IoT Management Console. Default value is 50. ②

The number of connection records to fetch in a paginated REST call to the Microsoft Defender for IoT Management Console. Default value is 50. ②

Get all devices. If not checked, then only devices created or updated since the last successful import will be imported. Default is No. ②

☐ Yes | No

Get all connections. If not checked, then only connections created or updated since the last successful import will be imported. Default is No. ②

☐ Yes | No

(Optional) Sys id of OT VR Integration (Scheduled Job) to execute after SG-OT Microsoft D4IoT Connections Import. ②

2. Klicken Sie **hier**, um den Datensatz zu bearbeiten.

3. Konfigurieren Sie die Systemeigenschaft `sn_msft4iotsgc.ot.vr.integration.id` mit der `sys_id` der OT VR-Integration.

4. Klicken Sie auf **Speichern**.

Konfigurieren Sie veraltete Erkennungen automatisch schließen

Aktivieren Sie Veraltete Erkennungen automatisch schließen, um veraltete angreifbare Erkennungen, die nicht kürzlich von Ihren Drittanbieterintegrationen gefunden wurden, automatisch zu schließen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die veralteten Erkennungen sind höchstwahrscheinlich das Ergebnis einer Korrektur, die auf ein angreifbares Element für kritische Risiken (Critical Risk Vulnerable Item, VIT) abzielt und auch mehrere zusätzliche VITs mit geringerer Relevanz und dem Status „**Offen**“ behandelt. Wenn Sie diese VITs in **den Status „Geschlossen“** verschieben, reduzieren Sie die Anzahl der aktiven VITs und Schwachstellen-Gruppen in Ihrer Instanz Now Platform.

Prozedur

1. Navigieren zu **Alle > Vulnerability Response > Administration > Konfiguration für automatisches Schließen > Veraltete Erkennungen**.

Das Formular „Veraltete Konfiguration automatisch schließen“ wird angezeigt.

2. Füllen Sie die Felder aus.

3. Wählen Sie für das Feld **Veraltete Erkennungen automatisch schließen auf Grundlage von** die Option **Erkennungen zuletzt in der Liste gefunden aus**.

Mit dieser Option wird nach dem aktuellen oder spätesten Datum gesucht, an dem Erkennungen vom Scanner erneut gefunden wurden.

i Hinweis:

Die Option „**Zuletzt gescannte Geräte**“ gilt nicht für OT-Scanner.

Ab v22.0 von Vulnerability Response können Sie zusätzliche Optionen für die Suche konfigurieren. Weitere Informationen finden Sie unter [Create auto-close rules](#) .

4. Um das Modul zu aktivieren, aktivieren Sie das Kontrollkästchen **Aktiv**.

5. Geben Sie im Feld **Zuletzt gefundene Erkennungen (vor Tagen)** das Alter älterer, veralteter Erkennungen in Tagen ein.

Der Standardwert ist 90 Tage. Sie können einen beliebigen positiven Wert für die Anzahl der Tage eingeben. Dieser Wert wird verwendet, um ein zuletzt erkanntes Datum abzugleichen, das von Microsoft Defender for IoT bereitgestellt wird. Wenn 90 und **Zuletzt gefundene Erkennungen** angezeigt werden, werden angreifbare Elemente, die in den letzten 90 Tagen nicht erkannt wurden, automatisch geschlossen.

6. **Wahlweise:** Um veraltete Erkennungen zu ignorieren, die zurückgestellten VITs zugeordnet sind oder VITs, die derzeit auf Zurückstellung überprüft werden, aktivieren Sie **das Kontrollkästchen Veraltete Erkennungen für zurückgestellte VIs ignorieren**.

Wenn Sie diese Option deaktiviert lassen, werden alle Erkennungen geschlossen, die Ihren Kriterien entsprechen und die zurückgestellten VITs oder VITs zugeordnet sind, die zur Zurückstellung überprüft werden. Die zurückgestellten oder in der Überprüfung befindlichen VITs, die diesen Erkennungen entsprechen, werden basierend auf der Rollup-Logik ebenfalls automatisch geschlossen. Weitere Informationen zur Rollup-Logik finden Sie unter [Closing stale detections in Vulnerability Response](#) .

Wenn Sie diese Option aktivieren, werden alle Erkennungen, die Ihren Kriterien entsprechen und den zurückgestellten VITs oder VITs zugeordnet sind, die zur Zurückstellung überprüft werden, während des automatischen Schließens übersprungen.

7. **Wahlweise:** Deaktivieren Sie das Kontrollkästchen **Veraltete Erkennungen für geschlossene VIs ignorieren**.

Standardmäßig ist dieses Kontrollkästchen aktiviert, damit das geschlossene VIT nicht erneut geöffnet wird, wenn eine neue Erkennung für dieses geschlossene VIT identifiziert wird. Weitere Informationen zur Rollup-Logik finden Sie unter [Closing stale detections in Vulnerability Response](#) .

8. Wählen Sie **Aktualisieren**.

Die regelmäßige *Auto-Close Stale Detections*-Aufgabe wird täglich ausgeführt. Die Aufgabe bestimmt, ob Sie das Datum ausgewählt haben, an dem Erkennungen zuletzt gefunden wurden, oder das Datum, an dem Assets zuletzt gescannt wurden. Anschließend werden die entsprechenden Erkennungen in den Status Veraltet versetzt. Es ist wichtig zu beachten, dass die Funktion Veraltete Erkennungen automatisch schließen nur veraltete Erkennungen für aktive Integrationsinstanzen schließt. Angreifbare Elemente und Erkennungen, die aktiven Integrationsinstanzen zugeordnet sind, werden geschlossen. Ab v21.1 von Vulnerability Response wurde die geplante Aufgabe geändert, um die allgemeine Tabelle [sn_vul_cmn_auto_close_rule] zu berücksichtigen.

Nachdem die Erkennungen als Veraltet markiert wurden und der Scanner meldet, dass diese Erkennung erneut gefunden wurde, wechselt das Feld Status der Erkennungen

in Offen. Die entsprechenden angreifbaren Elemente der Erkennung werden ebenfalls erneut geöffnet.

Wenn die Erkennung als Veraltet markiert ist und der Scanner feststellt, dass sie behoben ist, geht die Erkennung außerdem in den Status Geschlossen über. Für den Status wird auch ein Rollup zu den VITs durchgeführt.

Operational Technology Vulnerability Response verwenden

Nachdem Sie alle erforderlichen Einrichtungsaufgaben abgeschlossen haben (einschließlich des Imports angreifbarer Elemente aus einer Drittanbieterintegration), können Sie die Anwendung Operational Technology Vulnerability Response aus Industriell Arbeitsbereichverwenden.

Industriell Arbeitsbereich

Um Operational Technology Vulnerability Response zu verwenden, greifen Sie über Industriell Arbeitsbereich auf die folgende Zielseite und die folgenden Menüs zu.

Weitere Informationen zu Industriell Arbeitsbereich finden Sie unter [Industriell Arbeitsbereich](#).

OTVR (PA)-Dashboard im Industriell Arbeitsbereich

Verwenden Sie das OTVR (PA)-Dashboard, um das Volumen, die Leistung und den Fortschritt Ihrer angreifbaren Elemente von der ersten Analyse und Erkennung bis zur Eindämmung oder Behebung zu verfolgen. Sie können die Berichte nach Zuweisungsgruppe, Exploits, Risikobewertung oder Status filtern, um Einblicke in das Schwachstellenrisiko und die betroffenen Services zu erhalten.

Weitere Informationen zum OTVR (PA)-Dashboard finden Sie unter [Operational Technology Vulnerability Response \(PA\)-Dashboard](#)

Dashboard „OT Schwachstellenrisiko-Rollup“ – Übersicht

Das Operational Technology (OT) Schwachstellenrisiko-Rollup-Dashboard enthält zwei Tabellen für Ihre Schwachstellenrisiko-Punktzahlen.

- Tabelle „Schwachstellenrisiko“ für Ihre Anlagenmodell-Entitäten
- Schwachstellenrisikotabelle für OT-Geräte ohne zugewiesene Site

Listenmenü

Verwenden Sie das Menü Liste, um alle Datensätze für angreifbare OT-Elemente anzuzeigen, auf die Sie Zugriff haben, und Korrekturaufgaben, die entweder Ihnen oder einer Zuweisungsgruppe zugewiesen wurden, der Sie angehören.

- OT-Korrekturaufgaben
 - Mir zugewiesen
 - Meinen Gruppen zugewiesen
- Angreifbare OT-Elemente
 - Mir zugewiesen
 - Meinen Gruppen zugewiesen
 - Meine Ausnahmeanforderungen

- Alle Ausnahmen

Hinweis:

In der Liste „Alle Ausnahmen“ werden auch Ausnahmen mit dem Status **Abgelehnt** angezeigt.

Navigieren Sie zu Datensätzen unter den Menüs „OT-Korrekturaufgaben“ oder „Angreifbare OT-Elemente“, um mehr OT-bezogenen Kontext zu erhalten. Um den Verlauf des Datensatzes anzuzeigen, können Sie im Datensatz das Fenster **„Aktivität“** anzeigen, in dem verschiedene Arbeitsnotizen, Kommentare und Datensatzaktualisierungen erfasst werden. Sie können im Fenster **Verfassen** auch neue Kommentare oder Arbeitsnotizen hinzufügen.

Weitere Informationen zu Korrekturaufgaben finden Sie unter [Erstellen Sie eine Korrekturaufgabe](#).

Weitere Informationen zur Verwendung der Listenansicht in Industriell Arbeitsbereich für Operational Technology Vulnerability Response finden Sie [unter Listenansicht im IT-Korrekturarbeitsbereich verwenden](#) .

Menü „Anlagenmodell“.

Verwenden Sie den Anlagenmodell-Manager, um angreifbare OT-Elemente anzuzeigen und Korrekturaufgaben für OT-Geräte anzuzeigen und zu erstellen, die einer Anlagenmodell-Entität zugeordnet sind.

Schwachstellenbewertung für Hardware

Verwenden Sie das Menü „Bewertung von Hardware-Schwachstellen“, um die Schwachstellenbewertungen anzuzeigen und zu verwalten, die für die Firmwares der OT-Geräte im Bestand durchgeführt wurden.

Verwenden Sie die folgenden Registerkarten im Menü „Hardware Vulnerability Assessment“ (Bewertung von Hardware-Schwachstellen), um alle Bewertungsdatensätze und angreifbaren Elemente anzuzeigen, die automatisch erstellt werden:

- Vollständig abgegliche Bewertungen
- Teilweise abgegliche Bewertungen
- Angreifbare Elemente
- Ignorierte Bewertungen
- Warten auf Normalisierung

Zugehörige Informationen

[Vulnerability Response-Arbeitsbereiche](#) 

Erstellen Sie eine Korrekturaufgabe

Erstellen Sie Korrekturaufgaben, die OT-Geräten zugeordnet sind, die einer Anlagenmodell-Entität zugeordnet sind.

Vorbereitungen

Erforderliche Rolle:sn_otvr.remediation_owner

Prozedur

1. Navigieren zu **Alle > Industrial Workspace**.
2. Öffnen Sie die Seite **„Anlagenmodell“**.

- Wählen Sie im Feld **Anlagenmodell-Ansicht für** den Standort aus, für den Sie die Anlagenmodell-Informationen anzeigen möchten.
- Wählen Sie die entsprechende Anlagenmodell-Entität aus, und navigieren Sie zur Registerkarte der zugehörigen Liste „**Angreifbare Elemente**“.
- Wählen Sie die Datensätze für angreifbare Elemente aus, die Sie der Korrekturaufgabe hinzufügen möchten, und wählen Sie dann **Korrekturaufgabe erstellen** aus.

The screenshot shows the ServiceNow Industrial Workspace interface. The left sidebar displays a navigation tree with 'San Diego' and 'Airport' selected. The main content area is titled 'Equipment model view for San Diego' and shows a list of 'Vulnerable Items' (41 total). The list includes columns for Number, Summary, OT asset, Manufacturer, Risk score, Risk rating, State, and Remediation task. The first two items are highlighted in blue.

Number	Summary	OT asset	Manufacturer	Risk score	Risk rating	State	Remediation task
VIT0010001	[Clarity] Rockwell sending a CIP connection request to an affected device and upon successful connection enables sending a new IP configuration	90.73.88.104 @ e5:ec:fe:3a:ee:2e	BizLink	0	5 - None	Open	
VIT0010232	[Clarity] Rockwell sending a CIP connection request to an affected device and upon successful connection enables sending a new IP configuration	90.73.88.104 @ e5:ec:fe:3a:ee:2e	BizLink	80	2 - High	Open	
VIT0010235	[Clarity] Rockwell sending a CIP connection request to an affected device and upon successful connection enables sending a new IP configuration	90.73.88.104 @ e5:ec:fe:3a:ee:2e	BizLink	80	2 - High	Open	
VIT0010236	[Clarity] Rockwell sending a CIP connection request to an affected device and upon successful connection enables sending a new IP configuration	90.73.88.104 @ e5:ec:fe:3a:ee:2e	BizLink	40	3 - Medium	Open	
VIT0010237	[Clarity] Rockwell sending a CIP connection request to an affected device and upon successful connection enables sending a new IP configuration	90.73.88.104 @ e5:ec:fe:3a:ee:2e	BizLink	20	4 - Low	Open	
VIT0010238	[Clarity] Rockwell sending a CIP connection request to an affected device and upon successful connection enables sending a new IP configuration	90.73.88.104 @ e5:ec:fe:3a:ee:2e	BizLink	80	2 - High	Open	

- Geben Sie alle erforderlichen Details für die Korrekturaufgabe an.
Das Feld Zuweisungsgruppe weist automatisch basierend auf der Site-Zuweisungsgruppe zu.
- Wählen Sie **Speichern** aus, um den Aufgabendatensatz zu erstellen.

Ergebnisse

Sobald Sie eine Korrekturaufgabe erstellt haben, wird die Aufgabe während der nächsten geplanten Wartung übernommen, die vom Wartungsplan Ihrer Anlagenmodell-Entität bestimmt wird. Weitere Informationen zu Zeitplänen für Anlagenmodell-Entitäten finden Sie unter [Anlagenmodelle verwalten](#).

Sie können eine Startzeit für eine Korrekturaufgabe auch manuell auswählen. Weitere Informationen zum Auswählen einer Startzeit finden Sie unter [Wählen Sie eine Startzeit für eine Korrekturaufgabe aus](#).

Zeigen Sie Lösungen eines angreifbaren Elements im an Industrial Workspace

Zeigen Sie bevorzugte Lösungen oder alle verfügbaren Lösungen an, die von Operational Technology (OT) Vulnerability Solution Management in einem angreifbaren Element (VIT) bereitgestellt werden.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Industrial Workspace** > **Listenansicht** () > **Lösungen**.

- a. Wählen Sie **Alle** aus, um die vollständige Liste der verfügbaren Schwachstellenlösungen anzuzeigen.
- b. Wählen Sie **Mit angreifbaren Elementen** aus, um die Liste der Schwachstellenlösungen anzuzeigen, die für die entsprechenden angreifbaren Elemente bereitgestellt werden.

2. Navigieren Sie zur Liste der VITS.

- Navigieren zu **Alle** > **Industrial Workspace** > **Listenansicht** () > **Angreifbare OT-Elemente**.
- Navigieren zu **Alle** > **Industrial Workspace** > **Anlagenmodell-Ansicht** () > **Angreifbare Elemente**.
- a. Wählen Sie eine VIT aus der angezeigten Liste aus.
- b. Im Abschnitt „Nachbesserung“ der VIT können Sie die bevorzugte Lösung oder alle verfügbaren Lösungen für die VIT anzeigen.
- c. Wenn für die VIT mehr als eine Lösung verfügbar ist, wählen Sie Suchen  im Feld **Bevorzugte Lösung**, um alle verfügbaren Lösungen für die VIT zu suchen und anzuzeigen.

Zugehörige Informationen

[Operational Technology Vulnerability Solution Management](#)

Wählen Sie eine Startzeit für eine Korrekturaufgabe aus

Wählen Sie eine erwartete Startzeit für eine Korrekturaufgabe Operational Technology (OT) aus, indem Sie die Zeitfenster in den Zeitplänen für Anlagenmodell-Entitäten verwenden.

Vorbereitungen

Erforderliche Rolle: sn_otvr.remediation_owner

Warum und wann dieser Vorgang ausgeführt wird

Es gibt zwei Möglichkeiten, manuell eine Startzeit für eine OT-Korrekturaufgabe auszuwählen.

- Sie können eine Startzeit auswählen, wenn Sie eine Korrekturaufgabe erstellen, indem Sie im Formular „Neue Korrekturaufgabe erstellen“ **Planungsassistent** auswählen.
- Sie können eine vorhandene Korrekturaufgabe öffnen und von dort aus planen.

Der Planungsassistent verwendet die Zeitfenster aus den Zeitplänen der Anlagenmodell-Entitäten. Weitere Informationen finden Sie unter [Entitätszeitplan für Anlagenmodelle verwalten](#).

Prozedur

1. Wenn Sie beim Erstellen einer Korrekturaufgabe eine Startzeit auswählen möchten, gehen Sie wie folgt vor:

- a. Lesen Sie [Erstellen Sie eine Korrekturaufgabe](#), und führen Sie die Schritte 1–6 aus.
- b. Wählen Sie **Planungsassistent** aus.

c. Wählen Sie Datum und Uhrzeit für die Durchführung der Korrekturaufgabe

Create New Remediation Task

OT Remediation Task Details

Assignment group: OT VR Default Assignment Group

Assigned to:

Short description: Terminal 1 Vulnerabilities

Description: Terminal 1 (SD-SAN-T1)

Site: San Diego

Service: SD-SAN-T1

Planned downtime for Terminal 1

Next available date and time: 10:00 AM, Thursday, 03 November, 2022

Today < > October 30 - November 5, 2022

Sunday 30	Monday 31	Tuesday 01	Wednesday 02	Thursday 03	Friday 04	Saturday 05
No slots available	No slots available	No slots available	No slots available	10:00 AM 11:00 PM	07:00 AM 10:00 AM 11:00 PM	07:00 AM 10:00 AM

Time Zone : America/Los_Angeles
Selected time: 10:00 AM - 10:30 AM, Thursday, 03 November, 2022

Schedule

Attachments

No Attachments Available
Browse for a file to add it as an attachment

Browse

aus.

d. Wählen Sie **Zeitplan**.

2. Wenn Sie eine Startzeit für eine vorhandene Korrekturaufgabe auswählen möchten, gehen Sie wie folgt vor:
 - a. Navigieren zu **Alle > Industrial Workspace**.
 - b. Navigieren Sie in der Listenansicht zu **OT-Korrekturaufgaben > Mir zugewiesen**.
 - c. Wählen Sie aus der Liste die Korrekturaufgabe aus, für die Sie eine Startzeit festlegen möchten.
 - d. Wählen Sie **Planungsassistenten** aus.
 - e. Wählen Sie Datum und Uhrzeit für die Durchführung der Korrekturaufgabe aus.
 - f. Wählen Sie **Zeitplan**.

Ergebnisse

Die Korrekturaufgabe wird während der festgelegten Zeit ausgeführt.

Korrekturaufgabe aufteilen

Benutzer können die angreifbaren Elemente (VIs) aus einem Korrekturaufgabendatensatz aufteilen, um eine Korrekturaufgabe zu erstellen.

Vorbereitungen

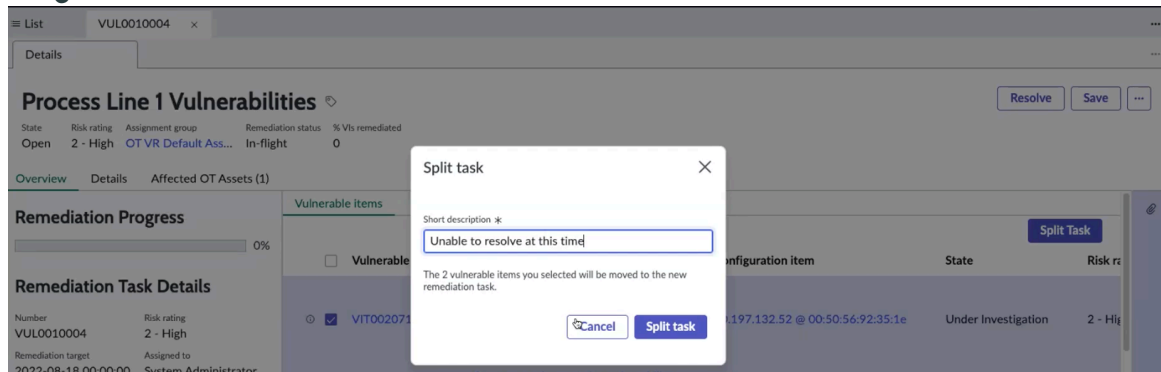
Erforderliche Rolle: sn_otvr.remediation_owner

Prozedur

1. Navigieren zu **Alle > Industrial Workspace > OT-Korrekturaufgaben > Mir zugewiesen**.
2. Wählen Sie aus der Liste die VIs aus, die Sie in eine neue Korrekturaufgabe verschieben möchten.
3. Klicken Sie auf **Aufgabe aufteilen**.
4. Füllen Sie im angezeigten Dialogfeld das Kurzbeschreibungsfeld aus.

Die Anzahl der VIs, die Sie aus der Liste ausgewählt haben, wird angezeigt.

Aufgabennachricht aufteilen



5. Klicken Sie erneut **auf Aufgabe aufteilen**.

Korrekturaufgabe zurückstellen

Stellen Sie eine Korrekturaufgabe zurück, um eine Ausnahmeanforderung zu erstellen, die Sie später lösen können.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle > Industrial Workspace**.
2. Um die Listenansicht Industriell Arbeitsbereich zu öffnen, wählen Sie das Listensymbol ().
3. Wählen Sie im Modul **OT-Korrekturaufgaben** eine der verfügbaren Listen aus.
4. Wählen Sie die Korrekturaufgabe aus, die Sie zurückstellen möchten.
5. Wählen Sie **Ausnahme anfordern** aus.
6. Füllen Sie die Felder des Formulars aus.

Feld	Beschreibung
Bis	Wählen Sie das Datum aus, an dem der Status „Zurückgestellt“ abläuft und die Korrekturaufgabe erneut aktiviert wird.
Grund	Geben Sie den Grund für das Zurückstellen des Problems ein. Zur Auswahl stehen: ○ Warten auf Wartungsfenster ○ Falsch positiv ○ Fix nicht verfügbar ○ Risiko akzeptiert ○ Ausgleichende Steuerung vorhanden ○ Sonstige

Feld	Beschreibung
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

7. Wählen Sie **Speichern**.

Ergebnisse

Eine Ausnahmeanforderung wird erstellt. Sie können Ihre Ausnahmeanforderungen in der Liste „**Meine Ausnahmeanforderungen**“ im Modul **OT-Korrekturaufgaben** anzeigen. Sie können auch alle vorhandenen Ausnahmeanforderungen in der Liste „**Alle Ausnahmen**“ im Modul **OT-Korrekturaufgaben** anzeigen.

Ausgleichssteuerungen für verstehen Operational Technology

Ausgleichssteuerungen in OT-Umgebungen sind alternative Sicherheitsmaßnahmen, wenn Risiken, die durch Schwachstellen entstehen, nicht sofort behoben werden können.

In OT-Umgebungen können Systeme aufgrund ihrer kritischen Rolle in Infrastruktur- und Produktionsprozessen häufig nicht offline genommen werden, um Updates durchzuführen. Ausgleichssteuerungen sichern die OT-Umgebung und reduzieren das Risiko, bis die Schwachstelle durch dauerhafte Lösungen wie Patches oder Hardware-Ersatz vollständig behoben werden kann.

Die folgende Tabelle beschreibt bestimmte Szenarien, in denen Ausgleichssteuerungen zur Risikoreduzierung beitragen:

Anwendungsfälle für Ausgleichssteuerungen

Anwendungsszenario	Ausgleichssteuerungen
Nicht autorisierter Zugriff auf speicherprogrammierbare Steuerungen (SPS).	• Implementieren Sie Zugriffssteuerungslisten (ACLs) auf Netzwerkgeräten. • Deaktivieren Sie nicht verwendete Ports und Services auf SPS. • Implementieren Sie sichere Passwörter und Authentifizierungsmechanismen.
Pufferüberlauf in HMI-Bereichen (Human Machine Interfaces).	• Wenden Sie die vom HMI-Panel-Hersteller veröffentlichten Firmware-Updates an. • Hardware-Watchdog-Timer für fehlersicheren Betrieb aktivieren. • Implementieren Sie Grenzenprüfungen im Anwendungscode.

Anwendungsfälle für Ausgleichssteuerungen (Fortsetzung)

Anwendungsszenario	Ausgleichssteuerungen
Man-in-the-Middle-Angriffe auf PROFINET	• Verwenden Sie verschlüsselte Kommunikation über VPNs oder IPSec. • Konfigurieren Sie PROFINET mit sicheren Zertifikaten. • Implementieren Sie eine Netzwerksegmentierung mit Firewalls.
Denial of Service (DoS) auf SCADA-Systemen	• Aktivieren Sie die Quotenbegrenzung für kritische OT-Netzwerkkomponenten. • Konfigurieren Sie SCADA-Systeme für Redundanz und Lastenausgleich. • Wenden Sie von Windows bereitgestellte Sicherheitspatches an.
Malware-Befall auf Engineering-Workstations	• Installieren Sie vom Hersteller empfohlene Anti-Malware-Software, und aktualisieren Sie sie regelmäßig. • Wenden Sie die Anwendungs-Allow-Liste an, um die Ausführung von nicht autorisierter Software zu verhindern. • Verwenden Sie sichere Richtlinien für Wechseldatenträger.

Verwenden Sie Ausgleichssteuerungen für Operational Technology

Konfigurieren Sie Ausgleichssteuerungen für Operational Technology (OT).

Warum und wann dieser Vorgang ausgeführt wird

Ausgleichssteuerungen tragen dazu bei, die Wahrscheinlichkeit oder die Auswirkungen eines erfolgreichen Exploits zu verringern. Weitere Informationen zu Ausgleichssteuerungen finden Sie unter [Understanding compensating controls for risk reduction](#) .

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin oder sn_vul.vulnerability_analyst

Prozedur

- 1. Navigieren zu **Alle > Industrial Workspace**.
- 2. Wählen Sie das Symbol Liste () aus.
- 3. Wählen Sie im Modul **Bibliotheken** die Liste **Ausgleichssteuerungen** aus.
- 4. Wählen Sie **Neu**.
- 5. Füllen Sie die folgenden Felder des Formulars aus.

Formular „Ausgleichssteuerungen“.

Feld	Beschreibung
Name	Der Name der Ausgleichssteuerung, die Sie hinzufügen möchten.
Beschreibung	Eine Erklärung der Ausgleichssteuerung, die Sie hinzufügen möchten.
Aktiv	Wenn diese Option ausgewählt ist, ist die Ausgleichssteuerung aktiviert.

6. Wählen Sie Speichern.**Zeigen Sie Einträge zu allgemeinen Schwachstellen im an Industriell Arbeitsbereich**

Zeigen Sie Common Vulnerability Entries (CVE) in Industriell Arbeitsbereich an, um auf Informationen zuzugreifen, die für Ausgleichssteuerungen erforderlich sind.

Vorbereitungen

Erforderliche Rolle: sn_vul.vulnerability_admin

Prozedur

1. Navigieren zu **Alle > Industrial Workspace**.
2. Wählen Sie das Symbol Liste () aus.
3. Wählen Sie im Modul **Bibliotheken** die Liste **CVEs** aus.

Operational Technology Vulnerability Response-Referenz

Referenzthemen enthalten zusätzliche Informationen zur Anwendung Operational Technology Vulnerability Response.

Mit Operational Technology Vulnerability Response installierte Komponenten

Bei Aktivierung des Plugins Operational Technology Vulnerability Response (com.sn_otvr) werden verschiedene Arten von Komponenten installiert, einschließlich Anwenderrollen und einer Geschäftsregel.

** Hinweis:**

In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter [Komponenten finden, die mit dieser Anwendung installiert wurden](#) .

Für diese Funktion sind Demodaten verfügbar.

Installierte Rollen

Rollentitel [Name]	Beschreibung	Enthält Rollen
Besitzer der OT-Schwachstellenkorrektur [sn_otvr.remediation_owner]	Kann Korrekturaufgaben erstellen. Kann auch vorhandene Korrekturaufgaben für angreifbare Elemente planen.	• cmdb_ot_isa_viewer • cmdb_ot_viewer

Rollentitel [Name]	Beschreibung	Enthält Rollen
		• sn_vul.close_vi_vg • sn_vul.remediation_owner
OT VR Integration Viewer [sn_otvr.integration_viewer]	Kann Operational Technology Vulnerability Response Integrationsdatensätze anzeigen.	Keine
OT VR-Integrationsadministrator [sn_otvr.integration_admin]	Kann Integrationsdatensätze Operational Technology Vulnerability Response von anzeigen und bearbeiten.	• sn_sec_cmnm.admin • sn_otvr.integration_viewer • sn_vul.read_all

Geschäftsregeln installiert

Business Rule	Tabelle	Beschreibung
Ordnen Sie der Korrekturaufgabe OT-VITs zu	Korrekturaufgabe [sn_vul_vulnerability]	Wenn eine OT-Korrekturaufgabe erstellt wird, gruppiert die angreifbaren Elemente, die der Aufgabe zugeordnet sind, gemäß der Filterbedingung, die in der Konfiguration von „Aufgabe->Filtergruppierung“ angegeben ist.

Operational Technology Vulnerability Response Formularfelder für angreifbare Elemente

Liste der Felder, die in angreifbaren Elementen angezeigt werden, die für OT-Geräte erstellt wurden.

Felder für angreifbare Elemente

Feld	Beschreibung
Überblick	
Nummer	Automatisch generierte Nummer des angreifbaren Elements für diesen Datensatz.
Status	Dieses Feld ist standardmäßig auf Offen eingestellt . Sie können es jedoch in „ Wird untersucht “ ändern, wenn die Schwachstelle zur sofortigen Korrektur bereit ist.
Risikobewertung	Quantifizierte Risikopunktzahl , die angreifbare Elemente in „Kritisch“, „Hoch“, „Mittel“, „Niedrig“ und „Keine“ unterteilt. Weitere Informationen zu Risikoeinstufungen finden Sie unter Vulnerability Response calculators and vulnerability calculator rules  .

Feld	Beschreibung
	i Hinweis: Diese Basisrisikobewertung ist nicht mit der Risikobewertung des Lösungsdatensatzes identisch.
Risikopunktzahl	Berechnetes Risiko, das das angreifbare Element für Ihre Umgebung darstellt. i Hinweis: Diese Basis- Risikopunktzahl ist nicht identisch mit der Risikopunktzahl des Lösungsdatensatzes. Weitere Informationen finden Sie unter Vulnerability Response calculators and vulnerability calculator rules .
Schwachstelle	ID der Schwachstelle, die diesem angreifbaren Element zugeordnet ist.
Quelle	Scanner, der dieses angreifbare Element gefunden hat.
Konfigurationselement	ID des OT-Assets, das diesem angreifbaren Element zugeordnet ist.
Zuweisungsgruppe	Gruppe für die Bearbeitung dieser Korrekturaufgabe ausgewählt.
Zugewiesen an	Einzelperson aus der ausgewählten Zuweisungsgruppe, die an dieser Schwachstelle arbeitet.
Erstellt	Datum, an dem dieses angreifbare Element in Ihrer Instanz erstellt wurde.
Zuletzt geöffnet	Datum, an dem das angreifbare Element zuletzt in Ihrer Instanz geöffnet wurde. Anfangs entspricht dies dem Erstellungsdatum des angreifbaren Elements. Wenn es jedoch geschlossen wurde, enthält das Feld „Zuletzt geöffnet“ das Datum und die Uhrzeit der erneuten Öffnung.
Aktualisiert	Datum des letzten Scans.
Zusammenfassung	Beschreibung der Schwachstelle.
Schweregrad	Normalisierter Schweregrad dieser Schwachstelle Schweregradzuordnungen werden für NVD und mit ServiceNow -Drittparteiintegrationen bereitgestellt. Weitere Informationen zum Erstellen oder Anpassen von Schweregradzuordnungen finden Sie unter .Create a Vulnerability Response severity map  .
Schwachstellenpunktzahl (v3)	CVSS v3-Punktzahl.
Schwachstellenpunktzahl (v2)	CVSS v2-Punktzahl.

Feld	Beschreibung
Exploit vorhanden	Ja, wenn mindestens ein Exploit den Schwachstellen zugeordnet ist, die diesem angreifbaren Element zugeordnet sind.
Exploit-Angriffsvektor	Angreifbarster Angriffsvektor der Exploits für die Schwachstellen, die diesem angreifbaren Element zugeordnet sind.
Exploit-Kompetenzniveau	Niedrigste Kompetenzebene, die zum Ausnutzen der mit diesem angreifbaren Element verbundenen Schwachstellen erforderlich ist.
Veröffentlichungsdatum	Datum, an dem die Schwachstelle veröffentlicht wurde.
Zuletzt geändert	Datum, an dem die Schwachstelle zuletzt geändert wurde.
Bedrohung	Relevante Informationen zur Bedrohung. Aus dem angreifbaren Eintragsdatensatz abgerufen. i Hinweis: Alle hier vorgenommenen Änderungen aktualisieren den Datensatz des angreifbaren Eintrags.
Korrekturhinweise	Relevante Lösung für die Bedrohung, abgerufen aus dem Datensatz des angreifbaren Eintrags.
Zusätzliche Kommentare/Arbeitsnotizen	Alle relevanten Informationen. Aktivieren Sie das Kontrollkästchen, um Zusätzliche Kommentare hinzuzufügen. Ab Vulnerability Response v20.0 können Sie im Abschnitt „Notizen“ für ein zurückgestelltes angreifbares Element Arbeitsnotizen hinzufügen.
Aktivität	Wird nur angezeigt, wenn eine Arbeitsnotiz erstellt wurde.
Zugehörige Links	
Risikopunktzahl berechnen	Wenn entweder der Schwachstellenschweregrad-Rechner oder der Risikopunktzahl -Rechner aktiviert ist, wird das Feld „ Risikopunktzahl “ aktualisiert.

Zugehörige Informationen

Weitere Informationen zur Erweiterungsklasse des Netzwerkangriffserkennungssystems (Network Intrusion Detection System, NIDS), zu OT-Erweiterungsklassen und zu zugehörigen Anwendungen.

Übersicht über Erweiterungsklassen

Die Erweiterungsklassen helfen Ihnen zu verstehen, wie Operational Technology-Management mit Configuration Management Database (CMDB) funktioniert.

Network Intrusion Detection System (NIDS) CI extension class

Die Klasse des Netzwerkangriffserkennungssystems (Network Intrusion Detection System, NIDS) [cmdb_ci_nids] erstellt die Beziehungen zwischen passiven Netzwerküberwachungsgeräten und den Geräten im Netzwerk, die erkannt werden.

Operational Technology (OT) extension classes

Configuration Management Database (CMDB) aktualisiert Klassen für OT.

Zugehörige Anwendungen**Vulnerability Response**

Bei Integration mit Operational Technology Vulnerability Response unterstützt Sie die Anwendung ServiceNow Vulnerability Response bei der Priorisierung und Behebung von OT-Schwachstellen basierend auf der Prozessrelevanz.

CMDB CI Class Models

Die Store-App CMDB CI-Klassenmodelle fügt Klassenmodelle hinzu, die die Klassenhierarchie CMDB erweitern, einschließlich Klassenbeschreibungen, Identifizierungsregeln, Bezeichnereinträge und abhängige Beziehungen.

Prozessmanager Industrie

Verwenden Sie die Anwendung Prozessmanager Industrie, um die Datengrundlage für das Anlagenmodell nach ISA-95 zu erstellen, die für die Lösung ServiceNow Industriell erforderlich ist. Auf diese Weise können Sie an jedem Ihrer Industriestandorte eine eigene Version der Anlagenmodelle erstellen.

Operational Technology Manager

Mit der Anwendung Operational Technology Manager können Sie OT-Gerät-Daten aus mehreren Quellen zusammenfassen, um die grundlegenden Datenbeziehungen aufzubauen, die in der Lösung Industriell verwendet werden.

Incident-Management für operative Technologie

Incident-Management für operative Technologie Mit können Hersteller OT-Geräte-Incidents von der Eröffnung bis zur Schließung verwalten.



Automatische Übersetzung

Incident-Management für operative Technologie erkunden

Erfahren Sie mehr über die Anwendung Incident-Management für operative Technologie.

Incident-Management für operative Technologie – Übersicht

Sehen Sie sich die Übersicht über die -Produktsuite Operational Technology Service Management an, um mehr über die Anwendung Incident-Management für operative Technologie zu erfahren.

[https://player.vimeo.com/video/1019801515?](https://player.vimeo.com/video/1019801515?badge=0&autoplay=0&player_id=0&app_id=58479)

[badge=0&autoplay=0&player_id=0&app_id=58479](https://player.vimeo.com/video/1019801515?badge=0&autoplay=0&player_id=0&app_id=58479)

Schlüsselfunktionen

Mit Incident-Management für operative Technologie können Sie die folgenden wichtigen Funktionen verwenden.

- Erstellen Sie OT-Incidents, und steuern Sie Workflows, um Produktionsprozesse, die durch OT-Geräte betroffen sind, schnell wiederherzustellen.
- Kontext und Auswirkungen von OT-Incidents auf Produktionsprozesse verstehen.
- Überwachen und verwalten Sie OT-Incidents getrennt von IT-Incidents.
- Weisen Sie dem OT-Incident-Erfüller eine separate Rolle zu.
- Verbesserte OT-Anwender-Experience.
- Unterstützung für Knowledge Management für operative Technologie. Weitere Informationen finden Sie unter [Knowledge Management für operative Technologie](#).

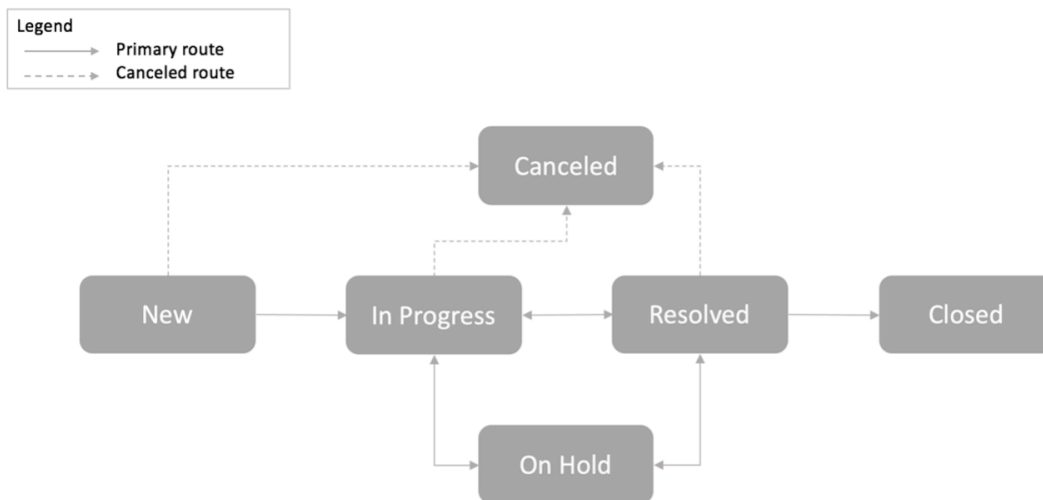
Incident-Management für operative Technologie

Incident-Management für operative Technologie ermöglicht es Ingenieuren, Probleme mit OT-Geräten (Operative Technology) und Produktionsprozessen schnell zu lösen.

Incident-Management für operative Technologie Mit können Sie OT-Incidents getrennt von IT-Incidents verwalten. OT-Incidents treten auf, wenn eine Serviceunterbrechung durch ein OT-Gerät in einem OT-Netzwerk auftritt. Manchmal ist das OT-Gerät möglicherweise nicht bekannt, wenn der Incident zum ersten Mal erstellt wird. Wenn das OT-Gerät unbekannt ist, kann ein Incident für eine Anlagenmodell-Entität ausgelöst werden, in der das Problem aufgetreten ist.

Der OT Incident-Manager ist für die Verwaltung des standardmäßigen Lebenszyklus von Incidents von der Erstellung bis zum Abschluss verantwortlich. Der OT Incident Management-Prozess hat viele Status, und jeder ist wichtig für den Erfolg des Prozesses und die Qualität des bereitgestellten Services. Die verschiedenen Status sind im folgenden Diagramm dargestellt.

Incident-Management für operative Technologie Prozessstatus



Die Incident-Status lauten wie folgt.

Status	Beschreibung
Neu	Incident wird protokolliert, wurde aber noch nicht untersucht.
In Bearbeitung	Der Incident wurde zugewiesen und wird untersucht.
Angehalten	Die Verantwortung für den Incident wird vorübergehend zu einer anderen Entität verschoben, um weitere Informationen, Nachweise oder eine Lösung bereitzustellen. Wenn Sie die Option Angehalten auswählen, wird die folgende Liste Grund für Warten angezeigt. Diese Listenooptionen geben an, woher Ihre zusätzlichen Informationen stammen. • Warten auf Anrufer • Warten auf Change • Warten auf Problem • Warten auf Lieferanten Wenn der Grund für Warten Auf Anrufer wartend ist, ist der Abschnitt Zusätzliche Kommentare erforderlich.

Status	Beschreibung
	 Hinweis: Wenn der Anrufer den Incident aktualisiert, wird das Feld Grund für Warten gelöscht und der Status des incident in In Bearbeitung geändert. Eine E-Mail-Benachrichtigung wird an den Benutzer, dessen Name im Feld Zugewiesen an aufgeführt ist, sowie an die Benutzer in der Beobachtungsliste gesendet. Sie können einen Incident mehrmals in den Wartestatus versetzen, bevor Sie ihn schließen.
Gelöst	Für den Incident wird eine akzeptable Korrektur bereitgestellt, um sicherzustellen, dass er nicht erneut auftritt.
Geschlossen	Der Incident wird als Geschlossen markiert, nachdem er sich für eine bestimmte Dauer im Status Gelöst befand und bestätigt wurde, dass der Incident zufriedenstellend gelöst wurde.
Abgebrochen	Der Incident wurde überprüft, aber es wurde festgestellt, dass es sich um einen doppelten Incident, einen unnötigen Incident oder überhaupt keinen Incident handelt.

Integration mit Prozessmanager Industrie

Integrieren Sie Incident-Management für operative Technologie mit Prozessmanager Industrie, um Incidents für Anlagenmodell-Entitäten zu melden.

Prozessmanager Industrie erstellt die Datengrundlage des Anlagenmodells nach ISA-95, die für die Lösung ServiceNow® Operational Technology erforderlich ist. Bei Integration mit Incident-Management für operative Technologie können Sie die Auswirkungen von Incidents auf Produktionsprozesse anzeigen.

Das mit Prozessmanager Industrie installierte Plugin „Anlagenmodell nach ISA“ (sn_isa_model) aktiviert Ansichten für angegebene Rollen. Weitere Informationen finden Sie unter [Anlagenmodell nach ISA-95](#).

Wenn ein OT-Incident aus einem OT-Gerät-Datensatz erstellt wird, geschieht Folgendes:

- Das Feld **OT-Gerät** im OT-Incident-Formular wird mit dem OT-Gerät-Wert gefüllt.
- Wenn dem OT-Gerät eine Anlagenmodell-Entität zugeordnet ist, wird die Anlagenmodell-Entität dem Feld **Anlagenmodell-Entität** im Formular „OT-Incident“ hinzugefügt.
- Das Feld **Standort** im Formular für OT-Incidents wird mit dem Standort des OT-Geräts gefüllt.

Wenn ein OT-Incident aus einem Anlagenmodell-Entitätsdatensatz erstellt wird, geschieht Folgendes:

- Das Feld **Anlagenmodell-Entität** im Formular „OT-Incident“ wird mit dem Wert der Anlagenmodell-Entität gefüllt.
- Das Feld **Standort** im Formular „OT Incident“ wird mit dem Standort der Anlagenmodell-Entität gefüllt.

Die zugehörige Liste „**OT Incident**“ im Datensatz der Anlagenmodell-Entität zeigt alle für diese Entität gemeldeten OT Incidents an. Das Feld **Anlagenmodell-Entität** im Formular kann nur Entitäten unter dem ausgewählten Standort enthalten.

Incident-Management für operative Technologie konfigurieren

Konfigurieren Sie die Anwendung Incident-Management für operative Technologie, um die Datengrundlage für die Lösung ServiceNow® Operational Technology zu erstellen.

Incident-Management für operative Technologie v2 ist abhängig von Tokyo P5 oder höher.

Hinweis: Wenn Sie über die Administratorrolle verfügen, können Sie das geführte Setup verwenden, um sich durch das Setup der Anwendung Incident-Management für operative Technologie führen zu lassen. Um auf das geführte Setup zuzugreifen, navigieren Sie zu **Industrial Workspace-Administrator > Geführtes Setup**.

Aufgabe	Zweck
1. Installieren Sie die Anwendung Incident-Management für operative Technologie aus dem ServiceNow Store.	Installiert die Anwendung Incident-Management für operative Technologie und unterstützende Plugins.
2. Weisen Sie Incident-Management für operative Technologie Rollen zu.	Weist Rollen zu, um die für jeden Benutzer verfügbaren Aktionen zu steuern.
3. Migrieren Sie OT-Incidents.	Migriert OT-Incidents aus der Incident-Tabelle in die OT-Incident-Tabelle. Hinweis: Dieser Schritt gilt nur beim Upgrade von Paris, San Diego oder Tokyo auf Utah.
4. Konfigurieren Sie Kategorien und Unterkategorien für OT-Incidents.	Konfiguriert Kategorien und Unterkategorien für OT-Incidents nach Bedarf.
5. Konfigurieren Sie Statusmodelle.	Konfiguriert Statusmodelle für OT-Incident-Sites.
6. (Optional) Erstellen Sie eine Zuweisungsregel.	Erstellen Sie eine Zuweisungsregel, um einen OT-Incident automatisch der richtigen Gruppe oder dem richtigen Benutzer zuzuweisen.

Incident-Management für operative Technologie installieren

Mit der Administratorrolle können Sie die Anwendung Incident-Management für operative Technologie (sn_ot_inc_mgmt) installieren. Die Anwendung installiert die zugehörigen ServiceNow® Store-Anwendungen und Plugins, falls sie nicht bereits installiert sind.

Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter [Rufen Sie eine Berechtigung für ab ServiceNow Produkt oder Anwendung](#) .

Automatische Übersetzung

- Incident-Management für operative Technologie erfordert die folgenden Plugins. Stellen Sie sicher, dass diese Plugins aktiviert sind, bevor Sie Incident-Management für operative Technologie installieren.

Benötigte ServiceNow-Plugins

CMDB CI-Klassenmodelle (sn_cmdb_ci_class)

Die Store-App CMDB-CI-Klassenmodelle fügt Klassenmodelle hinzu, die die CMDB-Klassenhierarchie erweitern, einschließlich Klassenbeschreibungen, Identifizierungsregeln, Bezeichnereinträge und abhängige Beziehungen. Weitere Informationen finden Sie unter [Store App CMDB-CI-Klassenmodelle](#).

Anlagenmodell nach ISA (sn_isa_model)

Das Datenmodell für Entitäten und Vorlagen des Anlagenmodells nach ISA-95. Weitere Informationen finden Sie unter [Anlagenmodell nach ISA-95](#).

- Incident-Management für operative Technologie erfordert eine oder beide der folgenden ServiceNow Store -Anwendungen. Stellen Sie sicher, dass mindestens eine dieser Anwendungen installiert ist, bevor Sie Incident-Management für operative Technologie installieren.

Erforderliche ServiceNow Store-Anwendungen

Operational Technology Manager

Die Anwendung Operational Technology Manager erstellt die grundlegenden Daten und Beziehungen, die es Ihrem Unternehmen ermöglichen, die Lösung ServiceNow® Operational Technology zu verwenden. Operational Technology Manager unterstützt die Verwendung der Anwendungen Configuration Management Database (CMDB), Service Graph Connectors und Discovery in Now Platform. Weitere Informationen hierzu finden Sie unter [Operational Technology Manager konfigurieren](#).

Prozessmanager Industrie

Die Anwendung Prozessmanager Industrie erstellt die Datengrundlage für das Anlagenmodell nach ISA-95, die für die Lösung ServiceNow® Industriell erforderlich ist. Damit können Sie an jedem Ihrer Industriestandorte eine eigene Version der Anlagenmodelle erstellen. Weitere Informationen finden Sie unter [Prozessmanager Industrie konfigurieren](#).

- Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Die folgenden Elemente werden mit Incident-Management für operative Technologie installiert:

- Plugins
- Store-Anwendungen
- Rollen und ACLs

Weitere Informationen zu den installierten Rollen und ACLs finden Sie unter [Mit Incident-Management für operative Technologie installierte Komponenten](#).

Hinweis:

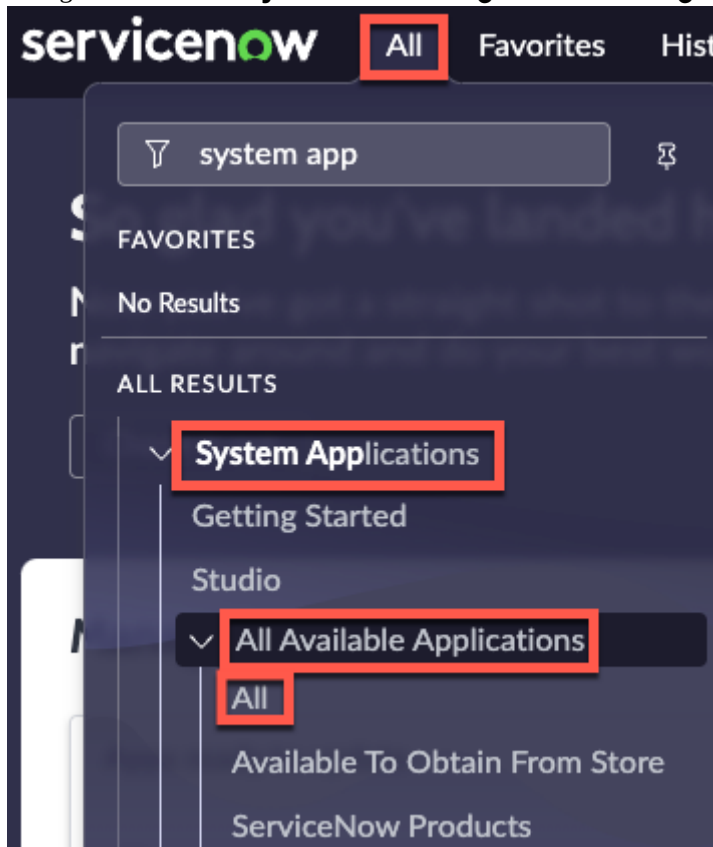
Beachten Sie für Operational Technology Service Management -Benutzer ohne Lizenz für Operational Technology -Transparenz Folgendes:

- Wenn Sie die neueste Version von Incident-Management für operative Technologie installiert haben, wird auch Prozessmanager Industrie installiert.
- Wenn Sie die neueste Version von Change-Management für operative Technologie installiert haben, wird auch Prozessmanager Industrie installiert.

Sie sollten ein Upgrade auf die neuesten Versionen durchführen, um Zugriff auf die Experience Operational Technology Service Management zu erhalten.

Prozedur

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



2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach der Anwendung Incident-Management für operative Technologie (sn_ot_inc_mgmt).

Sie können nach der Anwendung anhand ihres Namens oder ihrer ID suchen. Wenn Sie die 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. Überprüfen Sie im Dialogfeld „Anwendungsinstallation“ die Anwendungsabhängigkeiten.

Abhängige Plugins und Anwendungen werden aufgelistet, wenn sie installiert werden sollen, derzeit installiert sind oder installiert werden müssen. Wenn die Installation von

Plugins oder Anwendungen erforderlich ist, müssen Sie sie installieren, bevor Sie Incident-Management für operative Technologie installieren können.

4. Wählen Sie **Installieren** aus.

Migrieren Sie Incidents in die neue Incident-Tabelle

Migrieren Sie Incidents Operational Technology aus der alten Incident-Tabelle in die neue Incident-Tabelle. Durch die Migration von Incidents wird der Anwendung Incident-Management für operative Technologie mitgeteilt, dass die alte Tabelle nicht mehr anwendbar ist.

Vorbereitungen

- Legen Sie den Anwendungsbereich auf **Incident-Management für operative Technologie** fest.
- Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Industrial Workspace-Administrator** > **Geführtes Setup**.
2. Wählen Sie in der Kategorie Incident-Management für operative Technologie **Erste Schritte** aus.
3. Wählen Sie neben dem Abschnitt OT Incidents migrieren die **Option Konfigurieren** aus.
4. Starten Sie die Migration, indem Sie **Jetzt ausführen** wählen.
5. **Wahlweise:** Um das Aktivitätsprotokoll für diese geplante Aufgabe anzuzeigen, navigieren Sie zu **Alle** > **Systemprotokolle** > **Systemprotokoll** > **Alle**.

Ergebnisse

Die Incidents Operational Technology werden in die neue Incident-Tabelle migriert, und die Anwendung Incident-Management für operative Technologie verwendet die alte Tabelle nicht mehr.

Weisen Sie Ihren Anwendern Rollen zu

Weisen Sie Ihren Benutzern in der Anwendung Incident-Management für operative Technologie Rollen zu, um ihren Zugriff auf die Funktionen, Fähigkeiten und Daten von zu steuern.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Benutzer mit den in der folgenden Tabelle aufgeführten Rollen können die Anwendung Incident-Management für operative Technologie verwenden.

Hinweis:

Die Rolle „OT-Incident-Anwender“ [ot_incident_user] ist veraltet. Für Anwender, denen diese Rolle zugewiesen ist, können Sie die geplante Aufgabe „Neue OT-Incident-Rollen zuweisen“ ausführen, um ihnen neue Incident-Management für operative Technologie Rollen zuzuweisen. Weitere Informationen finden Sie unter [Weisen Sie Ihren Anwendern neue Rollen zu](#).

Rolle	Beschreibung
OT-Incident-Administrator [sn_ot_incident_admin]	Kann OT Incident-Datensätze für alle Anlagenmodell-Entitäten erstellen, anzeigen, löschen und bearbeiten. Benutzer mit dieser Rolle können die Systemeigenschaften für Regeln für die

Rolle	Beschreibung
	Prioritätssuche und Systemeigenschaften für OT-Incidents konfigurieren.
OT Incident Reader sn_ot_incident_read	OT-Incident-Datensätze können nur angezeigt werden.
Erfüller für OT-Incident sn_ot_incident_write	Kann OT-Incident-Datensätze erstellen, anzeigen und bearbeiten.

Prozedur

Weisen Sie Benutzern oder Gruppen mit der Benutzerverwaltungsfunktion Now Platform Rollen zu.

Weisen Sie Ihren Anwendern neue Rollen zu

Weisen Sie Anwendern, die die Rolle „OT Incident-Benutzer“ [ot_incident_user] innehatten, über eine geplante Aufgabe in der Anwendung Incident-Management für operative Technologie neue Rollen zu.

Vorbereitungen

- Legen Sie den Anwendungsbereich auf **Incident-Management für operative Technologiefest**.
- Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die Rolle „OT Incident-Anwender“ [ot_incident_user] ist veraltet. Sie können Benutzern, die zuvor die Rolle ot_incident_user innehatten, über eine geplante Skriptausführung neue Rollen zuweisen.

Prozedur

1. Navigieren zu **Alle > Systemdefinition > Geplante Aufgaben**.
2. Suchen Sie in der Suchleiste nach der geplanten Aufgabe **Neue OT-Incident-Rollen zuweisen**.
3. Starten Sie eine regelmäßige Aufgabe, indem Sie **Jetzt ausführen** wählen.
4. **Wahlweise:** Um das Aktivitätsprotokoll für diese geplante Aufgabe anzuzeigen, navigieren Sie zu **Alle > Systemprotokolle > Systemprotokoll > Alle**.

Ergebnisse

Die geplante Aufgabe wird ausgeführt, und Anwendern werden jetzt die neuen Incident-Management für operative Technologie -Rollen zugewiesen.

Zuweisungsgruppen erstellen

Erstellen Sie eine Operational Technology (OT)-spezifische Zuweisungsgruppe, um sie OT-Incident-Datensätzen zuzuweisen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Das Feld **Zuweisungsgruppe** in einem OT-Incident-Datensatz zeigt nur Zuweisungsgruppen vom Typ OT an. Dies hilft bei der Trennung von Operational Technology (OT) und Informationstechnologie-Incidents (IT).

Sie können OT-spezifische Zuweisungsgruppen erstellen, die in einem OT-Incident-Datensatz sichtbar sein sollen.

Prozedur

1. Navigieren zu **Alle > Anwenderadministration > Gruppen**.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular „Zuweisungsgruppen“.

Feld	Beschreibung
Name	Name der Zuweisungsgruppe.
Manager	Gruppenmanager oder Lead
Typ	Kategorie für diese Gruppe. Suchen Sie im Feld Zieldatensatz auswählen nach OT , um ihn dem Typfeld hinzuzufügen.
Gruppen-E-Mail	Gruppen-E-Mail-Verteilerliste oder E-Mail-Adresse des Kontaktpunkts.
Übergeordnet	Andere Gruppe, der die Gruppe angehört.
Beschreibung	Beschreibung der Zuweisungsgruppe.

4. Wählen Sie **Absenden**.

Ergebnisse

Jetzt ist die OT-spezifische Zuweisungsgruppe im Incident-Datensatz sichtbar.

Incident-Kategorien und Unterkategorien

Durch die Kategorisierung von Operational Technology (OT) Incidents können Sie die Suche nach bestimmten OT-Incidents gruppieren und eingrenzen.

Wenn Sie einen OT-Incident erstellen können, können Sie aus den Kategorien und Unterkategorien auswählen, die in der folgenden Tabelle aufgeführt sind.

Incident-Kategorien

Kategorie	Unterkategorie
Datenbank	• DB2 • MS SQL-Server • Oracle

Incident-Kategorien (Fortsetzung)

Kategorie	Unterkategorie
Hardware	• OT-Problem • CPU • Datenträger • Tastatur • Arbeitsspeicher • Überwachen • Maus
Anforderung/Hilfe	• Virenschutz • E-Mail • Interne Anwendung
Netzwerk	• DHCP • DNS • IP-Adresse • VPN • Drahtlos
Produktivität	• Kleinere Stopps • Langsame Ausführung • Setup und Anpassungen • Aufgliederung
Qualität	• Eingehendes Material • Startablehnungen • Prozessfehler – Qualitativ • Prozessfehler – Quantitativ
Sicherheit	• Knapp daneben • Gefahr • Sicherheitsbedenken • Unfall

Incident-Kategorien (Fortsetzung)

Kategorie	Unterkategorie
Software	• E-Mail • Betriebssystem

Bearbeiten Sie eine Kategorie oder Unterkategorie

Bearbeiten Sie Ihre vorhandenen Operational Technology Incident-Kategorien und Unterkategorien, um Ihre Incidents zu klassifizieren.

Vorbereitungen

- Legen Sie den Anwendungsbereich auf **Incident-Management für operative Technologiefest**.
- Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle > Systemdefinition > Auswahllisten**.
2. Legen Sie die Bedingungsfilter auf **[Tabelle] [ist] [sn_ot_incident]** und **[Element] [ist] [Kategorie]** oder **[Element] [ist] [Unterkategorie]** fest.
3. Wählen Sie den Kategorie- oder Unterkategorie-Datensatz aus.
4. Bearbeiten Sie das Formular entsprechend Ihren Anforderungen.
5. Wählen Sie **Speichern**.

Ergebnisse

Jetzt werden die Änderungen an der vorhandenen Kategorie oder Unterkategorie im Datensatz angezeigt.

Erstellen Sie eine Kategorie oder Unterkategorie

Erstellen Sie eine Incident-Kategorie oder Unterkategorie Operational Technology, die Sie zum Klassifizieren von Incidents verwenden möchten.

Vorbereitungen

- Legen Sie den Anwendungsbereich auf **Incident-Management für operative Technologiefest**.
- Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle > Systemdefinition > Auswahllisten**.
2. Um eine Kategorie zu erstellen, gehen Sie wie folgt vor:
 - a. Wählen Sie **Neu**.
 - b. Geben Sie im Feld **Element** das Wort Kategorie ein.
 - c. Geben Sie im Feld **Bezeichnung** den Kategorienamen ein.
 - d. Geben Sie im Feld **Wert** den Kategoriewert ein.

- e. Geben Sie im Feld **Sequenz** die Sequenznummer ein.
 - f. Wählen Sie **Absenden**.
3. Um eine neue Unterkategorie hinzuzufügen, gehen Sie wie folgt vor:
- a. Wählen Sie **Neu**.
 - b. Geben Sie im Feld **Element** das Wort Unterkategorie ein.
 - c. Geben Sie im Feld **Bezeichnung** den Namen der Unterkategorie ein.
 - d. Geben Sie im Feld **Wert** den Wert der Unterkategorie ein.
 - e. Geben Sie im Feld **Sequenz** die Sequenznummer ein.
 - f. Wählen Sie **Absenden**.

Ergebnisse

Die neue Kategorie oder Unterkategorie kann in einem Incident-Datensatz Operational Technology ausgewählt werden.

Löschen Sie eine Kategorie oder Unterkategorie

Löschen Sie eine Incident-Kategorie oder Unterkategorie Operational Technology, wenn Ihre Organisation diese Kategorie oder Unterkategorie nicht mehr verwendet.

Vorbereitungen

- Legen Sie den Anwendungsbereich auf **Incident-Management für operative Technologiefest**.
- Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle > Systemdefinition > Auswahllisten**.
2. Legen Sie die Bedingungsfilter auf **[Tabelle] [ist] [sn_ot_incident]** und **[Element] [ist] [Kategorie]** oder **[Element] [ist] [Unterkategorie]** fest.
3. Zeigen Sie auf den Datensatz der Kategorie oder Unterkategorie, den Sie löschen möchten, und aktivieren Sie das Kontrollkästchen.
4. Wählen Sie im Menü Aktionen für ausgewählte Zeilen **die Option Löschen aus**.

Ergebnisse

Die gelöschte Kategorie oder Unterkategorie ist für einen Incident-Datensatz Operational Technology nicht mehr verfügbar.

Erstellen Sie ein Incident-Statusmodell

Erstellen Sie ein Incident-Statusmodell Operational Technology (OT) für Ihre Sites. Durch die Verwendung eines Incident-Statusmodells können Sie den Lebenszyklus der zugehörigen Incidents verwalten.

Vorbereitungen

- Legen Sie den Anwendungsbereich auf **Incident-Management für operative Technologiefest**.
- Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Mit der Statusverwaltung können Sie ein Statusmodell für OT-Incident-Sites und ihre Incident-Lebenszyklen konfigurieren. Sie können ein Modell pro Site erstellen.

Weitere Informationen zu Statusmanagement und Statusmodellen finden Sie unter [Statusmanagement](#) .

Weitere Informationen zu Incident-Lebenszyklen finden Sie unter [Incident-Management für operative Technologie](#).

Prozedur

1. Navigieren zu **Alle > Statusmanagement > Statusmodelle**.
2. Wählen Sie das Modell **OT Incident: Standard-Flow** aus.
3. Legen Sie die **Bedingung fest**.
4. Konfigurieren Sie im Kontextmenü „Statusübergänge“ die Datensätze für den Statusübergang nach Bedarf. Wenn Sie beispielsweise das Feld **Eingabebedingung** des Statusdatensatzes **In Bearbeitung** bearbeiten möchten, wählen Sie den Statusdatensatz aus, fügen Sie Ihre Änderungen hinzu, und wählen Sie **Aktualisieren** aus.
5. Wählen Sie **Aktualisieren**.

Ergebnisse

Jetzt beschreibt das Statusmodell den erwarteten Datensatz-Workflow während des Lebenszyklus des Incident-Datensatzes genau.

Definieren Sie eine Suchregel mit Priorität für Incidents

Definieren Sie die Auswirkung und Dringlichkeit eines Incident Operational Technology, um seine Priorität zu berechnen. Anschließend können Sie die Prioritätsberechnung verwenden, um Ihre Arbeit zu priorisieren und Servicelevel-Vereinbarungen (SLAs) in Ihrer Organisation zu erfüllen.

Vorbereitungen

Erforderliche Rolle: ot_incident_admin

Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > Incident-Management für operative Technologie > Regeln für Suchvorgänge mit Priorität**.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular für Suchregel mit Priorität

Feld	Beschreibung
Auswirkung	Messwert für den Effekt, den ein Incident auf Geschäftsprozesse hat.
Dringlichkeit	Messen Sie, wie lange die Lösung hinausgezögert werden kann, bis ein Incident erhebliche geschäftliche Auswirkungen hat.
Priorität	Option, die auf der Auswirkung und der Dringlichkeit basiert. Die Priorität gibt an, wie

Feld	Beschreibung
	schnell der OT-Ingenieur die Aufgabe angehen sollte.
Anwendung	Umfang der Regeln. Der Anwendungsbereich legt fest, ob die Regeln für alle Anwendungen oder für bereichsbezogene Anwendungen verfügbar sind.
Aktiv	Über diese Option lässt sich festlegen, ob die Regel aktiv ist oder nicht.
Reihenfolge	Die Reihenfolge, in der die Regeln in der Nachschlageliste für Prioritäten angezeigt werden. Dieses Feld gibt an, welche Regel zuerst ausgeführt werden soll.

Hinweis:

Die Priorität wird gemäß den Beispielregeln für die Datensuche in der folgenden Tabelle berechnet.

Regeln für Datensuche mit Priorität

Auswirkung	Dringlichkeit	Priorität
1 – Hoch	1 – Hoch	1 - Kritisch
1 – Hoch	2 – Mittel	2 – Hoch
1 – Hoch	3 – Niedrig	3 – Mittel
2 – Mittel	1 – Hoch	2 – Hoch
2 – Mittel	2 – Mittel	3 – Mittel
2 – Mittel	3 – Niedrig	4 – Niedrig
3 – Niedrig	1 – Hoch	3 – Mittel
3 – Niedrig	2 – Mittel	4 – Niedrig
3 – Niedrig	3 – Niedrig	5 - In Planung

Standardmäßig ist das Feld **Priorität** schreibgeschützt und muss durch Auswahl der Werte für **Auswirkung** und **Dringlichkeit** festgelegt werden. Um zu ändern, wie die Priorität berechnet wird, können Sie entweder die Prioritätssuchregeln ändern oder die UI-Richtlinie **Priorität wird durch Datensuche verwaltet – als schreibgeschützt festgelegt** deaktivieren und ihre eigene Geschäftslogik erstellen.

4. Wählen Sie **Absenden**.

Legen Sie die Systemeigenschaften fest

Legen Sie die Systemeigenschaften für die Anwendung Incident-Management für operative Technologie fest, um die Incident-Eigenschaften nach Bedarf aktivieren zu können.

Vorbereitungen

- Legen Sie den Anwendungsbereich auf **Operational Technology Incident Management** fest, indem Sie in der Navigationsleiste das Globussymbol () wählen.
- Erforderliche Rolle: sn_ot_incident_admin

Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > Incident-Management für operative Technologie > Systemeigenschaften**.
2. Aktivieren Sie je nach Bedarf die folgenden Eigenschaften für Ihre Organisation.
3. Wählen Sie **Speichern** aus, um die Änderungen zu speichern.

Erstellen Sie eine Zuweisungsregel

Erstellen Sie eine Zuweisungsregel, um einen Operational Technology (OT)-Incident automatisch einer Gruppe oder einem Benutzer gemäß einer oder mehreren Bedingungen in der Zuweisungsregel zuzuweisen. Sie verwenden Zuweisungsregeln, die beim Öffnen eines OT-Incident ausgeführt werden.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle > Systemrichtlinie > Regeln > Zuweisung**.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars aus.
Eine Beschreibung der Feldwerte finden Sie unter [Formular „Zuweisungsregel“](#)..
4. Wählen Sie **Absenden**.

Nächste Maßnahme

Weitere Informationen zu Zuweisungsregeln finden Sie unter [Defining assignment rules](#) .

Incident-Management für operative Technologie verwenden

Nachdem Sie alle erforderlichen Einrichtungsaufgaben für die Anwendung Incident-Management für operative Technologie abgeschlossen haben, können Sie mit der Verwaltung von OT-Incidents beginnen.

OT-Incidents verwalten

Abhängig von der Ihnen zugewiesenen Anwenderrolle können Sie OT-Incidents in Industriell Arbeitsbereichsverwalten.

In Industriell Arbeitsbereich kann der OT-Incident-Autor ein OT-Incident-Formular an folgenden Stellen erstellen und aktualisieren:

- Ein OT-Gerät-Formular
- Ein Anlagenmodell-Entitätenformular
- Listenmodul

In Industriell Arbeitsbereich kann der OT-Incident-Betrachter OT-Incidents an folgenden Stellen anzeigen:

- Die zugehörige Liste „OT Incidents“ unter der Registerkarte **Zugehörige Datensätze** in einem OT-Gerät-Datensatz
- Die Registerkarte **„OT Incidents“** in einem Anlagenmodell-Entitätsdatensatz

- Die folgenden Listen unter dem Listenmodul **OT Incidents** :
 - Mir zugewiesen
 - Gehört zu meinen Standorten
 - Alle

Der OT Incident-Administrator kann zu jedem OT Incident-Datensatz in Industriell Arbeitsbereich wechseln und ihn löschen.

Zugriffssteuerung für Incidents

Um die Trennung von Operational Technology (OT) und Informationstechnologiedaten (IT) zu erleichtern, können nur OT-Benutzer OT-Incidents anzeigen.

In der folgenden Tabelle werden die Rollen und Berechtigungen für die Benutzer beschrieben, die über die Rollen Incident-Management für operative Technologie verfügen.

Rolle	Berechtigungen
sn_ot_incident_write	Kann OT-Incidents erstellen, bearbeiten und lesen.
sn_ot_incident_read	Kann nur OT-Incidents lesen.
sn_ot_incident_admin	Kann Incident-Datensätze für jede Anlagenmodell-Entität erstellen, anzeigen, bearbeiten und löschen.

Weitere Informationen zu Zugriffssteuerungsregeln finden Sie unter [Zugriffssteuerungsregeln in Anwendungsverwaltungs-Apps](#) .

Incident melden

Erstellen Sie einen Incident-Datensatz Operational Technology (OT), um eine Abweichung von einem erwarteten Betriebsstandard zu melden.

Vorbereitungen

Erforderliche Rolle: sn_ot_incident_write

Prozedur

1. Navigieren zu **Alle > Industrial Workspace**.
2. Wählen Sie einen Gerätedatensatz oder einen Anlagenmodell-Entitätsdatensatz aus.

Hinweis:

Sie können einen OT-Incident auch im Listenmodul OT-Incidents auslösen.

3. Wählen Sie die Registerkarte **OT Incidents**.
4. Wählen Sie **Neu**.
5. Füllen Sie die Felder des Formulars aus.

Wenn Sie einen Gerätedatensatz ausgewählt haben, werden die Felder Standort und OT-Gerät automatisch ausgefüllt. Wenn Sie einen Anlagenmodell-Entitätsdatensatz ausgewählt haben, werden die Felder Standort und Anlagenmodell-Entität automatisch ausgefüllt. Wenn der OT Incident über das Listenmodul OT Incidents ausgelöst wird, wird keines dieser Felder automatisch ausgefüllt.

i Hinweis:

Ihre Organisation hat das Incident-Formular und die zugehörigen Felder entsprechend dem Incident-Management-Prozess konfiguriert. In der folgenden Tabelle werden die typischen Formularfelder für OT-Incidents beschrieben.

Operational Technology Formular „Incident“.

Feld	Beschreibung
Kurzbeschreibung	Eine kurze Beschreibung des Incident.
Beschreibung	Detaillierte Erklärung zu dem Incident.
Nummer	Eindeutige, vom System generierte Incident-Nummer mit vorangestelltem Operational Technology Incident (OTINC).
Anrufer	Benutzer, der den OT-Ingenieur mit einem Problem kontaktiert hat.
Auswirkung	Messwert für den Effekt, den ein Incident auf industrielle Prozesse hat.
Dringlichkeit	Maß dafür, wie lange die Lösung hinausgezögert werden kann, bis ein Incident erhebliche geschäftliche Auswirkungen hat.
Status	Status des OT-Incidents. Der Status ändert sich und verfolgt Incidents durch mehrere Lösungsphasen.
Kategorie	Die Art des Problems. Nachdem Sie die Kategorie ausgewählt haben, wählen Sie ggf. die Unterkategorie aus.
Unterkategorie	Typ des Problems in der ausgewählten Kategorie.
Beobachtungsliste	Benutzer, die Benachrichtigungen zu diesem Incident erhalten, wenn Anmerkungen hinzugefügt werden.
Arbeitsnotizenliste	Benutzer, die Benachrichtigungen zu diesem Incident erhalten, wenn Arbeitsnotizen hinzugefügt werden.
Site	Standort, an dem das Problem aufgetreten ist.
OT-Gerät	Betroffenes OT-Gerät an der Site.
Anlagenmodell-Entität	Betroffenes Anlagenmodell – Anlagenmodell-Entität am Standort.
Geschäftsauswirkung	Weitere Informationen zu den geschäftlichen Auswirkungen des OT-Incidents.
Zuweisungsgruppe	Zugewiesene Gruppe, die den Incident bearbeitet. Die Zuweisungsgruppe kann eine beliebige Gruppe mit dem Typ OT sein.
Zugewiesen an	Benutzer, der an diesem Incident arbeitet. Wenn sich die Zuweisungsgruppe ändert, wird das Feld Zugewiesen an gelöscht.

Feld	Beschreibung
	Sie können nur Benutzer auswählen, die im Feld Zuweisungsgruppe enthalten sind und über die Rolle sn_ot_incident_write verfügen. Wenn das Feld Zuweisungsgruppe leer ist, kann jeder Site-Benutzer mit der Rolle sn_ot_incident_write ausgewählt werden.
Übergeordneter Incident	Eindeutige Nummer des übergeordneten Incident für diesen Incident-Datensatz
Zusätzliche Anmerkungen	Weitere Informationen zum Problem nach Bedarf. Alle Benutzer, die Incidents anzeigen können, können die zusätzlichen Kommentare sehen.
Arbeitsnotizen	Informationen darüber, wie der Incident behoben werden kann oder welche Schritte zur Lösung unternommen wurden, falls zutreffend.

6. Wählen Sie **Speichern**.

Ergebnisse

Jetzt wissen die Zuweisungsgruppe und der Beauftragte, dass ein OT-Incident behandelt werden muss.

Erstellen Sie einen Operational Technology -Incident aus einer Operational Technology -Change-Anforderung

Erstellen Sie einen Incident Operational Technology (OT), der sich auf eine OT-Change-Anforderung bezieht, direkt aus dem OT-Change-Datensatz in Industrial Workspace.

Vorbereitungen

Erforderliche Rolle: sn_ot_change_write und sn_ot_incident_write

Warum und wann dieser Vorgang ausgeführt wird

Die folgenden zugehörigen Listen sind in einem OT-Change-Datensatz in Industrial Workspace verfügbar, sodass Sie einen OT-Incident erstellen oder einen vorhandenen OT-Incident im Zusammenhang mit der Change-Anforderung hinzufügen können.

Durch den Change behobene Incidents

OT-Incidents, die vom ausgewählten Change-Datensatz behoben werden.

Durch den Change verursachte Incidents

OT-Incidents, die durch den ausgewählten Change-Datensatz verursacht werden.

Prozedur

1. Navigieren zu **Alle > Industrial Workspace**.
2. Öffnen Sie die Listenansicht Industrial Workspace.
3. Wählen Sie im Listenmodul OT Change-Anforderungen eine der verfügbaren Listen aus.
4. Wählen Sie in einem Ihrer Sites den Change-Datensatz aus, aus dem Sie einen Incident erstellen möchten.
5. Führen Sie die folgenden Aktionen aus, um einen OT-Incident zu erstellen.

- a. Wählen Sie in der zugehörigen Liste „Durch Change behobene Incidents“ oder in der zugehörigen Liste „Durch Change verursachte Incidents“ **Neu**.
- b. Füllen Sie die folgenden Felder des Formulars aus.

Formular für OT-Incidents

Feld	Beschreibung
Nummer	Eindeutige, vom System generierte Incident-Nummer mit vorangestelltem Operational Technology Incident (OTINC).
Geöffnet	Das Datum, an dem der Incident übermittelt wird.
Kurzbeschreibung	Eine kurze Beschreibung des Incident.
Site	Standort, an dem das Problem aufgetreten ist.
Anlagenmodell-Entität	Betroffenes Anlagenmodell – Anlagenmodell-Entität am Standort.
OT-Gerät	Betroffenes OT-Gerät an der Site.

- c. Wählen Sie **Speichern**.
6. Führen Sie die folgenden Aktionen aus, um dem Change-Anforderungsdatensatz einen vorhandenen OT-Incident hinzuzufügen.

Hinweis:

Ein OT-Incident kann höchstens durch eine OT-Change-Anforderung behoben und durch höchstens eine OT-Change-Anforderung verursacht werden. Sie können einen OT-Incident hinzufügen, der bereits einer anderen OT-Change-Anforderung zugeordnet ist. Dadurch wird jedoch die vorhandene Beziehung überschrieben.

- a. Wählen Sie in der zugehörigen Liste „Durch Change behobene Incidents“ oder in der zugehörigen Liste „Durch Change verursachte Incidents“ die Option **Hinzufügen aus**.
- b. Wählen Sie den OT-Incident aus, den Sie hinzufügen möchten.
- c. Wählen Sie **Hinzufügen**.

Ergebnisse

Nachdem Sie den Incident aus der Change-Anforderung erstellt haben, können Sie den Incident-Datensatz in der zugehörigen Liste anzeigen oder indem Sie zurück zur Listenansicht Industrial Workspace navigieren. Wählen Sie dann eine der verfügbaren Listen im Listenmodul **OT Incidents** aus.

Erstellen Sie Aufgaben, um einen Incident zu erfüllen

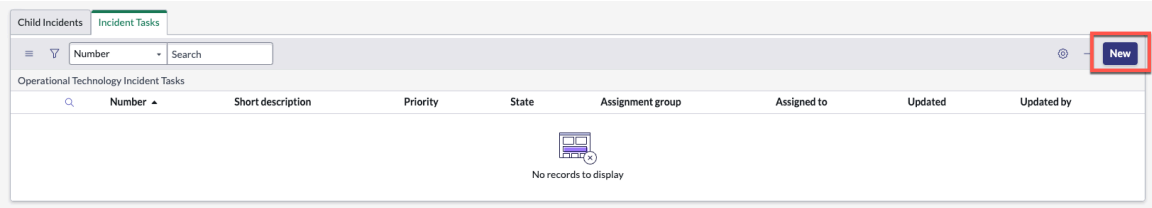
Erstellen Sie einen Satz von Incident-Aufgaben, um einen Operational Technology (OT)-Incident zu erfüllen. Incident-Aufgaben helfen Ihnen, die zur Lösung eines Incident erforderliche Arbeit aufzuteilen und zu kategorisieren.

Vorbereitungen

Erforderliche Rolle: sn_ot_incident_write

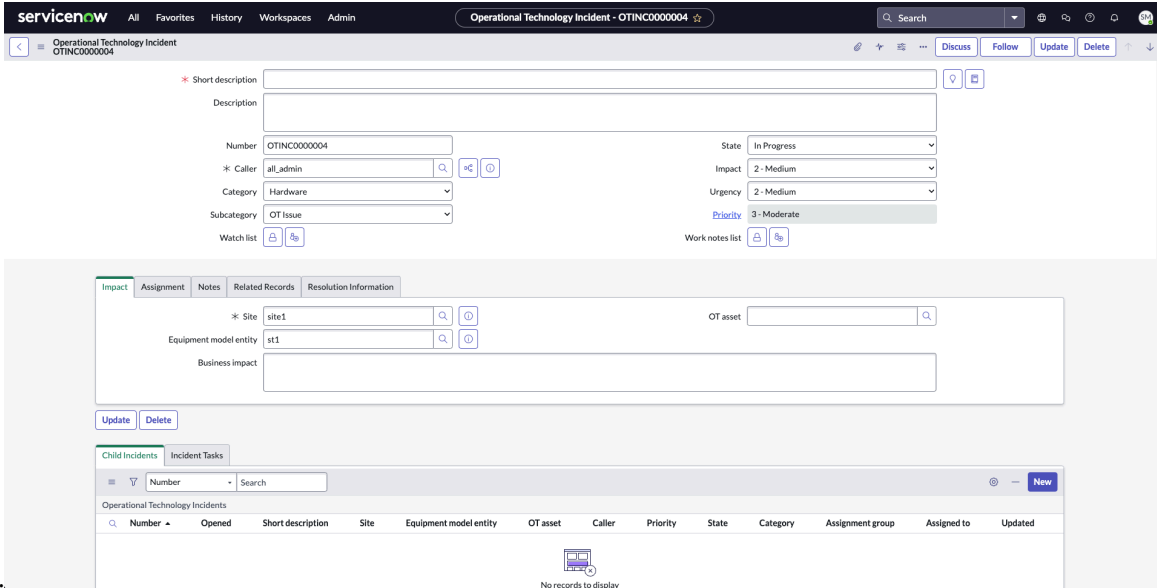
Prozedur

- 1. Navigieren zu **Alle > Incident > Offen**.
- 2. Öffnen Sie den OT-Incident-Datensatz, für den Sie eine Aufgabe erstellen möchten.
- 3. Wählen Sie in der zugehörigen Liste „Incident-Aufgaben“



Neu.
Wenn die zugehörige Liste Incident-Aufgaben nicht angezeigt wird, müssen Sie sie hinzufügen.

- 4. Füllen Sie die Felder des Formulars



aus.

Formular „Incident-Aufgabe“.

Feld	Beschreibung
Nummer	Eindeutige, für die Incident-Aufgabe vom System generierte Nummer.
Incident	Incident, mit dem die Aufgabe verknüpft ist.
Site	Betroffener Incident-Standort. Hinweis: Dieses Feld ist schreibgeschützt und wird ggf. automatisch mit dem zugehörigen Incident-Standort gefüllt.
Anlagenmodell-Entität	Betroffene Anlagenmodell-Entität. Hinweis: Dieses Feld ist schreibgeschützt und wird automatisch mit der zugehörigen Anlagenmodell-Entität gefüllt, falls zutreffend.

Automatische Übersetzung

Feld	Beschreibung
OT-Gerät	Betroffenes OT-Gerät. i Hinweis: Dieses Feld ist schreibgeschützt und wird ggf. automatisch mit dem zugehörigen OT-Gerät ausgefüllt.
Status	Status für die Nachverfolgung einer Incident-Aufgabe durch mehrere Phasen der Lösung des incident.
Priorität	Priorität der Incident-Aufgabe.
Zuweisungsgruppe	Gruppe, die an der Incident-Aufgabe arbeitet. Wenn Sie dieses Feld leer lassen, wird der Incident automatisch zugewiesen.
Zugewiesen an	Benutzer, dem die Incident-Aufgabe zugewiesen wurde. i Hinweis: Wenn sich die Zuweisungsgruppe ändert, wird das Feld Zugewiesen an gelöscht.
Kurzbeschreibung	Kurze Beschreibung der Incident-Aufgabe.
Beschreibung	Detaillierte Erklärung zu der Incident-Aufgabe.
Notizen	
Liste „Arbeitsnotizen“	Benutzer, die Benachrichtigungen zu dieser Incident-Aufgabe erhalten, wenn Arbeitsnotizen hinzugefügt werden. i Hinweis: Sie können das Symbol „Mich hinzufügen“  um sich der Liste „Arbeitsnotizen“ hinzuzufügen.
Arbeitsnotizen	Informationen darüber, wie die Incident-Aufgabe gelöst werden kann, oder welche Schritte erforderlich sind, um sie zu lösen, falls zutreffend.

5. Wählen Sie **Absenden**.

Ergebnisse

Jetzt können Sie die Incident-Aufgabe im zugehörigen OT-Incident-Datensatz auf der Registerkarte **Incident-Aufgaben** unter Now Platform oder im Industrial Workspace anzeigen und bearbeiten.

Incident-Aufgaben können Sie auch in der Listenansicht Industrial Workspace an folgenden Stellen anzeigen.

- Ihnen zugewiesene Incident-Aufgaben: **OT-Aufgaben > Mir zugewiesen**
- Ihrer Gruppe zugewiesene Incident-Aufgaben: **OT-Aufgaben > Meinen Gruppen zugewiesen**
- Nicht zugewiesene Incident-Aufgaben: **OT-Aufgaben > Nicht zugewiesen**

Nachfolge-Incident erstellen

Erstellen Sie einen untergeordneten Incident-Datensatz Operational Technology (OT), um einen Teil der gemeldeten Abweichung zu erfassen und separat zu bearbeiten. Durch das Erstellen untergeordneter Incidents können Sie mehrere Incidents organisieren, die sich auf dasselbe übergeordnete Incident beziehen.

Vorbereitungen

- Aktivieren Sie die Eigenschaft Funktion „Untergeordneten Incident erstellen“ (*com.snc.incident.create.child.enable*). Weitere Informationen finden Sie unter [Legen Sie die Systemeigenschaften fest](#).
- Erforderliche Rolle: `sn_ot_incident_write`

Warum und wann dieser Vorgang ausgeführt wird

Felder, die in den untergeordneten Incident kopiert werden, werden mithilfe der Systemeigenschaft *com.snc.sn_ot_incident.copy.attributes* konfiguriert.

Prozedur

1. Navigieren Sie zum Listenmodul **OT-Incidents** im Industriell Arbeitsbereich.
Alternativ können Sie zu einem OT-Gerät-Datensatz oder einem Anlagenmodell-Entitäts-Datensatz wechseln und die Registerkarte **OT Incidents** auswählen.
2. Öffnen Sie den OT-Incident, für den Sie einen untergeordneten Incident erstellen möchten.
3. Wählen Sie die zugehörige Liste Untergeordnete **Incidents** aus.
4. Wählen Sie **Neu**.
5. Füllen Sie die Details des untergeordneten Incident aus.
6. Wählen Sie **Speichern**.

Ergebnisse

Jetzt können Sie den untergeordneten Incident im übergeordneten Incident-Datensatz anzeigen und bearbeiten.

Sichtbarkeit von Incidents über Standorte hinweg

Mit der Rolle „Incident-Erfüller“ Operational Technology (OT) (`sn_ot_incident_write`) können Sie die Incidents, die zu Ihrem Standort gehören, anzeigen, erstellen oder bearbeiten. Sie können auch die Incidents anzeigen, die zu anderen Sites gehören, um ähnliche Incidents an Ihrer Site zu lösen.

Übersicht über die Sichtbarkeit von OT-Incidents

Wenn Sie ein Benutzer mit der Rolle „OT Incident-Erfüller“ (`sn_ot_incident_write`) sind, können Sie die folgenden Aufgaben ausführen:

- Zeigen Sie die Ihnen zugewiesenen OT-Incident-Datensätze oder die Incidents, die zu Ihrer Site gehören, an, und bearbeiten Sie sie.
- Erstellen Sie OT-Incidents.
- Zeigen Sie OT-Incidents an, die zu den anderen Sites gehören.

Vorteil der Rolle „OT Incident-Erfüller“.

Der Hauptvorteil als OT-Incident-Erfüller besteht darin, dass Sie schreibgeschützte Einblicke in Incidents über Sites hinweg haben. Wenn Sie andere Incidents standortübergreifend anzeigen, können Sie ähnliche Incidents an Ihrem Standort lösen.

Hinweis:

Sie können OT-Incidents für andere Sites nicht bearbeiten. Sie können nur Incidents bearbeiten, die zu Ihrem Standort gehören.

Ort zum Anzeigen oder Bearbeiten von Incidents

Die folgenden OT-Incident-Listen sind im Modul Listen in Industriell Arbeitsbereichverfügbar:

- Mir zugewiesen: Sie können die Ihnen zugewiesenen Incident-Datensätze anzeigen und bearbeiten, indem Sie zu navigieren **OT-Incidents > Mir zugewiesen**.
- Gehört zu meinen Sites: Sie können die Incident-Datensätze, die zu Ihren Sites gehören, anzeigen und bearbeiten, indem Sie zu navigieren **OT-Incidents > Gehört zu meinen Standorten**.
- Zeigen Sie die vorhandenen Incident-Datensätze an anderen Standorten an, indem Sie zu navigieren **OT-Incidents > Alle**.

Synchronisierung zwischen Incident und Incident-Aufgaben

Sie können Incident-Aufgaben Operational Technology (OT) verwenden, um mit anderen Stakeholdern zusammenzuarbeiten und von ihnen Arbeit anzufordern. Ein OT-Incident und seine Aufgaben werden synchronisiert, sodass sich der Status der Incident-Aufgaben abhängig vom Status des Incident ändert.

Die Eigenschaft `com.snc.incident.ot_incident_task.closure` schließt offene Incident-Aufgaben, wenn der zugehörige Incident geschlossen oder abgebrochen wird. Diese Eigenschaft ist für verschiedene Aktionen verantwortlich, die basierend auf dem Status des OT-Incidents für OT-Incident-Aufgaben ausgeführt werden.

Die Synchronisierung zwischen einem OT-Incident und seiner offenen OT-Incident-Aufgabe erfolgt wie folgt:

- Wenn ein OT-Incident geschlossen wird, wird der Status aller offenen OT-Incident-Aufgaben auf **Geschlossen – unvollständig** gesetzt.
- Wenn ein OT-Incident abgebrochen wird, wird der Status aller offenen OT-Incident-Aufgaben auf **Geschlossen – übersprungen** gesetzt.

E-Mail-Benachrichtigungen zu Incidents

Verwenden Sie E-Mail-Benachrichtigungen zu Incidents Operational Technology (OT), um Benutzer zu benachrichtigen, wenn Änderungen an einem Incident vorgenommen werden.

Die Benachrichtigungen sind in der folgenden Tabelle aufgelistet.

E-Mail-Benachrichtigungen für OT-Incidents

Name der Benachrichtigung	Absendezeitpunkt	Empfänger	Inhalt
Incident kommentiert	Wenn ein zusätzlicher Kommentar hinzugefügt wird	Zugewiesen an, Beobachtungsliste	Betreff:<Incident #> Kommentar hinzugefügt Text: Kommentar hinzugefügt URL zum Incident
Incident geöffnet und nicht zugewiesen	Wenn das Feld Zugewiesen an in leer geändert wird und der Wert für „Aktiv“ auf „wahr“ festgelegt wird	Person, die den Incident geöffnet hat	Betreff:<Incident #> ist nicht zugewiesen Text: Identifizieren Sie einen Mitarbeiter, der an diesem Incident arbeiten soll URL zum Incident
Incident geschlossen	Wenn der Incident geschlossen wird	Zuweisungsgruppe	Betreff:<Incident #> – ist geschlossen Text: Lösungscode und Lösungshinweise
Incident-Priorität geändert	Beim Auslösen	Zugewiesen an, Zuweisungsgruppe, Beobachtungsliste	Betreff:<Incident #> Priorität geändert Text: Neue Priorität:<priority>
Gelöster Incident	Wenn der Incident-Status in Gelöst wechselt	Anrufer, Beobachtungsliste	Betreff:<Incident #> – wurde gelöst Text: Lösungscode und Lösungshinweise
Meiner Gruppe zugewiesener Incident	Wenn sich das Feld „Zuweisungsgruppe“ ändert	Zuweisungsgruppe, Beobachtungsliste	Betreff:<Incident #> – ist zugewiesen<assignment group> Text: Priorität, Kurzbeschreibung, Beschreibung URL zum Incident

Automatische Übersetzung

E-Mail-Benachrichtigungen für OT-Incidents (Fortsetzung)

Name der Benachrichtigung	Absendezeitpunkt	Empfänger	Inhalt
Mir zugewiesener Incident	Wenn sich das Feld Zugewiesen an ändert	Zugewiesen an, Beobachtungsliste	Betreff:<Incident #> ist Ihnen zugewiesen Text: Priorität, Kurzbeschreibung, Beschreibung URL zum Incident
Für mich geöffneter Incident	Wenn ein neuer Incident erstellt wird	Anrufer	Betreff:<Incident #> – wird in Ihrer Anforderung geöffnet Text: Priorität, Kurzbeschreibung, Beschreibung URL zum Incident
Incident-Status geändert	Wenn sich der Status des incident ändert	Zugewiesen an, Beobachtungsliste	Betreff:<Incident #> Status geändert Text: Kurzbeschreibung, Alter Status, Neuer Status URL zum Incident

Verfassen Sie eine E-Mail aus einem OT-Incident-Datensatz

Verfassen Sie eine E-Mail direkt in einem OT-Incident-Datensatz, um Ihr Team und andere bequem über den Incident zu informieren.

Vorbereitungen

Erforderliche Rolle: sn_ot_incident_write

Prozedur

1. Navigieren zu **Alle > Industrial Workspace**.
2. Öffnen Sie die Listenansicht Industriell Arbeitsbereich.
3. Wählen Sie im Listenmodul OT Incidents eine der verfügbaren Listen aus.
4. Wählen Sie den Incident-Datensatz aus, für den Sie eine E-Mail senden möchten.
5. Öffnen Sie im Incident-Header das Menü, indem Sie auf die Schaltfläche **Weitere Aktionen** ... Schaltfläche.
6. Klicken Sie auf **E-Mail verfassen**.

7. Füllen Sie das Formular in der E-Mail-Vorlage aus.

E-Mail-Vorlagenformular

Feld	Beschreibung
An	Benutzer, an die Sie die E-Mail senden möchten. Dieses Feld füllt den Benutzer automatisch in das Feld Zugewiesen an des OT-Incident-Datensatzes aus.
Betreff	Betreff der E-Mail In dieses Feld werden automatisch die Nummer des OT-Incident-Datensatzes und die zugehörige Kurzbeschreibung eingetragen.
Textkörper	Updates, die Sie an einen oder mehrere Anwender senden möchten, die sich auf den OT-Incident beziehen.

8. Wahlweise: Wenn die E-Mail eine Antwort ist, können Sie eine Antwortvorlage im Feld **Antwortvorlagen** verwenden, um den E-Mail-Text auszufüllen.

9. Wahlweise: Um die E-Mail als Entwurf zu speichern, wählen Sie **Als Entwurf speichern** aus.

10. Wählen Sie **E-Mail senden aus**.

Ergebnisse

Die E-Mail wird an den oder die Benutzer gesendet, die Sie in der E-Mail-Vorlage angegeben haben.

Incidents lösen und schließen

Wenn ein Problem behoben ist, können Sie den Incident-Status Operational Technology (OT) auf **Gelöst** festlegen. Wenn Sie mit der Lösung zufrieden sind, können Sie den Incident schließen. Basierend auf den Eigenschaften für das automatische Schließen des Incident wird der Incident nach einer bestimmten Zeit automatisch geschlossen.

Vorbereitungen

Erforderliche Rolle: sn_ot_incident_write

Prozedur

1. Navigieren zu **Alle > Incident > Offen**.
2. Öffnen Sie den laufenden OT-Incident, den Sie lösen und schließen möchten.
3. Füllen Sie in der zugehörigen Liste **Lösungsdetails** die folgenden Felder aus.

Auflösungsinformationfelder

Feld	Beschreibung
Lösungscode	Informationen zur Kategorisierung von gelösten Fällen.

Feld	Beschreibung
Lösungsnotizen	Beschreibt, wie der Incident gelöst wurde.

4. Wählen Sie im Feld **Status** die Option **Gelöst** aus.

5. Klicken Sie auf **Aktualisieren**.

Bearbeiten Sie die zugehörigen Geräte und Anlagenmodell-Entitäten in einem Incident-Datensatz

Fügen Sie die zugehörigen Operational Technology (OT)-Geräte und Anlagenmodell-Entitäten direkt aus einem OT-Incident-Datensatz hinzu, oder entfernen Sie sie. Sie können die Beziehung zwischen dem Incident und den betroffenen Elementen nachverfolgen.

Vorbereitungen

Erforderliche Rolle: sn_ot_incident_write oder sn_ot_incident_admin

Prozedur

1. Navigieren zu **Alle > Industrial Workspace**.
2. Öffnen Sie die Listenansicht Industriell Arbeitsbereich.
3. Wählen Sie im Listenmodul OT Incidents eine der verfügbaren Listen aus.
4. Wählen Sie den Incident-Datensatz aus, den Sie bearbeiten möchten.
5. Fügen Sie ein zugehöriges OT-Gerät hinzu, oder entfernen Sie es.
Die OT-Geräte werden jetzt in der zugehörigen Liste „Betroffene OT-Geräte“ zum Change-Datensatz hinzugefügt oder daraus entfernt.
6. Fügen Sie einem Incident-Datensatz eine Anlagenmodell-Entität hinzu, oder entfernen Sie sie daraus, indem Sie die Schritte 4 und 5 wiederholen, jedoch in der zugehörigen Liste „Betroffene Anlagenmodell-Entitäten“.

Incident-Management für operative Technologie-Referenz

Referenzthemen enthalten zusätzliche Informationen zur Anwendung Incident-Management für operative Technologie.

Formular „Zuweisungsregel“.

Zuweisungsregeln weisen automatisch einen Operational Technology (OT)-Incident einer Gruppe oder einem Benutzer gemäß einer oder mehreren Bedingungen in der Zuweisungsregel zu.

In der folgenden Tabelle werden die Feldwerte für das Formular „Zuweisungsregel“ beschrieben.

Formular „Zuweisungsregel“.

Feld	Beschreibung
Name	Beschreibender Name für die Zuweisungsregel.
Aktiv	Option zum Aktivieren der Zuweisungsregel.
Betrifft	
Tabelle	Tabelle mit den Datensätzen, für die die Zuweisungsregel gilt.

Formular „Zuweisungsregel“. (Fortsetzung)

Feld	Beschreibung
	i Hinweis: Legen Sie für Zuweisungsregeln, die spezifisch für OT-Incidents sind, das Feld Tabelle auf Operational Technology Incident [sn_ot_incident] fest. Die Liste zeigt nur Tabellen und Datenbankansichten an, die sich im gleichen Umfang wie die Zuweisungsregel befinden. Wenn Sie eine anwenderdefinierte Tabelle auswählen, die die Aufgabentabelle erweitert, müssen Sie, um sicherzustellen, dass die Zuweisungsregel ordnungsgemäß funktioniert, den Instanzcache leeren, indem Sie zu <a href="https://<instance_name>.service-now.com/cache.do">https://<instance_name>.service-now.com/cache.do navigieren. i Wichtig: Das Leeren des Systemcaches kann die Gesamtleistung beeinträchtigen und die Systemantwortzeiten verschlechtern. Führen Sie während der Geschäftszeiten keine Cacheleerungen aus, und lösen Sie keine automatische Ausführung von Cacheleerungen aus.
Bedingungen	Bedingungen, für die die Zuweisungsregel gilt.
Zuweisen an	
Anwender	Benutzer, dem das Ereignis zugewiesen ist.
Gruppe	Gruppe, der das Ereignis zugewiesen ist.
Skript	
Skript	Skript zum Angeben der Funktionalität der erweiterten Zuweisungsregel. Der Variablensatz <code>current.variable_pool</code> ist verfügbar. i Hinweis: Stellen Sie sicher, dass die Eingabe im Skript korrekt ist und dass der Eingabetyp mit dem Feldtyp im Skript für die Zuweisungsregel übereinstimmt. Wenn beispielsweise das Zuweisungsregelskript den Wert eines Ganzzahlfelds festlegt und der Wert im Skript auf Zeichenfolge festgelegt ist, kann die Zuweisungsregel zu unerwarteten Ergebnissen führen.
Optionale Felder	
Bedingungen anpassen	Beliebig Wenn eine der Bedingungen erfüllt ist, gilt die Zuweisungsregel. Alle Wenn alle Bedingungen erfüllt sind, gilt die Zuweisungsregel.
Ausführungsbefehl	Reihenfolge, in der die Zuweisungsregel verarbeitet wird. Bei Konflikten zwischen den Zuweisungsregeln hat eine Regel mit einem niedrigeren Reihenfolgewert Vorrang vor einer Regel mit einem höheren Wert. Wenn die Reihenfolgenwerte auf dieselbe Zahl festgelegt sind, hat die Zuweisungsregel mit der ersten übereinstimmenden Bedingung Vorrang vor den anderen ohne die erste übereinstimmende Bedingung. Nur die erste Zuweisungsregel mit einer übereinstimmenden Bedingung wird für einen Datensatz ausgeführt.

Mit Incident-Management für operative Technologie installierte Komponenten

Bei der Aktivierung des Plugins Incident-Management für operative Technologie (sn_ot_inc_mgmt) können verschiedene Arten von Komponenten installiert werden, einschließlich Anwenderrollen.

Hinweis:

In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter [Komponenten finden, die mit dieser Anwendung installiert wurden](#) .

Installierte Rollen

Rolle	Beschreibung	Enthält Rollen
OT-Incident-Administrator [sn_ot_incident_admin]	Kann OT Incident-Datensätze für alle Anlagenmodell-Entitäten erstellen, anzeigen, löschen und bearbeiten. Kann Prioritätssuchregeln und Systemeigenschaften für OT-Incidents konfigurieren.	• cmdb_ot_isa_viewer_all • sn_ot_incident_write
OT Incident Reader sn_ot_incident_read	OT-Incident-Datensätze können nur angezeigt werden.	• cmdb_ot_viewer • cmdb_ot_isa_viewer
Erfüller für OT-Incident sn_ot_incident_write	Kann OT Incident-Datensätze anzeigen, erstellen und bearbeiten.	sn_ot_incident_read

Hinweis:

Die Rolle „OT-Incident-Anwender“ [ot_incident_user] ist veraltet. Für Anwender, denen diese Rolle zugewiesen ist, können Sie eine geplante Aufgabe ausführen, um ihnen neue Incident-Management für operative Technologie Rollen zuzuweisen. Weitere Informationen finden Sie unter [Weisen Sie Ihren Anwendern neue Rollen zu](#).

Installierte Tabellen

Tabelle	Beschreibung
OT-Incidents sn_ot_incident	Liste der Site-übergreifend gemeldeten OT-Incidents.
OT Incident-Aufgaben sn_ot_incident_task]	Liste der OT-Incident-Aufgaben, die unter verschiedenen OT-Incidents erstellt wurden.
Suche nach Prioritätsregel für OT-Incident [dl_ot_inc_priority]	Liste der Regeln zur Berechnung der Priorität eines OT-Incidents.

Zugehörige Informationen

Weitere Informationen zu OT-Erweiterungsklassen und zugehörigen Anwendungen.

Übersicht über Erweiterungsklassen

Die Erweiterungsklassen helfen Ihnen zu verstehen, wie Operational Technology-Management mit Configuration Management Database (CMDB) funktioniert.

Operational Technology (OT) extension classes [↗](#)

Configuration Management Database (CMDB) aktualisiert Klassen für OT.

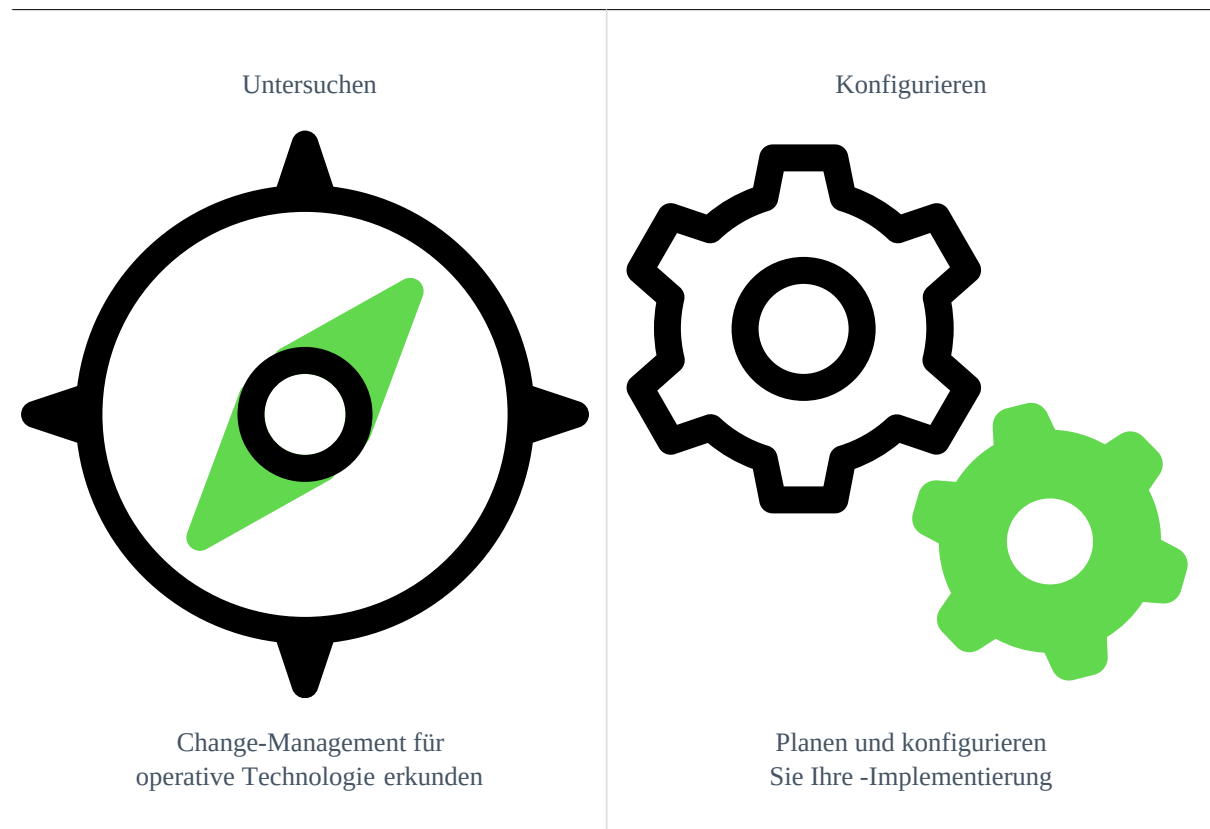
Zugehörige Anwendungen

IT Service Management [↗](#)

Bei Integration mit Incident-Management für operative Technologien können Techniker mit der Anwendung ServiceNow IT Service Management Probleme mit OT-Geräten und Produktionsprozessen schnell lösen.

Change-Management für operative Technologie

Mit der Anwendung ServiceNow® Change-Management für operative Technologie kann Ihr Unternehmen Changes an Operational Technology (OT-)Geräten und Produktionsprozessen implementieren.



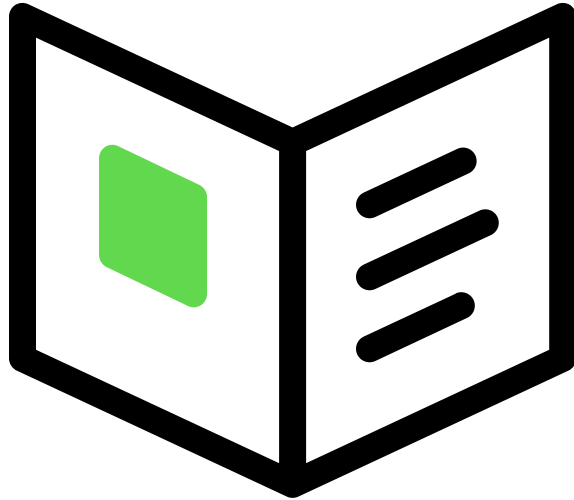
Automatische Übersetzung

Verwenden



Change-Management für
operative Technologie verwenden

Referenz



Erhalten Sie Details zu zugehörigen
Informationen und Anwendungen.

Automatische Übersetzung

Change-Management für operative Technologie erkunden

Erfahren Sie mehr über die Anwendung Change-Management für operative Technologie.

Change-Management für operative Technologie – Übersicht

Sehen Sie sich die Übersicht über die -Produktsuite Operational Technology Service Management an, um mehr über die Anwendung Change-Management für operative Technologie zu erfahren.

[https://player.vimeo.com/video/1019801515?](https://player.vimeo.com/video/1019801515?badge=0&autoplay=0&player_id=0&app_id=58479)

[badge=0&autoplay=0&player_id=0&app_id=58479](https://player.vimeo.com/video/1019801515?badge=0&autoplay=0&player_id=0&app_id=58479)

Schlüsselfunktionen

Mit der Anwendung Change-Management für operative Technologie können Sie die folgenden wichtigen Funktionen verwenden:

- Digitalisierter Change-Workflow, der alle Stakeholder verbindet
- Sites mit unterschiedlichen Change-Management-Prozessen (Workflows).
- IT Change Management und Change-Management für operative Technologiegetrennt, aber bei Bedarf kombinierbar.
- Workflow Change-Management für operative Technologie mit den Anwendungen Incident-Management für operative Technologie und Operational Technology Vulnerability Response integriert.
- Ausgerichtete Änderungen der Werksverkaufsfläche für die Anlagenmodell-Entitäten mit Ausfallzeitplänen.

Verwenden Sie Change-Management für operative Technologie, um Ihren Produktionsprozess zu optimieren

Die Anwendung Change-Management für operative Technologie ermöglicht Ihren Teammitgliedern, gemeinsam an Änderungen an Operational Technology-Geräten (OT) oder Konfigurationen von Industrieanlagen zu arbeiten. Diese Changes umfassen Optimierungen, Änderungen im Produktionsprozess oder Korrekturen von Schwachstellen.

Change-Management für operative Technologie – Übersicht

Mit der Anwendung Change-Management für operative Technologie können Sie Ihre OT-Change-Anforderungen getrennt von Ihren Change-Anforderungen für Informationstechnologie (IT) verwalten. Sie können OT-Change-Anforderungen von IT-Change-Anforderungen nach dem Netzwerktyp trennen und Sie können OT-Change-Anforderungen pro Site verwalten.

Die folgenden Beispiele zeigen, wie Sie Change-Management für operative Technologie auf Ihre Organisation anwenden können:

- Ein Besitzer der OT-Nachbesserung, der für die Behebung von Schwachstellen in OT-Geräten verantwortlich ist, möchte einen Change initiieren, um eine Gruppe von Schwachstellen zu beheben.
- Ein OT-Techniker, der für OT-Konfigurationen und Anlagen-Engineering-Aktivitäten verantwortlich ist, möchte einen Change ausführen, um einen defekten Roboterarm in der Industriewerkstatt zu reparieren.
- Ein Werksleiter, der für die gesamte Produktionsaktivität verantwortlich ist, möchte eine vom Engineering-Team angeforderte Änderung überprüfen und genehmigen.

OT-Change-Anforderungen

OT-Change-Anforderungen treten auf, wenn eine Serviceunterbrechung durch ein OT-Gerät in einem OT-Netzwerk auftritt. In einigen Fällen ist das OT-Gerät möglicherweise nicht bekannt, wenn die Change-Anforderung erstellt wird. Wenn Sie eine OT-Change-Anforderung aus Industriell Arbeitsbereich erstellen, wird der Change-Anforderung automatisch der Netzwerktyp **OT** zugewiesen. Dieses Attribut wird verwendet, um eine OT-Change-Anforderung von einer IT-Change-Anforderung zu unterscheiden. Dieses Feld wird standardmäßig nicht angezeigt. Weitere Informationen zu OT-Geräten finden Sie unter [Zugehörige Elemente und zugehörige Listen für OT-Geräte](#).

Weitere Informationen zum Erstellen einer OT-Change-Anforderung finden Sie unter [Change-Anforderungen erstellen](#).

Trennung eines IT- und OT-Change

Wenn die Anwendung Change-Management für operative Technologie auf Ihrer -Instanz installiert ist, können Sie als Netzwerktyp **IT**, **OT** oder **None (Keine)** auswählen. Neuen Change-Anforderungen wird standardmäßig der Netzwerktyp **Keine** zugewiesen.

Change-Management für operative Technologie Statusübergänge des Modells

In den folgenden Tabellen sind die Modellstatusübergänge des Modells Change-Management für operative Technologie für das Basis-OT-Change-Modell und das erweiterte OT-Change-Modell aufgeführt. Weitere Informationen zu den OT Change-Modellen finden Sie unter [Wählen Sie ein Change-Modell aus, um Change-Anforderungen zu erfüllen](#).

Status für das grundlegende OT-Change-Modell

Status	Beschreibung
Neu	Eine OT-Change-Anforderung wird initiiert.
Planen	Die OT-Change-Anforderung wird mit den folgenden Kriterien analysiert: • Begründung • Implementierungsplan • Risiko- und Auswirkungsanalyse • Rückfallplan • Testplan • Change planen
Implementierung	Der Change wird auf dem Ziel-OT-Gerät durchgeführt.
Geschlossen	Der Change-Datensatz wird geschlossen, nachdem der Change abgeschlossen ist.
Abgebrochen	Der Change-Datensatz wird abgebrochen, und der Change wird nicht auf das OT-Gerät angewendet.

Status für das erweiterte OT-Change-Modell

Status	Beschreibung
Neu	Eine OT-Change-Anforderung wird initiiert.
Planen	Die OT-Change-Anforderung wird mit den folgenden Kriterien analysiert: • Begründung • Implementierungsplan • Risiko- und Auswirkungsanalyse • Rückfallplan • Testplan • Change planen
Genehmigen	Die Überprüfer genehmigen die OT-Change-Anforderung oder lehnen sie ab.
Implementierung	Der Change wird auf dem Ziel-OT-Gerät durchgeführt.
Überprüfung nach der Implementierung	Fügen Sie bei Bedarf zusätzliche OT-Change-Aufgaben hinzu, und führen Sie die folgenden Prüfungen durch: • Elektroprüfung • Netzwerkprüfung

Status für das erweiterte OT-Change-Modell (Fortsetzung)

Status	Beschreibung
	• Qualitätsprüfung • Sicherheitscheck
Geschlossen	Der Change-Datensatz wird geschlossen, nachdem der Change abgeschlossen ist.
Abgebrochen	Der Change-Datensatz wird abgebrochen, und der Change wird nicht auf das OT-Gerät angewendet.

Change-Management für operative Technologie konfigurieren

Konfigurieren Sie die Anwendung Change-Management für operative Technologie, um die Datengrundlage für die Lösung ServiceNow® Operational Technology (OT) zu erstellen.

Wenn Sie über die Administratorrolle verfügen, können Sie sich von Geführtes Setup durch das Setup von Change-Management für operative Technologie führen lassen. Geführtes Setup ist ein Tool zur Unterstützung der Anwendungskonfiguration. Er ordnet die Konfigurationsaktivitäten in Kategorien. Diese Kategorien enthalten Informationen zu den Setup-Aufgaben, Schritte zum Abschließen der einzelnen Aufgaben und Links zu den Seiten in Ihrer Instanz, auf denen Sie die Konfiguration durchführen. Links zu nützlichen Hilfeinhalten werden ebenfalls bereitgestellt.

***i* Hinweis:**

Change-Management für operative Technologie ist abhängig von Utah P4 oder höher.

Um auf Geführtes Setup zuzugreifen, navigieren Sie zu *Administrator für den industriellen Arbeitsbereich* > **Geführtes Setup**.

In der folgenden Tabelle werden die Geführtes Setup -Aufgaben und ihr Zweck für die Change-Management für operative Technologie -Anwendung erläutert.

Aufgabe	Zweck
1. Installieren Sie die Anwendung Change-Management für operative Technologie aus dem ServiceNow Store.	Installiert die Anwendung Change-Management für operative Technologie und unterstützende Plugins.
2. Weisen Sie Change-Management für operative Technologie Rollen zu.	Weist Rollen zu, um die für jeden Benutzer verfügbaren Aktionen zu steuern.
3. Konfigurieren Sie Change-Management für operative Technologie -Kategorien.	Konfiguriert die Kategorien für die OT-Changes, die für Ihre Organisation erforderlich sind.
4. Wählen Sie das Modell Change-Management für operative Technologie aus.	Wählt das Change-Modell für Ihre Organisation aus.

Change-Management für operative Technologie installieren

Mit der Administratorrolle können Sie die Anwendung Change-Management für operative Technologie (sn_ot_chg_mgmt) installieren.

Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter [Rufen Sie eine Berechtigung für ab ServiceNow Produkt oder Anwendung](#) .
- Die Anwendung Change-Management für operative Technologie erfordert die folgenden Plugins. Stellen Sie sicher, dass diese Plugins aktiviert sind, bevor Sie die Anwendung Change-Management für operative Technologie installieren.

Benötigte ServiceNow-Plugins

CMDB CI-Klassenmodelle (sn_cmdb_ci_class)

Die Store-App Configuration Management Database (CMDB) CI-Klassenmodelle fügt Klassenmodelle hinzu, die die CMDB-Klassenhierarchie erweitern, einschließlich Klassenbeschreibungen, Identifizierungsregeln, Bezeichnereinträge und abhängige Beziehungen. Weitere Informationen finden Sie unter [Store App CMDB-CI-Klassenmodelle](#) .

Anlagenmodell nach ISA (sn_isa_model)

Das Datenmodell für Entitäten und Vorlagen des Anlagenmodells nach ISA-95. Weitere Informationen finden Sie unter [Anlagenmodell nach ISA-95](#).

- Die Anwendung Change-Management für operative Technologie erfordert eine oder beide der folgenden ServiceNow Store -Anwendungen. Stellen Sie sicher, dass mindestens eine dieser Anwendungen installiert ist, bevor Sie die Anwendung Change-Management für operative Technologie installieren.

Erforderliche ServiceNow Store-Anwendungen

Operational Technology Manager

Die Anwendung Operational Technology Manager erstellt die grundlegenden Daten und Beziehungen, die es Ihrer Organisation ermöglichen, die Lösung Operational Technology zu verwenden. Die Anwendung Operational Technology Manager unterstützt die Verwendung der Anwendungen Configuration Management Database (CMDB), Service Graph Connectors und Discovery in Now Platform. Weitere Informationen hierzu finden Sie unter [Operational Technology Manager konfigurieren](#).

Prozessmanager Industrie

Die Anwendung Prozessmanager Industrie erstellt die Datengrundlage für das Anlagenmodell nach ISA-95, die für die Lösung ServiceNow® Industriell erforderlich ist. Damit können Sie an jedem Ihrer Industriestandorte eine eigene Version der Anlagenmodelle erstellen. Weitere Informationen finden Sie unter [Prozessmanager Industrie konfigurieren](#).

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die folgenden Elemente werden mit der Anwendung Change-Management für operative Technologie installiert:

- Plugins
- Store-Anwendungen
- Rollen und ACLs

Weitere Informationen zu den installierten Rollen und ACLs finden Sie unter [Mit Change-Management für operative Technologie installierte Komponenten](#).

i Hinweis:

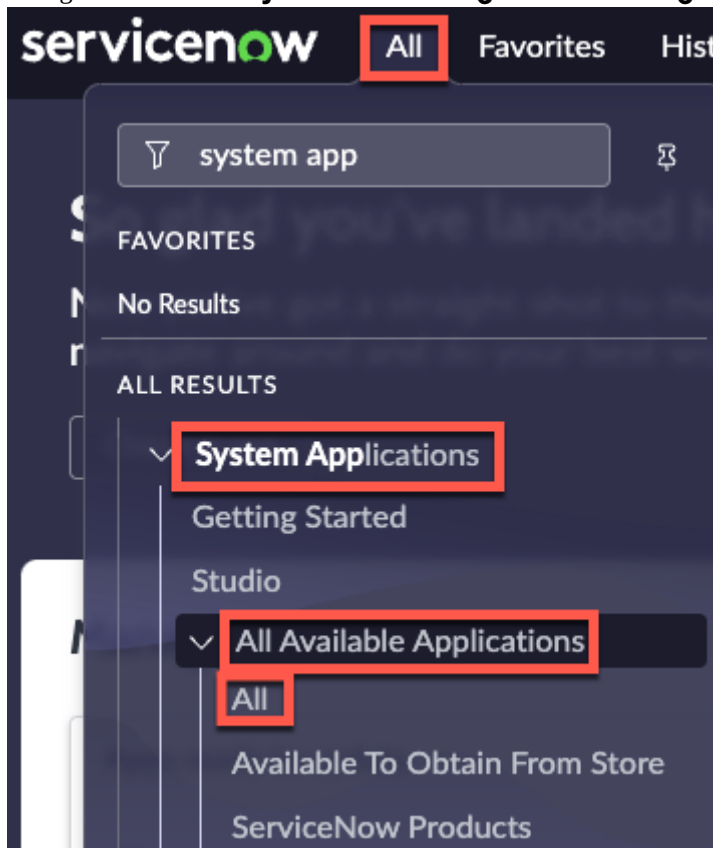
Beachten Sie für Operational Technology Service Management -Benutzer ohne Lizenz für Operational Technology -Transparenz Folgendes:

- Wenn Sie die neueste Version von Incident-Management für operative Technologie installiert haben, wird auch Prozessmanager Industrie installiert.
- Wenn Sie die neueste Version von Change-Management für operative Technologie installiert haben, wird auch Prozessmanager Industrie installiert.

Sie sollten ein Upgrade auf die neuesten Versionen durchführen, um Zugriff auf die Experience Operational Technology Service Management zu erhalten.

Prozedur

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



2. Suchen Sie die Anwendung Change-Management für operative Technologie mithilfe der Filterkriterien und der Suchleiste.

Sie können nach der Anwendung anhand ihres Namens oder ihrer ID suchen. Wenn Sie die 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. Überprüfen Sie im Dialogfeld „Anwendungsinstallation“ die Anwendungsabhängigkeiten.

Abhängige Plugins und Anwendungen werden aufgelistet, wenn sie installiert werden, derzeit installiert sind oder installiert werden müssen. Wenn Plugins oder Anwendungen installiert werden müssen, müssen Sie sie installieren, bevor Sie die Change-Management für operative Technologie-Anwendung installieren können.

4. Wählen Sie **Installieren** aus.

Weisen Sie Change-Management für operative Technologie Rollen zu

Weisen Sie Ihren Benutzern Rollen zu, damit Sie ihren Zugriff auf die Funktionen, Fähigkeiten und Daten in der Anwendung Change-Management für operative Technologie steuern können.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Benutzer mit den in der folgenden Tabelle aufgeführten Rollen können die Anwendung verwenden.

Rolle	Beschreibung
Change-Manager [sn_ot_change_manager]	Kann Datensätze für OT-Change-Modelle verwalten.
Change-Administrator [sn_ot_change_admin]	Kann OT-Change-Datensätze erstellen, anzeigen, löschen und bearbeiten. Kann Kategorien und Systemeigenschaften konfigurieren.
Change Write-Benutzer [sn_ot_change_write]	Kann OT-Change-Datensätze erstellen, anzeigen und bearbeiten. Ihnen können auch IT-Change-Aufgaben zugewiesen werden, und sie können die zugewiesene IT-Change-Aufgabe bearbeiten und schließen. Weitere Informationen finden Sie unter Verwaltet Change-Anforderungen standortübergreifend .
Change Read Anwender [sn_ot_change_read]	OT-Change-Datensätze können nur angezeigt werden.

Prozedur

Weisen Sie Benutzern und Gruppen mit der Benutzerverwaltungsfunktion Now Platform Rollen zu.

Wählen Sie ein Change-Modell aus, um Change-Anforderungen zu erfüllen

Wählen Sie ein Change-Modell Operational Technology (OT) aus, um mit der Erfüllung Ihrer Change-Anforderungen abhängig von den Anforderungen Ihrer Organisation zu beginnen.

Vorbereitungen

Erforderliche Rolle: sn_ot_change_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Zwei OT-Change-Modelle stehen Ihnen zur Verwendung zur Verfügung:

- OT Change Standard
- OT Change – Vertiefung

Das Modell OT Change Basic verwendet den Change-Prozess ohne Genehmigungen.

Weitere Informationen zum Basismodell für OT Change finden Sie unter [Grundlegendes Playbook für OT-Change-Modelle](#).

Das Modell „OT Change Advanced“ verwendet den Change-Prozess mit Genehmigungen. Sie können eine Richtlinie für Change-Genehmigungen erstellen und eine Genehmigungsgruppe zuweisen, um Ihre Change-Anforderung zu überprüfen. Weitere Informationen zu Change-Genehmigungen finden Sie unter [Operational Technology Change-Genehmigung](#).

Weitere Informationen zum erweiterten OT-Change-Modell finden Sie unter [Playbook für das erweiterte OT-Change-Modell](#).

Prozedur

1. Navigieren zu **Industrial Workspace-Administrator > Geführtes Setup**.
2. Wählen Sie in der Kategorie Change-Management für operative Technologie **die Option Erste Schritte aus**.
3. Wählen Sie neben dem Abschnitt Change-Modelle **Konfigurieren aus**.
4. Wählen Sie das Change-Modell aus, das den Anforderungen Ihrer Organisation entspricht.
5. Bearbeiten Sie den Datensatz nach Bedarf.

Ergebnisse

Das Change-Modell wird auf Ihr System angewendet, und Sie können mit der Erstellung von OT-Change-Anforderungen beginnen.

Grundlegendes Playbook für OT-Change-Modelle

Erfahren Sie mehr über die Playbook-Phasen des Change-Modells für grundlegende operative Technologie (OT), die ein OT-Change ohne Genehmigungen durchlaufen muss, bis er abgeschlossen ist.

Initiiert

Mit der Phase Initiieren einer OT-Change-Anforderung können Sie die Details des angeforderten Change erfassen und den Change nach Bedarf zuweisen. Diese Phase hat drei Aufgaben.

Beschreiben Sie den Change.

Feld	Beschreibung
Kurzbeschreibung	Kurze Beschreibung des Change.
Beschreibung	Details des Change.
Kategorie	Typ des Change.
Site	Standort, an dem der Change stattfindet.
Beobachtungsliste	Benutzer, die Benachrichtigungen über diesen Change erhalten, wenn Kommentare hinzugefügt werden.

Beschreiben Sie den Change. (Fortsetzung)

Feld	Beschreibung
Arbeitsnotizenliste	Benutzer, die Benachrichtigungen über diesen Change erhalten, wenn Arbeitsnotizen hinzugefügt werden.

Risiko erfassen

Feld	Beschreibung
Priorität	Auswirkung und Dringlichkeit, um zu ermitteln, wie schnell der Change behandelt werden sollte.
Risiko	Risiko, das der Change darstellt.
Auswirkung	Messwert für den Effekt, den ein Change auf Ihre Industrieprozesse hat.

Change zuweisen

Feld	Beschreibung
Angefordert von	Benutzer, der den Change anfordert.
Zuweisungsgruppe	Zugewiesene Gruppe, die am Change arbeitet. Die Zuweisungsgruppe kann eine beliebige Gruppe mit dem Typ OT sein.
Zugewiesen an	Benutzer, der an diesem Change arbeitet. Wenn sich die Zuweisungsgruppe ändert, wird das Feld Zugewiesen an gelöscht.

Planen

In der Phase „Planen“ einer OT-Change-Anforderung können Sie eine Begründung für den Change, einen Implementierungsplan, einen Risiko- und Auswirkungsplan, einen Rückfallplan, einen Testplan und eine Zeit für die Planung des Change hinzufügen. Diese Phase hat sechs Aufgaben.

Fügen Sie eine Begründung hinzu

Feld	Beschreibung
Begründung	Grund, warum der Change stattfinden muss.

Implementierungsplan hinzufügen

Feld	Beschreibung
Implementierungsplan	Details zur Implementierung des angeforderten Change.

Risiko- und Auswirkungsanalyse hinzufügen

Feld	Beschreibung
Risiko- und Auswirkungsanalyse	Details zu Risiko- und Einflussfaktoren im Zusammenhang mit diesem Change.

Rückfallplan hinzufügen

Feld	Beschreibung
Rückfallplan	Details dazu, wie der vorhandene Change bei Bedarf rückgängig gemacht werden kann.

Testplan hinzufügen

Feld	Beschreibung
Testplan	Details zum Testen des implementierten Change.

Change planen

Feld	Beschreibung
Geplantes Startdatum	Datum, an dem der Change stattfindet. i Hinweis: Sie können auch ein verfügbares Ausfallzeitfenster im Kalender auswählen, indem Sie die Schaltfläche Planungsassistent wählen, um das Feld für das geplante Startdatum automatisch auszufüllen.
Geplantes Enddatum	Datum, an dem der Change endet. i Hinweis: Sie können auch ein verfügbares Ausfallzeitfenster im Kalender auswählen, indem Sie die Schaltfläche Planungsassistent wählen, um das Feld für das geplante Enddatum automatisch auszufüllen.

Implementieren

Die Phase „Implementieren“ einer OT-Change-Anforderung enthält die Details der folgenden Aufgabe. Sie können diese Phase als abgeschlossen markieren, wenn sie abgeschlossen ist.

Change durchführen

Als abgeschlossen markieren, wenn der Change auf den Ziel-OT-Geräten ausgeführt und abgeschlossen wurde.

Schließen

Mit der Phase Schließen können Sie den Change Record schließen, nachdem der Change abgeschlossen wurde.

Schließen Sie den Change-Datensatz

Feld	Beschreibung
Abschlusscode	Grund, aus dem der Change-Datensatz geschlossen wurde.
Abschlussnotizen	Zusätzliche Details zum Schließen des Change-Datensatzes.

Playbook für das erweiterte OT-Change-Modell

Erfahren Sie mehr über die Playbook-Phasen des Change-Modells für erweiterte operative Technologie (OT), die ein OT-Change mit Genehmigungen durchlaufen muss, bis er abgeschlossen ist.

Initiiert

Mit der Phase Initiieren einer OT-Change-Anforderung können Sie die Details des angeforderten Change erfassen und den Change nach Bedarf zuweisen. Diese Phase hat drei Aufgaben.

Beschreiben Sie den Change.

Feld	Beschreibung
Kurzbeschreibung	Kurze Beschreibung des Change.
Beschreibung	Details des Change.
Kategorie	Typ des Change.
Site	Standort, an dem der Change stattfindet.
Beobachtungsliste	Benutzer, die Benachrichtigungen über diesen Change erhalten, wenn Kommentare hinzugefügt werden.
Arbeitsnotizenliste	Benutzer, die Benachrichtigungen über diesen Change erhalten, wenn Arbeitsnotizen hinzugefügt werden.

Risiko erfassen

Feld	Beschreibung
Priorität	Auswirkung und Dringlichkeit, um zu ermitteln, wie schnell der Change behandelt werden sollte.
Risiko	Risiko, das der Change darstellt.
Auswirkung	Messwert für den Effekt, den ein Change auf Ihre Industrieprozesse hat.

Change zuweisen

Feld	Beschreibung
Angefordert von	Benutzer, der den Change anfordert.
Zuweisungsgruppe	Zugewiesene Gruppe, die am Change arbeitet. Die Zuweisungsgruppe kann eine beliebige Gruppe mit dem Typ OT sein.
Zugewiesen an	Benutzer, der an diesem Change arbeitet. Wenn sich die Zuweisungsgruppe ändert, wird das Feld Zugewiesen an gelöscht.

Planen

In der Phase „Planen“ einer OT-Change-Anforderung können Sie eine Begründung für den Change, einen Implementierungsplan, einen Risiko- und Auswirkungsplan, einen Rückfallplan, einen Testplan und eine Zeit für die Planung des Change hinzufügen. Diese Phase hat sechs Aufgaben.

Begründung hinzufügen

Feld	Beschreibung
Begründung	Grund, warum der Change stattfinden muss.

Implementierungsplan hinzufügen

Feld	Beschreibung
Implementierungsplan	Details zur Implementierung des angeforderten Change.

Risiko- und Auswirkungsanalyse hinzufügen

Feld	Beschreibung
Risiko- und Auswirkungsanalyse	Details zu Risiko- und Einflussfaktoren im Zusammenhang mit diesem Change.

Rückfallplan hinzufügen

Feld	Beschreibung
Rückfallplan	Details dazu, wie der vorhandene Change bei Bedarf rückgängig gemacht werden kann.

Testplan hinzufügen

Feld	Beschreibung
Testplan	Details zum Testen des implementierten Change.

Change planen

Feld	Beschreibung
Geplantes Startdatum	Datum, an dem der Change stattfindet. i Hinweis: Sie können auch ein verfügbares Ausfallzeitfenster im Kalender auswählen, indem Sie die Schaltfläche Planungsassistent wählen, um das Feld für das geplante Startdatum automatisch auszufüllen.
Geplantes Enddatum	Datum, an dem der Change endet. i Hinweis: Sie können auch ein verfügbares Ausfallzeitfenster im Kalender auswählen, indem Sie die Schaltfläche Planungsassistent wählen, um das Feld für das geplante Enddatum automatisch auszufüllen.

Genehmigen

Über die Phase „Genehmigen“ einer OT Change-Anforderung können Überprüfer den OT Change genehmigen oder ablehnen. Diese Phase enthält nur eine Aufgabe.

Überprüfen und Maßnahmen ergreifen

Feld	Beschreibung
Schaltfläche „Genehmigen“.	Wenn Sie ein Überprüfer sind, der in der Tabelle im Aufgabenformular angezeigt wird, wählen Sie Genehmigen , um den Change zu akzeptieren.
Schaltfläche „Ablehnen“.	Wenn Sie ein Überprüfer sind, der in der Tabelle im Aufgabenformular angezeigt wird, wählen Sie Ablehnen , um den Change abzulehnen.
Kommentare	Zusätzliche Informationen zur Genehmigung oder Ablehnung des Change.

Weitere Informationen zu Change-Genehmigungen finden Sie unter [Operational Technology Change-Genehmigung](#).

Implementieren

Die Phase „Implementieren“ einer OT-Change-Anforderung enthält die Details der folgenden Aufgaben. Sie können diese Phase als abgeschlossen markieren, wenn sie abgeschlossen ist.

Funktion anhalten

Markieren Sie bei Bedarf als abgeschlossen, nachdem Sie die Funktion der Ziel-OT-Geräte beendet haben.

LOTO sicherstellen

Lockout/Target (LOTO) ist ein Sicherheitsverfahren, um ein versehentliches oder unbeabsichtigtes Starten von Maschinen während Wartung oder Service zu verhindern. Als abgeschlossen markieren, wenn LOTO abgeschlossen ist.

Change durchführen

Als abgeschlossen markieren, wenn der Change auf den Ziel-OT-Geräten ausgeführt und abgeschlossen wurde.

Überprüfung nach der Implementierung

In der Phase „Überprüfung nach der Implementierung“ einer OT-Change-Anforderung können Sie die durchgeführten Aufgaben abchecken, zusätzliche OT-Change-Aufgaben für die verbleibende Arbeit erstellen, die während der Überprüfung identifiziert wurde, und den Prozess zum Widerrufen des LOTO-Prozesses als abgeschlossen markieren.

Führen Sie Prüfungen durch

Feld	Beschreibung
Elektroprüfung durchführen	Checkbox, die Sie aktivieren, nachdem die Elektroprüfung abgeschlossen wurde.
Netzwerkprüfung durchführen	Checkbox, die Sie aktivieren, nachdem die Netzwerkprüfung abgeschlossen wurde.
Qualitätscheck durchführen	Kontrollkästchen, das Sie aktivieren, nachdem die Qualitätsprüfung abgeschlossen wurde.
Sicherheitscheck durchführen	Kontrollkästchen, das Sie aktivieren, nachdem die Sicherheitsprüfung abgeschlossen wurde.

Ausgliederungsaufgaben empfehlen

Feld	Beschreibung
OT Change-Aufgaben	Liste der Change-Aufgaben, die sich auf den OT-Change beziehen.
Status	Status des OT-Change. Der Status ändert sich und verfolgt Changes durch mehrere Lösungsphasen.
Zugewiesen an	Benutzer, der an diesem Change arbeitet. Wenn sich die Zuweisungsgruppe ändert, wird das Feld Zugewiesen an gelöscht.
Kurzbeschreibung	Kurze Beschreibung der Change-Aufgabe.

LOTO widerrufen

Nachdem der Change implementiert und überprüft wurde, markieren Sie ihn als abgeschlossen, wenn das Sperrziel widerrufen wird.

Ausgliederungsaufgaben

In der Phase „Spin-off-Aufgaben“ werden alle Change-Aufgaben in der Überprüfung nach der Implementierung aufgelistet, die abgeschlossen werden müssen.

Schließen

Mit der Phase Schließen können Sie den Change Record schließen, nachdem der Change abgeschlossen wurde.

Change-Datensatz schließen

Feld	Beschreibung
Abschlusscode	Grund, aus dem der Change-Datensatz geschlossen wurde.
Abschlussnotizen	Zusätzliche Details zum Schließen des Change-Datensatzes.

Change-Management für operative Technologie verwenden

Nachdem Sie alle erforderlichen Setup-Aufgaben für die Anwendung Change-Management für operative Technologie abgeschlossen haben, können Sie mit der Verwaltung von Change-Anforderungen für Operational Technology (OT) beginnen.

Change-Anforderungen erstellen

Erstellen Sie eine Change-Anforderung Operational Technology (OT), um eine Änderung an Ihrer -Site zu melden.

Vorbereitungen

Erforderliche Rolle: sn_ot_change_write

Prozedur

1. Navigieren zu **Alle > Industrial Workspace**.
2. Wählen Sie in der Listenansicht „**OT Change-Anforderungen**“ die Liste aus, die Sie öffnen möchten.
3. Wählen Sie **Neu**.
4. Wählen Sie das OT Change-Modell aus, das für Ihre Organisation gilt.
5. Wählen Sie **OT Change-Datensatz erstellen aus**.
6. Schließen Sie das Playbook nach Bedarf ab, während Ihr Team an der Change-Anforderung arbeitet.
Weitere Informationen zum Playbook „Basis-OT-Change-Modell“ finden Sie unter [Grundlegendes Playbook für OT-Change-Modelle](#). Weitere Informationen zum Playbook „Erweitertes OT-Change-Modell“ finden Sie unter [Playbook für das erweiterte OT-Change-Modell](#).

Hinweis:

Wenn Playbook nicht aktiviert ist, können Sie im Datensatz der OT-Change-Anforderung nur die Registerkarten **Details** und **Zugehörige Datensätze** anzeigen.

Erstellen Sie eine Change-Aufgabe, um eine Change-Anforderung zu erfüllen

Erstellen Sie eine Change-Aufgabe, um eine Change-Anforderung Operational Technology (OT) zu erfüllen. Mithilfe von Change-Aufgaben können Sie alle Aufgaben erfassen, die während einer Change-Anforderung ausgeführt werden müssen.

Vorbereitungen

Erforderliche Rolle: sn_ot_change_write

Warum und wann dieser Vorgang ausgeführt wird

Change-Aufgaben sind die einzelnen Schritte, die ausgeführt werden müssen, um eine Change-Anforderung zu erfüllen und abzuschließen.

Prozedur

1. Navigieren zu **Alle > Industrial Workspace**.
2. Wählen Sie den Change-Datensatz aus, für den Sie eine Aufgabe erstellen möchten.
3. Wählen Sie in der zugehörigen Liste „Change-Aufgaben“ **Neu**.
Wenn die zugehörige Liste „Change-Aufgaben“ nicht angezeigt wird, müssen Sie sie hinzufügen.
4. Füllen Sie die Felder des Formulars aus.

Formular „Incident-Aufgabe“.

Feld	Beschreibung
OT-Change-Aufgabe	
Kurzbeschreibung	Kurze Beschreibung der Change-Aufgabe.
Beschreibung	Details der Change-Aufgabe.
OT-Gerät	Betroffenes OT-Gerät.
OT-Change-Anforderung	Datensatznummer der zugehörigen OT-Change-Anforderung.
Status	Status für die Nachverfolgung einer Change-Aufgabe durch mehrere Phasen der Change-Implementierung.
Typ	Typ des Change.
Zuweisung	
Zuweisungsgruppe	Gruppe, die an der Change-Aufgabe arbeitet. Wenn Sie dieses Feld leer lassen, wird die Change-Aufgabe automatisch zugewiesen.
Zugewiesen an	Benutzer, dem die Change-Aufgabe zugewiesen wurde. 📘 Hinweis: Wenn sich die Zuweisungsgruppe ändert, wird das Feld Zugewiesen an gelöscht.
Notizen	
Beobachtungsliste	Benutzer, die Benachrichtigungen über diesen Change erhalten, wenn Kommentare hinzugefügt werden.
Arbeitsnotizenliste	Benutzer, die Benachrichtigungen über diesen Change erhalten, wenn Arbeitsnotizen hinzugefügt werden.
Arbeitsnotizen (privat)	Arbeitsnotizen, die Kunden nicht zur Verfügung stehen.

5. Wählen Sie **Speichern**.

Ergebnisse

Sie können die Change-Aufgabe im zugehörigen OT-Change-Datensatz anzeigen und bearbeiten.

Sie können Change-Aufgaben in der Listenansicht Industriell Arbeitsbereich an folgenden Stellen anzeigen.

- Ihnen zugewiesene Change-Aufgaben: **OT-Aufgaben > Mir zugewiesen**
- Ihrer Gruppe zugewiesene Change-Aufgaben: **OT-Aufgaben > Meinen Gruppen zugewiesen**
- Nicht zugewiesene Change-Aufgaben: **OT-Aufgaben > Nicht zugewiesen**

Erstellen Sie eine Change-Anforderung aus OT-Gerät-Details

Erstellen Sie eine Change-Anforderung Operational Technology (OT) aus einem OT-Gerät-Datensatz. Durch das Erstellen einer Change-Anforderung aus einem Gerätedatensatz werden die Informationen in Ihrem Change-Anforderungsdatsatz automatisch ausgefüllt, z. B. der Standort oder der Business-Service und das Feld OT-Gerät.

Vorbereitungen

Erforderliche Rolle: sn_ot_change_write

Prozedur

1. Navigieren zu **Alle > Industrial Workspace**.
2. Wählen Sie in der Liste „Alle OT-Geräte“ einen OT-Gerät-Datensatz aus.
3. Wählen Sie auf der Registerkarte **Zugehörige Datensätze** die zugehörige Liste OT Change-Anforderungen aus.
4. Wählen Sie **Neu**.
5. Wählen Sie das OT Change-Modell aus, das für Ihre Organisation gilt.
6. Wählen Sie **OT Change-Datensatz erstellen aus**.
7. Schließen Sie das Playbook nach Bedarf ab, während Ihr Team an der Change-Anforderung arbeitet.

Weitere Informationen zum Playbook „Basis-OT-Change-Modell“ finden Sie unter [Grundlegendes Playbook für OT-Change-Modelle](#). Weitere Informationen zum Playbook „Erweitertes OT-Change-Modell“ finden Sie unter [Playbook für das erweiterte OT-Change-Modell](#).

Die folgenden Felder werden abhängig von den von Ihnen festgelegten Bedingungen automatisch ausgefüllt.

- Das Feld **OT-Gerät** wird nur dann automatisch ausgefüllt, wenn die Anwendung Prozessmanager Industrie aktiviert ist.
- Wenn Prozessmanager Industrie installiert ist, wird die Site, die dem OT-Gerät zugewiesen ist, im Feld **Site** angezeigt.
- Wenn Prozessmanager Industrie aktiviert ist und nur eine Entität dem OT-Gerät zugeordnet ist, wird das Feld **Anlagenmodell-Entität** automatisch ausgefüllt.

Hinweis:

Wenn einem Gerät mehrere Entitäten zugeordnet sind, bleibt das Feld **Anlagenmodell-Entität** leer.

Ergebnisse

Die Change-Anforderung wird erstellt, und die Benutzer in den Feldern Zuweisungsgruppe, Zugewiesen an und Beobachtungsliste werden benachrichtigt.

Erstellen Sie eine Change-Anforderung aus einer Korrekturaufgabe

Erstellen Sie eine Change-Anforderung Operational Technology (OT) aus einer OT-Korrekturaufgabe. Durch das Erstellen einer Change-Anforderung aus einer Korrekturaufgabe werden die Informationen in Ihrem Change-Anforderungsdatensatz automatisch ausgefüllt, z. B. die Felder Standort und OT-Gerät.

Vorbereitungen

Erforderliche Rolle: sn_ot_change_write oder sn_otvr.remediation_owner

Prozedur

1. Navigieren zu **Alle > Industrial Workspace**.
2. Öffnen Sie den Korrekturaufgaben-Datensatz, aus dem Sie eine Change-Anforderung erstellen möchten.
3. Wählen Sie die Schaltfläche **OT Change erstellen aus**, wie im folgenden Beispiel gezeigt.

The screenshot displays the ServiceNow interface for a task titled 'California Vulnerabilities'. At the top right, the 'Create OT Change' button is highlighted. The left sidebar contains sections for 'Remediation Progress' (showing 0%) and 'Remediation Task Details' (including fields like Number, Risk rating, Remediation target, and Short description). The main content area features a table of 'Vulnerable items' with columns: Vulnerable item, Summary, Configuration item, State, and Risk rating. A single item is listed with ID VIT0010002. To the right of the table is an 'Attachments' section indicating no attachments are available.

i Hinweis:

Wenn kein aktives Change-Modell vorhanden ist, wird der folgende Fehler

angezeigt.

Error creating Change Request: No active change model available. Please contact your OT Change admin

4. Wählen Sie das OT Change-Modell aus, das für Ihre Organisation gilt.
5. Wählen Sie **Weiter**.
6. Schließen Sie das Playbook nach Bedarf ab, während Ihr Team an der Change-Anforderung arbeitet.

Weitere Informationen zum Playbook „Basis-OT-Change-Modell“ finden Sie unter [Grundlegendes Playbook für OT-Change-Modelle](#). Weitere Informationen zum Playbook „Erweitertes OT-Change-Modell“ finden Sie unter [Playbook für das erweiterte OT-Change-Modell](#).

Automatische Übersetzung

Die folgenden Felder werden abhängig von den von Ihnen festgelegten Bedingungen automatisch ausgefüllt.

- Das Feld **OT-Gerät** wird nur dann automatisch ausgefüllt, wenn die Anwendung Prozessmanager Industrie aktiviert ist.
- Wenn Prozessmanager Industrie installiert ist, wird die Site, die dem OT-Gerät zugewiesen ist, im Feld **Site** angezeigt.
- Wenn Prozessmanager Industrie aktiviert ist und nur eine Entität dem OT-Gerät zugeordnet ist, wird das Feld **Anlagenmodell-Entität** automatisch ausgefüllt.

i Hinweis:

Wenn einem Gerät mehrere Entitäten zugeordnet sind, bleibt das Feld **Anlagenmodell-Entität** leer.

Erstellt eine Change-Anforderung aus einem Incident-Datensatz

Erstellen Sie eine Change-Anforderung Operational Technology (OT) aus einem OT-Incident-Datensatz. Wenn Sie einen Change Request direkt aus einem Incident-Datensatz erstellen, werden die Daten automatisch dem neuen Change Request aus dem Incident-Datensatz zugeordnet.

Vorbereitungen

Erforderliche Rolle: sn_ot_incident_write, sn_ot_incident_admin oder sn_ot_change_write

Prozedur

1. Navigieren zu **Alle > Industrial Workspace**.
2. Wählen Sie im Listenmodul OT Incidents eine der verfügbaren Listen aus.
3. Wählen Sie den Incident-Datensatz aus, aus dem Sie eine OT-Change-Anforderung erstellen möchten.
4. Wählen Sie die Schaltfläche **OT Change erstellen aus**.
Das Formular „OT-Change auswählen“ wird geöffnet.
5. Wählen Sie das Change-Modell aus, das für Ihre Organisation geeignet ist.
Weitere Informationen finden Sie unter [Wählen Sie ein Change-Modell aus, um Change-Anforderungen zu erfüllen](#).
6. Wählen Sie **OT Change-Datensatz erstellen aus**.
7. Füllen Sie das Playbook und zugehörige Formulare nach Bedarf aus.

Weitere Informationen zum Playbook und zu zugehörigen Formularen finden Sie unter [Grundlegendes Playbook für OT-Change-Modelle](#) und [Playbook für das erweiterte OT-Change-Modell](#), je nachdem, welches OT-Change-Modell Sie ausgewählt haben.

i Hinweis:

In der zugehörigen Liste „Details“ der neuen Change-Anforderung werden die folgenden Felder und zugehörigen Listen automatisch mit den Werten aus dem zugehörigen OT-Incident-Datensatz gefüllt:

- Site
- Anlagenmodell-Entität
- OT-Gerät (CI)
- Kurzbeschreibung
- Beschreibung
- Priorität

i Hinweis:

Ein Wert im Feld **Priorität** von 1 bis 4 ist im neuen Change Record identisch. Ein Wert von 5 im Feld **Priorität** des Incident-Datensatzes wird im neuen Change-Datensatz in 4 geändert.

Bearbeiten Sie die zugehörigen Geräte und Anlagenmodell-Entitäten in einem Change-Datensatz

Fügen Sie die zugehörigen Operational Technology (OT)-Geräte und Anlagenmodell-Entitäten direkt aus einem OT Change-Datensatz hinzu, oder entfernen Sie sie. Sie können die Beziehung zwischen der Change-Anforderung und den betroffenen Elementen nachverfolgen.

Vorbereitungen

Erforderliche Rolle: sn_ot_change_write oder sn_ot_change_admin

Prozedur

- 1.** Navigieren zu **Alle > Industrial Workspace**.
- 2.** Öffnen Sie die Listenansicht Industriell Arbeitsbereich.
- 3.** Wählen Sie im Listenmodul OT Change-Anforderungen eine der verfügbaren Listen aus.
- 4.** Wählen Sie den Change-Datensatz aus, den Sie bearbeiten möchten.
- 5.** Fügen Sie ein zugehöriges OT-Gerät hinzu, oder entfernen Sie es.
Die OT-Geräte werden jetzt in der zugehörigen Liste „Betroffene OT-Geräte“ zum Change-Datensatz hinzugefügt oder daraus entfernt.
- 6.** Fügen Sie einem Change-Datensatz eine Anlagenmodell-Entität hinzu, oder entfernen Sie sie daraus, indem Sie die Schritte 4 und 5 wiederholen, jedoch in der zugehörigen Liste „Betroffene Anlagenmodell-Entitäten“.

Operational Technology Change-Genehmigung

Mit der Change-Genehmigung Operational Technology (OT) können Überprüfer Ihre angeforderten Änderungen genehmigen und bei Bedarf Verbesserungen vorschlagen.

Übersicht über Change-Genehmigungen

Eine OT-Change-Genehmigung mit dem erweiterten OT-Change-Modell ermöglicht Genehmigern, eine Change-Anforderung zu überprüfen, die Anforderung nach Bedarf zu bearbeiten und die Change-Anforderung zu genehmigen.

i Hinweis:

Die Change-Genehmigung gilt nur für das erweiterte OT-Change-Modell. Auf das Basis-OT-Change-Modell wird keine Change-Genehmigungsrichtlinie angewendet.

Change-Genehmigungsanforderungen

Anforderung	Beschreibung
Standortebene	Standort oder Bereich, in dem der Change stattfindet.
Standortgenehmigungsgruppe	Mitglieder, die einer Genehmigungsgruppe zugewiesen sind und Change-Anforderungen überprüfen und genehmigen können.
Erforderliche Rolle	Genehmiger müssen über die Rolle „sn_ot_change_read“ verfügen.
Prozentsatz der Genehmigungen	51 % der Genehmigungsgruppe müssen den Change genehmigen, damit er fortgesetzt wird.

Flow für OT-Change-Genehmigung

Der OT-Change-Genehmigungs-Flow sieht wie folgt aus.

1. Erstellen Sie die Change-Anforderung.
2. Der Flow wird basierend auf dem Change-Modell aufgerufen.
3. Der Flow wendet die Change-Genehmigungsrichtlinie an.
4. Verschiedene Entscheidungsdatensätze werden ausgewertet.
5. Übereinstimmende Genehmigungsdefinitionen werden ausgeführt.
6. Fügen Sie dem Change-Datensatz eine Liste von Genehmigern auf Site-Ebene hinzu.

Das Advanced OT Change-Modell enthält eine Change-Genehmigungsrichtlinie. Sie können auch eine eigene Genehmigungsrichtlinie erstellen. Weitere Informationen zum Erstellen einer Genehmigungsrichtlinie finden Sie unter [Create change approval policies](#) .

Fügen Sie einen Genehmiger hinzu, um eine Change-Anforderung zu überprüfen

Fügen Sie Ihrer Genehmigungsgruppe manuell ein Gruppenmitglied oder einen Genehmiger hinzu, um Ihre Operational Technology (OT) Change-Anforderung zu überprüfen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle > Anwenderadministration > Gruppen**.
2. Wählen Sie in der Liste Gruppen die Gruppe **OT Change Standardgenehmiger** aus.
3. Wählen Sie die zugehörige Liste Gruppenmitglieder aus.
4. Wählen Sie **Bearbeiten**.

5. Wählen Sie in der Liste Sammlung die Mitglieder aus, die Sie der Genehmigungsgruppe hinzufügen möchten.
6. Verschieben Sie die ausgewählten Mitglieder mithilfe der mittleren Pfeile in die Liste der Standardgenehmiger für OT-Change.
7. Wählen Sie **Speichern**.

Ergebnisse

Ihrer Genehmigungsgruppe wurden neue Mitglieder hinzugefügt. Jetzt kann die Genehmigungsgruppe Ihre Change-Anforderung überprüfen.

Sobald Sie die Phasen „Initiieren“ und „Planen“ Ihrer OT-Change-Anforderung im Playbook „Erweitertes OT-Change-Modell“ abgeschlossen haben, können Sie in der Phase „Genehmigen“ eine Genehmigung anfordern. Die Mitglieder Ihrer Genehmigungsgruppe müssen den Change-Anforderungsdatensatz öffnen, um sie mit einer der folgenden Methoden in Industrial Workspace zu genehmigen.

- Wählen Sie im Datensatz Change-Anforderung die Registerkarte **Genehmiger** aus, und ändern Sie das Feld **Status** von **Angefordert** in die entsprechende Option.
- Wählen Sie auf der Registerkarte **Playbook** die Phase Genehmigen aus, und ändern Sie das Feld **Status** von **Angefordert** in die entsprechende Option.

Verwaltet Change-Anforderungen standortübergreifend

Mit der Anwendung Change-Management für operative Technologie können Sie die Change-Anforderungen, die zu Ihrer Site oder anderen Sites gehören, anzeigen, erstellen oder bearbeiten. Durch Anzeigen der Change-Anforderungen von anderen Sites können Sie ähnliche Changes an Ihrem Standort implementieren.

Übersicht über Site-übergreifende Change-Anforderungen

Mit der Rolle `sn_ot_change_write` können Sie folgende Aufgaben ausführen:

- Zeigen Sie die Operational Technology (OT) Change-Anforderungen an, die Ihnen zugewiesen sind, oder die Change-Anforderungen, die zu Ihrem Standort gehören, und bearbeiten Sie sie.
- Erstellen Sie die OT-Change-Anforderungen.
- Zeigen Sie die OT-Change-Anforderungen an, die zu den anderen Sites gehören.

Der Hauptvorteil der Rolle `sn_ot_change_write` besteht darin, dass Sie einen schreibgeschützten Einblick in die Site-übergreifenden Changes haben. Durch das Anzeigen weiterer Site-übergreifender Changes können Sie ähnliche Changes an Ihrer Site implementieren.

Hinweis:

Sie können nur OT-Change-Anforderungen bearbeiten, die zu Sites gehören, auf die Sie Zugriff haben. Erfahren Sie in den folgenden Abschnitten mehr über zusätzliche Rollen, die für die Verwaltung von websiteübergreifenden OT-Change-Anforderungen erforderlich sind.

Andere OT-Rollen und Berechtigungen, die Sie mit der Rolle `sn_ot_change_write` benötigen

Die folgende Tabelle beschreibt die zusätzlichen Rollen, die Sie als Benutzer mit der Rolle `sn_ot_change_write` benötigen, um auf die Change-Anforderungen für Ihre Site oder eine beliebige Site zugreifen zu können.

Andere Rollen, die Sie mit der Rolle sn_ot_change_write benötigen

Rolle	Berechtigungen
sn_ot_change_write mit der Rolle cmdb_ot_isa_editor	Erstellen und bearbeiten Sie die Change-Anforderungen für Ihre Site.
sn_ot_change_write mit Rolle cmdb_ot_isa_viewer	Erstellen und bearbeiten Sie die Change-Anforderungen für Ihre Site.
sn_ot_change_write und cmdb_ot_isa_viewer_all	Erstellen und bearbeiten Sie die Change-Anforderungen für eine beliebige Site.
sn_ot_change_write ohne Site-Rolle	Zeigen Sie die Change-Anforderungen für einen beliebigen Standort an.

Andere OT-Rollen und Berechtigungen, die Sie mit der Rolle sn_ot_change_read benötigen

Die folgende Tabelle beschreibt die zusätzlichen Rollen und Berechtigungen, die Sie als Benutzer mit der Rolle sn_ot_change_read benötigen, um die Change-Anforderungen für Ihre Site oder eine beliebige Site anzuzeigen.

Andere Rollen, die Sie mit der Anwenderrolle sn_ot_change_read benötigen

Rolle	Berechtigungen
sn_ot_change_read mit der Rolle cmdb_ot_isa_editor	Zeigen Sie die Change-Anforderungen für Ihre Site an.
sn_ot_change_read mit Rolle cmdb_ot_isa_viewer	Zeigen Sie die Change-Anforderungen für Ihre Site an.
sn_ot_change_read und cmdb_ot_isa_viewer_all	Zeigen Sie die Change-Anforderungen für einen beliebigen Standort an.
sn_ot_change_read ohne Site-Rolle	Zeigen Sie die Change-Anforderungen für einen beliebigen Standort an.

Ort zum Anzeigen oder Bearbeiten von Change-Anforderungen

Die folgenden Listen für OT-Change-Anforderungen sind im Modul Listen unter Industriell Arbeitsbereich verfügbar:

- Mir zugewiesen: Zeigen Sie Ihre zugewiesenen Change-Datensätze an, und bearbeiten Sie sie, indem Sie zu navigieren **OT-Change-Anforderungen > Mir zugewiesen**.
- Gehört zu meinen Sites: Zeigen Sie die Change-Datensätze an, die zu Ihren Sites gehören, und bearbeiten Sie sie, indem Sie zu navigieren **OT-Change-Anforderungen > Gehört zu meinen Standorten**.
- Zeigen Sie die vorhandenen Change-Datensätze an anderen Standorten an, indem Sie zu navigieren **OT-Change-Anforderungen > Alle**.

Sichtbarkeit von Datensätzen von Change-Modellen über Standorte hinweg

Abhängig von Ihrer Change-Rolle Operational Technology (OT) und Ihrer Site-Rolle können Sie den Change-Modell-Datensatz für Ihre Site oder andere Sites anzeigen, erstellen oder bearbeiten.

OT Change-Rollen und Sichtbarkeit für Change-Modelldatensätze

In den folgenden Tabellen werden die Rollen und Berechtigungen für verschiedene OT Change-Benutzer für den Zugriff auf Datensätze von Change-Modellen beschrieben.

Berechtigungen für Benutzer mit der Rolle sn_ot_change_write

Rolle	Berechtigungen
Site-Rolle sn_ot_change_write mit cmdb_ot_isa_editor	Ein Change-Modell für ihre Datensätze verwenden.
Site-Rolle sn_ot_change_write mit cmdb_ot_isa_viewer	Ein Change-Modell für ihre Datensätze verwenden.
Site-Rolle sn_ot_change_write mit cmdb_ot_isa_viewer_all	Ein Change-Modell für ihre Datensätze verwenden.
sn_ot_change_write ohne Site-Rolle	Kein Zugriff auf Change-Modelle.

Berechtigungen für Benutzer mit der Rolle sn_ot_change_read

Rolle	Berechtigungen
sn_ot_change_read mit cmdb_ot_isa_editor-Site-Rolle	Kein Zugriff auf Change-Modelle.
Site-Rolle sn_ot_change_read mit cmdb_ot_isa_viewer	Kein Zugriff auf Change-Modelle.
sn_ot_change_read ohne Site-Rolle	Kein Zugriff auf Change-Modelle.
Site-Rolle sn_ot_change_read mit cmdb_ot_isa_viewer_all	Kein Zugriff auf Change-Modelle.

Berechtigungen für Benutzer mit der Rolle sn_ot_change_manager

Rolle	Berechtigungen
sn_ot_change_manager mit cmdb_ot_isa_editor Site-Rolle	• Change-Modelle für beliebige Standorte erstellen, bearbeiten und löschen. • Jeder Site Change-Modelle zuweisen • Entfernen Sie Change-Modelle von allen Standorten.
Site-Rolle sn_ot_change_manager mit cmdb_ot_isa_viewer	• Change-Modelle für beliebige Standorte erstellen, bearbeiten und löschen. • Jeder Site Change-Modelle zuweisen • Entfernen Sie Change-Modelle von allen Standorten.
sn_ot_change_manager ohne Site-Rolle	Change-Modelle können für keine Site angezeigt oder bearbeitet werden. Es können nur die Change-

Berechtigungen für Benutzer mit der Rolle sn_ot_change_manager (Fortsetzung)

Rolle	Berechtigungen
	Modelle des Basissystems angezeigt werden, die keiner Site zugeordnet sind.

Wenn Sie über die Rolle sn_ot_change_admin verfügen, können Sie die Change-Modelle verwenden, um eine Change-Anforderung für jede Site zu erstellen.

E-Mail-Benachrichtigungen für Changes

Verwenden Sie E-Mail-Benachrichtigungen, um Benutzer zu benachrichtigen, wenn eine Operational Technology (OT)-Change-Anforderung oder eine Change-Aufgabe aktualisiert wird.

Die Benachrichtigungen für OT-Change-Anforderungen und Change-Aufgaben sind in den folgenden Tabellen aufgeführt.

E-Mail-Benachrichtigungen zu OT-Change-Anforderung

Name	Absendezeitpunkt	Empfänger	Inhalt
Mir zugewiesener Change	Wenn sich das Feld Zugewiesen an ändert und nicht leer ist	Benutzer, dem der Change zugewiesen ist	Betreff:<Change request #> -Benachrichtigung Textkörper: Kurzbeschreibung:<Short description> Klicken Sie hier, um die Change-Anforderung anzuzeigen:<URL to the change request> Standort:<Site name> OT-Gerät:<OT device> Anlagenmodell-Entität:<Equipment model entity> Beschreibung:<Description>
Meiner Gruppe zugewiesener Change	Wenn sich das Feld Zuweisungsgruppe ändert und nicht leer ist	Zuweisungsgruppe	Betreff:<Change request #> wurde der Gruppe zugewiesen<assignment group> Textkörper: Kurzbeschreibung:<Short description> Klicken Sie hier, um die Change-

E-Mail-Benachrichtigungen zu OT-Change-Anforderung (Fortsetzung)

Name	Absendezeitpunkt	Empfänger	Inhalt
			Anforderung anzuzeigen:<URL to the change request> Standort:<Site name> OT-Gerät:<OT device> Anlagenmodell- Entität:<Equipment model entity> Beschreibung:<description>
Kommentierter Change	Wenn die Change-Anforderung kommentiert wird	• Angefordert von • Beobachtungsliste	Betreff:<Change request #> Kommentare hinzugefügt Textkörper: Kurzbeschreibung:<Short description> Klicken Sie hier, um die Change- Anforderung anzuzeigen:<URL to the change request> Kommentare:<Comments added to the change request>
Change in Arbeitsnotiz umgewandelt	Wenn dem Change Request eine Arbeitsnotiz hinzugefügt wird.	• Arbeitsnotizliste • Zugewiesen an • Zuweisungsgruppe	Betreff:<Change request #> Arbeitsnotizen hinzugefügt Textkörper: Kurzbeschreibung:<Short description> Klicken Sie hier, um die Change- Anforderung anzuzeigen:<URL to change request> Arbeitshinweise:<Work notes added to change request>

Automatische Übersetzung

E-Mail-Benachrichtigungen zu OT-Change-Anforderung (Fortsetzung)

Name	Absendezeitpunkt	Empfänger	Inhalt
Change genehmigt	Wenn die Change-Anforderung genehmigt wird	• Zugewiesen an • Zuweisungsgruppe	Betreff:<Change request #> wurde genehmigt Textkörper: Kurzbeschreibung:<Short description> Klicken Sie hier, um anzuzeigen<URL to change request> Beschreibung:<Description>
Abgelehnter Change	Wenn die Change-Anforderung abgelehnt wird	• Zugewiesen an • Zuweisungsgruppe	Betreff:<Change request #> wurde abgelehnt Textkörper: Kurzbeschreibung:<Short description> Klicken Sie hier, um anzuzeigen<URL to change request> Beschreibung:<Description>
Change angehalten	Wenn die Change-Anforderung in die Warteschleife gestellt wird	Angefordert von	Betreff:<Change request #> wurde in die Warteschleife gestellt Textkörper: Hallo<user who created change request> , Die<Change request #> angeforderte Datei wurde in die Warteschleife gestellt. Der Grund für das Setzen der Anforderung in die Warteschleife ist:<Reason for change request being put on hold> Klicken Sie hier, um Ihre Change-Anforderung

Automatische Übersetzung

E-Mail-Benachrichtigungen zu OT-Change-Anforderung (Fortsetzung)

Name	Absendezeitpunkt	Empfänger	Inhalt
			anzuzeigen:<URL to change request>
Change aus der Warteschleife	Wenn die Change-Anforderung aus der Warteschleife genommen wird	Angefordert von	Betreff:<Change request #> wurde aus der Warteschleife genommen Textkörper: Hallo<user who created change request> , Die<Change request #> Das von Ihnen angeforderte Element wurde aus der Warteschleife genommen und befindet sich in<Updated state field> Status Klicken Sie hier, um Ihre Change-Anforderung anzuzeigen:<URL to change request>

E-Mail-Benachrichtigungen für OT-Change-Aufgaben

Name	Absendezeitpunkt	Empfänger	Inhalt
Mir zugewiesene Change-Aufgabe	Wenn sich das Feld Zugewiesen an ändert und nicht leer ist	Person, der die Change-Aufgabe zugewiesen ist	Betreff:<Change task #> Benachrichtigung --<Short description> Textkörper: Kurzbeschreibung:<Short description> Klicken Sie hier, um die Change-Aufgabe anzuzeigen:<URL to change task> Standort:<Site name> OT-Gerät:<OT device>

E-Mail-Benachrichtigungen für OT-Change-Aufgaben (Fortsetzung)

Name	Absendezeitpunkt	Empfänger	Inhalt
			Anlagenmodell-Entität:<Equipment model entity> Beschreibung:<Description>
Change-Aufgabe, die meiner Gruppe zugewiesen ist	Wenn sich das Feld Zuweisungsgruppe ändert und nicht leer ist	Zuweisungsgruppe	Betreff: Betreff:<Change task #> Benachrichtigung --<Short description> Textkörper: Kurzbeschreibung:<Short description> Klicken Sie hier, um die Change-Aufgabe anzuzeigen:<URL to change task> Standort:<Site name> OT-Gerät:<OT device> Anlagenmodell-Entität:<Equipment model entity> Beschreibung:<Description>
Change-Aufgabe in Arbeitsnotiz umgewandelt	Wenn der Change-Aufgabe eine Arbeitsnotiz hinzugefügt wird	• Arbeitsnotizliste • Zugewiesen an • Zuweisungsgruppe	Betreff:<Change task #> Arbeitsnotizen hinzugefügt --<Short description> Textkörper: Kurzbeschreibung:<Short description> Klicken Sie hier, um die Change-Aufgabe anzuzeigen:<URL to change task> Arbeitshinweise:<Work notes added to change task>

Automatische Übersetzung

Change-Management für operative Technologie-Referenz

Referenzthemen enthalten zusätzliche Informationen zur Anwendung Change-Management für operative Technologie.

Change-Kategorien

Durch Kategorisierung der Operational Technology (OT)-Change-Anforderungen können Sie die Suche nach bestimmten OT-Change-Anforderungen gruppieren und eingrenzen. Kategorien helfen Stakeholdern auch zu wissen, worum es bei dem Change geht.

Wenn Sie eine OT-Change-Anforderung erstellen können, können Sie aus den in der folgenden Tabelle aufgeführten Kategorien auswählen.

Kategorien von OT-Change-Anforderungen

Kategorie	Beschreibung
Hardware	Changes zum Hinzufügen, Entfernen oder Konfigurieren von OT-Geräten.
Software	Changes zum Hinzufügen, Entfernen oder Konfigurieren von OT-Software.
Service	Ändert einen OT-Service.
Systemsoftware	Änderungen an der OT-Systemsoftware.
Anwendungssoftware	Änderungen an der OT-Anwendungssoftware.
Netzwerk	Änderungen an Subnetzen, IP-Adressen und MAC-Adressen.
Telekommunikation	Änderungen an der in Ihrem OT-System verwendeten Telekommunikation.
Dokumentation	Änderungen an der OT-Dokumentation.
Firmware	Änderungen an der OT-Firmware.
Sonstige	Andere Changes, die in den oben genannten Kategorien nicht erfasst werden.

Mit Change-Management für operative Technologie installierte Komponenten

Bei Aktivierung der Anwendung Change-Management für operative Technologie (sn_ot_chg_mgmt) können verschiedene Arten von Komponenten installiert werden, einschließlich der Anwenderrollen.

Hinweis:

In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter [Komponenten finden, die mit dieser Anwendung installiert wurden](#) .

Installierte Rollen

Rolle	Beschreibung	Enthält Rollen
Change-Manager [sn_ot_change_manager]	Kann Datensätze für OT-Change-Modelle verwalten.	- sn_ot_change_write - sn_strum_condition_read

Rolle	Beschreibung	Enthält Rollen
Change-Administrator [sn_ot_change_admin]	Kann OT-Change-Datensätze erstellen, anzeigen, löschen und bearbeiten. Kann Kategorien und Systemeigenschaften konfigurieren.	• cmdb_ot_isa_viewer_all • sn_ot_change_write
Change Write-Benutzer [sn_ot_change_write]	Kann OT-Change-Datensätze erstellen, anzeigen und bearbeiten. Ihnen können auch IT-Change-Aufgaben zugewiesen werden, und sie können die zugewiesene IT-Change-Aufgabe bearbeiten und schließen. Weitere Informationen finden Sie unter Verwaltet Change-Anforderungen standortübergreifend.	• cmdb_ot_viewer • cmdb_ot_isa_viewer • sn_ot_change_read
Change Read Anwender [sn_ot_change_read]	OT-Change-Datensätze können nur angezeigt werden.	• cmdb_ot_viewer • cmdb_ot_isa_viewer

Zugehörige Informationen

Weitere Informationen zu OT-Erweiterungsklassen und zugehörigen Anwendungen.

Übersicht über Erweiterungsklassen

Die Erweiterungsklassen helfen Ihnen zu verstehen, wie Operational Technology-Management mit Configuration Management Database (CMDB) funktioniert.

Operational Technology (OT) extension classes [↗](#)

Configuration Management Database (CMDB) aktualisiert Klassen für OT.

Zugehörige Anwendungen

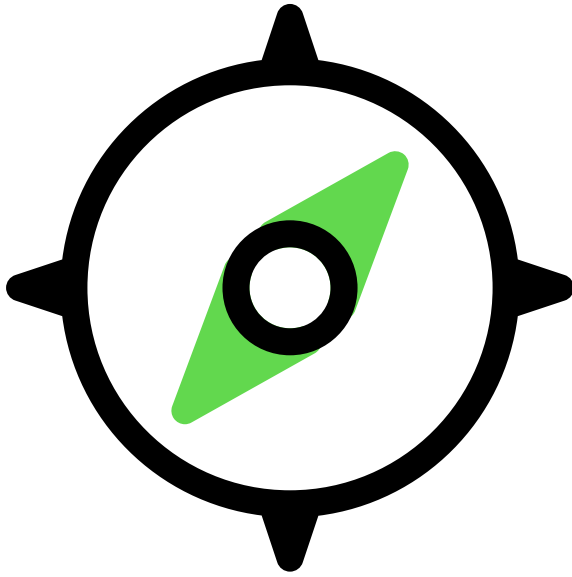
IT Service Management [↗](#)

Bei Integration mit Change-Management für operative Technologie können Techniker mit der Anwendung ServiceNow IT Service Management Probleme mit OT-Geräten und Produktionsprozessen schnell lösen.

Knowledge Management für operative Technologie

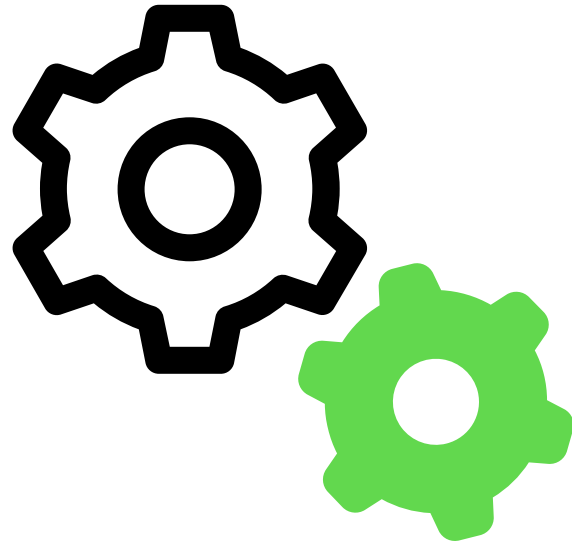
ServiceNow[®] Knowledge Management für operative Technologie kann Ihnen helfen, Wissen über Ihr OT-System Operational Technology, seine Geräte und die gelösten Incidents in Ihrer Organisation zu sammeln, zu organisieren und zu teilen.

Untersuchen



Knowledge Management für
operative Technologie erkunden

Konfigurieren



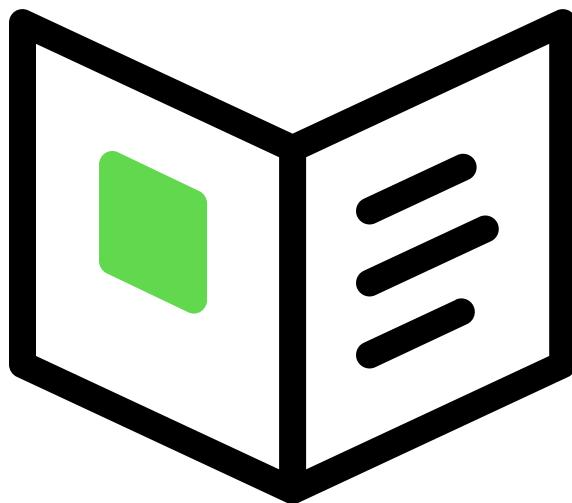
Planen und konfigurieren
Sie Ihre -Implementierung

Verwenden



Knowledge Management für
operative Technologie verwenden

Referenz



Erhalten Sie Details zu zugehörigen
Informationen und Anwendungen.

Automatische Übersetzung

Knowledge Management für operative Technologie erkunden

Knowledge Management für operative Technologie hilft Ihnen, Informationen über Ihr Operational Technology (OT)-System in Wissensartikeln zu erfassen, die sich auf OT-Incidents beziehen. Ihre Organisation kann diese Wissensartikel dann verwenden, um Ihren Anwendern zu

helfen, auf die richtigen Informationen zuzugreifen, und Fehlkommunikation mit Ihren Anwendern verhindert.

Knowledge Management für operative Technologie – Übersicht

Sehen Sie sich die Übersicht über die -Produktsuite Operational Technology Service Management an, um mehr über Knowledge Management für operative Technologie zu erfahren.

[https://player.vimeo.com/video/1019801515?](https://player.vimeo.com/video/1019801515?badge=0&autoplay=0&player_id=0&app_id=58479)

[badge=0&autoplay=0&player_id=0&app_id=58479](https://player.vimeo.com/video/1019801515?badge=0&autoplay=0&player_id=0&app_id=58479)

Knowledge Management für operative Technologie – Vorteile

Mit Knowledge Management für operative Technologie können Sie die folgenden wichtigen Funktionen verwenden:

- Fähigkeit, den vorhandenen Wissensmanagement Funktionen der Now Platform mit der Lösung Operational Technology-Management zu verwenden.
- Möglichkeit, alle Knowledge Base-Artikel zu durchsuchen, die sich auf einen OT-Incident beziehen, und Wissensartikel direkt aus einem Incident-Datensatz zu erstellen.
- Fähigkeit, eine OT-Wissensdatenbank für Wissensmanager und Wissensanwender zu konfigurieren.
- Fähigkeit, Wissensartikel in Industriell Arbeitsbereich zu erstellen.
- Möglichkeit, Genehmigungen zum Veröffentlichen, Bearbeiten, Deaktivieren oder Löschen eines Wissensartikels anzufordern.
- Möglichkeit, vorhandene Wissensartikel mit aktualisierten Informationen zu bearbeiten.

Knowledge Management für operative Technologie konfigurieren

Konfigurieren Sie Knowledge Management für operative Technologie, um die Datengrundlage für die Lösung Operational Technology (OT) zu erstellen.

Wenn Sie über die Administratorrolle verfügen, können Sie sich von Geführtes Setup durch die Einrichtung von Knowledge Management für operative Technologie führen lassen. Geführtes Setup ist ein Tool zur Unterstützung der Anwendungskonfiguration. Er ordnet die Konfigurationsaktivitäten in Kategorien. Diese Kategorien enthalten Informationen zu den Setup-Aufgaben, die Schritte zum Abschließen jeder Aufgabe und die Links zu den Seiten in Ihrer Instanz, auf denen Sie die Konfiguration durchführen. Außerdem werden Links zu nützlichen Hilfeinhalten bereitgestellt.

Um auf Geführtes Setup zuzugreifen, navigieren Sie zu **Industrial Workspace-Administrator > Geführtes Setup**.

In der folgenden Tabelle sind die Geführtes Setup -Aufgaben und ihre Zwecke für Knowledge Management für operative Technologie aufgeführt.

i Hinweis:

Knowledge Management für operative Technologie ist in der Anwendung Incident-Management für operative Technologie enthalten. Solange Sie die Anwendung Incident-Management für operative Technologie (Version 2.0.2) installiert und konfiguriert haben, können Sie Knowledge Management für operative Technologie konfigurieren. Es sind keine zusätzlichen Plugins erforderlich.

Die folgende Tabelle zeigt die Aufgaben, die Ihre Benutzer für eine erfolgreiche Einrichtung und Konfiguration ausführen müssen.

Knowledge Management für operative Technologie-Setupaufgaben

Aufgabe	Zweck
Weisen Sie Wissensmanagement Knowledge Management für operative Technologie-Rollen zu.	Weist Rollen zu, um die für jeden Benutzer verfügbaren Aktionen zu steuern.
Erstellen Sie eine OT-Knowledge Base.	Konfiguriert eine OT-Knowledge Base, um Manager hinzuzufügen und den Zugriff zu konfigurieren.
Erstellen Sie Anwenderkriterien, die auf eine OT-Wissensdatenbank angewendet werden sollen.	Erstellt einen Anwenderkriteriendatensatz, um die Anwender zu bestimmen, die eine OT-Knowledge Base lesen oder dazu beitragen können.
Weisen Sie einer OT-Knowledge Base Anwenderkriterien zu.	Weist die Anwenderkriteriendatensätze einer OT-Knowledge Base zu, um zu steuern, welche Anwender in der Knowledge Base Wissensartikel erstellen, lesen, schreiben und stilllegen können.
Konfigurieren Sie den Zugriff auf OT-Knowledge Bases für nicht authentifizierte Anwender.	Überprüft die OT-Knowledge Bases, auf die nicht authentifizierte Anwender zugreifen können. Der Zugriff basiert auf den Anwenderkriterien und den Einstellungen für die Eigenschaft „glide.knowman.block_access_with_no_user_criteria“.
Weisen Sie einer OT-Wissensdatenbank Knowledge-Workflows zu.	Weist jeder OT-Wissensdatenbank unterschiedliche Wissens-Workflows für die Veröffentlichungs- und Lösungsprozesse zu.
Überprüfen Sie die Wissensmanagement -Eigenschaften, die für Knowledge Management für operative Technologie verwendet werden.	Konfiguriert das Erscheinungsbild und die Funktionen von OT-Knowledge Bases mit den entsprechenden Wissensmanagement -Eigenschaften.

Weisen Sie Ihren Knowledge Management für operative Technologie -Benutzern Rollen zu

Weisen Sie den Benutzern die Rollen Wissensmanagement zu, damit Sie ihren Zugriff auf die Funktionen, Fähigkeiten und Daten von Knowledge Management für operative Technologiesteuern können.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Wenn Ihnen die Rolle Wissensmanagement zugewiesen ist, können Sie die Fähigkeiten Knowledge Management für operative Technologie verwenden.

Hinweis:

Die Anwenderkriterien bestimmen den Zugriff auf Wissensartikel. Weitere Informationen finden Sie unter [Managing access to knowledge bases and knowledge articles](#) .

Weitere Informationen zu den für Wissensmanagement geltenden -Rollen Knowledge Management für operative Technologie finden Sie unter [Knowledge Management für operative Technologie Rollen](#).

Prozedur

Weisen Sie Benutzern und Gruppen mit der Benutzerverwaltungsfunktion Now Platform Rollen zu.

Erstellen Sie eine OT-Knowledge Base

Erstellen Sie eine Knowledge Base Operational Technology (OT), um OT-Wissensanwendern eine Selfservice-Plattform zum Speichern, Freigeben und Verwalten von Inhalten im Zusammenhang mit OT-Incidents bereitzustellen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Wissen > Administration > Knowledge Bases**.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular „Knowledge Base“ aus.
Eine Beschreibung der Feldwerte finden Sie unter [Knowledge Base-Formular](#).
4. Klicken Sie mit der rechten Maustaste auf den Formular-Header, und wählen Sie **Speichern** aus.
5. Zeigen Sie im Abschnitt „Zugehörige Liste“ die Elemente in der folgenden Tabelle an, die sich auf die OT-Wissensdatenbank beziehen, oder konfigurieren Sie sie.

Name	Beschreibung
Wissen	Liste der Wissensartikel, die in dieser Knowledge Base gespeichert sind.
Kann lesen	Liste der Anwenderkriterien, die Lesezugriff gewähren und es einem Anwender, der die Kriterien erfüllt, ermöglichen, Artikel in der OT-Knowledge Base zu lesen.
Kann mitwirken	Liste von Anwenderkriterien, die Beitragenden Zugriff gewähren und es Anwendern, die die Kriterien erfüllen, ermöglichen, die Artikel in der OT-Knowledge Base zu erstellen und zu ändern.
Artikelvorlagen	Wenn Sie das Plugin Wissensmanagement Advanced (com.snc.knowledge_advanced) aktiviert haben, wird die zugehörige Liste Artikelvorlagen angezeigt. Wenn sich Artikelvorlagen in der zugehörigen Liste befinden, können die Artikel in dieser Knowledge Base nur mit einer der aufgeführten Artikelvorlagen erstellt werden. Wenn die zugehörige Liste „Artikelvorlagen“ leer ist, können Artikel mit einer beliebigen Artikelvorlage erstellt werden. Ordnen Sie der Knowledge Base Artikelvorlagen zu, indem Sie Bearbeiten wählen.

Name	Beschreibung
	 Hinweis: Administratoren, Knowledge-Administratoren und Knowledge Manager können die Artikelvorlagen für die Knowledge Base bearbeiten.
Knowledge Base-Kategorien	Liste der Wissenskategorien, die der OT-Knowledge Base zugeordnet sind.  Hinweis: Wenn die Kategorie als inaktiv markiert ist, können Sie ihr keine Artikel zuordnen. Es wirkt sich jedoch nicht auf die vorhandenen Artikel dieser Kategorie aus.

6. Wählen Sie **Absenden**.

Erstellen Sie die Anwenderkriterien für eine OT-Knowledge Base

Erstellen Sie einen Anwenderkriteriendatensatz, um die Anwender zu bestimmen, die eine Operational Technology (OT)-Knowledge Base lesen oder dazu beitragen können.

Vorbereitungen

Erforderliche Rolle: user_criteria_admin

Hinweis:

Um einen Benutzerkriteriendatensatz aus dem Knowledge-Modul zu erstellen, müssen Sie zusätzlich zur Knowledge-Rolle über die Rolle user_criteria_admin verfügen. Weitere Informationen zum Zugriff finden Sie unter [Managing access to knowledge bases and knowledge articles](#) .

Warum und wann dieser Vorgang ausgeführt wird

Verwenden Sie die Anwenderkriterien in Wissensmanagement, um zu bestimmen, ob bestimmte Benutzer auf OT-Knowledge Bases und Wissensartikel zugreifen können. Nachdem Sie einen Benutzerkriteriendatensatz erstellt haben, können Sie ihn einer OT-Knowledge Base zuweisen, um zu steuern, wer eine Knowledge Base und ihre Artikel lesen und dazu beitragen kann. Darüber hinaus können Sie die Anwenderkriterien auf Artekebene zuweisen, um zu steuern, wer sie lesen kann.

Prozedur

1. Navigieren zu **Alle > Wissen > Administration > Anwenderkriterien**.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular „Anwenderkriterien“

Feld	Beschreibung
Name	Eindeutiger Name der Anwenderkriterien.
Anwender	Benutzer, die den Anwenderkriterien entsprechen müssen.
Gruppen	Gruppen, die den Anwenderkriterien entsprechen müssen.

Feld	Beschreibung
Rollen	Rollen, die den Anwenderkriterien entsprechen. i Hinweis: - Da die Auswertung einer Rolle in der Sitzung zwischengespeichert wird, müssen Sie sich bei jeder Änderung der Rolle erneut anmelden. - Anwenderkriterien gelten nicht für Rollen mit erweiterten Berechtigungen.
Erweitert	Option zum Ein- oder Ausblenden der erweiterten Option, die das Feld Skript im Formular „Anwenderkriterien“ enthält.
Skript	Ein Skript zum Definieren zusätzlicher Anwenderkriterien, das „true“ oder „false“ zurückgibt. Dieses Feld ist verfügbar, wenn im Formular „Anwenderkriterien“ die Option Erweitert ausgewählt ist. i Hinweis: - Ein Skript wird in dem Umfang ausgewertet, in dem die Anwenderkriterien erstellt werden. - Die Bewertung eines Skripts wird in der Sitzung zwischengespeichert, sodass Sie sich bei jeder Änderung der Bewertung erneut anmelden müssen. Wenn ein geskriptetes Benutzerkriterium für eine Knowledge Base definiert ist, wird der Benutzerzugriff auf die Knowledge Bases nach jeder Sitzung ausgewertet. Wenn das Skript zu Änderungen führt, nachdem ein Sitzungscache erstellt wurde, wird das Ergebnis in der nächsten Sitzung wirksam. - Verwenden Sie nicht <code>gs.getUser()</code> oder andere Sitzungs-APIs, da sie bei der Verwendung in Diagnosetools Konflikte verursachen. Verwenden Sie die im Skript verfügbare vordefinierte Variable <code>user_id</code>, um die Anwender-ID des Benutzers abzurufen, der zum Auswerten des Skripts verwendet wird. - Skripts werden dynamisch ausgewertet. Daher kann das Einbeziehen von Skripts in Benutzerkriterien die Leistung Ihres Systems beeinträchtigen.
Aktiv	Option zum Aktivieren der Anwenderkriterien.
Unternehmen	Unternehmen, denen der Benutzerdatensatz entsprechen muss.
Standorte	Standorte, denen der Benutzerdatensatz entsprechen muss.
Abteilungen	Abteilungen, denen der Benutzerdatensatz entsprechen muss.
Alle abgleichen	Eine Option, mit der bestimmt wird, ob alle Elemente aus jedem gefüllten Anwenderkriterienfeld übereinstimmen müssen. Wenn diese Option ausgewählt ist, erhalten nur die Benutzer Zugriff, die allen Anwenderkriterien entsprechen. Wenn diese Option deaktiviert ist, muss der Benutzer eines oder mehrere der festgelegten Anwenderkriterien erfüllen, um Zugriff zu erhalten. Standardmäßig ist dieses Kontrollkästchen deaktiviert, sodass alle erfüllten Bedingungen eine Übereinstimmung ergeben.

Feld	Beschreibung
	Betrachten Sie beispielsweise einen Benutzerkriteriendatensatz für die folgenden Bedingungen: ◦ Standorte A oder B ◦ Unternehmen C oder D Wenn Alle abgleichen ausgewählt ist, werden nur die Benutzer abgeglichen, die alle diese Bedingungen erfüllen. Zum Beispiel ein Benutzer mit einem Standort A und einem Unternehmen C. Wenn „Alle abgleichen“ nicht ausgewählt ist, werden Anwender abgeglichen, die eine dieser Bedingungen erfüllen. Zum Beispiel ein Benutzer mit einem Standort B. i Hinweis: Wenn Sie Alle abgleichen auswählen, stellen Sie sicher, dass keine widersprüchlichen Bedingungen erstellt werden, die niemals erfüllt werden können. Wenn beispielsweise alle Benutzer an Standort A für Unternehmen G arbeiten, können die Bedingungen in diesem Beispiel nicht erfüllt werden.

4. Wählen Sie **Absenden**.

Nächste Maßnahme

Jetzt können Sie die Anwenderkriterien einer OT-Knowledge Base zuweisen. Weitere Informationen finden Sie unter [Weisen Sie die Anwenderkriterien einer OT-Knowledge Base zu](#).

Weisen Sie die Anwenderkriterien einer OT-Knowledge Base zu

Weisen Sie die Anwenderkriteriendatensätze einer Knowledge Base Operational Technology (OT) zu, um zu steuern, welche Anwender in der Knowledge Base Wissensartikel erstellen, lesen, schreiben und stilllegen können.

Vorbereitungen

Erforderliche Rolle: knowledge_manager, knowledge_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können einer OT-Knowledge Base Anwenderkriterien zuweisen, um den Lese- oder Mitwirkzugriff zu steuern.

Prozedur

1. Navigieren zu **Alle > Wissen > Administration > Knowledge Bases**.
2. Wählen Sie den OT-Knowledge Base-Datensatz aus, den Sie verwalten möchten.
3. Fügen Sie der OT-Knowledge Base Anwenderkriterien hinzu.
 - a. Wählen Sie je nach Anwenderkriterien, die Sie festlegen möchten, eine oder mehrere der zugehörigen Listen aus.

Zugehörige Liste	Beschreibung
Kann lesen	Benutzer können Wissensartikel in der Knowledge Base lesen.

Zugehörige Liste	Beschreibung
Lesen nicht möglich	Anwender können keine Wissensartikel in der Knowledge Base lesen.
Kann mitwirken	Benutzer können Wissensartikel in einer Knowledge Base erstellen, ändern und stilllegen. Der Mitwirkzugriff auf eine Knowledge Base bietet auch Lesezugriff auf alle Artikel in der Knowledge Base.
Kann nicht mitwirken	Anwender können in der Knowledge Base keine Wissensartikel erstellen, ändern, stilllegen oder lesen.

b. Fügen Sie in der ausgewählten zugehörigen Liste die erforderlichen Anwenderkriterien hinzu.

- Fügen Sie als Benutzer mit der Administratorrolle einen neuen Benutzerkriteriendatensatz hinzu, indem Sie **Neu** auswählen, die erforderlichen Felder angeben und **Absenden** auswählen.
- Fügen Sie als Benutzer mit der Rolle „knowledge_manager“, „knowledge_admin“ oder „admin“ einen vorhandenen Anwenderkriteriendatensatz hinzu, indem Sie **Bearbeiten** auswählen, die erforderlichen Anwenderkriterien aus der Spalte Sammlung in die Spalte Wissen verschieben und **Speichern** wählen.

4. Wählen Sie im Knowledge Base-Formular **Aktualisieren** aus.

Überprüfen Sie den Zugriff auf OT-Knowledge Bases für nicht authentifizierte Anwender

Überprüfen Sie die Knowledge Bases Operational Technology (OT), die für nicht authentifizierte Benutzer zugänglich sind, mithilfe der Einstellungen für die Eigenschaften Anwenderkriterien und `glide.knowman.block_access_with_no_user_criteria`.

Vorbereitungen

Erforderliche Rolle: knowledge_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie nicht authentifizierte Benutzer für eine Knowledge Base einschränken möchten, können Sie die Benutzerkriterien oder die `glide.knowman.block_access_with_no_user_criteria`-Eigenschaftseinstellungen verwenden.

Prozedur

1. Navigieren zu **Alle > Wissen > Administration > Knowledge Bases**.
2. Überprüfen Sie die OT-Knowledge Bases, die für nicht authentifizierte Anwender zugänglich sind.
3. **Wahlweise:** Um nicht authentifizierte Benutzer für eine Knowledge Base mithilfe von Anwenderkriterien einzuschränken, wählen Sie den Knowledge Base-Datensatz aus, und aktualisieren Sie seine Anwenderkriterien.
Weitere Informationen zum Erstellen der Anwenderkriterien finden Sie unter [Erstellen Sie die Anwenderkriterien für eine OT-Knowledge Base](#). Weitere Informationen zum Zuweisen der Anwenderkriterien finden Sie unter [Weisen Sie die Anwenderkriterien einer OT-Knowledge Base zu](#).

- 4. Wahlweise:** Mit den `glide.knowman.block_access_with_no_user_criteria`-Eigenschaftseinstellungen können Sie nicht authentifizierte Anwender für eine Knowledge Base einschränken.
- Navigieren zu **Alle > Wissen > Administration > Eigenschaften**.
 - Legen Sie die Einstellungen für die Eigenschaft `glide.knowman.block_access_with_no_user_criteria` auf „wahr“ fest.
 - Wählen Sie **Speichern**.

Zuweisen von Wissens-Workflows an eine OT-Wissensdatenbank

Sie können jeder Operational Technology (OT)-Knowledge Base unterschiedliche Wissensmanagement -Workflows für die Veröffentlichungs- und Lösungsprozesse zuweisen.

Übersicht über den Knowledge-Workflow

Sie können die Standard-Workflows Wissensmanagement in der folgenden Tabelle für Knowledge Management für operative Technologie verwenden und auf OT-Knowledge Bases anwenden.

Hinweis:

Für die Workflows, für die eine Genehmigung erforderlich ist, können Sie konfigurieren, welche Benutzer durch Bearbeiten der Funktion `getApprovers()` im Skript KBWorkflow genehmigen oder ablehnen können.

Standard-Workflows Wissensmanagement .

Workflow	Beschreibung
Knowledge - Approval Publish	Fordert die Genehmigung von einem Manager der Knowledge Base an. In der Genehmigung befindliche Artikel haben den Status Wird überprüft, bevor sie nach der Genehmigung in den Status Veröffentlicht geändert werden. Wenn sie später veröffentlicht werden sollen, werden sie in den Status „Geplant“ versetzt. Wenn der Manager die Anforderung ablehnt, wird der Workflow abgebrochen, und der Artikel verbleibt im Status Entwurf. Wenn die Option Besitzgruppen aktiviert ist, werden E-Mail-Benachrichtigungen mit einem Link zum Artikel zur Genehmigung an die Mitglieder der Besitzgruppe gesendet. Wenn die Option „Besitzgruppen“ nicht aktiviert ist, werden E-Mail-Benachrichtigungen mit einem Link zum Artikel zur Genehmigung an die Knowledge Base-Manager gesendet. Außerdem wird eine Benachrichtigung an die Autoren oder Überprüfer der Artikel gesendet, um sie darüber zu informieren, dass ihr Artikel genehmigt oder abgelehnt wurde.

Standard-Workflows Wissensmanagement . (Fortsetzung)

Workflow	Beschreibung
	Um die E-Mail-Benachrichtigungen für Genehmigungen zu aktivieren, legen Sie die Eigenschaft <code>glide.knowman.enable_approval_notification</code> auf truefest. Hinweis: Nur der aktive Benutzer erhält die Benachrichtigungen.
Knowledge - Approval Retire	Fordert die Genehmigung eines Managers der Knowledge Base an, bevor der Artikel in den ausgeschiedenen Zustand versetzt wird. Wenn ein Manager die Anforderung ablehnt, wird der Workflow abgebrochen, und der Artikel verbleibt im Status Veröffentlicht. Wenn die Option Besitzgruppen aktiviert ist, werden E-Mail-Benachrichtigungen mit einem Link zum Artikel zur Genehmigung an die Mitglieder der Besitzgruppe gesendet. Wenn die Option „Besitzgruppen“ nicht aktiviert ist, werden E-Mail-Benachrichtigungen mit einem Link zum Artikel zur Genehmigung an die Knowledge Base-Manager gesendet.
Knowledge - Instant Publish	Veröffentlicht einen Entwurfsartikel sofort, ohne dass eine Genehmigung erforderlich ist, oder veröffentlicht ihn am geplanten Veröffentlichungsdatum, wenn er später veröffentlicht werden soll.
Knowledge - Instant Retire	Ein veröffentlichter Artikel wird ohne Genehmigung sofort zurückgezogen.
Knowledge - Publish Knowledge	Subflow, der den Wissensartikel in den Status „ Veröffentlicht “ versetzt. Sie können diesen Subflow verwenden, wenn Sie Ihren eigenen Workflow definieren.
Knowledge - Wissen archivieren	Subflow, der den Wissensartikel in den Status „ Stillgelegt “ versetzt. Sie können diesen Subflow verwenden, wenn Sie Ihren eigenen Workflow definieren.

Automatische Übersetzung

E-Mail-Benachrichtigungen für Genehmigungs-Workflows

Sie können E-Mail-Benachrichtigungen für Genehmigungs-Workflows senden.

- Benachrichtigen Sie genehmigende Personen über die Wissensartikel, die zur Genehmigung eingereicht wurden.
- Benachrichtigen Sie Autoren über den Genehmigungsstatus ihrer Wissensartikel

Um E-Mail-Benachrichtigungen für Genehmigungs-Workflows zu senden, aktivieren Sie die Eigenschaft **Benachrichtigung an Genehmiger und Autoren in Artikelgenehmigungs-Workflow senden** (*glide.knowman.enable_approval_notification*). Ab Release New York ist diese Eigenschaft standardmäßig aktiviert. Bestandskunden mit Release-Versionen vor Release New York können diese Eigenschaft zum Senden von E-Mail-Benachrichtigungen aktivieren. Deaktivieren Sie alle anwenderdefinierten Benachrichtigungen für Artikelgenehmigungen, bevor Sie diese Eigenschaft aktivieren. Wenn die Eigenschaft *glide.knowman.enable_approval_notification* nicht verfügbar ist, kann ein Administrator sie erstellen und ihren Wert auf „true“ festlegen. Weitere Informationen finden Sie unter [Knowledge Management properties](#) .

Die Eigenschaft Wissensmanagement für eine Knowledge Base Operational Technology wird überprüft

Als Administrator können Sie das Aussehen und die Funktionen von Operational Technology (OT)-Knowledge Bases mit den Wissensmanagement -Eigenschaften konfigurieren.

Sie können auf die Eigenschaften Wissensmanagement von zugreifen, indem Sie zu navigieren **Alle > Wissen > Administration > Eigenschaften**.

Verwenden Sie die in der folgenden Tabelle aufgeführte Eigenschaft, um zu steuern, welche Rollen unvollständige oder ungenaue Artikel in Knowledge Bases kennzeichnen können.

Eigenschaft „Glide.knowman.show_flag.roles“.

Eigenschaft	Beschreibung
Liste der Rollen (kommagetrennt), die unvollständige/falsche Artikel kennzeichnen können (<i>glide.knowman.show_flag.roles</i>)	Geben Sie die Rollennamen genau so ein, wie sie in angezeigt werden Anwenderadministration > Rollen. Wenn die beiden Eigenschaften Artikelbewertungsabschnitt anzeigen und „Artikel kennzeichnen“-Option anzeigen ausgewählt sind, sehen Anwender mit den in dieser Eigenschaft aufgeführten Rollen die Option Artikel kennzeichnen in der Artikelansicht. Alle in dieser Eigenschaft aufgeführten Rollen müssen auch in der Liste der Rollen, die die Bewertungsabschnittseigenschaft eines Artikels anzeigen können, aufgeführt sein.

Weitere Informationen zu den anderen verfügbaren Wissensmanagement -Eigenschaften finden Sie unter [Knowledge Management properties](#) .

Knowledge Management für operative Technologie verwenden

Nachdem Sie alle erforderlichen Setupaufgaben für Knowledge Management für operative Technologie abgeschlossen haben, können Sie mit der Verwaltung von Wissensartikeln beginnen, die sich auf Incidents Operational Technology (OT) beziehen.

Knowledge Management für operative Technologie – Übersicht

Mit Knowledge Management für operative Technologie können Sie Wissensartikel je nach Bedarf Ihres Teams erstellen, bearbeiten und stilllegen. Bei Verwendung mit der Anwendung

Incident-Management für operative Technologie können Sie Artikel durchsuchen, die sich auf einen Incident beziehen, und Artikel aus einem Incident erstellen.

Die folgenden Beispiele zeigen, wie Knowledge Management für operative Technologie auf Ihr Team angewendet wird:

- Ein OT-Ingenieur mit mehrjähriger Erfahrung möchte sein Wissen über OT-Geräte an einem Ort für Guide Worker und Nachfolgetechniker erfassen.
- Außendienstmitarbeiter und Techniker, die für den Betrieb des Produktionsprozesses verantwortlich sind, haben ein Problem in der Produktionsanlage festgestellt und benötigen einen Wissensartikel, in dem die Behebung erläutert wird.

Basisprozess Knowledge Management für operative Technologie

Im Folgenden Workflow wird der grundlegende Prozess für Knowledge Management für operative Technologie beschrieben.

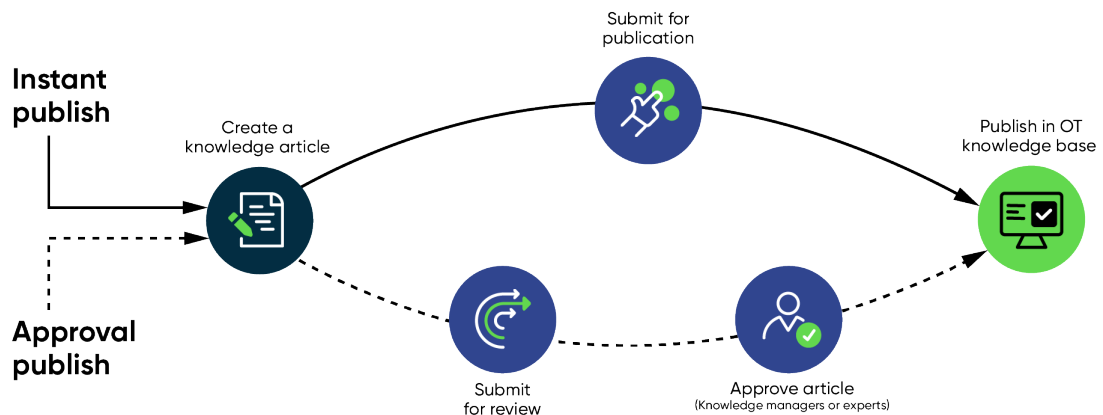
Grundlegender OT-Wissens-Workflow



Veröffentlichen Sie einen Wissensartikel

Im Folgenden Workflow wird beschrieben, wie ein Wissensartikel mit Genehmigung von (Veröffentlichung genehmigen) und ohne Genehmigung (Sofortveröffentlichung) erstellt und veröffentlicht wird.

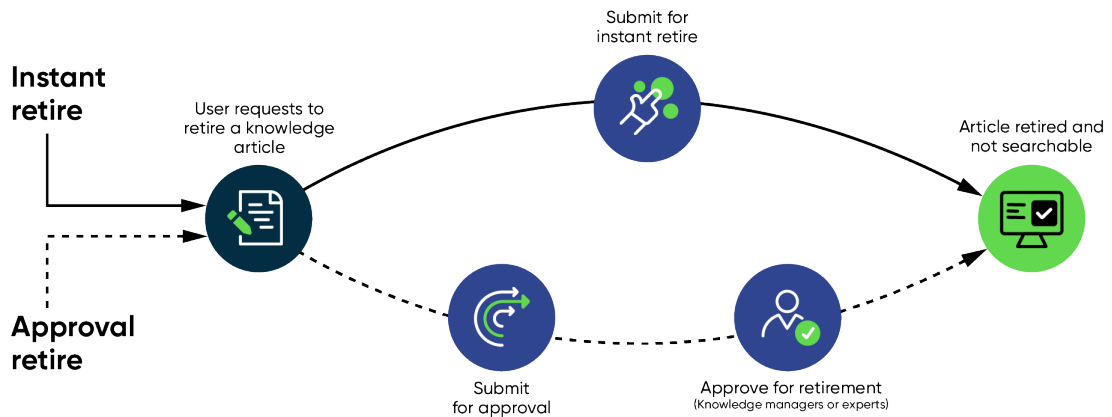
Workflow veröffentlichen



Einen Wissensartikel stilllegen

Im Folgenden Workflow wird beschrieben, wie ein Wissensartikel sowohl mit Genehmigung von (Stilllegung genehmigen) als auch ohne Genehmigung von (Sofortige Stilllegung) stillgelegt wird. Mit dem Workflow „Sofort stilllegen“ können Sie Artikel ohne Genehmigung sofort stilllegen. Der Workflow „Genehmigungslöschung“ sendet eine Genehmigungsanforderung an Knowledge Manager oder Experten, um sicherzustellen, dass das Löschen des Artikels erforderlich ist.

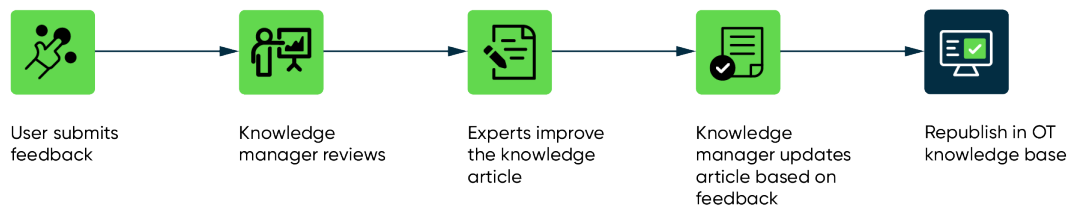
Workflow deaktivieren



Überprüfen und genehmigen Sie Änderungen an einem Wissensartikel

Im Folgenden Workflow wird beschrieben, wie ein vorhandener Wissensartikel mit Benutzerfeedback aktualisiert wird.

Workflow für Benutzerfeedback



Wissensartikel

Wissensartikel enthalten Informationen zu Arbeitsplatzaktualisierungen, Selbsthilfe, Schritten zur Problembehandlung und andere Informationen, auf die Ihr OT-Team zugreifen muss. Sie können beispielsweise die folgenden Wissensartikel für die folgenden Fälle erstellen:

- Eine Vorlage für standardmäßige Betriebsverfahren, die in Ihrer gesamten Organisation verwendet wird.
- Während eines Incidents gelernte Lektionen.
- Ein Bild, das die verschiedenen Produktionsmaterialien mit Anmerkungen versehen

Sie können die Wissensartikel in Industriell Arbeitsbereich wie folgt anzeigen:

- Unter dem Knowledge-Modul in der Listenansicht Industriell Arbeitsbereich.
- Im Agent Assist-Fenster, wenn Sie einen OT-Incident öffnen.
- Verwendung der globalen Suchfunktion im Header Industriell Arbeitsbereich.

Unter dem Wissensmodul in der Listenansicht Industriell Arbeitsbereich können Sie Wissensartikel in den folgenden Listen anzeigen:

Hinweis:

Ihnen muss die Knowledge-Rolle zugewiesen sein, um diese Listenmodule in Industriell Arbeitsbereich anzuzeigen.

Ihre unveröffentlichten Artikel

Die von Ihnen erstellten Artikel, die noch nicht in der OT-Knowledge Base veröffentlicht wurden.

Ihre veröffentlichten Artikel

Die von Ihnen erstellten Artikel, die in der OT-Knowledge Base veröffentlicht werden.

Alle Artikel

Alle Artikel, die in der OT-Knowledge Base verfügbar sind.

Erstellen Sie einen Wissensartikel aus einem OT-Incident-Datensatz

Erstellen Sie einen Wissensartikel, um Informationen aufzuzeichnen und zu speichern, die sich auf einen Operational Technology (OT)-Incident und seine Lösung beziehen.

Vorbereitungen

Erforderliche Rolle: sn_ot_incident_write

Hinweis:

Sie benötigen außerdem den **Zugriff** auf mindestens eine Knowledge Base. Weitere Informationen finden Sie unter [Erstellen Sie eine OT-Knowledge Base](#).

Warum und wann dieser Vorgang ausgeführt wird

Durch das Erstellen eines Wissensartikels direkt aus einem Incident-Datensatz wird sichergestellt, dass der Wissensartikel mit dem richtigen Incident verknüpft ist, um kontextbezogene Informationen zu erhalten. Der Wissensartikel kann Ihrem Team auch helfen, ähnliche Incidents in Zukunft zu lösen, wenn er die richtigen Verfahren, Herausforderungen und Lösungen enthält.

Prozedur

1. Navigieren zu **Alle > Industrial Workspace**.
2. Öffnen Sie in der Listenansicht unter dem Modul OT Incident eine der verfügbaren Listen.
3. Wählen Sie den OT-Incident-Datensatz aus, für den Sie einen Wissensartikel erstellen möchten.
4. Wählen Sie das Symbol **Weitere Aktionen** (), um das Menü zu erweitern.

5. Wählen Sie **Knowledge erstellen**

Save

Create OT Change

Assign to me

...

Create Incident Task

Create Knowledge

Create Problem

aus.

i Hinweis:

Sie müssen den Status des Incident-Datensatzes auf **Gelöst** setzen, um die Schaltfläche „**Wissen erstellen**“ anzuzeigen.

6. Füllen Sie die Felder des Formulars aus.

Formular „Wissensartikel“.

Feld	Beschreibung
Knowledge Base	Knowledge Base, in die der Wissensartikel aufgenommen werden soll. i Hinweis: Wenn Sie die Sichtbarkeit der OT-Knowledge Base richtig konfiguriert haben, können OT-Anwender die Knowledge Base in dieser Referenzliste finden.
Kategorie	Klassifizierung des Wissensartikels.
Kurzbeschreibung	Kurze Beschreibung der Incident-Lösung, die als Titel des Wissensartikels verwendet wird.
Artikeltext	Inhalt des Wissensartikels, der Verfahren, Herausforderungen und Lösungen für den Incident beschreibt.
Gültig bis	Datum, bis zu dem der Wissensartikel gültig ist.

7. Wählen Sie **Speichern**.

Der Wissensartikel wird als Entwurf gespeichert und an den übergeordneten OT-Incident angehängt.

8. Wählen Sie **Veröffentlichen** aus.

Ergebnisse

Der Wissensartikel wird jetzt in Ihrer OT-Knowledge Base veröffentlicht. Um den Wissensartikel anzuzeigen, öffnen Sie die zugehörige Liste Angehängtes Wissen im Incident-Datensatz.

Hinweis:

Wenn Sie das **Workflow-Feld Veröffentlichen** in Ihrer OT-Knowledge Base auf **Wissen – Genehmigungsveröffentlichung** festlegen, muss der Artikel vor der Veröffentlichung genehmigt werden.

Erstellen Sie einen Wissensartikel in Industriell Arbeitsbereich

Erstellen Sie einen Wissensartikel in Industriell Arbeitsbereich, um den Inhalt eines Artikels auf die Anforderungen und Lösungen abzustimmen, die nicht in direktem Zusammenhang mit einem Operational Technology (OT)-Incident stehen.

Vorbereitungen

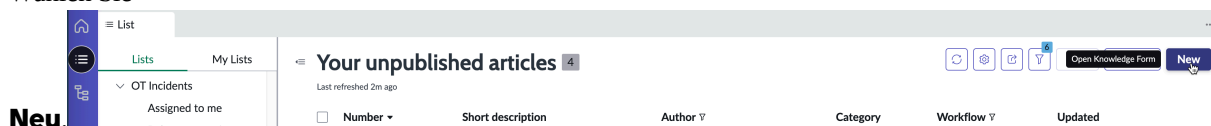
Erforderliche Rolle: knowledge

Hinweis:

Sie benötigen außerdem den **Zugriff** auf mindestens eine Knowledge Base. Weitere Informationen finden Sie unter [Erstellen Sie eine OT-Knowledge Base](#).

Prozedur

1. Navigieren zu **Alle > Industrial Workspace**.
2. Öffnen Sie in der Listenansicht unter dem Wissensmodul eine der verfügbaren Listen.
3. Wählen Sie



4. Füllen Sie die Felder des Formulars aus.

Formular „Wissensartikel“.

Feld	Beschreibung
Knowledge Base	Knowledge Base, in die der Wissensartikel aufgenommen werden soll. Hinweis: Wenn Sie die Sichtbarkeit der OT-Knowledge Base richtig konfiguriert haben, können OT-Anwender die Knowledge Base in dieser Referenzliste finden.
Kategorie	Klassifizierung des Wissensartikels.
Kurzbeschreibung	Kurze Beschreibung der Incident-Lösung, die als Titel des Wissensartikels verwendet wird.
Artikeltext	Inhalt des Wissensartikels, der Verfahren, Herausforderungen und Lösungen für den Incident beschreibt.
Gültig bis	Datum, bis zu dem der Wissensartikel gültig ist.

5. Wählen Sie **Speichern**.

Der Wissensartikel wird als Entwurf gespeichert und an den übergeordneten OT-Incident angehängt.

6. Wählen Sie **Veröffentlichen** aus.

Ergebnisse

Der Wissensartikel wird jetzt in Ihrer OT-Knowledge Base veröffentlicht.

i Hinweis:

Wenn Sie das **Workflow-Feld Veröffentlichen** in Ihrer OT-Knowledge Base auf **Wissen – Genehmigungsveröffentlichung** festlegen, muss der Artikel vor der Veröffentlichung genehmigt werden.

Melden Sie eine Wissenslücke aus einem OT-Incident-Datensatz

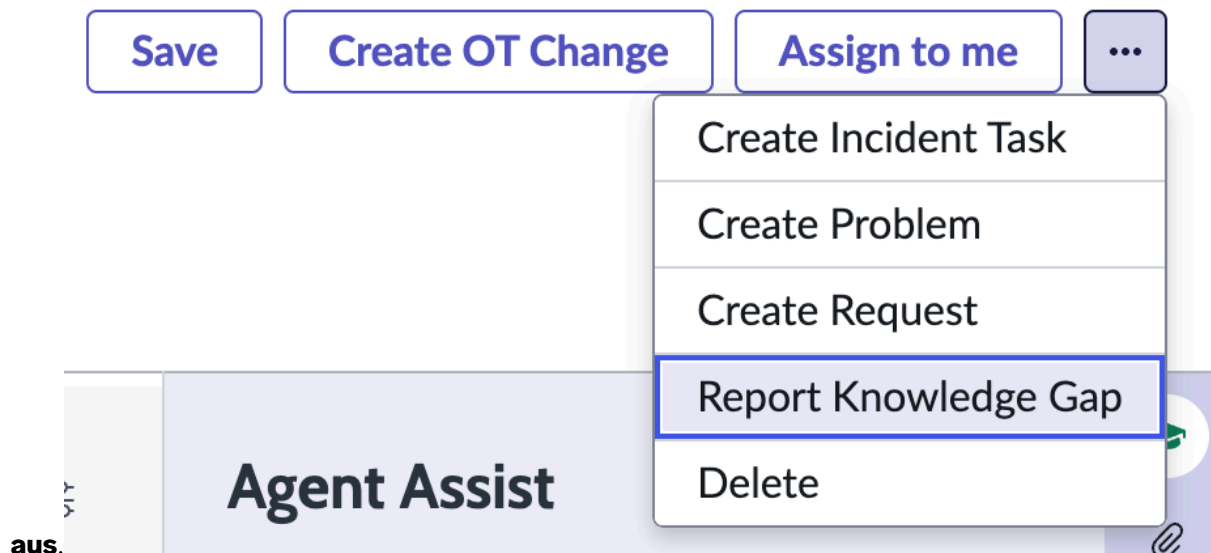
Melden Sie eine Wissenslücke aus einem Operational Technology (OT)-Incident, wenn Sie keine relevanten Wissensartikel zum Incident finden können.

Vorbereitungen

Erforderliche Rolle: sn_ot_incident_read

Prozedur

1. Navigieren zu **Alle > Industrial Workspace**.
2. Öffnen Sie in der Listenansicht unter dem Modul OT Incident eine der verfügbaren Listen.
3. Wählen Sie den Incident-Datensatz aus, für den Sie eine Wissenslücke melden möchten.
4. Wählen Sie das Symbol **Weitere Aktionen** (), um das Menü zu erweitern.
5. Wählen Sie **Wissenslücke melden**



6. Füllen Sie im Formular das Feld **Beschreibung** mit einer Zusammenfassung der Wissenslücke aus.

i Hinweis:

Das Feld **Thema** wird automatisch mit dem Namen des incident-Datensatzes ausgefüllt. Bei Bedarf können Sie dieses Feld ändern.

7. Wählen Sie **Absenden**.

Ergebnisse

Die Wissenslücke wird gemeldet, und eine Feedback-Aufgabe wird erstellt.

Nächste Maßnahme

Sie können die Feedback-Aufgabe unter der zugehörigen Liste „Wissenslücken“ im Incident-Datensatz anzeigen.

Informationen zum Zuweisen von Feedbackaufgaben an den richtigen Benutzer oder die richtige Benutzergruppe finden Sie unter [Weisen Sie Feedbackaufgaben zu](#).

Genehmigen Sie Anforderungen zum Veröffentlichen oder Löschen eines Wissensartikels

Genehmigen Sie Anforderungen zum Veröffentlichen oder Löschen eines Wissensartikels, um sicherzustellen, dass die Knowledge Base auf dem neuesten Stand ist.

Vorbereitungen

Erforderliche Rolle: knowledge_manager

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie als Manager einer OT-Knowledge Base „Empfangen“ zugewiesen sind, können Sie Genehmigungsanforderungen für die Veröffentlichung und Löschung von Artikeln erhalten, die zur Knowledge Base gehören.

Prozedur

1. Öffnen Sie die E-Mail-Benachrichtigung bezüglich der Genehmigungsanforderung.
2. Wählen Sie den Link in der E-Mail aus, um die Anforderung zu öffnen.
3. Sie können die Anforderung genehmigen oder ablehnen.
4. **Wahlweise:** Falls abgelehnt, hinterlassen Sie einen Kommentar, in dem erläutert wird, warum die Artikelanforderung abgelehnt wurde.

Ergebnisse

Der Benutzer, der die Genehmigungsanforderung erstellt hat, wird per E-Mail benachrichtigt.

Weisen Sie Feedbackaufgaben zu

Weisen Sie einem Anwender Feedback-Aufgaben zu, um sicherzustellen, dass die Feedback-Aufgabe behandelt und der zugehörige Wissensartikel aktualisiert wird.

Vorbereitungen

Erforderliche Rolle: knowledge_manager

Prozedur

1. Navigieren zu **Alle > Industrial Workspace**.
2. Öffnen Sie in der Listenansicht unter dem Wissensmodul die Liste Nicht zugewiesene OT-Wissenslücken.
3. Wählen Sie die Feedbackaufgabe aus, die Sie einem Anwender oder einer Zuweisungsgruppe zuweisen möchten.
4. Fügen Sie im Feld **Zugewiesen** an den Benutzer hinzu, dem Sie die Feedbackaufgabe zuweisen möchten.
5. Wählen Sie **Speichern**.

Ergebnisse

Der zugewiesene Benutzer kann die Feedbackaufgabe jetzt in der Liste „Meine Feedbackaufgaben“ in der Listenansicht des Wissensmoduls anzeigen.

Um andere zugewiesene Feedbackaufgaben anzuzeigen, wählen Sie die Liste Zugewiesene Feedbackaufgaben in der Listenansicht des Wissensmoduls in Industriell Arbeitsbereich aus.

Um die nicht zugewiesenen OT-Wissenslücken anzuzeigen, wählen Sie die Liste Nicht zugewiesene OT-Wissenslücken in der Ansicht Wissensmodulliste in Industriell Arbeitsbereich aus.

Informationen finden Sie in den zugehörigen Wissensartikeln für einen OT-Incident

Suchen Sie nach Informationen in den zugehörigen Wissensartikeln, die an einen Incident-Datensatz Operational Technology (OT) für frühere Lösungen angehängt sind, die möglicherweise zutreffend sind.

Vorbereitungen

Erforderliche Rolle: sn_ot_incident_read

Hinweis:

Sie müssen über die Rolle sn_ot_incident_read und Lesezugriff auf die Knowledge Base verfügen, die die Artikel enthält, die dem Kontext dieses Incidents entsprechen.

Prozedur

1. Navigieren zu **Alle > Industrial Workspace**.
2. Öffnen Sie in der Listenansicht unter dem Modul OT Incident eine verfügbare Liste.
3. Wählen Sie den Incident-Datensatz aus, den Sie anzeigen möchten.
4. Wählen Sie im Incident-Datensatz die Option **Agent Assist**- Schaltfläche  um das Agent Assist-Fenster zu öffnen, falls es noch nicht geöffnet ist.
5. Um den vollständigen Wissensartikel anzuzeigen, wählen Sie die Schaltfläche **Weitere Aktionen** .
6. Wählen Sie **Vollständige Ansicht** aus.
7. **Wahlweise:** Um den Wissensartikel an den geöffneten Incident-Datensatz anzuhängen, wählen Sie **Anfügen** im Fenster Agent Assist aus.
8. **Wahlweise:** Um den Wissensartikel zu kennzeichnen, wählen Sie im Fenster „Agent Assist“ die Option **Kennzeichnung** aus.
9. **Wahlweise:** Um den Wissensartikel als hilfreich zu markieren, wählen Sie die Schaltfläche **Weitere Aktionen**  und wählen Sie **Hilfreich**.

Knowledge Management für operative Technologie-Referenz

Referenzthemen enthalten zusätzliche Informationen zu Knowledge Management für operative Technologie.

Knowledge Management für operative Technologie Rollen

Sie können Ihren Knowledge Management für operative Technologie -Benutzern [Wissensmanagement -Rollen zuweisen.

In der folgenden Tabelle sind die Wissensmanagement -Rollen aufgeführt, die Sie Ihren Benutzern zuweisen können, damit sie auf die Fähigkeiten Knowledge Management für operative Technologie von zugreifen können.

Wissensmanagement Rollen, die für gelten Knowledge Management für operative Technologie

Rolle	Beschreibung
Wissen	Die Knowledge-Rolle kann zur Standard-Knowledge Base beitragen und auf das Knowledge-Anwendungsmenü zugreifen. Die Wissensrolle ist eine Erfüllerrolle und keine Rolle für anfordernde Personen. i Hinweis: Anfordernde Personen können die Wissensartikel anzeigen, kommentieren und Feedback dazu geben. Eine anfordernde Person kann jedoch keine Artikel erstellen oder bearbeiten.
knowledge_manager	Der Knowledge Manager kann Verwaltungsfunktionen für die von ihm verwalteten Knowledge Bases ausführen, z. B. das Definieren der Kategorien, das Anheften der wichtigen Artikel und das Genehmigen der Änderungen an den Artikeln. Benutzer, die als Manager einer Knowledge Base ausgewählt wurden, erhalten diese Rolle automatisch. i Hinweis: Die Wissensrolle ist eine untergeordnete Rolle.
knowledge_admin	Der Knowledge-Administrator kann alle administrativen Aufgaben ausführen, die mit der Wartung des Wissensmanagement -Systems verbunden sind. i Hinweis: • Ein als Wissensadministrator ausgewählter Benutzer kann Änderungen an allen Knowledge Bases mit Ausnahme der bereichsbezogenen Knowledge Base vornehmen. • Die Wissensrolle ist eine untergeordnete Rolle.

Knowledge Base-Formular

Füllen Sie beim Erstellen einer neuen Knowledge Base die folgenden Formularfelder aus.

Knowledge Base-Formularfelder

Feld	Beschreibung
Titel	Eindeutiger Name für die OT-Knowledge Base.

Knowledge Base-Formularfelder (Fortsetzung)

Feld	Beschreibung
Artikelgültigkeit	Anzahl der Standardtage, die Artikel nach dem Erstellungsdatum gültig sind.
Symbol	Bild, das eine visuelle Referenz zur Beschreibung der OT-Knowledge Base bietet. Das Bild wird neben allen Artikeln aus dieser Knowledge Base auf der Suchergebnisseite für den Artikel angezeigt.
Kommentar deaktivieren	Option zum Deaktivieren des Kommentars. Wenn diese Option ausgewählt ist, können Anwender Artikel in der OT-Knowledge Base nicht kommentieren.
Vorschlag deaktivieren	Option zum Deaktivieren von Bearbeitungsvorschlägen. Wenn diese Option ausgewählt ist, können Anwender keine Bearbeitungen von Artikeln in der OT-Knowledge Base vorschlagen.
Kategoriebearbeitungen deaktivieren	Option zum Deaktivieren der Bearbeitung von OT-Wissenskategorien. Wenn diese Option ausgewählt ist, können nur OT-Wissensmanager die Wissenskategorien für die OT-Knowledge Base hinzufügen oder bearbeiten.
Bewertung deaktivieren	Option zum Deaktivieren der Bewertung für Artikel. Wenn diese Option ausgewählt ist, können Anwender den Artikel in der OT-Knowledge Base nicht bewerten.
„Als hilfreich markieren“ deaktivieren	Option zum Deaktivieren der Markierung als hilfreich. Wenn diese Option ausgewählt ist, kann der Anwender keinen Artikel in der OT-Knowledge Base als hilfreich markieren.
Blöcke aktivieren	Option zum Aktivieren der Funktion „Wissensblöcke“. Wenn diese Option ausgewählt ist, können Sie Wissensblöcke erstellen, die Wissensartikeln in der OT-Knowledge Base hinzugefügt werden.
Prüfliste	Prüfliste zur Bewertung der Qualität von Artikeln in der OT-Knowledge Base.
Anwendung	Anwendungsbereich der OT-Knowledge Base.
Besitzer	Anwender, der für die OT-Knowledge Base verantwortlich ist. Ein Eigentümer der Knowledge Base kann andere Rollen zur Knowledge Base zuweisen.
Manager	Benutzer, die administrative Funktionen in der OT-Knowledge Base ausführen.
Workflow veröffentlichen	Workflow zum Veröffentlichen der Artikel in der Knowledge Base:

Knowledge Base-Formularfelder (Fortsetzung)

Feld	Beschreibung
	• Wissen – Sofort veröffentlichen: Veröffentlicht Artikel in der Knowledge Base, ohne dass eine Genehmigung erforderlich ist. • Knowledge - Genehmigungsveröffentlichung: Fordert eine Genehmigung vom Manager der Knowledge Base an, bevor die Artikel in den veröffentlichten Status versetzt werden.
Workflow deaktivieren	Workflow zum Deaktivieren der Artikel in der OT-Knowledge Base: • Wissen – Sofort stilllegen: Legt die Artikel in der Knowledge Base still, ohne dass eine Genehmigung erforderlich ist. • Wissen – Genehmigung stilllegen: Fordert eine Genehmigung vom Manager der Knowledge Base an, bevor die Artikel in den stillgelegten Zustand versetzt werden.
Aktiv	Option, um anzugeben, dass die OT-Knowledge Base aktiv ist. Wenn diese Option nicht ausgewählt ist, können nur Benutzer mit der Rolle „admin“ oder Wissensadministratoren die Artikel erstellen, suchen oder anzeigen.
Beschreibung	
Standardmäßige Wissensfeldwerte einstellen	Standardkonfigurationseinstellungen für die OT-Knowledge Base.
Zugehörige Produkte	Liste der Produkte, die sich auf den Inhalt der OT-Knowledge Base beziehen.

Zugehörige Informationen

Weitere Informationen zu OT-Erweiterungsklassen und zugehörigen Anwendungen.

Übersicht über Erweiterungsklassen

Die Erweiterungsklassen helfen Ihnen zu verstehen, wie Operational Technology-Management mit Configuration Management Database (CMDB) funktioniert.

[Operational Technology \(OT\) extension classes](#)

CMDB aktualisiert Klassen für OT.

Zugehörige Anwendungen

[Knowledge Management](#)

Die Anwendung Wissensmanagement ermöglicht die gemeinsame Nutzung von Informationen in Knowledge Bases. Diese Knowledge Bases enthalten Artikel, die Benutzer mit Informationen wie Selbsthilfe, Fehlerbehebung und Aufgabenlösung versorgen.

Incident-Management für operative Technologie

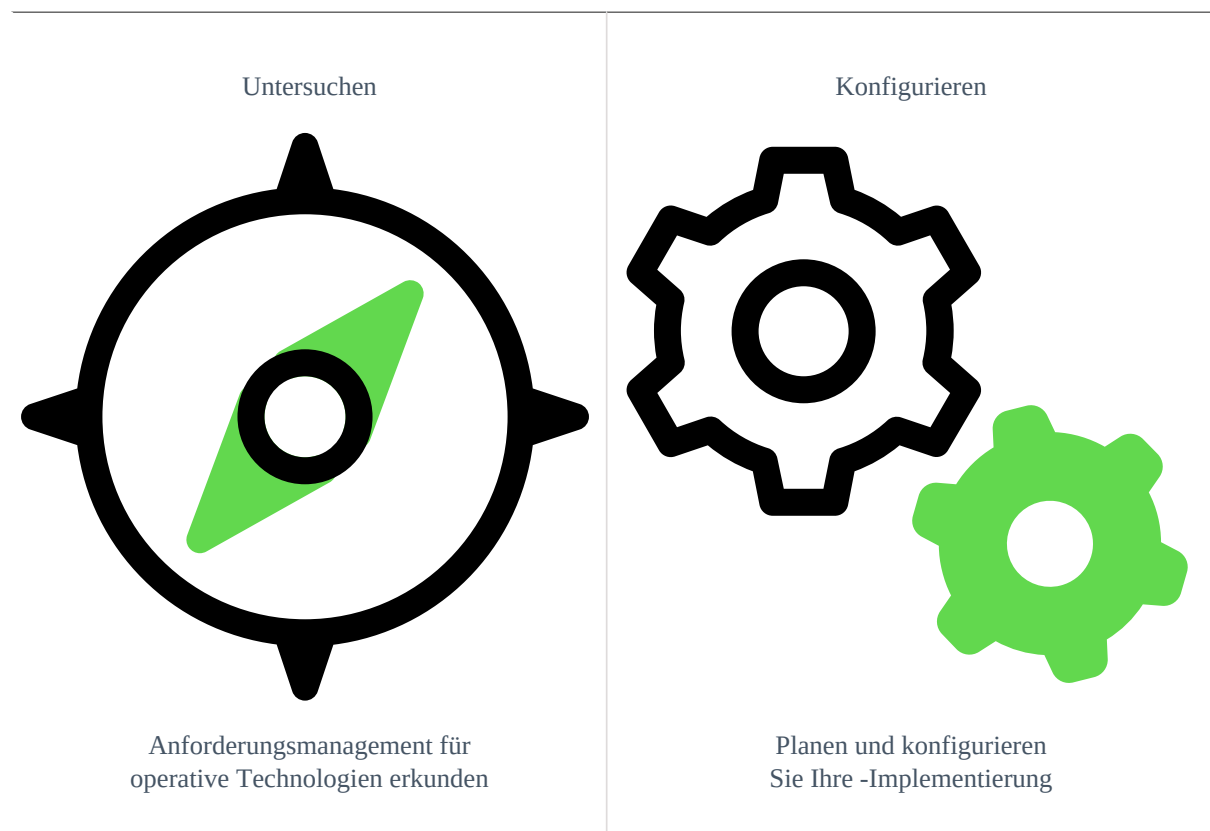
Mit der Anwendung Incident-Management für operative Technologie können Hersteller OT-Geräte-Incidents vom Zeitpunkt des Öffnens des incident bis zu seinem Abschluss verwalten.

IT Service Management

Bei Integration mit Knowledge Management für operative Technologie können Techniker mit der Anwendung ServiceNow IT Service Management Probleme mit OT-Geräten und Produktionsprozessen schnell lösen.

Anforderungsmanagement für operative Technologie

Anforderungsmanagement für operative Technologie Mit können Sie Katalogelemente anfordern und basierend auf den definierten Flows erfüllen.



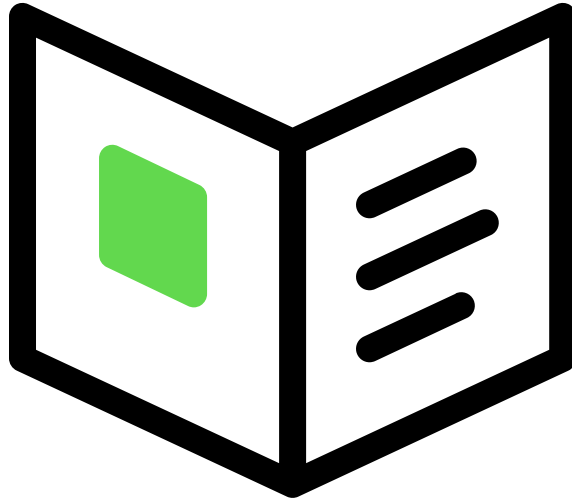
Automatische Übersetzung

Verwenden



Anforderungsmanagement für
operative Technologien verwenden

Referenz



Erhalten Sie Details zu zugehörigen
Informationen und Anwendungen.

Automatische Übersetzung

Anforderungsmanagement für operative Technologie erkunden

Mit Anforderungsmanagement für operative Technologie können Sie auf den Servicekatalog Operational Technology (OT) zugreifen, um OT-Katalogelemente anzufordern und basierend auf den definierten Flows zu erfüllen. OT-Mitarbeiter können dann eine OT-Anforderung aus einem Katalogelement erstellen und übermitteln, was zu einer konsistenten Experience beiträgt und funktionsübergreifende Anforderungen erleichtert.

Anforderungsmanagement für operative Technologie – Übersicht

Sehen Sie sich die Übersicht über die -Produktsuite Operational Technology Service Management an, um mehr über Anforderungsmanagement für operative Technologie zu erfahren.

[https://player.vimeo.com/video/1019801515?](https://player.vimeo.com/video/1019801515?badge=0&autoplay=0&player_id=0&app_id=58479)

[badge=0&autoplay=0&player_id=0&app_id=58479](https://player.vimeo.com/video/1019801515?badge=0&autoplay=0&player_id=0&app_id=58479)

Anforderungsmanagement für operative Technologie – Vorteile

Mit Anforderungsmanagement für operative Technologie können Sie die folgenden Vorteile auf Ihr OT-System anwenden und Ihr Team bei der Verwaltung von Kataloganforderungen unterstützen:

- Bietet eine zentrale Ansicht für die effiziente Verwaltung mehrerer Kataloganforderungen ☑
- Fördert Transparenz, beschleunigt Anforderungsprozesse und minimiert Verzögerungen durch automatische Benachrichtigungen und Genehmigungen.
- Verwaltet das Produkt- und Servicemenü, das Sie zum Erstellen und Aktualisieren von Kataloganforderungen verwenden können.

Anforderungsmanagement für operative Technologie wird auf Ihr OT-System angewendet

Sie können Anforderungsmanagement für operative Technologie auf Ihr Operational Technology (OT)-System anwenden, um anderen Benutzern das Erstellen und Senden von OT-Anforderungen für OT-Produkte und -Services zu ermöglichen.

Anforderungsmanagement für operative Technologie – Übersicht

Anforderungsmanagement für operative Technologie Mit können Sie Katalogelemente anfordern und basierend auf den definierten Flows erfüllen. OT-Mitarbeiter können dann eine Anforderung im OT-Servicekatalog erstellen und das Katalogelement auswählen, das ihren Anforderungen am besten entspricht.

Anwendungsfälle

In der folgenden Tabelle werden verschiedene OT-Personas und wie sie Anforderungsmanagement für operative Technologie verwenden können.

Anwendungsfälle für Operational Technology Request Management

Persona	Beschreibung
OT-Ingenieur	Kann Anforderungsmanagement für operative Technologie verwenden, um OT-Anforderungen für verschiedene OT-Produkte und -Services an einem Ort zu archivieren und zu verwalten. Einige Beispiele für Katalogelemente, die angefordert werden können, sind Remotezugriff von Drittparteien, neue OT-PCs, neue OT-Geräte und neue OT-Hostverbindungen.
Werksleiter oder Vorgesetzter	Kann Anforderungsmanagement für operative Technologie verwenden, um mit dem richtigen Team zu interagieren und einen in der Produktionsumgebung gemeldeten Incident zu beheben.

Anforderungsmanagement für operative Technologie konfigurieren

Konfigurieren Sie Anforderungsmanagement für operative Technologie, um die Datengrundlage für die Lösung Operational Technology (OT) zu erstellen.

Wenn Sie über die Administratorrolle verfügen, können Sie sich von Geführtes Setup durch die Einrichtung von Anforderungsmanagement für operative Technologieführen lassen. Geführtes Setup ist ein Tool, das bei der Konfiguration von Anwendungen oder Fähigkeiten hilft. Er ordnet die Konfigurationsaktivitäten in Kategorien. Diese Kategorien enthalten Informationen zu den Setup-Aufgaben, die Schritte zum Abschließen jeder Aufgabe und die Links zu den Seiten in Ihrer Instanz, auf denen Sie die Konfiguration durchführen. Außerdem werden Links zu nützlichen Hilfeinhalten bereitgestellt.

Um auf Geführtes Setup zuzugreifen, navigieren Sie zu **Industrial Workspace-Administrator > Geführtes Setup**.

In der folgenden Tabelle sind die Geführtes Setup -Aufgaben und ihre Zwecke für Anforderungsmanagement für operative Technologie aufgeführt.

Hinweis:

Anforderungsmanagement für operative Technologie ist im Lieferumfang von Industrial Workspace Common enthalten. Es sind keine zusätzlichen Plugins erforderlich.

Die folgende Tabelle zeigt die Aufgaben, die Ihre Benutzer für eine erfolgreiche Einrichtung und Konfiguration ausführen müssen.

Anforderungsmanagement für operative Technologie-Setupaufgaben

Aufgabe	Zweck
Laden Sie die Demodaten.	Um die Demodaten für Anforderungsmanagement für operative Technologie zu laden, müssen Sie die Demodaten des Plugins „Industrial Workspace Common“ laden. Führen Sie die folgenden Schritte aus, um die Demodaten zu laden. 1. Navigieren zu Alle > Systemdefinition > Plugins. 2. Suchen Sie in der Suchleiste nach dem Plugin „Industrial Workspace Common“. 3. Sobald die Ergebnisse geladen sind, wählen Sie die Registerkarte Installiert, und öffnen Sie die Seite Industrial Workspace Common. 4. Wählen Sie unter Schnellaktionen die Option Demodaten laden aus.
Weisen Sie Anforderungsmanagement für operative Technologie Rollen zu.	Weist Rollen zu, um die für jeden Benutzer verfügbaren Aktionen zu steuern.
Erstellen Sie mit dem Katalog-Generator Katalogelemente für Ihren OT-Servicekatalog.	Erstellen Sie mit dem Katalog-Generator Katalogelemente für den OT-Servicekatalog, damit andere Anwender ihre OT-Anforderungen übermitteln und das Katalogelement auswählen können, das ihren Anforderungen am besten entspricht.
Fügen Sie Katalogelementkategorien für die Katalogelemente hinzu, die Sie im OT-Servicekatalog erstellen.	Wählen Sie verschiedene Kategorien für die Katalogelemente aus, die Sie im OT-Servicekatalog erstellen, um OT-Katalogelemente in logischen Gruppen zu organisieren.
Erstellen Sie einen Erfüllungs-Flow für eine OT-Anforderung in Workflow-Studio.	Erstellen Sie nach Bedarf einen Erfüllungs-Flow mit Katalogaufgaben in Workflow-Studio für Ihr Katalogelement, um eine OT-Anforderung zu erfüllen.

Weisen Sie Ihren Anforderungsmanagement für operative Technologie -Benutzern Rollen zu

Weisen Sie Ihren Anwendern Rollen zu, damit Sie ihren Zugriff auf die Funktionen, Fähigkeiten und Daten von Anforderungsmanagement für operative Technologie steuern können.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Weitere Informationen zu den Anforderungsmanagement für operative Technologie -Rollen, die Sie Ihren Benutzern zuweisen können, finden Sie unter [Mit Anforderungsmanagement für operative Technologie installierte Komponenten](#).

Prozedur

Weisen Sie Benutzern und Gruppen mit der Benutzerverwaltungsfunktion Now Platform Rollen zu.

Katalogelementkategorien

Sie können verschiedene Kategorien für die Katalogelemente auswählen, die Sie im Servicekatalog Operational Technology (OT) erstellen. Kategorien helfen beim Organisieren von OT-Katalogelementen in logischen Gruppen. Wenn anfordernde Personen eine OT-Anforderung senden, können sie basierend auf der festgelegten Kategorie das Katalogelement auswählen, das ihren Anforderungen am besten entspricht.

Bei Bedarf können Sie Kategorien und Unterkategorien definieren, um die OT-Katalogelemente zu organisieren und Anwendern zu helfen, die benötigten Produkte und Services zu finden. Weitere Informationen zum Definieren von Katalogelementkategorien finden Sie unter [Create a category](#) .

Erstellen Sie ein Katalogelement für den Servicekatalog Operational Technology

Erstellen Sie mit dem Katalog-Generator ein Katalogelement für den Servicekatalog Operational Technology (OT), damit andere Anwender OT-Anforderungen kategorisiert nach Katalogelement einreichen können.

Vorbereitungen

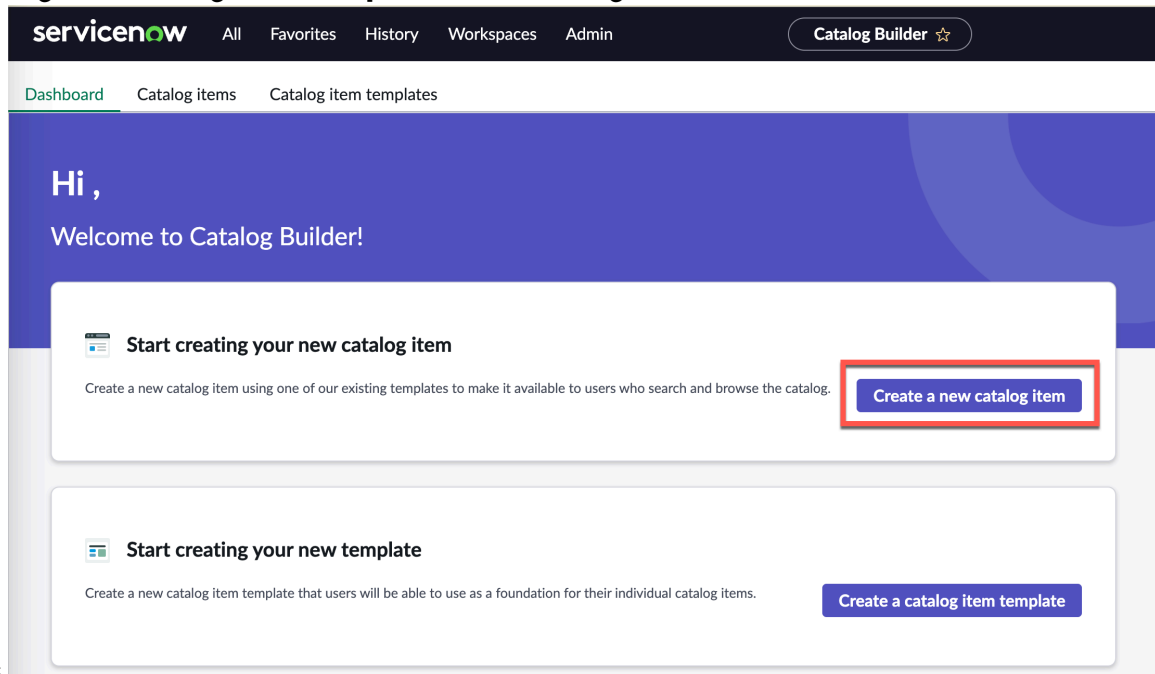
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Sie können Katalogelemente für den OT-Servicekatalog im Katalog-Generator erstellen. Wenn andere Benutzer eine OT-Anforderung senden, können sie das Katalogelement auswählen, das ihren Anforderungen am besten entspricht. Beispielsweise kann das Anfordern des Remotezugriffs auf ein OT-Gerät ein Katalogelement sein, das im OT-Servicekatalog verfügbar ist. Dies ermöglicht es Drittparteien, an Problemen im Zusammenhang mit OT-Geräten zu arbeiten.

Prozedur

1. Navigieren zu **Alle > Servicekatalog > Katalog-Generator**.
2. Wählen Sie auf der Registerkarte **Dashboard** unter **Erstellung des neuen Katalogelements** beginnend die Option **Neues Katalogelement erstellen**



aus.

Alternativ wählen Sie die Registerkarte **Katalogelemente**, und klicken Sie auf **Neu**.

3. Wählen Sie auf der Seite „**Erste Schritte**“ **Fortsetzen** aus.
4. Wählen Sie auf der Seite **Select your item template (Elementvorlage auswählen)** **OT-Katalogelementvorlage** aus.
5. Wählen Sie **Diese Elementvorlage verwenden** aus.
6. Füllen Sie die Felder im Formular „**Katalogelement erstellen**“ aus.

Weitere Informationen zu den Feldern des Formulars „Katalogelement“ finden Sie unter [Operational Technology Formular „Katalogelement“](#).

i Hinweis:

Sie können den Variablensatz des OT-Katalogelements nicht aus dem Abschnitt „Fragen“ entfernen. Der Variablensatz des OT-Katalogelements ist es, was OT-Anforderungen von anderen Anforderungen unterscheidet. Sie können stattdessen neue Fragen für Ihr Elementformular erstellen, indem Sie **Neue Frage einfügen** wählen. Weitere Informationen zum Einfügen einer neuen Frage finden Sie unter [Create a question for a catalog item in Catalog Builder](#).

7. **Wahlweise:** Um eine Vorschau Ihres Katalogelements anzuzeigen, wählen Sie **Vorschau**.
8. **Wahlweise:** Um Ihren Fortschritt zu speichern, wählen Sie **Speichern**.
9. Wenn Sie den Abschnitt **Überprüfen und Absenden** erreicht haben, überprüfen Sie die hinzugefügten Katalogelementinformationen, und wählen Sie **Absenden** aus.
10. Wiederholen Sie die Schritte 1 bis 9 für jedes Katalogelement, das Sie erstellen möchten.

Ergebnisse

Das Katalogelement wird erstellt und steht anderen Anwendern zur Auswahl, wenn sie eine OT-Anforderung im OT-Servicekatalog erstellen.

Erstellen Sie einen Erfüllungs-Flow für eine Operational Technology -Anforderung

Erstellen Sie einen Erfüllungs-Flow mit Katalogaufgaben in Workflow-Studio für Ihr Katalogelement nach Bedarf, um eine Operational Technology (OT)-Anforderung zu erfüllen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Sie können einen Erfüllungs-Flow mit Ihrem Katalogelement verknüpfen. Erfüllungs-Flows lösen die Erstellung von Katalogaufgaben und Benachrichtigungen aus, wenn ein anderer Benutzer eine OT-Anforderung sendet.

Prozedur

1. Navigieren zu **Alle > Prozessautomatisierung > Flow Designer**.
2. Wählen Sie die Schaltfläche **Flows** aus.
3. Wählen Sie in der Dropdown-Liste **Neudie Option Flow** aus.
4. Füllen Sie die Felder im Formular „**Eigenschaften**“ aus.
Weitere Informationen zum Formular „**Eigenschaften**“ finden Sie unter [Create a flow in Workflow Studio](#) .
5. Wählen Sie **Flow erstellen** aus.
6. Fügen Sie Ihrem Flow einen Auslöser hinzu.
Weitere Informationen finden Sie unter [Create a flow in Workflow Studio](#) .
7. Fügen Sie Aktionen, Flows, Subflows oder Glimmlogik hinzu.
Weitere Informationen finden Sie unter [Create a flow in Workflow Studio](#) .
8. Wählen Sie **Speichern**.

Ergebnisse

Workflow-Studio speichert einen Entwurf des Flows, der Auslöser und der Aktionen für den Erfüllungs-Flow. Sie können jetzt den Erfüllungs-Flow auswählen und auf ein Katalogelement anwenden.

Anforderungsmanagement für operative Technologie verwenden

Nachdem Sie alle erforderlichen Setupaufgaben für Anforderungsmanagement für operative Technologie abgeschlossen haben, können Benutzer mit dem Erstellen und Verwalten von Operational Technology (OT)-Anforderungen beginnen.

Operational Technology -Anforderung in Industriell Arbeitsbereich erstellen

Erstellen Sie eine Operational Technology (OT)-Anforderung in Industriell Arbeitsbereich, um ein Produkt oder einen Service zu behandeln, das bzw. der für ein OT-Gerät oder einen Incident benötigt wird.

Vorbereitungen

Erforderliche Rolle: ein beliebiger OT-Anwender

Prozedur

1. Navigieren zu **Alle > Industrial Workspace**.
2. Öffnen Sie die Listenansicht Industriell Arbeitsbereich.
3. Wählen Sie im Listenmodul **OT-Anforderungen** die Liste **Meine Anforderungen aus**.

Hinweis:

Die Liste **Meine Anforderungen** ist für alle OT-Anwender zugänglich, die auf Industriell Arbeitsbereich zugreifen können.

4. Wählen Sie **Neu**.
5. Wählen Sie im OT-Servicekatalog eines der verfügbaren Katalogelemente aus, das Ihren Anforderungen am besten entspricht.
6. Füllen Sie die Felder nach Bedarf für Ihre Anforderung aus.
7. Wählen Sie **Anforderung** aus.

Nächste Maßnahme

Sobald die OT-Anforderung übermittelt wurde, erhalten Sie eine E-Mail mit den Details Ihrer Anforderung. Sie können den Link in der E-Mail verwenden, um den Anforderungsdatensatz zu öffnen und seinen Status zu verfolgen. Sie können den Anforderungsdatensatz auch mit weiterem Kontext bearbeiten, der zum Abschließen der Anforderung erforderlich ist.

Wenn am Anforderungsdatensatz Änderungen vorgenommen werden, werden Sie mit einer E-Mail benachrichtigt, in der die vorgenommenen Änderungen beschrieben werden. Beispielsweise wurden dem Datensatz Arbeitsnotizen hinzugefügt, oder sein Status wurde aktualisiert.

Anforderungsmanagement für operative Technologie Listen in Industriell Arbeitsbereich

Sie können Ihre Operational Technology (OT) Anforderungen und Katalogaufgaben in der Listenansicht Industriell Arbeitsbereich anzeigen.

OT-Anforderungen

Die folgenden Listen sind verfügbar, um OT-Anforderungen in der Listenansicht Industriell Arbeitsbereich unter dem Modul **OT-Anforderung** anzuzeigen und darauf zuzugreifen.

Hinweis:

Sie müssen über die Rolle `sn_request_read` verfügen, um auf diese Listen zugreifen zu können.

OT-Anforderungslisten

Liste	Beschreibung
Meine Anforderungen	OT-Anforderungen, die von Ihnen oder vom Administrator für Sie gestellt wurden.
Offene Anforderungselemente	Alle OT-Anforderungen

OT-Katalogaufgaben

Sie können Ihre OT-Katalogaufgaben in den Listen anzeigen, die im Modul **OT-Aufgaben** verfügbar sind. Für OT-Katalogaufgaben lautet der Wert der Spalte „Aufgabentyp“ **Katalogaufgabe**.

Anforderungsmanagement für operative Technologie-Referenz

Referenzthemen enthalten zusätzliche Informationen zu Anforderungsmanagement für operative Technologie.

Mit Anforderungsmanagement für operative Technologie installierte Komponenten

Mit der Aktivierung von Anforderungsmanagement für operative Technologie können verschiedene Arten von Komponenten installiert werden, einschließlich Anwenderrollen und Servicekataloge.

Installierte Rollen

Rollen für das Anforderungsmanagement für operative Technologie

Name	Beschreibung	Enthält Rollen
sn_request_read	Lesezugriff auf die Anforderung (sc_request), das angeforderte Element (sc_req_item) oder die Katalogaufgabe (sc_task).	NA
sn_request_write	Schreibzugriff auf das angeforderte Element (sc_request), das angeforderte Element (sc_req_item) oder die Katalogaufgabe (sc_task).	• task_editor • dependency_views • agent_workspace_user • view_changer • cmdb_read • cmdb_query_builder_read • sn_request_read
sn_request_comment_write	Schreibzugriff auf die Kommentare für das angeforderte Element (sc_req_item). i Hinweis: Die Rolle sn_request_comment_write allein gewährt keinen Zugriff zum Schreiben von Kommentaren. Sie benötigen Schreibzugriff für die Tabelle.	NA

Servicekataloge installiert

Servicekatalog für Anforderungsmanagement für operative Technologie

Name	Beschreibung
OT-Servicekatalog	Servicekatalog, der Anwendern zum Übermitteln von OT-Anforderungen bereitgestellt wird.

Operational Technology Formular „Katalogelement“.

Wenn Sie ein neues Katalogelement für den Servicekatalog Operational Technology (OT) erstellen, füllen Sie die folgenden Formularfelder aus.

In den folgenden Tabellen werden die Felder beschrieben, die in den einzelnen Abschnitten des Formulars „OT-Katalogelement“ verfügbar sind.

Details

Feld	Beschreibung
Grundlegende Informationen	
Elementname	Name, der im Katalog angezeigt werden soll.
Kurzbeschreibung	Text, der auf der Homepage des Servicekatalogs, in den Suchergebnissen und in der Titelleiste des Auftragsformulars angezeigt wird.
Artikeldetails	
Image	Bild des Artikels.
Beschreibung	Vollständige Beschreibung des Elements. Diese Beschreibung wird im Katalog angezeigt, wenn ein Benutzer das Element auswählt oder auf den zugehörigen Link Vorschau klickt. Sie können Videos, Bilder, Links zu Artikeln der internen Knowledge Base (KB) und Links zu externen Informationsquellen und Anleitungen einbetten.

Standort

Feld	Beschreibung
Kataloge	
Ausgewählte Kataloge	Kataloge, in denen dieses Element angezeigt wird.
Kategorien	
Ausgewählte Kategorien	Kategorie für das Element. Kategorien können nur ausgewählt werden, nachdem das Feld Kataloge ausgefüllt wurde.

Standort (Fortsetzung)

Feld	Beschreibung
	Katalogsuchen finden nur Artikel, die einer Kategorie im Serviceportal zugewiesen sind.
Themen	
Ausgewählte Themen	Themen für das Element. Anfordernde Personen können die von Ihnen hinzugefügten Themen verwenden, um das Katalogelement zu finden und darauf zuzugreifen, sobald das Katalogelement veröffentlicht wurde.

Fragen

Feld	Beschreibung
Variablensatz des OT-Katalogelements	
Site	Standort, der vom Katalogelement betroffen ist.

Einstellungen

Feld	Beschreibung
Portaleinstellungen	
Schaltflächenbezeichnung „Senden“	Bezeichnung für die Schaltfläche „Absenden“, nachdem die anfordernde Person das Katalogelementformular ausgefüllt hat.
Schaltfläche „In den Einkaufswagen“ ausblenden	Wenn diese Option ausgewählt ist, wird die Schaltfläche In den Einkaufswagen nicht für den Artikel angezeigt. Wenn die Instanzoption „In den Einkaufswagen“ anzeigen des Widgets auf „falsch“ festgelegt ist, wird diese Einstellung ignoriert. Diese Einstellung ist standardmäßig ausgewählt, wenn die Anforderungsmethode auf Anfordern oder Absenden festgelegt ist. Wenn in Upgradeszenarien das Feld Kein Einkaufswagen in der Plattform ausgewählt ist, führen Sie die Skripteinbindung <code>CatalogPortalSettingsMigration</code> aus, um diese Einstellung auf das Feld „In den Einkaufswagen“ ausblenden auf der Registerkarte Portaleinstellungen zu aktualisieren. i Hinweis: Gilt für ein Katalogelement und eine Bestellanleitung.

Einstellungen (Fortsetzung)

Feld	Beschreibung
Schaltfläche „Als Entwurf speichern“ ausblenden	Wenn diese Option ausgewählt ist, wird die Schaltfläche Als Entwurf speichern für das Element nicht angezeigt.
Mengenauswahl ausblenden	Wenn diese Option ausgewählt ist, wird die Liste Menge nicht für das Katalogelement angezeigt. Diese Einstellung ist standardmäßig ausgewählt, wenn die Anforderungsmethode auf Anfordern oder Absenden festgelegt ist. Wenn bei Upgradekunden das Feld Keine Menge in der Plattform ausgewählt ist, führen Sie das Migrationsskript <code>CatalogPortalSettingsMigration</code> aus, um diese Einstellung auf das Feld Menge ausblenden auf der Registerkarte Portaleinstellungen zu aktualisieren. i Hinweis: Gilt für ein Katalogelement. Ein Bestelleitfaden erbt diese Einstellung von dem enthaltenen Katalogelement.
Lieferzeit ausblenden	Wenn diese Option ausgewählt ist, wird das Feld Lieferzeit nicht für das Katalogelement angezeigt. Diese Einstellung ist standardmäßig ausgewählt, wenn die Anforderungsmethode auf Absenden festgelegt ist. i Hinweis: Gilt für ein Katalogelement. Ein Bestelleitfaden erbt diese Einstellung von dem enthaltenen Katalogelement.
Schaltfläche „Anhang“ ausblenden	Wenn diese Option ausgewählt ist, wird die Schaltfläche Anhänge hinzufügen für das Katalogelement nicht angezeigt. i Hinweis: Gilt für ein Katalogelement und einen Datensatzersteller. Ein Bestelleitfaden erbt diese Einstellung von dem enthaltenen Katalogelement.

Einstellungen (Fortsetzung)

Feld	Beschreibung
Anhang vorschreiben	Wenn diese Option ausgewählt ist, ist das Hinzufügen einer Anlage für das Katalogelement obligatorisch. i Hinweis: Gilt für ein Katalogelement und einen Datensatzersteller.

Zugriff

Feld	Beschreibung
Verfügbar für	
Anwenderkriterien gewähren Zugriff	Wählen Sie die Anwenderkriterien aus, die auf das Katalogelement zugreifen können.
Nicht verfügbar für	
Anwenderkriterien verweigern Zugriff	Wählen Sie die Anwenderkriterien aus, die nicht auf das Katalogelement zugreifen können.

Erfüllung

Feld	Beschreibung
Erfüllungsmethode	
Prozessmodul	Sequenz für die Erfüllung von Elementanforderungen.
Ausgewählter Flow	Flow, der definiert, wie die Elementanforderung erfüllt wird. i Hinweis: Dieses Feld ist nur sichtbar, wenn Sie Flow Designer Flow im Feld Prozess-Engine auswählen.
Ausgewählter Workflow	Workflow, der definiert, wie die Elementanforderung erfüllt wird. i Hinweis: Dieses Feld ist nur sichtbar, wenn Sie Workflow im Feld Prozess-Engine auswählen.

Zugehörige Informationen

Weitere Informationen zu den Erweiterungsklassen Operational Technology (OT) und zugehörigen Anwendungen.

Übersicht über Erweiterungsklassen

Die Erweiterungsklassen helfen Ihnen zu verstehen, wie Operational Technology-Management mit Configuration Management Database (CMDB) funktioniert.

Operational Technology (OT) extension classes

CMDB aktualisiert Klassen für OT.

Zugehörige Anwendungen

Request Management

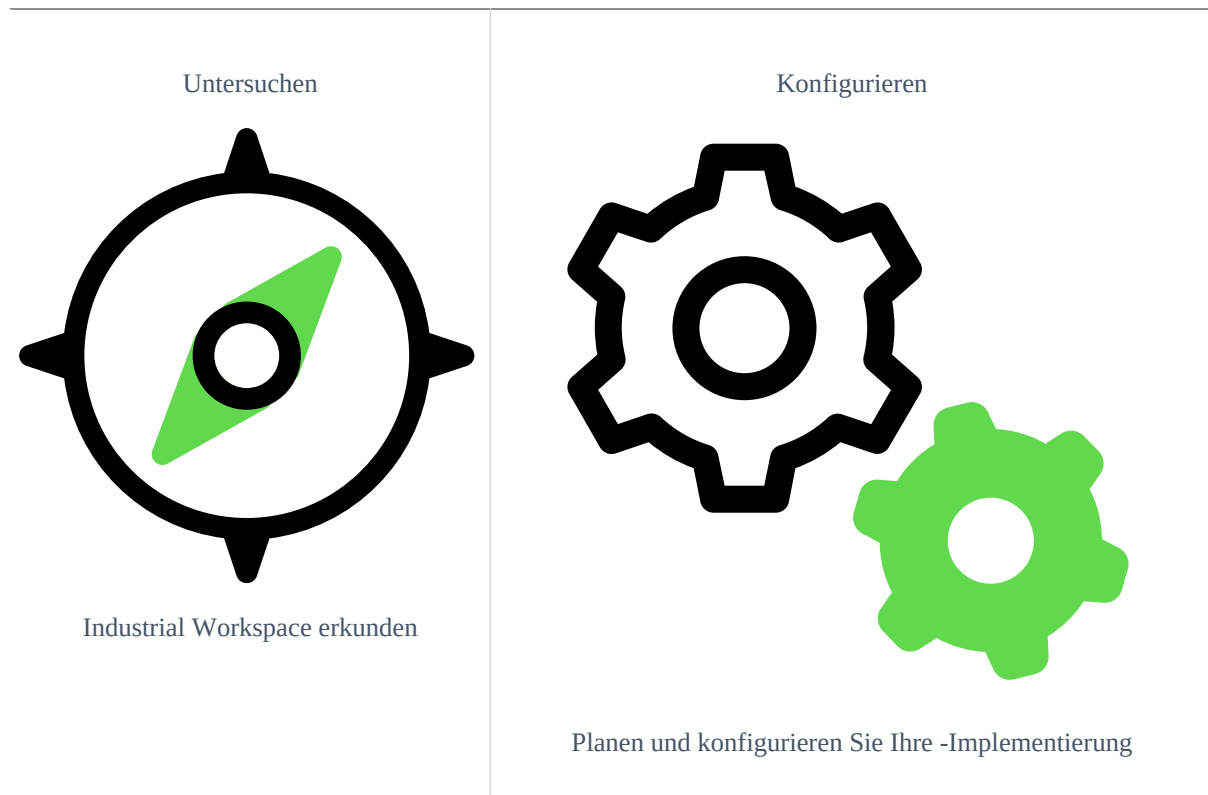
Mit Anforderungsmanagement können Katalogelemente basierend auf definierten Flows angefordert und erfüllt werden.

IT Service Management

Die Anwendung ServiceNow IT Service Management ermöglicht es Ingenieuren, Probleme mit OT-Geräten und Produktionsprozessen schnell zu lösen.

Industriell Arbeitsbereich

Industriell Arbeitsbereich ist eine Anwenderoberfläche, die Anwendern Operational Technology von (OT) die Tools zur Verfügung stellt, die sie zur Verwaltung ihrer OT-Daten benötigen.



Automatische Übersetzung

Verwenden



Industrial Workspace verwenden

Industrial Workspace erkunden

Industriell Arbeitsbereich ist eine Anwenderoberfläche, die Anwendern Operational Technology von (OT) die Tools zur Verfügung stellt, die sie zur Verwaltung ihrer OT-Daten benötigen.

Industriell Arbeitsbereich Navigation

Industriell Arbeitsbereich ist auf den folgenden Seiten organisiert.

Seiten von Industriell Arbeitsbereich

Seite	Beschreibung
Aktionsorientierte OT-Zielseite	Wenn Sie das Homepage -Symbol () auswählen, gelangen Sie zur OT-aktionsorientierten Zielseite. Die Zielseite hilft Ihnen, kritische Aufgaben in Bezug auf Ihr OT-Netzwerk zu verfolgen.
Dashboard-Bibliothek	Wenn Sie das Symbol Dashboardbibliothek () wählen, gelangen Sie zur Dashboardbibliothek, die die folgenden Dashboards enthält. Dashboard für OT-Transparenz Enthält die Daten, die sich auf Ihre OT-Geräte beziehen. Operational Technology Vulnerability Response (PA)-Dashboard Verfolgt das Volumen, die Leistung und den Fortschritt der angreifbaren OT-Elemente von der ersten Analyse und Erkennung bis zur Eindämmung oder Korrektur. Dashboard „OT-Schwachstellenrisiko-Rollup“.

Seiten von Industriell Arbeitsbereich (Fortsetzung)

Seite	Beschreibung
	Enthält die Risikopunktzahl der OT-Geräte auf jeder Ebene des Anlagenmodells.
OT-Fortschrittsbewertungsliste	Wenn Sie das Symbol OT-Fortschrittsbewertungsliste () wählen, gelangen Sie zur OT-Fortschrittsbewertungsliste. Mit der OT-Fortschrittsbewertungsliste können Sie Site-Daten in einer Ansicht vergleichen.
Listenansicht „Industrial Workspace“.	Wenn Sie das Symbol Liste () auswählen, gelangen Sie zur Listenansicht Industriell Arbeitsbereich, die Ihnen Zugriff auf alle Listen im Zusammenhang mit Ihren OT-Datensätzen gewährt. Sie können auf die folgenden Listenmodule und die zugehörigen Listen zugreifen: • Operative Technologien (OT) • Informationstechnologie(IT)-Hardware • Industrial Process Manager • OT-Incidents • OT-Change-Anforderungen • OT-Korrekturaufgaben • Angreifbare OT-Elemente • OT-Aufgaben • Wissen
Anlagenmodell-Manager	Wenn Sie das Symbol Anlagenmodell () wählen, gelangen Sie zum Anlagenmodell-Manager, wo Sie Ihre Sites und deren Anlagenmodelldaten anzeigen können.

Operational Technology Aktionsorientierte Zielseite

Sie können die aktionsorientierte Zielseite Operational Technology (OT) verwenden, um kritische Aufgaben in Bezug auf Ihr OT-Netzwerk nachzuverfolgen.

Übersicht über die aktionsorientierte OT-Zielseite

Die aktionsorientierte OT-Zielseite hilft Anwendern, z. B. OT-Ingenieure, Aufgaben anzuzeigen, die ihnen, ihrem Standort oder ihrer Gruppe zugewiesen sind. Die Zielseite ruft wichtige Aktionen auf, die für den angemeldeten Benutzer priorisiert werden müssen, und enthält eine Übersicht über vorhandene OT-Incidents, OT-Change-Anforderungen, OT-Korrekturaufgaben, angreifbare OT-Elemente und andere Aufgaben.

Die Zielseite bietet eine detaillierte und rollenbasierte Ansicht der täglichen Aufgaben und wichtigen Aktionen. Für jede Aufgabe im Abschnitt „**Wichtige Aktion**“ werden die Aufgaben

standardmäßig nach dem **Öffnungsdatum** sortiert. Wenn die Aufgabe kritisch ist, wird sie im Abschnitt „**Wichtige Aktion**“ angezeigt.

Um auf die OT-aktionsorientierte Zielseite zuzugreifen, navigieren Sie zu **Alle > Industrial Workspace**, wählen Sie das Homepage-Symbol ().

Inhalte der Zielseite

Die folgenden Abschnitte beschreiben die Inhalte, die Sie auf der aktionsorientierten OT-Zielseite anzeigen können.

Wichtige Aktionen

Der Abschnitt „Wichtige Aktionen“ enthält OT-Aufgaben oder -Aktionen, die als kritisch eingestuft werden und so bald wie möglich behandelt werden müssen. Standardmäßig werden die Aufgaben nach dem **Öffnungsdatum** organisiert, wobei die zuletzt erstellte kritische Aufgabe, die dem angemeldeten Benutzer zugewiesen ist, zuerst angezeigt wird.

Die in diesem Abschnitt angezeigten Aufgaben sind die kritischsten Aufgaben aus dem Abschnitt „**Übersicht**“, auf die Sie reagieren können. Die Relevanz der Aufgabe wird durch die folgenden Kriterien bestimmt:

- Ihre Priorität ist von entscheidender Bedeutung
- Die Aufgabe ist eine Korrekturaufgabe, und ihre Risikobewertung ist kritisch

Die in diesem Abschnitt enthaltenen Aufgaben sind folgendermaßen organisiert:

- Alle Aufgaben, die dem angemeldeten Anwender direkt zugewiesen sind, werden zuerst angezeigt.
- Aufgaben, die der Gruppe eines Anwenders zugewiesen sind, aber auch keinem Anwender, werden hinter angezeigt.
- Aufgaben, die keiner Gruppe oder keinem Anwender zugewiesen sind, aber einer Site zugewiesen sind, auf die der angemeldete Anwender Zugriff hat, werden zuletzt angezeigt.

Überblick

Der Abschnitt „Übersicht“ enthält eine Übersicht über OT-Incidents, Change-Anforderungen, Korrekturaufgaben, angreifbare Elemente und andere Aufgaben, die Ihnen, Ihrer Gruppe oder Ihrem Standort zugewiesen sind.

Sie können die folgenden Filter verwenden, um die Datensätze anzuzeigen, die basierend auf den Feldern **Zugewiesen an**, **Zuweisungsgruppe** und **Site** in den Datensätzen angezeigt werden:

Ihre Arbeit

Ihnen zugewiesene Datensätze.

Arbeit Ihrer Gruppe

Datensätze, die Ihrer Gruppe oder Ihren Gruppen zugewiesen sind.

Die Arbeit Ihrer Site

Datensätze, die Ihrer Site oder Ihren Sites zugewiesen sind.

In der folgenden Tabelle werden die Kacheln im Abschnitt „Übersicht“ beschrieben.

Übersichtskacheln

Kachel	Beschreibung
Ihnen zugewiesene OT-Incidents/Ihren Gruppen zugewiesene OT-Incidents/Ihren Sites zugewiesene OT-Incidents	Anzahl der OT-Incident-Datensätze, die Ihnen, Ihrer Zuweisungsgruppe oder Ihrem Standort zugewiesen sind. Um eine Liste aller OT-Incident-Datensätze anzuzeigen, wählen Sie Alle Datensätze aus. Um die Liste der Datensätze nur basierend auf ihrem Status oder Typ anzuzeigen, wählen Sie den entsprechenden Abschnitt des verfügbaren Diagramms aus. Wenn Sie beispielsweise nur die Incident-Datensätze basierend auf ihrer Priorität anzeigen möchten, wählen Sie den Abschnitt „Kritisch“ des Diagramms aus.
Ihnen zugewiesene OT-Change-Anforderungen/OT Change-Anforderungen, die Ihren Gruppen zugewiesen sind/OT Change-Anforderungen, die Ihren Sites zugewiesen sind	Anzahl der Datensätze für OT-Change-Anforderungen, die Ihnen, Ihrer Zuweisungsgruppe oder Ihrem Standort zugewiesen sind. Um eine Liste aller Datensätze der OT-Change-Anforderung anzuzeigen, wählen Sie Alle Datensätze aus. Um die Liste der Datensätze nur basierend auf ihrem Status anzuzeigen, wählen Sie den entsprechenden Abschnitt des verfügbaren Diagramms aus. Wenn Sie beispielsweise nur die geplanten Change-Anforderungsdatsätze anzeigen möchten, wählen Sie den Abschnitt Geplant des Diagramms.
Ihnen zugewiesene OT-Korrekturaufgaben/Ihren Gruppen zugewiesene OT-Korrekturaufgaben/Ihren Sites zugewiesene OT-Korrekturaufgaben	Anzahl der Datensätze für OT-Korrekturaufgaben, die Ihnen, Ihrer Zuweisungsgruppe oder Ihrem Standort zugewiesen sind. Um eine Liste aller Datensätze für OT-Korrekturaufgaben anzuzeigen, wählen Sie Alle Datensätze aus. Um die Liste der Datensätze nur basierend auf ihrem Status anzuzeigen, wählen Sie den entsprechenden Abschnitt des verfügbaren Diagramms aus. Wenn Sie beispielsweise nur die Datensätze für Korrekturaufgaben anzeigen möchten, die überprüft werden, wählen Sie den Abschnitt Wird überprüft des Diagramms.
Ihnen zugewiesene angreifbare OT-Elemente/Ihren Gruppen zugewiesene angreifbare OT-Elemente/Ihren Sites zugewiesene angreifbare OT-Elemente	Anzahl der Datensätze für angreifbare OT-Elemente, die Ihnen, Ihrer Zuweisungsgruppe oder Ihrem Standort zugewiesen sind. Um eine Liste aller Datensätze zu angreifbaren OT-Elementen anzuzeigen, wählen Sie Alle Datensätze aus. Um nur die Liste der Datensätze basierend auf ihrer Risikobewertung anzuzeigen, wählen Sie den entsprechenden Abschnitt des verfügbaren Diagramms aus. Wenn Sie beispielsweise nur die Datensätze zu angreifbaren Elementen mit hoher Priorität anzeigen möchten, wählen Sie den Abschnitt Hoch des Diagramms.
Andere Ihnen zugewiesene OT-Aufgaben/Andere OT-Aufgaben, die Ihren Gruppen zugewiesen	Anzahl der anderen OT-Aufgabendatsätze, die Ihnen, Ihrer Zuweisungsgruppe oder Ihrem Standort zugewiesen sind.

Übersichtskacheln (Fortsetzung)

Kachel	Beschreibung
sind/Andere OT-Aufgaben, die Ihren Sites zugewiesen sind	Um eine Liste aller anderen OT-Aufgabendatensätze anzuzeigen, wählen Sie Alle Datensätze aus. Um die Liste der Datensätze nur basierend auf ihrer Priorität anzuzeigen, wählen Sie den entsprechenden Abschnitt des verfügbaren Diagramms aus. Wenn Sie beispielsweise nur die OT-Aufgaben mit niedriger Priorität anzeigen möchten, wählen Sie den unteren Abschnitt des Diagramms aus.

OT CMDB Integrität

Die OT CMDB -Integrität hilft Ihnen, die Integrität Ihrer Geräte in Configuration Management Database (CMDB) zu überwachen und aufrechtzuerhalten. Sie können die Anzahl Ihrer OT-Geräte nach Typ organisiert anzeigen.

Hinweis:
Dieser Abschnitt wird nur angezeigt, wenn Operational Technology Manager installiert ist.

In der folgenden Tabelle werden die Kacheln im Abschnitt „OT CMDB -Integrität“ beschrieben. Um den Abschnitt „OT CMDB -Integrität“ anzuzeigen, benötigen Sie die Rolle **cmdb_ot_isa_viewer**.

OT-CMDB-Integritätskacheln

Kachel	Beschreibung
Nicht klassifizierte OT-Geräte	Anzahl der OT-Geräte in Ihrem OT-Netzwerk, die keiner OT-Gerätetypkategorie zugewiesen sind. Um die Liste der nicht klassifizierten OT-Gerät-Datensätze anzuzeigen, wählen Sie Alle Datensätze aus.
Nicht zugewiesene OT-Geräte	Anzahl der OT-Geräte in Ihrem OT-Netzwerk, die keinem Benutzer zugewiesen sind. Um die Liste der nicht zugewiesenen OT-Gerät-Datensätze anzuzeigen, wählen Sie Alle Datensätze aus.
Nicht zugeordnete OT-Geräte	Anzahl der OT-Geräte in Ihrem OT-Netzwerk, die keiner Anlagenmodell-Entität für den zugewiesenen Standort zugeordnet sind. Um die Liste der nicht zugeordneten OT-Gerät-Datensätze anzuzeigen, wählen Sie Alle Datensätze aus.

OT-CMDB-Integritätskacheln (Fortsetzung)

Kachel	Beschreibung
	i Hinweis: Diese Kachel ist nur verfügbar, wenn Prozessmanager Industrie installiert ist und der angemeldete Benutzer über die Rolle „cmdb_ot_isa_viewer“ verfügt. Die Kachel erfordert, dass Ihre Organisation über ein Anlagenmodell für die Zuordnung von OT-Geräten zu einem Produktionsprozess verfügt.
Keine Site zugewiesen	Anzahl der OT-Geräte in Ihrem OT-Netzwerk, die keinem Standort zugewiesen sind. i Hinweis: Diese Kachel ist nur verfügbar, wenn der angemeldete Anwender über die Rolle „cmdb_ot_isa_viewer“ verfügt. Um die Liste der OT-Gerät-Datensätze ohne Standort anzuzeigen, wählen Sie Alle Datensätze aus.
OT-Geräte ohne IP-Adresse	Anzahl der OT-Geräte in Ihrem OT-Netzwerk, denen keine IP-Adresse zugewiesen ist. Um die Liste der OT-Gerät-Datensätze ohne IP-Adresse anzuzeigen, wählen Sie Alle Datensätze aus.

Dashboard-Bibliothek im Industrial Workspace

Die Dashboard-Bibliothek in Industrial Workspace enthält die Dashboards für Operational Technology Transparenz, Operational Technology Vulnerability Response (PA) und das Dashboard Operational Technology Rollup für Schwachstellenrisiko.

Operational Technology Transparenz-Dashboard

Mit dem Transparenz-Dashboard Operational Technology (OT) können Sie Ihr OT-Gerät an einem zentralen Ort verwalten. Über das OT-Transparenz-Dashboard können Sie auf Ihre OT-Gerät-Daten zugreifen.

Übersicht über das OT-Transparenz-Dashboard

Das OT-Transparenz-Dashboard ist ein zentraler Ort in Industriell Arbeitsbereich. Sie können dieses Dashboard verwenden, um Ihre Daten für Operational Technology Manager und Prozessmanager Industrie zu überprüfen. Sie können es auch verwenden, um die Detailinformationen für die OT-Geräte und Anlagenmodell-Entitäten in Ihrem OT-Netzwerk zu überprüfen oder zu bearbeiten.

Mit dem OT-Transparenz-Dashboard können Sie:

- Nachvollziehen, welche OT-Gerät-Informationen sich in der letzten Woche in Ihrem OT-Netzwerk geändert haben.
- Zeigen Sie den Fortschritt eines OT-Gerät-Bestands in einer Industrieanlage an.
- Analysieren Sie Ihre OT-Geräte sinnvoll. Sie können beispielsweise Einblicke darüber erhalten, wie viele Ihrer Produktionsgeräte Ihren Produktionsprozessen zugeordnet sind.

Dashboard-Inhalte

Um auf die OT-Gerät-Daten im OT-Transparenz-Dashboard zuzugreifen, navigieren Sie zu **Alle > Industrial Workspace**, wählen Sie das Symbol Dashboard-Bibliothek () und anschließend **Operational Technology Visibility**. Um auf das Diagramm der Leistungskennzahlen (Key Performance Indicators, KPI) für eine der in der folgenden Tabelle beschriebenen Kacheln zuzugreifen, wählen Sie die Anzahl oder Diagrammkomponente in der Kachel aus.

Die folgende Tabelle beschreibt die OT-Gerät-Daten, die Sie auf den verschiedenen Kacheln im Dashboard sehen können.

Dashboard-Kacheln

Kachel	Beschreibung
Updates aus den letzten 7 Tagen	
Neue OT-Geräte erkannt	Anzahl der neuen OT-Geräte, die von Discovery für Operational Technology und andere automatisierte Prozesse in Ihrem OT-Netzwerk in den letzten sieben Kalendertagen erkannt wurden.
Inaktive OT-Geräte	Anzahl der OT-Geräte, die in den letzten sieben Kalendertagen nicht in Ihrem OT-Netzwerk aufgetreten sind. Diese Geräte werden als inaktiv betrachtet.
OT-Geräteübersicht	
Gesamtzahl CMDB OT-Geräte	
Nicht klassifizierte OT-Geräte	Anzahl der OT-Geräte in Ihrem OT-Netzwerk, die keiner OT-Gerätetypkategorie zugewiesen sind.
Nicht zugewiesene OT-Geräte	Anzahl der OT-Geräte in Ihrem OT-Netzwerk, die keinem Benutzer zugewiesen sind.
Nicht zugeordnete OT-Geräte	Anzahl der OT-Geräte in Ihrem OT-Netzwerk, die keiner Anlagenmodell-Entität für den zugewiesenen Standort zugeordnet sind.  Hinweis: Diese Kachel ist nur verfügbar, wenn Prozessmanager Industrie installiert ist, da Ihre Organisation über ein Anlagenmodell für die Zuordnung von OT-Geräten zu einem Produktionsprozess verfügen muss.
OT-Geräte nach Kategorie	

Dashboard-Kacheln (Fortsetzung)

Kachel	Beschreibung
Überwachungssysteme	Anzahl der OT-Geräte in Ihrem OT-Netzwerk, die einer Kategorie für Überwachungssysteme zugewiesen sind.
Steuerungssysteme	Anzahl der OT-Geräte in Ihrem OT-Netzwerk, die der Kategorie „Steuerungssysteme“ zugewiesen sind. i Hinweis: Steuerungsmodule sind in dieser Anzahl nicht enthalten.
Feldgeräte	Anzahl der OT-Geräte in Ihrem OT-Netzwerk, die der Kategorie „Feldgeräte“ zugewiesen sind.
Computer und Server	Anzahl der OT-Geräte in Ihrem OT-Netzwerk, die der Kategorie „Computer und Server“ zugewiesen sind.
Netzwerkgerät	Anzahl der OT-Geräte in Ihrem OT-Netzwerk, die der Kategorie Netzwerkgeräte zugewiesen sind.
Industrielles IoT	Anzahl der OT-Geräte in Ihrem OT-Netzwerk, die der Kategorie Industrielles Internet der Dinge (IoT) zugewiesen sind.
OT-Geräte nach Purdue-Ebene	Balkendiagramm, das die Anzahl der OT-Geräte in Ihrem OT-Netzwerk anhand der zugewiesenen Purdue-Ebene anzeigt. i Hinweis: Weitere Informationen zu den Purdue-Ebenen in den OT-Systemen finden Sie unter https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lv1sec10/the-purdue-model-for-industrial-control-systems .
OT-Geräte nach Typ (oberste Ebene)	Balkendiagramm, das die OT-Gerät-Daten nach den OT-Gerät-Typen kategorisiert.
OT-Geräte nach Hersteller (oberste Ebene)	Kreisdiagramm, das die Anzahl der OT-Geräte in Ihrem OT-Netzwerk nach dem zugewiesenen Hersteller anzeigt.
OT-Geräte nach Relevanz	Kreisdiagramm, das die Anzahl der OT-Geräte in Ihrem OT-Netzwerk anhand ihrer zugewiesenen Relevanz anzeigt.

Erforderliche Rollen zum Anzeigen des Dashboards

Für den Zugriff auf das OT-Transparenz-Dashboard benötigen Sie die Rollen **cmdb_ot_viewer** und **cmdb_ot_isa_viewer**.

Standortfilter

Sie können den Filter **Site** verwenden, um die Site zu suchen und auszuwählen, die Sie im Dashboard anzeigen möchten. Um auf den Site-Filter zuzugreifen und ihn zu verwenden, müssen Sie über die Rolle **cmdb_ot_isa_viewer** mit Zugriff auf die Site verfügen, die Sie anzeigen möchten.

Weitere Informationen finden Sie unter [Verwenden Sie den Site-Filter](#).

Operational Technology Vulnerability Response (PA)-Dashboard

Verfolgen Sie das Volumen, die Leistung und den Fortschritt der Operational Technology (OT) angreifbaren Elemente (VIs) von der ersten Analyse und Erkennung bis zur Eindämmung oder Nachbesserung. Sie können die Berichte nach Zuweisungsgruppe, Exploits, Risikobewertung oder Status filtern, um Einblicke in das Schwachstellenrisiko und die betroffenen Services zu erhalten.

Erforderliche Rollen Operational Technology und Operational Technology Vulnerability Response.

Für den Zugriff auf das OTVR (PA)-Dashboard benötigen Sie die Rolle **sn_otvr.remediation_owner** .

Um das Dashboard Operational Technology Vulnerability Response (PA) anzuzeigen, navigieren Sie zu **Alle > Industrial Workspace** und wählen Sie im Navigationsbereich das Symbol

Dashboard-Bibliothek (). Wählen Sie dann **Operational Technology Vulnerability Response** aus.

Anwendungsfälle

Die folgende Tabelle enthält einige Beispiele dafür, wie verschiedene Personen in Ihrer Organisation dieses Dashboard verwenden können.

Operational Technology Vulnerability Response Anwendungsfälle im Dashboard für (PA).

Anwender	Dashboard-Verwendung
OT-Standortmanager, OT-Analysten, Besitzer der Schwachstellenkorrektur	Helfen Sie Ihrer Organisation, mit der Zunahme von Security Incidents aufgrund von ausgenutzten Schwachstellen umzugehen, indem Sie ermitteln, welche angreifbaren OT-Elemente das meiste Risiko darstellen. Dieses Dashboard bietet eine grafische Ansicht der Aktivität angreifbarer OT-Elemente und kann Ihnen helfen, die Korrekturpläne und den Statusfortschritt zu entwerfen. Sie können sich auf die Leistungskennzahlen (Key Performance Indicators, KPIs) konzentrieren, die den kritischen betroffenen Geräten und Schwachstellen mit hoher Sichtbarkeit zugeordnet sind.

Dashboard-Registerkarten

Sie können die Berichte anzeigen, die die Trenddaten im Zeitverlauf zeigen, und die Berichte mit Echtzeitdaten. Sie können die Trends der wichtigen Metriken auch regelmäßig anzeigen,

um Ihre allgemeinen Geschäftsprozesse zu analysieren und die Bereiche zu identifizieren, die verbessert werden müssen.

Erfahren Sie, was sich auf den Registerkarten „**Angreifbare Elemente**“, „**Nachbesserung**“ und „**Ausnahmen**“ befindet.

Registerkarte „**Angreifbare Elemente**“.

Auf der Registerkarte „**Angreifbare Elemente**“ werden die KPIs für Schwachstellenrisiko und -verbreitung, betroffene Geräte, Einhaltung der Korrekturziele und Korrekturfortschritt angezeigt.

Auf der Registerkarte „**Angreifbare Elemente**“ können Sie die folgenden Berichte anzeigen:

- Angreifbare OT-Elemente insgesamt
- Neue angreifbare OT-Elemente
- Nicht zugewiesene angreifbare OT-Elemente
- Angreifbare OT-Elemente nach Status
- Angreifbare OT-Elemente nach Risikobewertung
- OT-VIs mit erfülltem Korrekturziel

i Hinweis:

Sie können die Daten nach Monat, 3 Monat, 6 Monat, Jahr oder für alle Zeiten anzeigen.

- Durchschnittliche Zeit bis zur Korrektur für OT-VI (MTTR)

i Hinweis:

Sie können die Daten nach Monat, 3 Monat, 6 Monat, Jahr oder für alle Zeiten anzeigen.

- OT AE nach Alter
- Geschlossene angreifbare OT-Elemente nach Korrekturzielstatus
- Kritische angreifbare OT-Elemente nach Zuweisungsgruppe
- Überfällige kritische angreifbare OT-Elemente nach Zuweisungsgruppe

Registerkarte „**Remediation**“.

Auf der Registerkarte **Nachbesserung** können Sie den Fortschritt Ihrer Nachbesserungsaktionen nachvollziehen und sehen, welche Supportteams bei der Durchführung am meisten Unterstützung benötigen.

Auf der Registerkarte „**Nachbesserung**“ können Sie die folgenden Berichte in Echtzeit anzeigen:

- OT-Korrekturaufgaben
- Kritische OT-Korrekturaufgaben kurz vor der Fälligkeit
- OT-Korrekturaufgabe nach Risikobewertung
- OT-Korrektur nach Zielstatus
- OT-Korrekturaufgabe nach Status
- Nicht zugewiesene OT-Korrekturaufgaben

- Kritische OT-Korrekturaufgabe nach Zuweisungsgruppe
- Überfällige kritische OT-Korrekturaufgabe nach Zuweisungsgruppe

Registerkarte „**Ausnahme**“.

Die Registerkarte „**Ausnahme**“ hilft Ihnen zu verstehen, wo Ihre Organisation aufgrund möglicherweise übermäßiger Zurückstellungen von Remediationen ein Risiko eingeht.

Auf der Registerkarte „**Ausnahme**“ können Sie die folgenden Berichte in Echtzeit anzeigen:

- Zurückgestellte angreifbare OT-Elemente nach Grund
- OT-Ausnahmen für kritische angreifbare Elemente nach Zuweisungsgruppe.

Standortfilter

Sie können den Filter **Site** verwenden, um die Site zu suchen und auszuwählen, die Sie im Dashboard anzeigen möchten. Um auf den Site-Filter zuzugreifen und ihn zu verwenden, müssen Sie über die Rolle **cmdb_ot_isa_viewer** mit Zugriff auf die Site verfügen, die Sie anzeigen möchten.

Weitere Informationen finden Sie unter [Verwenden Sie den Site-Filter](#).

Indikatorquellen

Die Indikatoren Operational Technology Vulnerability Response erfassen Daten aus den folgenden Quellen:

- OTVI.Aktiv
- OTVI.Geschlossen
- OTRT.Aktiv

Weitere Informationen zu den für das Dashboard verwendeten Indikatorquellen finden Sie unter [Indikatorquellen und Indikatoren für das Dashboard Operational Technology Vulnerability Response \(PA\)](#).

Wenn Sie erwarten, dass mehr als 1 Million Datensätze aus den Indikatorquellen gesammelt werden, müssen Sie die erwartete Anzahl im Abschnitt „Datensatzsammlung“ der Indikatorquelle überschreiben. Weitere Informationen finden Sie unter [Überprüfen Sie die Indikatorquellen für eine größere Anzahl von Datensätzen](#).

Indikatoren

Mehrere Indikatoren werden verwendet, um den Fortschritt der Nachbesserung von Schwachstellen in der Anwendung Operational Technology Vulnerability Response zu messen und nachzuverfolgen. Weitere Informationen zu den für das Dashboard verwendeten -Indikatoren finden Sie unter [Indikatorquellen und Indikatoren für das Dashboard Operational Technology Vulnerability Response \(PA\)](#).

Die Option **zum Sammeln von Datensätzen** für -Indikatoren ist für die Anwendung Operational Technology Vulnerability Response standardmäßig deaktiviert. Diese Option ist deaktiviert, um Leistungsprobleme zu vermeiden, die auftreten können, wenn Sie für jeden Indikator eine große Datenmenge erfassen.

Aufgliederungen

Aufgliederungen filtern und gruppieren die gesammelten Datensätze nach einem qualitativen Attribut. Die folgenden Aufgliederungen gelten für die Indikatoren im Dashboard:

- Alter
- Geschlossen mit Alter
- Zuweisungsgruppe
- CI-Manager
- Aufschiebungsgrund
- Exploit-Angriffsvektor
- Exploit vorhanden
- Exploit-Kompetenzniveau
- Korrekturzielregel
- Nachbesserungszielstatus
- Nachbesserungszielstatus (geschlossen)
- Risikobewertung
- Schweregrad
- Status

Die Aufgliederungsquellen geben die eindeutigen Werte an, die eine Aufgliederung enthält. Die eindeutigen Werte werden als Aufgliederungselemente bezeichnet. Das Dashboard verwendet die folgenden Aufgliederungsquellen:

- Zuweisungsgruppe
- Zurückgestellt.Grund.Nicht.Geschlossen
- Exploit-Angriffsvektor
- Exploit vorhanden
- Exploit-Kompetenzniveau
- OT-Altersbereich☒
- Korrekturzielstatus
- Korrekturzielstatus (Geschlossen)
- Korrektur.Ziel.Regel☒
- Risikobewertung
- Schweregrad
- Status
- Schwachstelle.Element.CI.Manager

Weitere Informationen zu den Aufgliederungen und Aufgliederungsquellen finden Sie unter [Operational Technology Vulnerability Response \(PA\) Dashboard-Aufgliederungen](#).

Erfassungsaufgaben

Das Dashboard verwendet die folgenden Erfassungsaufgaben, um die OT-Schwachstellendaten zu sammeln, die im Dashboard angezeigt werden.

- [PA OT VR] Sammlung historischer Schwachstellendaten
- [PA OT VR] Tägliche Sammlung für Korrekturaufgaben
- [PA OT VR] Tägliche Sammlung für angreifbare Elemente 1
- [PA OT VR] Tägliche Sammlung für angreifbare Elemente 2

Weitere Informationen zu den Erfassungsaufgaben finden Sie unter [Operational Technology Vulnerability Response \(PA\) Dashboard-Sammlungsaufträge](#).

Datenvisualisierungen

Das Dashboard Operational Technology Vulnerability Response (PA) verwendet Datenvisualisierungen, um Ihre OT-Schwachstellendaten anzuzeigen. Beispielsweise wird die Gesamtzahl der angreifbaren OT-Elemente in Ihrem System im Balkendiagramm **„Angreifbare OT-Elemente insgesamt“** angezeigt und nach OT-Gerät-Typ gruppiert.

Weitere Informationen zu den im Dashboard verwendeten Datenvisualisierungen finden Sie unter [Im Dashboard Operational Technology Vulnerability Response \(PA\) verwendete Datenvisualisierungen](#).

Operational Technology Dashboard „Schwachstellenrisiko-Rollup“.

Das Dashboard Operational Technology (OT) Rollup für Schwachstellenrisiken enthält die Risikopunktzahl der OT-Geräte auf jeder Ebene des Anlagenmodells.

Dashboard „OT Schwachstellenrisiko-Rollup“ – Übersicht

Das Dashboard „OT-Schwachstellenrisiko-Rollup“ enthält zwei Tabellen für Ihre Schwachstellenrisiko-Punktzahlen.

- Tabelle „Schwachstellenrisiko“ für Ihre Anlagenmodell-Entitäten
- Schwachstellenrisikotabelle für OT-Geräte ohne zugewiesene Site

Dashboard-Tabellen für OT-Schwachstellenrisiko-Rollup

Tabelle	Beschreibung
Tabelle „Schwachstellenrisiko“ für Ihre Anlagenmodell-Entitäten	Tabelle, in der die Risikopunktzahlen für die Anlagenmodell-Entitäten Ihrer Site und ihre angreifbaren Elemente angezeigt werden. Außerdem werden der Bereich, der das höchste Risiko darstellt, und die Anzahl der angreifbaren Elemente hervorgehoben.
Schwachstellenrisikotabelle für OT-Geräte ohne zugewiesene Site	Tabelle, die die Risikopunktzahlen und die Anzahl der angreifbaren Elemente für OT-Geräte anzeigt, die keinem Standort zugewiesen sind

Erforderliche Rollen zum Anzeigen des Dashboards

Für den Zugriff auf das Dashboard „OT-Schwachstellenrisiko-Rollup“ benötigen Sie die Rolle **sn_otvr.remediation_owner**.

Standortfilter

Sie können den Filter **Site** verwenden, um die Site zu suchen und auszuwählen, die Sie im Dashboard anzeigen möchten. Um auf den Site-Filter zuzugreifen und ihn zu verwenden, müssen Sie über die Rolle **cmdb_ot_isa_viewer** mit Zugriff auf die Site verfügen, die Sie anzeigen möchten.

Weitere Informationen finden Sie unter [Verwenden Sie den Site-Filter](#).

Operational Technology Fortschrittsbewertungsliste

Mit der Fortschrittsbewertungsliste Operational Technology für (OT) können Sie Gerätedaten und Daten zu angreifbaren Elementen zwischen Ihren Sites vergleichen.

Übersicht über die OT-Fortschrittsbewertungsliste

Die OT-Fortschrittsbewertungsliste ist ein zentraler Ort in Industriell Arbeitsbereich, mit dem Sie Ihre Site-Daten vergleichen können. Standortdaten umfassen sowohl OT-Gerät-Daten als auch Schwachstellendaten. Mit der OT-Fortschrittsbewertungsliste können Sie den Site-Fortschritt nachverfolgen und die Sites bestimmen, die Aufmerksamkeit erfordern.

Sie können auch die Standortdaten für die folgenden Operational Technology -Anwendungen anzeigen:

- Operational Technology Manager
- Operational Technology Vulnerability Response
- Incident-Management für operative Technologie
- Change-Management für operative Technologie

Inhalte der Bewertungsliste

Um auf die OT-Fortschrittsbewertungsliste zuzugreifen, navigieren Sie zu **Alle > Industrial Workspace** und wählen Sie das Symbol **OT-Fortschrittsbewertungsliste** ().

In der folgenden Tabelle werden Spalten in der OT-Fortschrittsbewertungsliste beschrieben.

Spalten der OT-Fortschrittsbewertungsliste

Spalte	Beschreibung
Gesamtpunktzahl (%)	Der Fortschritt Ihrer Website, der durch die -Indikatoren in der Bewertungsliste bestimmt wird. Sie können die Gewichtung bearbeiten, um zu steuern, wie viel ein Indikator zur Gesamtpunktzahl beiträgt. Weitere Informationen finden Sie unter Legen Sie die Systemeigenschaften für die Fortschrittsbewertungsliste Operational Technology fest .
% der erwarteten OT-Geräte in CMDB	Der Prozentsatz Ihrer OT-Geräte, den Sie voraussichtlich in Configuration Management Database (CMDB)haben.

Spalten der OT-Fortschrittsbewertungsliste (Fortsetzung)

Spalte	Beschreibung
	Hinweis: Wenn Sie einen Wert von –1 sehen, fehlt für mindestens einen der Werte im Indikator „% der erwarteten OT-Geräte in CMDB“ das Attribut „Erwartetes OT-Gerät“ in der Tabelle OTPSC-Attribute. Informationen zur Konfiguration von erwarteten OT-Geräten finden Sie unter Konfigurieren Sie die erwarteten OT-Geräte für eine Site.
Klassifizierte OT-Geräte (%)	Der Prozentsatz der klassifizierten OT-Geräte. Klassifizierte OT-Geräte (%) enthält keine OT-Geräte, die als cmdb_ci_ot klassifiziert sind.
Zugewiesene OT-Geräte (%)	Der Prozentsatz der OT-Geräte mit Werten in den folgenden Feldern: • Zugewiesen an • Eigentum von • Verwaltet von • Support durch • Freigabegruppe • Verwaltete Gruppe • Support by (Support durch) • Gruppe ändern
Vollständigkeit der OT-Gerätedaten (%)	Der Prozentsatz der OT-Geräte, die Ihre Datenziele erfüllen. Diese Metrik hängt vom Auftrag CMDB Integritäts-Dashboard – Berechnung der Vollständigkeitsbewertung ab, und Sie müssen die erforderlichen und empfohlenen Felder im CI-Klassenmanager festlegen. Weitere Informationen finden Sie unter Set up and configure CMDB Health . Vollständigkeit ist ein KPI, der durch die folgenden Metriken bestimmt wird: Erforderlich Misst den Prozentsatz der CIs, in denen als erforderlich definierte Felder nicht ausgefüllt sind. Fehlende Felder werden als unvollständig markiert mit dem Hinweis, dass für dieses CI einige Informationen fehlen. Empfohlen

Spalten der OT-Fortschrittsbewertungsliste (Fortsetzung)

Spalte	Beschreibung
	Misst den Prozentsatz der CIs, in denen empfohlene Felder nicht ausgefüllt sind. Weitere Informationen zur Vollständigkeit von Daten finden Sie unter CMDB Health KPIs and metrics .  Hinweis: Wenn Sie einen Wert von -1 sehen, wurde der Auftrag CMDB Integritäts-Dashboard – Berechnung der Vollständigkeitsbewertung noch nicht ausgeführt. Oder der Auftrag wurde mit einem Status „Unvollständig“ ausgeführt.
Zugeordnete OT-Geräte (%)	Der Prozentsatz der OT-Geräte, die einer Anlagenmodell-Entität zugeordnet sind.  Hinweis: Wenn Sie einen Wert von 0 sehen, wurden keine OT-Geräte gefunden.
Gesicherte OT-Geräte (%)	Der Prozentsatz der OT-Geräte mit erstellten Sicherungsdatensätzen.  Hinweis: Wenn Sie einen Wert von 0 sehen, wurden keine OT-Geräte gefunden.
Zugewiesene angreifbare OT-Elemente (%)	Der Prozentsatz der angreifbaren OT-Elemente, die nicht geschlossen und behandelt wurden.  Hinweis: Wenn Sie einen Wert von 0 sehen, wurden keine OT-Geräte gefunden.
Genehmigte OT-Change-Anforderungen (%)	Der Prozentsatz der OT-Change-Anforderungen, die übermittelt und genehmigt wurden.  Hinweis: Wenn Sie einen Wert von 0 sehen, wurden keine OT-Geräte gefunden.
OT-Incidents mit OT-Kontext (%)	Der Prozentsatz der OT-Incidents, die OT-Gerät- oder Anlagenmodell-Daten enthalten.  Hinweis: Wenn Sie einen Wert von 0 sehen, wurden keine OT-Geräte gefunden.

Operational Technology Experience mit einheitlicher Übersicht im Industrial Workspace

Die einheitliche Übersicht Operational Technology (OT), die in Industrial Workspace verfügbar ist, bietet eine einheitliche Experience, um die Beziehungen zwischen Geräten und anderen Configuration Items (CIs) anzuzeigen und zugehörige Elemente wie OT-Incidents und Change-Anforderungen anzuzeigen.

Übersicht über einheitliche Übersicht

Die Experience der einheitlichen OT-Übersicht zeigt eine hierarchische Zuordnung von CIs und ihren Beziehungen, während sie auf einem ausgewählten CI zentriert ist, das als Startknoten bezeichnet wird. Die Experience von kombiniert die Fähigkeiten von Abhängigkeitsansichten und Service-Mapping in einer einzigen Zuordnungs-Experience.

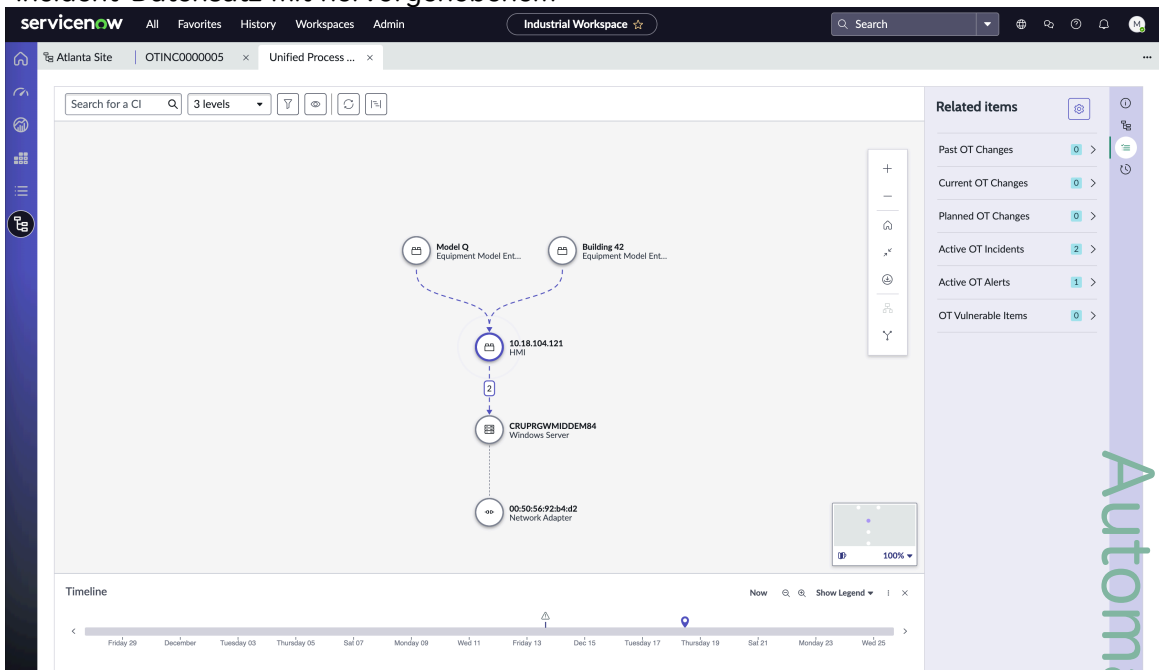
Sie können an folgenden Stellen in Industrial Workspace auf eine einheitliche Übersicht zugreifen.

- ISA-Datensatz im Anlagenmodell-Manager
- OT-Incident-Datensatz
- OT-Change-Datensatz

In der einheitlichen Übersicht können Sie auch die hervorgehobenen Knoten der folgenden zugehörigen Elemente sehen.

- Bisherige OT-Changes
- Aktuelle OT-Changes
- Geplante OT-Changes
- Aktive OT-Incidents
- Aktive OT-Warnungen
- Angreifbare OT-Elemente

Die folgende Abbildung zeigt eine einheitliche Übersicht für einen OT-Incident-Datensatz mit hervorgehobenem



Startknoten.

Weitere Informationen zum Konfigurieren der Experience von OT Einheitliche Übersichten finden Sie unter [Einrichten der Experience Operational Technology Einheitliche Übersicht](#).

Weitere Informationen zum Anzeigen einer einheitlichen OT-Übersicht finden Sie unter [Zeigen Sie eine Operational Technology Einheitliche Übersicht an](#).

Operational TechnologyBewertung von Hardware-Schwachstellen

Mit der Anwendung Operational Technology (OT) Bewertung von Hardware-Schwachstellen (HVA) können Sie die Firmware-Schwachstellen der OT-Geräte in Ihres Bestands bewerten und angreifbare Elemente (VIT) für die betroffenen OT-Geräte erstellen.

Bewertung von Hardware-Schwachstellen – Übersicht

Bewertung von Hardware-Schwachstellen verwendet normalisierte Inhalte für das Firmware-Discovery-Modell und das Common Platform Enumeration-Format (CPE), die von der National Vulnerability Database (NVD) bereitgestellt werden, um Bewertungen durchzuführen. Der normalisierte Inhalt enthält OT-Gerät-Daten wie Hersteller, Firmware-Version und Produktmodell. Sie basiert auf dem in Enterprise Asset Managementverfügbaren Normalisierungsprozess. Der normalisierte Inhalt für OT-Geräte wird den Common Vulnerabilities and Exposures (CVEs) zugeordnet, die in im NVD verfügbar sind. Das Menü Hardware-Schwachstellenbewertung, das in Industrial Workspace verfügbar ist, zeigt die OT-Geräte an, die gefährdet sind, wenn die CVE-Daten mit den im normalisierten Inhalt verfügbaren OT-Gerät-Daten übereinstimmen.

Sie müssen die folgenden geplanten Aufgaben ausführen, um automatisch und regelmäßig eine Hardware-Schwachstellenbewertung durchzuführen:

- *Hardware Vulnerability Assessment - Full*
- *Hardware Vulnerability Assessment - Delta*

Erforderliche Rollen Operational Technology und Bewertung von Hardware-Schwachstellen.

Sie müssen über die folgenden Rollen verfügen, um das Menü Bewertung von Hardware-Schwachstellen (HVA) verwenden zu können:

- **sn_vul.manage_exposure_assessment:** Weisen Sie Administratoren oder Anwendergruppen nach Bedarf Rollen zu, damit sie Eigenschaften für HVA-Anzeigen oder bearbeiten können.
- **sn_otvr.vul_event_manager (OT-Schwachstellenereignis-Manager):** Weisen Sie Anwendern oder Anwendergruppen von Hardware-Schwachstellen nach Bedarf Rollen zu, damit sie Bewertungsdatensätze anzeigen und entsprechend handeln können.

Anwendungsfall

Mit HVA können Analysten für OT-Hardware-Schwachstellen:

- Identifizieren Sie Cybersicherheitsrisiken in OT-Geräten.
- Fokus auf Schwachstellen mit hohem Risiko, indem Bewertungen von und für OT-Gerät-Daten vollständig abgeglichen werden.
- Richten Sie die automatische Erstellung von angreifbaren Elementen für vollständig abgeglichene Bewertungen ein.
- Untersuchen und beheben Sie teilweise übereinstimmende Bewertungen, um potenzielle Risiken zu identifizieren und entsprechend zu handeln.
- Überwachen Sie unverarbeitete OT-Geräte auf der Registerkarte **Warten auf Normalisierung**, für die die vollständige Erkennung oder Inhaltsaktualisierungen ausstehen.

HVA-Registerkarten

Das Menü HVA zeigt HVA -Datensätze an, die für die OT-Geräte erstellt wurden. Diese Bewertungsdatensätze werden basierend auf vielen Kriterien erstellt. Beispiel: CVE-Schwachstelle, gefährdetes OT-Gerät, Bewertung des Common Vulnerability Bewertungssystems (CVSS) und Geräterelevanz.

- Auf der Registerkarte **„Bewertungen mit vollständiger Übereinstimmung“** werden die Bewertungsdatensätze angezeigt, bei denen die CVEs vollständig mit dem Hersteller, dem Produktmodell und der Firmware-Version der OT-Geräte übereinstimmen. Eine vollständig übereinstimmende Bewertung bedeutet, dass ein OT-Gerät alle in einem CVE angegebenen Schwachstellenfaktoren erfüllt.
- Auf der Registerkarte **Teilweise abgeglichene Bewertungen** werden die Bewertungsdatensätze angezeigt, bei denen die CVEs teilweise mit dem Hersteller und dem Modell auf dem OT-Gerät übereinstimmen, die Übereinstimmung der Firmware-Version ist jedoch unbestimmt.
- Auf der Registerkarte **Angreifbare Elemente** werden die VITs angezeigt, die automatisch erstellt werden, oder , die Sie manuell erstellen, basierend auf den Bewertungen.
- Auf der Registerkarte **Ignorierte Bewertungen** werden die Bewertungen der Geräte angezeigt, die Sie ignorieren möchten.
- Auf der Registerkarte **„Warten auf Normalisierung“** werden die OT-Gerät-Daten angezeigt, die nicht die normalisierten Daten enthalten und nicht für die Bewertung verwendet wurden.

Wichtig:

- Wenn die Eigenschaft zum Erstellen einer automatischen VIT aktiviert ist, werden auf der Registerkarte „**Vollständig übereinstimmende Bewertungen**“ keine Daten angezeigt. Sie können diese Informationen oder auf der Registerkarte „**Angreifbare Elemente**“ anzeigen.
- Aktivieren Sie die Opt-in-Funktion in Enterprise Asset Management, damit OT-Gerätedaten für die Normalisierung verfügbar sind. Weitere Informationen finden Sie unter [Opt-in to Enterprise Asset Management Content Service](#) .

Löschen Sie veraltete Bewertungen

Sie können auch die automatische Löschung veralteter Bewertungsdatensätze einrichten.

1. Navigieren zu **Alle > Systemdatenverwaltung > Datenverwaltungsrichtlinien**.
2. Suchen Sie nach , und wählen Sie die Richtlinie **sn_vul_analyst_firmware_vulnerability_assessment** aus.
3. Konfigurieren Sie Bereinigungsregeln, und aktivieren Sie das Kontrollkästchen **Aktiv**.
4. Wählen Sie **Aktualisieren**.

Zugehörige Informationen

[Enterprise Asset Management normalization](#)

[Industriell Arbeitsbereich](#)

[Richten Sie ein und richten Sie die Bewertung von Hardware-Schwachstellen von Operational Technology -Geräten mithilfe des geführten Setups ein](#)

[Verwenden Sie und im Menü Bewertung von Hardware-Schwachstellen in Industrial Workspace](#)

Konfigurieren von Industriell Arbeitsbereich

Konfigurieren Sie Industriell Arbeitsbereich, um Ihre Operational Technology (OT)-Daten zu verwalten.

Wenn Sie über die Administratorrolle verfügen, können Sie sich von Geführtes Setup durch das Setup von Industriell Arbeitsbereich führen lassen. Geführtes Setup ist ein Tool, das bei der Konfiguration von Anwendungen oder Fähigkeiten hilft. Er ordnet die Konfigurationsaktivitäten in Kategorien. Diese Kategorien enthalten Informationen zu den Setup-Aufgaben, die Schritte zum Abschließen jeder Aufgabe und die Links zu den Seiten in Ihrer Instanz, auf denen Sie die Konfiguration durchführen. Außerdem werden Links zu nützlichen Hilfeinhalten bereitgestellt.

Um auf Geführtes Setup zuzugreifen, navigieren Sie zu **Industrial Workspace-Administrator > Geführtes Setup**.

In der folgenden Tabelle sind die -Aufgaben Geführtes Setup und ihre Zwecke für Industriell Arbeitsbereich aufgeführt.

Industriell Arbeitsbereich Setup-Aufgaben

Aufgabe	Zweck
Weisen Sie die Rolle Industriell Arbeitsbereich zu.	Weist die Rolle Industrie-Arbeitsbereich konfigurieren [configure_industrial_workspace]

Industriell Arbeitsbereich Setup-Aufgaben (Fortsetzung)

Aufgabe	Zweck
	Benutzern zu, die Industriell Arbeitsbereich konfigurieren müssen.
Überprüfen Sie die Zielregeln der Homepage.	Leitet Anwender basierend auf Anwenderkriterien zu anderen Seiten in Industriell Arbeitsbereich um.
Schließen Sie die Konfigurationsaufgaben für die OT-aktionsorientierte Zielseite ab.	Konfiguriert die aktionsorientierte OT-Zielseite, sodass Anwender auf die Zielseite in Industriell Arbeitsbereich zugreifen können.
Schließen Sie die Konfigurationsaufgaben für die OT-Fortschrittsbewertungsliste ab.	Konfiguriert die OT-Fortschrittsbewertungsliste, damit Benutzer mit dem Vergleich von Standortdaten und Fortschritt in Industriell Arbeitsbereich beginnen können.
Schließen Sie die Konfigurationsaufgaben für das OT-Transparenz-Dashboard ab.	Konfiguriert die Registerkarten im OT-Transparenz-Dashboard, damit Anwender auf das Dashboard in Industriell Arbeitsbereich zugreifen können.
Schließen Sie die Konfigurationsaufgaben für das Dashboard Operational Technology Vulnerability Response (PA) ab.	Konfiguriert das Dashboard Operational Technology Vulnerability Response (PA) in Industriell Arbeitsbereich.
Schließen Sie die Konfigurationsaufgaben für die Experience der einheitlichen OT-Übersicht ab	Konfiguriert die Experience der einheitlichen OT-Übersicht, wenn Sie die Standardeinstellungen ändern möchten.

Weisen Sie die Rolle Industriell Arbeitsbereich zu

Weisen Sie Ihren Anwendern die Rolle Industriell Arbeitsbereich zu, damit Sie ihren Zugriff auf die Funktionen, Fähigkeiten und Daten des -Arbeitsbereichs steuern können.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Benutzer mit der in der folgenden Tabelle aufgeführten Rolle können auf Geführtes Setup für die OT-aktionsorientierte Zielseite und die OT-Fortschrittsbewertungsliste zugreifen.

Rolle für OT-Fortschrittsbewertungsliste

Rolle	Beschreibung
Industrial Workspace konfigurieren [configure_industrial_workspace]	Kann auf Industriell Arbeitsbereich und Geführtes Setup für die aktionsorientierte OT-Zielseite und die OT-Fortschrittsbewertungsliste zugreifen.

Prozedur

Weisen Sie Benutzern und Gruppen mit der Benutzerverwaltungsfunktion Now Platform Rollen zu.

Überprüfen Sie die Zielregeln der Homepage für Industriell Arbeitsbereich

Überprüfen Sie die Zielregeln der Homepage für Industriell Arbeitsbereich.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die Zielregeln der Homepage leiten Anwender basierend auf Anwenderkriterien zu verschiedenen Seiten in Industriell Arbeitsbereich weiter. Weitere Informationen zu den Zielregeln für Homepages finden Sie unter [Industrial Workspace Zielregeln für Homepages](#).

Prozedur

1. Navigieren Sie zu **Alle**.
2. Fügen Sie im Feld **Filter** `sys_homepage_destination_rule.list` hinzu.
3. Drücken Sie die Eingabetaste.
4. Wählen Sie eine der folgenden Industriell Arbeitsbereich Zielregeln für die Homepage aus, deren Anwenderkriterien Sie bearbeiten möchten:
 - Seite mit OT-Fortschrittsbewertungsliste
 - Industrial Workspace-Homepage
 - OT Dashboard-Bibliothekssseite

i Hinweis:
Die Regel „OT-Dashboard-Bibliothekssseite“ wird nur angezeigt, wenn Operational Technology Manager installiert ist.

 - Seite für Anlagenmodell nach ISA

i Hinweis:
Die Seitenregel „Anlagenmodell nach ISA anzeigen“ wird nur angezeigt, wenn Prozessmanager Industrie installiert ist.

 - Listenseite „Arbeitsbereich Industrie“.
5. Kopieren Sie im Feld **Benutzerkriterien** die Anwenderkriterien.
6. Führen Sie die folgenden Schritte aus, um die Anwenderkriterien anzuwenden, die Anwender auf die Seite im von Ihnen ausgewählten Industriell Arbeitsbereich umleiten.
 - a. Navigieren zu **Alle > Anwenderkriterien**.
 - b. Suchen Sie in der Suchleiste der Listenansicht nach den Anwenderkriterien der Homepage-Zielregel, die Sie in Schritt 5 kopiert haben.
 - c. Ändern Sie den Benutzerkriteriendatensatz so, dass die Benutzer, die Sie umleiten möchten, den Anwenderkriterien entsprechen.
 - d. Wählen Sie **Aktualisieren**.

Ergebnisse

Die im Benutzerkriteriendatensatz definierten Benutzer, Gruppen und Rollen werden jetzt automatisch zur ausgewählten Seite in Industriell Arbeitsbereichumgeleitet.

Einrichtung der aktionsorientierten Zielseite „Operative Technologie“

Richten Sie die aktionsorientierte Zielseite Operational Technology (OT) in Industriell Arbeitsbereich ein, damit Ihre Anwender auf ihre kritischen Aufgaben zugreifen können.

In der folgenden Tabelle sind die Geführtes Setup -Aufgaben und ihre Zwecke für die OT-aktionsorientierte Zielseite aufgeführt.

Setup-Aufgaben für die OT-aktionsorientierte Zielseite

Aufgabe	Zweck
1. Legen Sie die Systemeigenschaften für die OT-aktionsorientierte Zielseite fest.	Ändert die Anzahl der unter „ Wichtige Aktionen “ angezeigten Karten mit der Systemeigenschaft <code>sn_mfg_common.landing_page_important_actions_limit</code> .

Legen Sie die Systemeigenschaften für die aktionsorientierte Zielseite Operational Technology fest

Legen Sie die Systemeigenschaften für die aktionsorientierte Zielseite Operational Technology (OT) fest, damit Sie die Eigenschaften nach Bedarf aktivieren können.

Vorbereitungen

Erforderliche Rolle: konfigurieren_industrial_workspace

Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > Systemeigenschaften des Arbeitsbereichs**.
2. Bearbeiten Sie die folgenden Eigenschaften nach Bedarf.

Systemeigenschaft	Beschreibung
Systemeigenschaften der OT-Startseite (aktionsorientierte Zielseite).	
<code>sn_mfg_common.landing_page_important_actions_limit</code>	Maximale Anzahl der wichtigen Aktionen, die für den Abschnitt „ Wichtige Aktionen “ auf der OT-aktionsorientierten Zielseite abgerufen werden. Der Standardwert ist 50.

3. Wählen Sie **Speichern**.

Operational Technology Fortschrittsbewertungsliste einrichten

Richten Sie die Fortschrittsbewertungsliste für Operational Technology (OT) in Industriell Arbeitsbereich ein, damit Ihre Anwender Site-Daten und Fortschritt vergleichen können.

In der folgenden Tabelle sind die Geführtes Setup -Aufgaben und ihre Zwecke für die OT-Fortschrittsbewertungsliste aufgeführt.

Setup-Aufgaben für OT-Fortschrittsbewertungsliste

Aufgabe	Zweck
1. Weisen Sie die Rollen der OT-Fortschrittsbewertungsliste zu.	Weisen Sie Ihren Anwendern die Rollen der OT-Fortschrittsbewertungsliste zu, damit Sie ihren Zugriff auf die Funktionen, Fähigkeiten und Daten der OT-Fortschrittsbewertungsliste steuern können.
2. Validieren Sie die Berechnung der Vollständigkeitsbewertung.	Validieren Sie, dass „ CMDB-Integritäts-Dashboard – Berechnung der Vollständigkeitsbewertung “ zur

Setup-Aufgaben für OT-Fortschrittsbewertungsliste (Fortsetzung)

Aufgabe	Zweck
	Ausführung aktiviert ist, wenn Sie den Indikator „ Vollständigkeit der OT-Gerätedaten (%) “ in die OT-Fortschrittsbewertungsliste aufnehmen möchten.
3. [Optional] Überprüfen Sie die Indikatorquellen.	Prüft die Indikatorquellen für eine größere Anzahl von Datensätzen. Wenn Sie mehr als den Standardwert von insgesamt 1 Million Datensätzen erwarten, müssen Sie die Datensatzsammlung überschreiben.
4. Konfigurieren Sie die erwarteten OT-Geräte für eine Site.	Konfigurieren Sie die Anzahl der erwarteten OT-Geräte für eine Site, damit Sie den Indikator „ % der erwarteten OT-Geräte in CMDB “ in der OT-Fortschrittsbewertungsliste verwenden können.
5. Schließen Sie den Auftrag „[OTPSC] Monatliche Datensammlung“ ab.	Sammelt die täglichen Daten für alle Indikatoren von Performance Analytics für die Registerkarte „OT-Fortschrittsbewertungsliste“ und zeigt sie an. Sie müssen diesen Schritt abschließen, bevor andere die Daten auf dieser Registerkarte anzeigen können.
6. Konfigurieren Sie die Indikatoren der OT-Fortschrittsbewertungsliste.	Konfigurieren Sie die Indikatoren der OT-Fortschrittsbewertungsliste so, dass die Anzeige jedes Indikators Ihren Anforderungen entspricht.
7. Legen Sie die Systemeigenschaften für die OT-Fortschrittsbewertungsliste fest.	Konfiguriert die Schwellenwerte, die in der OT-Fortschrittsbewertungsliste angezeigt werden, und die Komponenten, die zur Bestimmung der berechneten Punktzahl verwendet werden.
8. Passen Sie den Modulnamen an.	Passen Sie den Modulnamen der OT-Fortschrittsbewertungsliste an, um den Namen vom Standardwert in einen Namen zu ändern, der Ihren Anforderungen besser entspricht.

Weisen Sie die Operational Technology Fortschrittsbewertungslisten-Rollen zu

Weisen Sie Ihren Anwendern die Rollen Operational Technology (OT) Fortschrittsbewertungsliste zu, damit Sie ihren Zugriff auf die Funktionen, Fähigkeiten und Daten der OT-Fortschrittsbewertungsliste steuern können.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Benutzer mit der in der folgenden Tabelle aufgeführten Rolle können die OT-Fortschrittsbewertungsliste verwenden.

Rolle für OT-Fortschrittsbewertungsliste

Rolle	Beschreibung
Betrachter der OT-Fortschrittsbewertungsliste [ot_progress_scorecard_viewer]	Kann die OT-Fortschrittsbewertungsliste mit allen verfügbaren Site-Daten anzeigen.

Rolle für OT-Fortschrittsbewertungsliste (Fortsetzung)

Rolle	Beschreibung
Editor für OT-Fortschrittsbewertungsliste [ot_progress_scorecard_editor]	Kann die OT-Fortschrittsbewertungsliste mit allen verfügbaren Site-Daten anzeigen und bearbeiten.

Prozedur

Weisen Sie Benutzern und Gruppen mit der Benutzerverwaltungsfunktion Now Platform Rollen zu.

Validiert die Berechnung der Vollständigkeitsbewertung

Validieren Sie, dass „**CMDB-Integritäts-Dashboard – Berechnung der Vollständigkeitsbewertung**“ für die Ausführung aktiviert ist, wenn Sie den Indikator „**Vollständigkeit der OT-Gerätedaten (%)**“ in die Fortschrittsbewertungsliste Operational Technology (OT) aufnehmen möchten.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > Geführtes Setup**.
2. Wählen Sie im Abschnitt „**Industrial Workspace**“ **OT-Fortschrittsbewertungsliste** aus.
3. Wählen Sie in der Aufgabe „**Berechnung der Vollständigkeitsbewertung validieren**“ die Option **Konfigurieren aus**.
4. Validieren Sie im Datensatz „**CMDB-Integritäts-Dashboard – Geplante Skriptausführung für die Berechnung der Vollständigkeitsbewertung**“ die folgenden Elemente:
 - a. Stellen Sie sicher, dass das Kontrollkästchen **Aktiv** aktiviert ist.
 - b. Um sicherzustellen, dass genaue Punktzahlen für das Reporting zum Monatsende gesammelt werden, überprüfen Sie, ob das Feld **Ausführen** konfiguriert ist
5. Wählen Sie **Aktualisieren**.

Weitere Informationen zur Berechnung der Vollständigkeit finden Sie im Abschnitt „**Vollständigkeit**“ in [CMDB Health KPIs and metrics](#) .

Überprüfen Sie die Indikatorquellen für eine große Anzahl von Datensätzen

Überprüfen Sie die Indikatorquellen, wenn Sie eine große Anzahl von Datensätzen benötigen. Sie können die Datensatzsammlung überschreiben, sodass die Fortschrittsbewertungsliste Operational Technology (OT) mehr Datensätze als den Standardwert von 1 Million anzeigt.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Aufgrund der Migration mit Performance Analytics kann jeder Indikator der OT-Fortschrittsbewertungsliste standardmäßig nur 1 Million Datensätze anzeigen. Wenn Sie die Administratorrolle innehaben und die Datensätze nach der Ausführung der monatlichen Datensammlung [PA OTPSC] 1 Million überschreiten, werden Sie durch eine Fehlermeldung zu den Aufgabenprotokollen weitergeleitet.

i Hinweis:

Wenn Sie nicht über die Administratorrolle verfügen und die Datensätze nach der Ausführung des Auftrags „[OTPSC] Monatliche Datensammlung“ 1 Million überschreiten, werden Sie durch eine Fehlermeldung aufgefordert, sich an einen Administrator zu wenden, um Hilfe zu erhalten.

Wenn Sie über die Administratorrolle verfügen, können Sie die zugehörige Liste der Aufgabenprotokolle über den Link in der Fehlermeldung überprüfen und die Informationen herausfiltern, um zu sehen, welche Indikatorquelle den Fehler aufweist. Nachdem Sie die Indikatorquelle mit dem Fehler gefunden haben, können Sie die Indikatorquellen für eine größere Anzahl von Datensätzen ändern und die Indikatorquellendaten überschreiben. Dann wird für die anderen Benutzer keine Fehlermeldung mehr angezeigt, und die Daten werden für die Indikatorquelle angezeigt. Weitere Informationen zu den Indikatorquellen finden Sie unter [Indicator sources](#) .

i Hinweis:

Wenn Sie neue Indikatoren erstellen müssen, müssen Sie die Site-Aufgliederung verwenden, die in Industrial Workspace Common enthalten ist. Der Site-Aufgliederungsteil der Anwendung Operational Technology Manager ist veraltet.

Die Aufgabenprotokolle enthalten möglicherweise Fehler, die sich nicht auf die Indikatorquellen beziehen. Sie müssen den Datensatz der Aufgabenprotokolle anhand der Spalte „Ebene“ filtern und die Fehlermeldungen zu den Indikatorquellen finden.

Prozedur

1. Navigieren zu **Alle > Performance Analytics > Quellen > Indikatorquellen**.
2. Wenden Sie einen Filter an, indem Sie das Symbol Filter ein-/ausblenden () auswählen, und fügen Sie den folgenden Filter hinzu:
[Anwendung] [ist] [Industrial Workspace Common]
3. Wählen Sie den Indikatorquellendatensatz aus, den Sie ändern möchten.
Welche Indikatorquelle angepasst werden muss, können Sie dem Link „Aufgabenprotokolle“ in der Fehlermeldung entnehmen.
4. Aktivieren Sie auf der Registerkarte **Datensatzsammlung** das Kontrollkästchen neben dem Feld **Datensatzsammlung überschreiben**.
5. Ändern Sie den Wert im Feld **Maximale Anzahl abgerufener Datensätze** in XM.
6. Wählen Sie **Aktualisieren**.

Konfigurieren Sie die erwarteten OT-Geräte für eine Site

Konfigurieren Sie die Anzahl der erwarteten OT-Geräte für eine Site, damit Sie den Indikator „% der erwarteten OT-Geräte in CMDB“ in der OT-Fortschrittsbewertungsliste verwenden können.

Vorbereitungen

Erforderliche Rolle: ot_progress_scorecard_editor und cmdb_ot_isa_viewer mit Site-Zugriff, der für relevante Sites über Anwenderkriterien zugewiesen ist

i Hinweis:

Weitere Informationen zum Standortzugriff über Benutzerkriterien finden Sie unter [Überprüfen Sie die Zielregeln der Homepage für Industriell Arbeitsbereich](#).

Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > Attribute der OT-Fortschrittsbewertungsliste**.
2. Wenn Sie einen Datensatz mit Ihrer Site erstellen müssen, führen Sie die folgenden Aktionen aus.
 - a. Wählen Sie **Neu**.
 - b. Fügen Sie im Feld **Website** Ihre Website hinzu.
 - c. Fügen Sie im Feld **Wert** die Anzahl der erwarteten OT-Geräte für diese Site hinzu.

Hinweis:

OT-Steuerungsmodule in diesem Wert nicht einbeziehen.

- d. Wählen Sie **Speichern**.

3. Wenn ein Datensatz mit Ihrer Site vorhanden ist und Sie die erwarteten Geräte ändern möchten, führen Sie die folgenden Aktionen aus.
 - a. Wählen Sie den Datensatz aus, den Sie bearbeiten möchten.
 - b. Ändern Sie im Feld **Wert** die Anzahl der erwarteten OT-Geräte für diese Site.

Hinweis:

OT-Steuerungsmodule in diesem Wert nicht einbeziehen.

- c. Wählen Sie **Aktualisieren**.

Konfigurieren Sie die Datensammlung für die Fortschrittsbewertungsliste Operational Technology .

Konfigurieren Sie die Datensammlung für die Fortschrittsbewertungsliste für Operational Technology (OT), damit Sie die täglichen Daten für alle Indikatoren von Performance Analytics sammeln und anzeigen können. Diese Konfiguration stellt sicher, dass Ihre OT-Daten in der Bewertungsliste genau angezeigt werden.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie den Auftrag „[OTPSC] Monatliche Datensammlung“ nicht ausführen, sind für die OT-Fortschrittsbewertungsliste keine Daten verfügbar. Wenn Sie über die Administratorrolle verfügen, wird eine Warnmeldung angezeigt, die Sie auffordert, die Aufgabe auszuführen.

Hinweis:

Wenn Sie keine Administratorrolle haben, wird eine Warnmeldung angezeigt, die Sie auffordert, sich an den Administrator zu wenden, um Hilfe zu erhalten.

Prozedur

1. Navigieren zu **Alle > Datenerfasser > Performance Analytics > Aufträge**.
Wenn Sie sich in der OT-Fortschrittsbewertungsliste befinden, navigieren Sie zur Tabelle „Geplante Datensammlung“, indem Sie in der Fehlermeldung **Auftrag jetzt ausführen** auswählen.
2. Wenden Sie einen Filter an, indem Sie das Symbol Filter anzeigen/ausblenden () wählen, und fügen Sie den Filter [Name] [ist] [[PA OTPSC] Monatliche Datensammlung] hinzu.

3. Beginnen Sie mit der Erfassung der Daten, indem Sie das Kontrollkästchen neben dem Feld **Aktiv** im Abschnitt mit den Auftragsparametern aktivieren, und planen Sie dann eine Zeit im Feld **Zeit**. Sie können die Daten manuell sammeln, indem Sie auf die Schaltfläche **Jetzt ausführen** klicken. Andernfalls werden beim Anzeigen der Registerkarte keine Daten angezeigt. Verwenden Sie die Schaltfläche **Jetzt ausführen** nur, wenn Sie den Auftrag zum ersten Mal ausführen. Die Daten, die nach diesem Punkt gesammelt werden, sollten zu einem geplanten Zeitpunkt gesammelt werden.
4. Überprüfen Sie, ob die standardmäßige Zeitplan-Sammelungszeit für Sie geeignet ist. Die Standardzeit ist 00:00:00 Uhr am Anfang jedes Monats. Wenn Sie die Standardsammelungszeit ändern möchten, können Sie sie nach der Aktivierung des Auftrags ändern. Achten Sie darauf, Ihre Anwender über diese Änderung zu benachrichtigen.

Ergebnisse

Die OT-Fortschrittsbewertungsliste zeigt jetzt die richtigen Site-Daten für Ihre Anwender an.

Hinweis:

Die OT-Fortschrittsbewertungsliste verwendet Performance Analytics. Performance Analytics speichert die Punktzahlen nur 5 Monate lang. Wenn Sie Ihre Punktzahlen speichern und Standortdaten länger als 5 Monate vergleichen möchten, lesen Sie [Activating your Performance Analytics subscription](#) .

Konfigurieren Sie einen Indikator nach Schwellenwert, Gewichtung und Reihenfolge

Konfigurieren Sie die Indikatoren der Fortschrittsbewertungsliste für Operational Technology (OT) so, dass die Anzeige jedes Indikators Ihren Anforderungen entspricht.

Vorbereitungen

Erforderliche Rolle: ot_progress_scorecard_editor oder konfigurieren_industrial_workspace

Warum und wann dieser Vorgang ausgeführt wird

Sie können die folgenden Indikatoren konfigurieren.

- Gesamtpunktzahl (%)
- % der erwarteten OT-Geräte in CMDB
- Klassifizierte OT-Geräte (%)
- Zugewiesene OT-Geräte (%)
- Vollständigkeit der OT-Gerätedaten (%)
- Zugeordnete OT-Geräte (%)
- Gesicherte OT-Geräte (%)
- Genehmigte OT-Change-Anforderungen (%)
- OT-Incidents mit OT-Kontext (%)

Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > Konfiguration der OT-Fortschrittsbewertungsliste**.
2. Wählen Sie den Indikator aus, den Sie bearbeiten möchten.
3. Füllen Sie die folgenden Felder des Formulars aus.

Konfigurationsfelder für Indikatoren

Feld	Beschreibung
Niedriger Schwellenwert	Der niedrigste Schwellenwert, den der Indikator erfüllen kann
Hoher Schwellenwert	Der höchste Schwellenwert, den der Indikator erfüllen kann
Gewichtung	Gesamtgewichtung, mit der der Indikator zur Gesamtpunktzahl beiträgt.
Reihenfolge	Der Rang des Indikators nach Wichtigkeit von links nach rechts.

4. Wenn kein Indikator angezeigt werden muss, deaktivieren Sie das Feld **Aktiv**.

5. Wählen Sie **Aktualisieren**.

Legen Sie die Systemeigenschaften für die Fortschrittsbewertungsliste Operational Technology fest

Legen Sie die Systemeigenschaften für die Fortschrittsbewertungsliste Operational Technology (OT) fest, damit Sie die Eigenschaften nach Bedarf aktivieren können.

Vorbereitungen

Erforderliche Rolle: konfigurieren_industrial_workspace

Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > Systemeigenschaften des Arbeitsbereichs**.
2. Bearbeiten Sie die folgenden Eigenschaften nach Bedarf.

Systemeigenschaft	Beschreibung
Konfiguration der OT-Fortschrittsbewertungsliste	
sn_mfg_common.otpsc.page_title	Der Seitentitel, der in der OT-Fortschrittsbewertungsliste angezeigt wird. Der Standardwert ist OT-Fortschrittsbewertungsliste.
sn_mfg_common.otpsc.records_per_page	Die Anzahl der pro Seite angezeigten Datensätze. Der Standardwert ist 10.
sn_mfg_common.otpsc.low_threshold_color	Eine Farbe, die den unteren Schwellenwert in der OT-Fortschrittsbewertungsliste darstellt.
sn_mfg_common.otpsc.medium_threshold_color	Eine Farbe, die den mittleren Schwellenwert in der OT-Fortschrittsbewertungsliste darstellt.
sn_mfg_common.otpsc.high_threshold_color	Eine Farbe, die den hohen Schwellenwert in der OT-Fortschrittsbewertungsliste darstellt.

3. Wählen Sie **Speichern**.

Passen Sie den Modulnamen an

Passen Sie den Modulnamen der Fortschrittsbewertungsliste Operational Technology (OT) an, um den Namen vom Standardwert in einen Namen zu ändern, der Ihren Anforderungen besser entspricht.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle > Industrial Workspace-Administrator > Geführtes Setup**.
2. Wählen Sie im Modul **Industrial Workspace** den **Abschnitt OT-Fortschrittsbewertungsliste** aus.
3. Wählen Sie in der Aufgabe **[OPTIONAL] Customize Module Name (Modulnamen anpassen)** die Option **Konfigurieren** aus.
4. Bearbeiten Sie im Feld **Wert** den Wert für „Nachricht“ aus der OT-Fortschrittsbewertungsliste in einen Namen, der Ihren Anforderungen entspricht.
5. Wählen Sie **Aktualisieren**.

Einrichten des Transparenz-Dashboards Operational Technology

Schließen Sie die Aufgaben Geführtes Setup ab, um mit der Einrichtung des Dashboards Operational Technology (OT) Transparenz mit den Datensammlungen, Indikatorressourcen und Filtern für Ihre Organisation zu beginnen.

Um auf Geführtes Setup für das OT-Transparenz-Dashboard zuzugreifen, navigieren Sie zu **Alle > Industrial Workspace-Administrator > Geführtes Setup** und wählen Sie den Abschnitt „Dashboard für die Transparenz der operativen Technologie“ unter Operational Technology Manager aus.

Weitere Informationen zum OT-Transparenz-Dashboard und zu seinen Inhalten finden Sie unter [Operational Technology Transparenz-Dashboard](#).

Die folgende Tabelle zeigt die Geführtes Setup -Aufgaben, die zum Einrichten des -Dashboards verwendet werden.

Aufgaben des OT-Transparenz-Dashboards Geführtes Setup .

Aufgabe	Zweck
1. Schließen Sie den Auftrag „Tägliche Datensammlung für OT-Geräte“ ab.	Sammelt die täglichen Daten für alle Indikatoren von Performance Analytics für das Dashboard „OT-Transparenz“ und zeigt sie an. Sie müssen diesen Schritt abschließen, bevor andere die Dashboard-Daten anzeigen können.
2. [Optional] Überprüfen Sie die Indikatorquellen.	Prüft die Indikatorquellen für eine größere Anzahl von Datensätzen. Wenn Sie mehr als den Standardwert von insgesamt 1 Million Datensätzen erwarten, müssen Sie die Datensatzsammlung überschreiben.

Konfigurieren Sie die -Datenerfassung für Operational Technology -Geräte

Konfigurieren Sie die Datensammlung für Operational Technology (OT)-Geräte, damit Sie die täglichen Daten für alle Indikatoren von Performance Analytics erfassen und anzeigen können.

Diese Konfiguration stellt sicher, dass Ihre OT-Daten im Dashboard „OT-Transparenz“ genau angezeigt werden.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Wenn der Auftrag „Tägliche Datensammlung für OT-Geräte“ noch nicht ausgeführt wurde, bedeutet dies, dass für das Dashboard „OT-Transparenz“ keine Daten verfügbar sind und der Zeitstempel „**Zuletzt aktualisiert**“ ausgeblendet ist. Wenn Sie über die Administratorrolle verfügen, wird die folgende Warnmeldung angezeigt, die Sie auffordert, den Auftrag „Tägliche Datensammlung für OT-Geräte“ auszuführen:

ⓘ No Data is shown on the dashboard because the 'OT Devices Daily Data Collection' job has not been run yet. [Run job now](#)

Hinweis:

Wenn Sie keine Administratorrolle haben, wird eine Warnmeldung angezeigt, die Sie auffordert, sich an den Administrator zu wenden, um Hilfe zu erhalten.

Prozedur

1. Navigieren zu **Alle > Datenerfasser > Performance Analytics > Aufträge**.

Wenn Sie sich im Dashboard „OT-Transparenz“ befinden, können Sie zur Tabelle „Geplante Datensammlung“ navigieren, indem Sie in der Fehlermeldung **Auftrag jetzt ausführen** auswählen.

2. Wenden Sie einen Filter an, indem Sie das Symbol Filter anzeigen/ausblenden () wählen, und fügen Sie den Filter [Name] [ist] [Tägliche Datensammlung für OT-Geräte]hinzu.

3. Beginnen Sie mit der Erfassung der Daten, indem Sie das Kontrollkästchen neben dem Feld **Aktiv** im Abschnitt mit den Auftragsparametern aktivieren, und planen Sie dann eine Zeit im Feld **Zeit**. Sie können die Daten manuell sammeln, indem Sie auf die Schaltfläche **Jetzt ausführen** klicken. Andernfalls werden beim Anzeigen des Dashboards keine Daten angezeigt. Verwenden Sie die Schaltfläche **Jetzt ausführen** nur, wenn Sie den Auftrag zum ersten Mal ausführen. Die Daten, die nach diesem Punkt gesammelt werden, sollten zu einem geplanten Zeitpunkt gesammelt werden.

4. Überprüfen Sie, ob die standardmäßige Zeitplan-Sammelungszeit für Sie geeignet ist. Die Standardzeit ist täglich 00:00:00. Wenn Sie die Standardsammelungszeit ändern möchten, können Sie sie nach der Aktivierung des Auftrags ändern. Achten Sie darauf, Ihre Anwender über diese Änderung zu benachrichtigen.

Ergebnisse

Das OT-Transparenz-Dashboard zeigt jetzt die richtigen Daten für die gesammelten OT-Geräte für Ihre Anwender an.

Nächste Maßnahme

Jetzt können Sie die Indikatorquellen überprüfen und feststellen, ob Sie die standardmäßige Datensatzsammlung überschreiben müssen. Weitere Informationen finden Sie unter [Überprüfen Sie die Indikatorquellen für eine große Anzahl von Datensätzen](#).

Überprüfen Sie die Indikatorquellen für eine große Anzahl von Datensätzen

Überprüfen Sie die Indikatorquellen, wenn Sie eine große Anzahl von Datensätzen benötigen. Sie können die Datensatzsammlung überschreiben, sodass im Dashboard Operational Technology „(OT) Transparenz []“ mehr Datensätze als der Standardwert von 1 Million angezeigt werden.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Aufgrund der Migration mit Performance Analytics kann jeder Indikator des OT-Transparenz-Dashboards standardmäßig nur 1 Million Datensätze anzeigen. Wenn Sie über die Administratorrolle verfügen und die Datensätze nach der Ausführung des Auftrags „Tägliche Datensammlung für OT-Geräte“ 1 Million überschreiten, werden Sie durch eine Fehlermeldung zu den Auftragsprotokollen weitergeleitet.

i Hinweis:

Wenn Sie nicht über die Administratorrolle verfügen und die Datensätze nach der Ausführung des Auftrags „Tägliche Datensammlung für OT-Geräte“ 1 Million überschreiten, werden Sie durch eine Fehlermeldung aufgefordert, sich an einen Administrator zu wenden, um Hilfe zu erhalten.

Wenn Sie über die Administratorrolle verfügen, können Sie die zugehörige Liste der Aufgabenprotokolle über einen Link in der Fehlermeldung überprüfen und die Informationen herausfiltern, um zu sehen, welche Indikatorquelle den Fehler aufweist. Nachdem Sie die Indikatorquelle mit dem Fehler gefunden haben, können Sie die Indikatorquellen für eine größere Anzahl von Datensätzen ändern und die Indikatorquellendaten überschreiben. Dann wird für die anderen Benutzer keine Fehlermeldung mehr angezeigt, und die Daten werden für die Indikatorquelle angezeigt. Weitere Informationen zu den Indikatorquellen finden Sie unter [Indicator sources](#).

i Hinweis:

Wenn Sie neue Indikatoren erstellen müssen, müssen Sie die Site-Aufgliederung verwenden, die in Industrial Workspace Common enthalten ist. Der Site-Aufgliederungsteil der Anwendung Operational Technology Manager ist veraltet.

Die Aufgabenprotokolle enthalten möglicherweise Fehler, die sich nicht auf die Indikatorquellen beziehen. Sie müssen den Datensatz der Aufgabenprotokolle anhand der Spalte „Ebene“ filtern, um die Fehlermeldungen zu den Indikatorquellen zu finden.

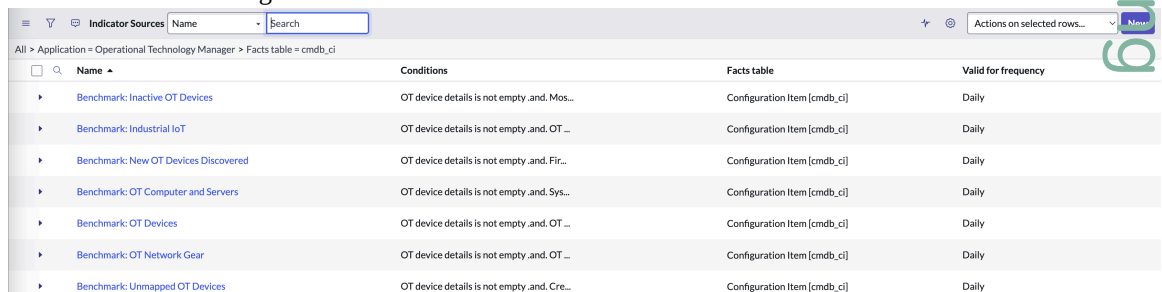
Prozedur

1. Navigieren zu **Alle > Performance Analytics > Quellen > Indikatorquellen**.

2. Wenden Sie einen Filter an, indem Sie das Symbol Filter ein-/ausblenden () wählen, und fügen Sie die folgenden Filter hinzu.

- [Anwendung] [ist] [Operational Technology Manager]
- [Faktentabelle] [ist] [cndb_ci]

Nach dem Anwenden der Filter zeigt die Tabelle sieben Geräteindikator-



Name	Conditions	Facts table	Valid for frequency
Benchmark: Inactive OT Devices	OT device details is not empty.and. Mos...	Configuration Item [cndb_ci]	Daily
Benchmark: Industrial IoT	OT device details is not empty.and. OT ...	Configuration Item [cndb_ci]	Daily
Benchmark: New OT Devices Discovered	OT device details is not empty.and. Fir...	Configuration Item [cndb_ci]	Daily
Benchmark: OT Computer and Servers	OT device details is not empty.and. Sys...	Configuration Item [cndb_ci]	Daily
Benchmark: OT Devices	OT device details is not empty.and. OT ...	Configuration Item [cndb_ci]	Daily
Benchmark: OT Network Gear	OT device details is not empty.and. OT ...	Configuration Item [cndb_ci]	Daily
Benchmark: Unmapped OT Devices	OT device details is not empty.and. Cre...	Configuration Item [cndb_ci]	Daily

Datensätze.

3. Wählen Sie den Indikatorquellendatensatz aus, den Sie ändern möchten.

Welche Indikatorquelle angepasst werden muss, können Sie dem Link „Aufgabenprotokolle“ in der Fehlermeldung entnehmen.

4. Aktivieren Sie auf der Registerkarte **Datensatzsammlung** das Kontrollkästchen neben dem Feld **Datensatzsammlung überschreiben**.

5. Ändern Sie den Wert im Feld **Maximale Anzahl abgerufener Datensätze** in XM.

6. Wählen Sie **Aktualisieren**.

Einrichtung des Dashboards Operational Technology Vulnerability Response (PA).

Richten Sie das Dashboard Operational Technology Vulnerability Response (PA) in Industriell Arbeitsbereich ein, damit Ihre Benutzer auf ihre kritischen Aufgaben zugreifen können.

In der folgenden Tabelle sind die Geführtes Setup -Aufgaben und ihre Zwecke für das Operational Technology Vulnerability Response (PA)-Dashboard aufgeführt.

Operational Technology Vulnerability Response Setup-Aufgaben für das Dashboard von (PA).

Aufgabe	Zweck
1. Konfigurieren Sie die Datensammlungsaufträge.	Sammelt die täglichen Daten für alle -Indikatoren von Performance Analytics für das OTVR (PA)-Dashboard und zeigt sie an. Sie müssen diesen Schritt abschließen, bevor andere die Daten auf dieser Registerkarte anzeigen können.
2. [Optional] Überprüfen Sie die Indikatorquellen.	Prüft die Indikatorquellen für eine größere Anzahl von Datensätzen. Wenn Sie mehr als den Standardwert von insgesamt 1 Million Datensätzen erwarten, müssen Sie die Datensatzsammlung überschreiben.

Konfigurieren Sie die Datensammlung für das Dashboard Operational Technology Vulnerability Response (PA).

Konfigurieren Sie die Datensammlung für die im Dashboard Operational Technology Vulnerability Response (PA) angezeigten Daten. Geplante Aufgaben sind automatisierte Aufgaben, die zu einem bestimmten Zeitpunkt oder nach einem wiederkehrenden Zeitplan ausgeführt werden können.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle > Datenerfasser > Performance Analytics > Aufträge**.

2. Wenden Sie einen Filter an, indem Sie das Symbol Filter ein-/ausblenden () auswählen, und fügen Sie die folgenden Filter hinzu.

- [Anwendung] [ist] [Operational Technology Vulnerability Response]
- [Klasse] [ist] [Geplante Datensammlung]

Wenn Sie den Filter anwenden, werden die folgenden geplanten Aufgaben angezeigt.

- [PA OT VR] Sammlung historischer Schwachstellendaten

Hinweis:

Die Aufgabe „[PA OT VR] Historische Schwachstellendatensammlung“ ist eine bedarfsgesteuerte Aufgabe, die Sie nur einmal ausführen müssen. Nachdem die Verlaufsdaten gesammelt wurden, werden die täglichen Datensammlungsaufgaben jeden Tag zu einer geplanten Zeit ausgeführt. Weitere Informationen zu Verlaufsdaten finden Sie unter [Collect historical data](#) .

- [PA OT VR] Tägliche Sammlung für Korrekturaufgaben
- [PA OT VR] Tägliche Sammlung für angreifbare Elemente 1
- [PA OT VR] Tägliche Sammlung für angreifbare Elemente 2
- [PA OT VR] Tägliche Sammlung für angreifbare Konfigurationselemente (CIs)

3. Um die Erfassung der Daten zu starten, wählen Sie den Datensatz einer geplanten Aufgabe aus.

4. Aktivieren Sie das Kontrollkästchen neben dem Feld **Aktiv** im Abschnitt „Auftragsparameter“, und planen Sie dann eine Zeit im Feld **Zeit**.

Sie können die Daten manuell sammeln, indem Sie auf die Schaltfläche **Jetzt ausführen** klicken. Andernfalls werden beim Anzeigen der Registerkarte keine Daten angezeigt. Verwenden Sie die Schaltfläche **Jetzt ausführen** nur, wenn Sie den Auftrag zum ersten Mal ausführen. Die Daten, die nach diesem Punkt gesammelt werden, sollten zu einem geplanten Zeitpunkt gesammelt werden.

5. Überprüfen Sie, ob die standardmäßige Zeitplan-Sammelungszeit für Sie geeignet ist.

Die Standardzeit ist täglich 00:00:00. Wenn Sie die Standardsammelungszeit ändern möchten, können Sie sie nach der Aktivierung des Auftrags ändern. Achten Sie darauf, Ihre Anwender über diese Änderung zu benachrichtigen.

6. Wiederholen Sie die Schritte 3 bis 5 für jede geplante Aufgabe.

Ergebnisse

Im Dashboard Operational Technology Vulnerability Response (PA) werden jetzt die richtigen Daten für Ihre Anwender angezeigt.

Nächste Maßnahme

Jetzt können Sie die Indikatorquellen überprüfen und feststellen, ob Sie die standardmäßige Datensatzsammlung überschreiben müssen. Weitere Informationen finden Sie unter [Überprüfen Sie die Indikatorquellen für eine größere Anzahl von Datensätzen](#).

Überprüfen Sie die Indikatorquellen für eine größere Anzahl von Datensätzen

Überprüfen und aktualisieren Sie eine Indikatorquelle, um die erwartete Datensatzanzahl zu überschreiben, wenn Sie erwarten, dass mehr als 1.000.000 Datensätze aus den Indikatorquellen gesammelt werden. Diese Aktion hilft, Probleme mit der Systemleistung beim Sammeln von Daten für Industriell Arbeitsbereich zu vermeiden.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle > Performance Analytics > Indikatoren > Automatisierte Indikatoren**.
2. Wenden Sie den Filter **[Anwendung] [ist] [Operational Technology Vulnerability Response]** an.
3. Wählen Sie in der Spalte Indikatorquelle den Indikatorquell Datensatz aus, den Sie bearbeiten möchten.
4. Aktivieren Sie im Abschnitt „Datensatzsammlung“ das Kontrollkästchen neben dem Feld **Datensatzsammlung überschreiben**.

5. Fügen Sie im Feld **Maximale Anzahl abgerufener Datensätze** eine Zahl hinzu, die größer als der Standardwert von 1.000.000 Datensätzen ist.
Zum Beispiel **2 Millionen**.
6. Wählen Sie **Aktualisieren**.

Einrichten der Experience Operational Technology Einheitliche Übersicht

Richten Sie die Experience der einheitlichen Übersicht von Operational Technology (OT) in Industrial Workspace ein, damit Ihre Anwender auf einheitliche Übersichten zugreifen können.

In der folgenden Tabelle sind die Geführtes Setup -Aufgaben und ihre Zwecke für die Experience der einheitlichen OT-Übersicht aufgeführt. Die Administratorrolle ist erforderlich.

Hinweis:

Diese Geführtes Setup -Aufgaben können optional abgeschlossen werden, da sie die Standardeinstellungen des verfügbaren Konfigurationsbezeichners ändern.

Diese Einstellungen für den Konfigurationsbezeichner betreffen alle Anwender. Einzelne Benutzer können die Einstellungen nicht konfigurieren.

Setup-Aufgaben für die OT Einheitliche Übersichts-Experience

Aufgabe	Zweck
Ändern Sie die Standardeinstellungen des Konfigurationsbezeichners für Industrial Workspace.	Ändern Sie die folgenden Standardeinstellungen des Konfigurationsbezeichners für Industrial Workspace, um die Experience der einheitlichen OT-Übersicht zu konfigurieren: • Konfigurationseigenschaften des -Arbeitsbereichs • Knotenzuordnungsprofile • Zugehörige Elemente der Knotenzuordnung • Modi des Betriebslebenszyklus • Tabellenattribute

Standardeinstellungen der Experience Operational Technology Einheitliche Übersicht

Sie können die Standardeinstellungen ändern, die für die Experience Einheitliche Übersicht von Operational Technology (OT) verfügbar sind.

Mit der Administratorrolle können Sie die Standardeinstellungen des Konfigurationsbezeichners für Industrial Workspace ändern, der in der einheitlichen OT-Experience verfügbar ist. Ein Konfigurationsbezeichner oder Konfigurationsbezeichner ist ein Konfigurationselement im Framework für Konfigurationsbezeichner. Ein Konfigurationsbezeichner enthält Einstellungen und tabellengesteuerte Konfigurationen, die in einer UX-Anwendung wie einem Arbeitsbereich verwendet werden.

Wenn keine Eigenschaft festgelegt ist oder keine Einträge in der tabellengesteuerten Konfiguration vorhanden sind, verwendet die Suche stattdessen die Werte im Standardkonfigurationsbezeichner. Weitere Informationen zum Framework für Konfigurations-Identifizierer finden Sie unter [Configuration identifiers framework](#) .

Um auf den Datensatz „Industrial Workspace Config Identifier“ zuzugreifen, navigieren Sie zu **Alle** und geben in der Filterleiste `sn_cmdb_ws_config_identifizier.liste` ein. Wählen Sie dann **Industrial Workspace Config Identifier** aus.

In den folgenden Abschnitten werden die Standardeinstellungen beschrieben, die im Konfigurationsbezeichner für Industrial Workspace geändert werden können.

Hinweis:

Die beschriebenen Einstellungen gelten für alle Benutzer. Einzelne Anwender können die Einstellungen nicht konfigurieren.

Konfigurationseigenschaften des Arbeitsbereichs

Standardmäßig sind die folgenden Konfigurationseigenschaften in der Liste `sn_cmdb_ws_config_property.list` aufgeführt und dem Standard-Konfigurationsbezeichner zugewiesen.

- `unifiedmap.map_search.max_nodes`
- `unifiedmap.map_search_filter.default_levels`
- `unifiedmap.map_search_filter.max_levels`
- `unifiedmap.map_search_filter.endpoint_deduplication_fields`

Knotenzuordnungsprofile

Sie können Profile konfigurieren, die Standardkartenfilter und die Standardkartenausrichtung für eine Klasse festlegen. Beispielsweise, um die Service-Mapping-Daten für die Klasse der zugeordneten Anwendungsservices anzuzeigen.

Diese Klassenprofile helfen bei der Identifizierung, welche Ebenen in der einheitlichen Übersicht für einen bestimmten Knoten für ein bestimmtes Konfigurationselement bzw. Configuration Item (CI) angezeigt werden. Klassenprofile werden angewendet, wenn für die aktuelle Zuordnung keine Filtervoreinstellung verwendet wird. Diese Anwendung tritt normalerweise auf, wenn Sie eine Zuordnung zum ersten Mal ohne Filtervoreinstellung laden oder wenn Sie die Filtervoreinstellung auf die Standardansicht festlegen.

Bei Klassenprofilen können Sie im Filterbereich nur die Kategorie „**Ebene**“ konfigurieren.

Knotenzuordnungsreferenzen

Zuordnungsreferenzen ermöglichen Verbindungen in der Zuordnung zwischen CIs aus zwei Klassen, die nicht durch eine Beziehung verbunden sind.

Zugehörige Knotenelemente zuordnen

Sie können das Modul Zugehörige Elemente in Einheitliche Übersicht verwenden, um die Kategorien zugehöriger Elemente festzulegen, die für CIs angezeigt werden, z. B. aktive Incidents und aktive Probleme. Wenn Sie das Modul Zugehörige Elemente auswählen, werden zugehörige Elemente im kontextbezogenen Seitenbereich nach Kategorien gruppiert.

Modi des Betriebslebenszyklus

Sie können den Betriebsstatus angeben, den CIs aufweisen müssen, um in die einheitliche Übersicht aufgenommen zu werden.

Tabellenattribute

Jede Klasse verfügt über einen eindeutigen Satz erweiterter Eigenschaften, die im Bereich Attribute für einheitliche Übersicht für ein CI angezeigt werden. Viele allgemeine Klassen

sind mit diesen Eigenschaften vorkonfiguriert. Sie können die Standardeinstellungen ändern und erweiterte Eigenschaften für zusätzliche Klassen global konfigurieren.

Richten Sie ein und richten Sie die Bewertung von Hardware-Schwachstellen von Operational Technology -Geräten mithilfe des geführten Setups ein

Verwenden Sie das geführte Setup Administrator für den industriellen Arbeitsbereich g, um durch die Konfiguration der Funktion Bewertung von Hardware-Schwachstellen zu führen, die im Menü Industrial Workspace verfügbar ist.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Verwenden Sie das geführte Setup für Administrator für den industriellen Arbeitsbereich, um die erforderlichen Anwenderrollen zuzuweisen, für eine Systemeigenschaft für zu konfigurieren und Aufgaben zur Durchführung der Hardware-Schwachstellenbewertung von Operational Technology -Geräten zu planen.

Prozedur

- 1. Navigieren zu **Alle > Industrial Workspace-Administrator > Geführtes Setup > Operational Technology Vulnerability Response**.
- 2. Wählen Sie **Erste Schritte** für die Anwendung *Operational Technology Vulnerability Response* aus.
- 3. Wählen Sie die Aufgabe *Bewertung von Hardware-Schwachstellen* aus.
- 4. Wählen Sie die folgenden Aufgabenregisterkarten aus, und wählen Sie dann **Konfigurieren** aus, um die Konfigurationsaufgaben abzuschließen.

Zugehörige Informationen

- [Guided Setup](#)
- [Operational TechnologyBewertung von Hardware-Schwachstellen](#)

Weisen Sie Rollen für zu Bewertung von Hardware-Schwachstellen

Weisen Sie Anwendern Rollen zu, damit sie Eigenschaften konfigurieren und Funktionen, Fähigkeiten und Daten von Hardware-Schwachstellenbewertungen verwenden können.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Weisen Sie die folgenden Rollen Anwendern und Anwendergruppen oder Anwendern von Hardware-Schwachstellenanalysten zu, die in der folgenden Tabelle aufgeführt sind:

Bewertung von Hardware-Schwachstellen roles

Rolle	Beschreibung
[sn_vul.manage_exposure_assessment]	Kann Eigenschaften für Bewertung von Hardware-Schwachstellenanzeigen oder bearbeiten.
Manager für OT-Schwachstellenereignisse	Kann Bewertungen in Bezug auf Bewertung von Hardware-Schwachstellenanzeigen und durchführen.

Bewertung von Hardware-Schwachstellen roles (Fortsetzung)

Rolle	Beschreibung
[sn_otvr.vul_event_manager]	

Prozedur

1. Navigieren zu **Zuweisung von Anwenderrollen > Konfigurieren > Anwender**.
2. Weisen Sie Benutzern und Gruppen mit der Benutzerverwaltungsfunktion Now Platform Rollen zu.

Konfigurieren Sie die Eigenschaft für Bewertung von Hardware-Schwachstellen, um VIT automatisch zu erstellen

Konfigurieren Sie diese Eigenschaft, um automatisch angreifbare Elemente (VIT) basierend auf der Hardware-Schwachstellenbewertung zu erstellen.

Vorbereitungen

Erforderliche Rolle: sn_vul.manage_exposure_assessment

Warum und wann dieser Vorgang ausgeführt wird

Durch die Konfiguration dieser Eigenschaft wird bestimmt, ob für vollständig abgestimmte Hardware-Schwachstellenbewertungen automatisch neue Datensätze für angreifbare Elemente erstellt werden. Alternativ können Sie VITs auch manuell erstellen.

Prozedur

1. Navigieren zu **Konfigurieren der Eigenschaften der Schwachstellenbewertung > Konfigurieren > Vulnerability Response-Eigenschaften > Schwachstellenbewertung**.
2. Wählen Sie **Ja**.

Der Standardwert lautet **Ja**.

Wenn diese Option auf **Ja** festgelegt ist, werden für vollständig übereinstimmende Hardware-Schwachstellenbewertungen automatisch neue Datensätze für angreifbare Elemente erstellt. Wenn Sie VITs manuell erstellen möchten, können Sie den Wert auf **Nein** festlegen.

3. Wählen Sie **Speichern**.

Führen Sie geplante Aufgaben aus, um auszuführen Bewertung von Hardware-Schwachstellen

Führen Sie geplante Aufgaben aus, um eine Schwachstellenbewertung der Hardware durchzuführen.

Vorbereitungen

Erforderliche Rolle: sn_otvr.vul_event_manager

Bewertung von Hardware-Schwachstellen basiert auf der Schwachstellenbewertungsfunktion in Vulnerability Response. Navigieren Sie vor dem Planen der Aufgaben für HVAz zu **Alle > Vulnerability Response > Administration > Integrationen** und führen Sie die folgenden National Vulnerability Database (NVD) Integrationen aus:

NVD-Integrationen

Integration	Beschreibung
NIST National Vulnerability Database Integration – API (nur CVE)	Ruft nur NIST NVD-Schwachstellendaten (CVE) ab. Standardmäßig ist diese Integration auf „Täglich ausgeführt“ festgelegt.
NIST National Vulnerability Database Integration-API (nur CPE)	Ruft CPE-Daten von dem National Institute of Standards and Technology (NIST) NVD ab. Diese Integration ist standardmäßig inaktiv. Aktivieren Sie diese Integration, um CPE-Daten zu erfassen, die ein formales Namensformat, eine Methode zum Überprüfen von Namen mit einem System und ein Beschreibungsformat zum Binden von Text und Tests an einen Namen umfassen. Diese Informationen werden in der Software vangreifbare Elemente gespeichert. Diese Integration wird täglich ausgeführt und ist standardmäßig inaktiv. Weitere Informationen finden Sie unter Activate the NIST National Vulnerability Database-API (CPE only) .
NIST National Vulnerability Database Integration-API (Nicht zugeordnete CPE)	Ruft CPE-Daten ab, die dem abgerufenen CVE von dem NIST NVD zugeordnet sind. Diese Integration ist standardmäßig inaktiv. Aktivieren Sie diese Integration, um CPE-Daten zu erfassen, die ein formales Namensformat, eine Methode zum Überprüfen von Namen mit einem System und ein Beschreibungsformat zum Binden von Text und Tests an einen Namen umfassen. Diese Informationen werden in einer zugehörigen Liste für einen NVD-Schwachstelleneintragsdatensatz gespeichert. Diese Integration ist auf die Ausführung bei Bedarf festgelegt und standardmäßig inaktiv. Weitere Informationen finden Sie unter Activate the NIST National Vulnerability Database-API (Unmapped CPE) .

Weitere Informationen finden Sie unter:

- [Understanding the NVD integrations](#) .
- [Install the Vulnerability Response Integration with the NIST National Vulnerability Database](#) .

Warum und wann dieser Vorgang ausgeführt wird

Sie müssen die folgenden geplanten Aufgaben ausführen, um Firmware-Schwachstellen von OT-Geräten im Bestand zu erkennen:

Prozedur

1. Navigieren zu **Geplante Aufgaben zur Schwachstellenbewertung > Konfigurieren > Geplante Aufgaben**.

Wichtig:

- Sie müssen **„Hardwarebewertung – Vollständig“** ausführen, bevor Sie die Aufgabe **„Hardwarebewertung – Delta“** planen. Sie können die **Aufgabe „Hardwarebewertung – Vollständig“** bei Bedarf ausführen.
- Sie können den Auftrag **„Hardwarebewertung – Delta“** so planen, dass er täglich, wöchentlich oder entsprechend Ihrer gewünschten Häufigkeit ausgeführt wird.

2. Auswahlvorgang **Hardwarebewertung – Vollständig > Jetzt ausführen**.

Dieser Auftrag führt eine Bewertung für alle OT-Geräte im Bestand durch, um Firmware-Schwachstellen unabhängig von vorherigen Bewertungen zu erkennen.

3. Auswahlvorgang **Hardwarebewertung – Delta > Aktiv**.

Wählen Sie **Ausführen** und anschließend eine Häufigkeit aus der Liste aus. Der Auftrag **„Hardwarebewertung – Delta“** wird gemäß der von Ihnen ausgewählten Häufigkeit ausgeführt.

Dieser Auftrag führt inkrementelle Bewertungen durch, die nur Änderungen oder Aktualisierungen seit dem letzten Bewertungslauf zum Ziel haben. Erfasst Änderungen an Firmware, normalisierten Inhalten und Schwachstellen seit der letzten erfolgreichen Ausführung der Hardware-Schwachstellenbewertung. Dieser Auftrag stellt eine kontinuierliche Überwachung und rechtzeitige Aktualisierungen sicher.

Zugehörige Informationen

[Scheduled jobs](#) 

Verwenden von Industriell Arbeitsbereich

Nachdem Sie alle erforderlichen Setupaufgaben für Industrial Workspace abgeschlossen haben, können Benutzer mit der Verwaltung ihrer Operational Technology -Daten auf den verschiedenen Seiten und Dashboards beginnen, die in Industrial Workspace verfügbar sind.

Industrial Workspace Zielregeln für Homepages

Abhängig von den Ihnen zugewiesenen Rollen werden Sie zu verschiedenen Seiten im Industriell Arbeitsbereich mit Homepage-Zielregeln weitergeleitet. Dadurch können Sie schneller und effizienter auf die benötigten Daten zugreifen.

Übersicht über die Zielregeln der Homepage

Jede Zielregel leitet verschiedene OT-Anwender basierend auf der ihnen zugewiesenen Rolle oder Rollen zu verschiedenen Seiten im Industriell Arbeitsbereich um. Einige Rollen haben möglicherweise keinen Zugriff auf die Daten auf einer Seite. Wenn Sie Benutzer auf eine Seite umleiten, auf der Daten zur Ansicht verfügbar sind, können sie besser in Industriell Arbeitsbereich navigieren. Beispielsweise können Benutzer, die nur über die Rolle „Editor für operative Technologie“ [cmdb_ot_editor] verfügen, keine Daten auf der OT-aktionsorientierten Zielseite anzeigen, sondern sehen nur eine leere Zielseite. Stattdessen werden sie zu den Listen des Arbeitsbereichs Industrie weitergeleitet, wo sie die entsprechenden OT-Gerät-Daten anzeigen können.

Industriell Arbeitsbereich Beschreibungen der Zielregel für Homepage

In der folgenden Tabelle werden die Zielregeln der Homepage Industriell Arbeitsbereich und ihre Ziele beschrieben.

Zielregeln für Homepage

Regel	Ziel	Rollen umgeleitet	Beschreibung
Seite mit OT-Fortschrittsbewertungsliste	now/mfg/ot-progress-scorecard/ (OT-Fortschrittsbewertungsliste)	ot_progress_scorecard_viewer	Über die Regel der OT-Fortschrittsbewertungsliste werden Benutzer mit den in der Regel beschriebenen Rollen bei der Anmeldung direkt zur OT-Fortschrittsbewertungsliste weitergeleitet.
Industrial Workspace-Homepage	now/mfg/home (OT-aktionsorientierte Zielseite)	• sn_ot_incident_read • sn_ot_change_read • sn_otvr.remediation_owner	Die Regel „Industrial Workspace Homepage“ leitet Anwender mit den in der Regel beschriebenen Rollen bei der Anmeldung direkt zur OT-aktionsorientierten Zielseite.
OT Dashboard-Bibliothekssseite	now/mfg/dashboard-library (OT-Dashboard-Bibliothek)	cmdb_ot_viewer + cmdb_ot_isa_viewer	Über die Regel „OT-Dashboard-Bibliothekssseite“ gelangen Benutzer mit den in der Regel beschriebenen Rollen bei ihrer Anmeldung direkt zum OT-Transparenz-Dashboard. ⓘ Hinweis: Die Regel „OT-Dashboard-Bibliothekssseite“ wird nur angezeigt, wenn Operational Technology Manager installiert ist.
Seite für Anlagenmodell nach ISA	now/mfg/isa-equipment-model (Anlagenmodell-Manager)	cmdb_ot_isa_viewer	Über die Regel „Anlagenmodell nach ISA zuweisen“ werden Benutzer mit den in der Regel beschriebenen Rollen nach ihrer Anmeldung direkt zum Anlagenmodell-Manager weitergeleitet.

Zielregeln für Homepage (Fortsetzung)

Regel	Ziel	Rollen umgeleitet	Beschreibung
			 Hinweis: Die Seitenregel „Anlagenmodell nach ISA anzeigen“ wird nur angezeigt, wenn Prozessmanager Industrie installiert ist.
Listenseite „Arbeitsbereich Industrie“.	now/mfg/list (Listen für Industrie-Arbeitsbereich)	cmdb_ot_viewer	Die Listenseitenregel „Industrial Workspace“ leitet Anwender mit den in der Regel beschriebenen Rollen bei der Anmeldung direkt zu den Listen „Industrial Workspace“ weiter.

Standortfilter in Industrial Workspace

Sie können den Site-Filter im Dashboard Operational Technology für (OT) Transparenz, im Dashboard Operational Technology Vulnerability Response (PA) und im Dashboard für OT-Schwachstellenrisiko-Rollup verwenden, um Daten für bestimmte Sites anzuzeigen.

Mit dem Site-Filter können Sie das OT-Gerät oder die Schwachstellendaten angeben, die in den folgenden Dashboards angezeigt werden sollen.

- Dashboard für OT-Transparenz
- OTVR (PA)-Dashboard
- Dashboard „OT-Schwachstellenrisiko-Rollup“.

Zur Verwendung des Site-Filters benötigen Sie die Rolle **cmdb_ot_isa_viewer** mit Zugriff auf die Site, die Sie anzeigen möchten.

Mit dem Site-Filter können Sie die folgenden Aktionen ausführen:

- Suchen Sie nach einer bestimmten Website.
- Zeigen Sie die OT-Daten für einen oder mehrere Sites an.
- OT-Daten für keinen zugewiesenen Standort anzeigen.

** Hinweis:**

Wenn einem OT-Gerät keine Site zugewiesen ist, zeigt der Filter **Keine Site zugewiesen an**. Damit die richtigen Sites im Dashboard angezeigt werden, müssen Sie dem Gerät eine Site und dann dieser Site einen Geschäftsbereich zuweisen.

Verwenden Sie den Site-Filter

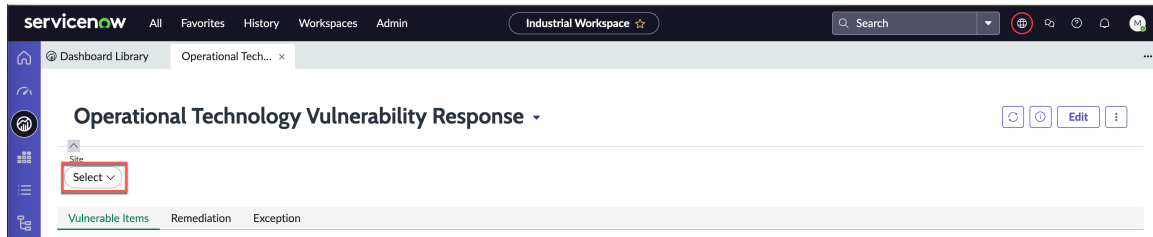
Verwenden Sie die Site im Dashboard Operational Technology „(OT) Transparenz, im Dashboard Operational Technology Vulnerability Response (PA) und im Dashboard OT-Schwachstellenrisiko-Rollup, um die Daten nach der ausgewählten Site(s) zu filtern.

Vorbereitungen

Erforderliche Rolle: cmdb_ot_isa_viewer mit Websitezugriff

Prozedur

1. Navigieren zu **Alle > Industrial Workspace**.
2. Wählen Sie das Symbol **Dashboard-Bibliothek** () aus.
3. Wählen Sie entweder das Dashboard „OT-Transparenz“ oder das Dashboard „Operational Technology Vulnerability Response“ aus.
4. Klicken Sie unter dem **Site**-Header auf die Schaltfläche **Auswählen**.



5. **Wahlweise:** Verwenden Sie die Suchfunktion, um nach einer bestimmten Website zu suchen.
6. Führen Sie die folgenden Aktionen aus, um eine oder mehrere Sites auf das Dashboard anzuwenden.
 - a. Wählen Sie in der Spalte **Verfügbar** die Sites aus, für die Sie Daten anzeigen möchten.
 - b. Um die ausgewählten Sites in die Spalte **Angewendet** zu verschieben, klicken Sie auf das Symbol **Ausgewählte Elemente verschieben** .

Operational Technology Filter für Fortschrittsbewertungsliste

Sie können die Filter in der Fortschrittsbewertungsliste Operational Technology (OT) verwenden, um die Daten, die in Ihrer Bewertungsliste angezeigt werden sollen, nach Standort, Geschäftsbereich (BU) oder Datum anzugeben.

Übersicht über Bewertungslistenfilter

Mit den Filtern für Geschäftsbereich, Standort und Datum können Sie die Bewertungslistenmetriken angeben, die in der OT-Fortschrittsbewertungsliste angezeigt werden sollen. Sie können nach einem oder mehreren Geschäftsbereichen, den jeweiligen Sites und einem bestimmten Kalendermonat filtern.

Geschäftsbereichfilter

Mit dem Filter für den Geschäftsbereich (Geschäftsbereich) können Sie die folgenden Aktionen ausführen:

- Zeigen Sie die Bewertungslistenmetriken für alle Geschäftsbereiche an.
- Zeigen Sie die Bewertungslistenmetriken für einen bestimmten Geschäftsbereich an.
- Zeigen Sie die Bewertungslistenmetriken für mehrere Geschäftsbereiche an.

Standardmäßig zeigt die Bewertungsliste die Metriken für alle verfügbaren BUs an (siehe folgendes

OT Progress Scorecard

Hello, welcome to OT Progress Scorecard

All business units All Sites May 2024

Site progress

Sites	Calculated Score (%)	Assigned OT Devices (%)	Classified OT Devices (%)	Mapped OT Devices (%)
California	0	100	100	0
Hyderabad	0	0	0	0

Showing 1-2 of 2 Records per page 10

Beispiel).

Nachdem Sie den BU-Filter festgelegt haben, zeigt die Bewertungsliste die Daten von jedem Standort an, der in den ausgewählten BUs enthalten ist. Sie können dann einen Standort aus dem Menü „Alle Standorte“ auswählen, das im nächsten Abschnitt beschrieben wird. Wenn Sie den BU-Filter ändern und andere BUs auswählen, wird der Site-Filter so aktualisiert, dass er nur die Sites enthält, die dem ausgewählten BU zugeordnet sind.

Weitere Informationen zur Verwendung von BU- und Site-Filtern finden Sie unter [Verwenden Sie die Filter der Fortschrittsbewertungsliste Operational Technology](#) ..

Standortfilter

Mit dem Site-Filter können Sie die folgenden Aktionen ausführen:

- Zeigen Sie die Bewertungslistenmetriken für alle Sites an.
- Zeigen Sie die Bewertungslistenmetriken für eine bestimmte Site an.
- Zeigen Sie die Bewertungslistenmetriken für mehrere Sites an.

Standardmäßig zeigt die Bewertungsliste die Metriken für alle im folgenden Beispiel gezeigten Sites

OT Progress Scorecard

Hello, welcome to OT Progress Scorecard

All business units All Sites May 2024

Site progress

Sites	Calculated Score (%)	Assigned OT Devices (%)	Classified OT Devices (%)	Mapped OT Devices (%)
California	0	100	100	0
Hyderabad	0	0	0	0

Showing 1-2 of 2 Records per page 10

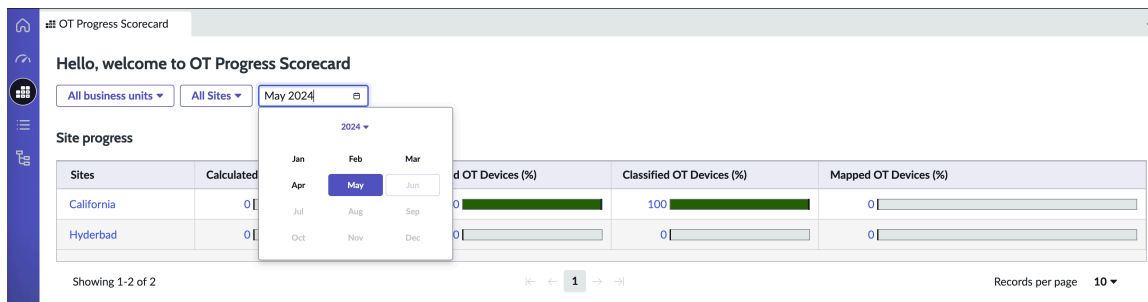
an.

Datumsfilter

Mit dem Datumsfilter können Sie die Bewertungslistenmetriken für einen bestimmten Kalendermonat im ausgewählten Jahr anzeigen. Standardmäßig zeigt die Bewertungsliste die Metriken für den vorherigen Monat und das vorherige Jahr an.

i Hinweis:

Wenn der Auftrag [PA OTPSC] Monatliche Datensammlung“ noch nicht ausgeführt wurde, zeigt die Bewertungsliste eine Punktzahl von 0 an. Weitere Informationen zum Auftrag [PA OTPSC] Monatliche Datensammlung finden Sie unter [Konfigurieren Sie die Datensammlung für die Fortschrittsbewertungsliste Operational Technology](#) ..



Verwenden Sie die Filter der Fortschrittsbewertungsliste Operational Technology .

Verwenden Sie die Filter „Geschäftsbereich“ (BU) und „Standort“ in der Fortschrittsbewertungsliste Operational Technology (OT), um die Daten nach Geschäftsbereich, Standort oder Datum zu filtern.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle > Industrial Workspace**.
2. Öffnen Sie die OT-Fortschrittsbewertungsliste.
3. Zeigen Sie die Bewertungslistenmetriken für einen oder mehrere BUs an.
 - a. Wählen Sie im Header das Menü **Alle Geschäftsbereiche** aus.
 - b. Wählen Sie aus der Liste einen oder mehrere BUs aus, für die Sie die Daten anzeigen möchten. Mit der Suchfunktion können Sie nach einem bestimmten BU suchen.
4. Zeigen Sie die Bewertungslistenmetriken für eine oder mehrere Sites an.
 - a. Wählen Sie im Header das Menü **Alle Sites**.
 - b. Wählen Sie in der Liste eine oder mehrere Sites aus, für die Sie die Daten anzeigen möchten.

Hinweis:

Mit der Suchfunktion können Sie nach einer bestimmten Website suchen. Geben Sie den Namen der Website oder die Kurzwahl in die Suchleiste ein. Die Kurzwahl ist eine Abkürzung für Ihre Site.

5. Zeigen Sie die Bewertungslistenmetriken für ein Kalenderdatum an.
 - a. Wählen Sie im Header das Kalendersymbol ().
 - b. Wählen Sie den Monat und das Jahr aus, für den Sie die Daten abrufen möchten.

Konfigurieren Sie die Reihenfolge Ihrer wichtigen Aktionen auf der Operational Technology aktionsorientierten Zielseite

Konfigurieren Sie die Reihenfolge Ihrer wichtigen Aktionen auf der aktionsorientierten Zielseite Operational Technology (OT), um die Anzeige Ihrer Aufgaben zu personalisieren.

Vorbereitungen

Erforderliche Rolle: cmdb_ot_viewer

Prozedur

1. Navigieren zu **Alle > Industrial Workspace**.
2. Zum **Homepage** -Symbol ().
3. Wählen Sie das Symbol **Wichtige Aktionen konfigurieren** () aus.
4. Wählen Sie **Elemente sortieren** aus.
5. Wählen Sie im Feld **Attribut auswählen** das Attribut aus, nach dem Ihre wichtigen Aktionen gefiltert werden sollen.
Über das Feld **Suchen** können Sie das Attribut finden, nach dem Sie Ihre Aktionen sortieren möchten.
6. Wählen Sie im Feld **Reihenfolge** die Option **Aufsteigend** oder **Absteigend** aus.

Indikatorquellen und Indikatoren für das Dashboard Operational Technology Vulnerability Response (PA).

Die Anwendung Operational Technology Vulnerability Response verwendet Indikatorquellen und Indikatoren, um Daten zu sammeln und den Fortschritt der Nachbesserung von Schwachstellen zu verfolgen.

Indikatorquellen

Die Operational Technology Vulnerability Response -Indikatoren sammeln Daten aus den folgenden Indikatorquellen. Wenn Sie erwarten, dass mehr als 1 Million Datensätze aus den Indikatorquellen gesammelt werden, müssen Sie die erwartete Anzahl im Abschnitt „Datensatzsammlung“ der Indikatorquelle überschreiben. Weitere Informationen finden Sie unter [Überprüfen Sie die Indikatorquellen für eine größere Anzahl von Datensätzen](#).

OTVI.Neu

Verwendet die Tabelle sn_vul_vulnerable_item und sammelt die neuen angreifbaren OT-Elemente.

OTVI.Aktiv

Verwendet die Tabelle sn_vul_vulnerable_item und schließt alle aktiven angreifbaren Elemente in Ihr OT-System ein.

OTVI.Geschlossen

Verwendet die Tabelle sn_vul_vulnerable_item und enthält alle geschlossenen angreifbaren Elemente in Ihrem OT-System.

OTRT.Aktiv

Verwendet die Tabelle sn_vul_vulnerability und enthält alle aktiven Korrekturaufgaben in Ihrem OT-System.

Indikatoren

Mehrere Indikatoren werden verwendet, um den Fortschritt der Nachbesserung von Schwachstellen in der Anwendung Operational Technology Vulnerability Response zu messen und nachzuverfolgen.

Die Option **zum Sammeln von Datensätzen** für -Indikatoren ist für die Anwendung Operational Technology Vulnerability Response standardmäßig deaktiviert. Diese Option ist deaktiviert, um Leistungsprobleme zu vermeiden, die auftreten können, wenn Sie für jeden Indikator eine große Datenmenge erfassen.

Angreifbare OT-Elemente

Anzahl der angreifbaren OT-Elemente in der Datenquelle „OTVI.Aktiv“, die die Tabelle „sn_vul_vulnerable_item“ verwendet. Ziel ist es, die Anzahl der angreifbaren Elemente in Ihrem System zu minimieren.

Kritische angreifbare OT-Elemente

Anzahl der kritischen angreifbaren OT-Elemente in der Datenquelle „OTVI.Aktiv“, die die Tabelle „sn_vul_vulnerable_item“ verwendet. Ziel ist es, die Anzahl der kritischen angreifbaren Elemente in Ihrem System zu minimieren.

Nicht zugewiesene angreifbare OT-Elemente

Alle aktiven angreifbaren OT-Elemente, bei denen die Felder „Zuweisungsgruppe“ und „Zugewiesen an“ leer sind. Ziel ist es, die Anzahl der nicht zugewiesenen angreifbaren Elemente zu minimieren.

Geschlossene angreifbare OT-Elemente

Der Indikator „Geschlossene angreifbare OT-Elemente“ wird täglich als numerische Einheit gemessen. Das Ziel besteht darin, die Anzahl der geschlossenen angreifbaren Elemente in Ihrem System zu maximieren.

Zurückgestellte angreifbare OT-Elemente

Anzahl der zurückgestellten angreifbaren OT-Elemente in der Datenquelle „OTVI.Aktiv“, die die Tabelle „sn_vul_vulnerable_item“ verwendet. Ziel ist es, die Anzahl der zurückgestellten angreifbaren Elemente in Ihrem System zu minimieren.

Kritische zurückgestellte angreifbare OT-Elemente

Anzahl der kritischen zurückgestellten angreifbaren OT-Elemente in der Datenquelle „OTVI.Aktiv“, die die Tabelle „sn_vul_vulnerable_item“ verwendet. Ziel ist es, die Anzahl der kritischen zurückgestellten angreifbaren Elemente zu minimieren.

Nicht zurückgestellte überfällige kritische angreifbare OT-Elemente

Anzahl der nicht zurückgestellten überfälligen kritischen angreifbaren OT-Elemente in der Datenquelle „OTVI.Aktiv“, die die Tabelle „sn_vul_vulnerable_item“ verwendet. Ziel ist es, die Anzahl der nicht zurückgestellten, überfälligen kritischen angreifbaren Elemente in Ihrem System zu minimieren.

OT-Korrekturaufgaben

Anzahl der OT-Korrekturaufgaben in der Datenquelle „OTRT.Aktiv“, die die Tabelle „sn_vul_vulnerability“ verwendet. Das Ziel besteht darin, die Anzahl der Korrekturaufgaben in Ihrem System zu minimieren.

Nicht zurückgestellte überfällige kritische OT-Korrekturaufgaben

Anzahl der nicht zurückgestellten überfälligen kritischen OT-Korrekturaufgaben in der Datenquelle „OTRT.Aktiv“, die die Tabelle „sn_vul_vulnerability“ verwendet. Das Ziel besteht darin, die Anzahl der nicht zurückgestellten, überfälligen, kritischen Korrekturaufgaben in Ihrem System zu minimieren.

Nicht zurückgestellte OT-Korrekturaufgaben

Anzahl der nicht zurückgestellten OT-Korrekturaufgaben in der Datenquelle „OTRT.Aktiv“, die die Tabelle „sn_vul_vulnerability“ verwendet. Ziel ist es, die Anzahl der nicht zurückgestellten Korrekturaufgaben in Ihrem System zu minimieren.

Nicht zurückgestellte kritische OT-Korrekturaufgaben

Anzahl der nicht zurückgestellten kritischen OT-Korrekturaufgaben in der Datenquelle „OTRT.Aktiv“, die die Tabelle „sn_vul_vulnerability“ verwendet. Ziel ist es, die Anzahl der nicht zurückgestellten kritischen Korrekturaufgaben in Ihrem System zu minimieren.

Nicht zugewiesene OT-Korrekturaufgaben

Alle aktiven Korrekturaufgaben, bei denen die Felder „Zuweisungsgruppe“ und „Zugewiesen an“ leer sind. Das Ziel besteht darin, die Anzahl der nicht zugewiesenen Korrekturaufgaben in Ihrem System zu minimieren.

% der angreifbaren Elemente mit erfülltem Korrekturziel

$$\frac{[[\text{Geschlossene angreifbare Elemente} > \text{Korrekturziel} = \text{Ziel erfüllt}]]}{[[\text{Geschlossene angreifbare Elemente}]]} * 100$$

Ziel ist es, den Prozentsatz der angreifbaren Elemente zu maximieren, die das Korrekturziel in Ihrem System erfüllen.

Durchschnittliche Zeit bis zur Fehlerkorrektur für angreifbare OT-Elemente

$$\frac{[[\text{Summierte Dauer der geschlossenen angreifbaren Elemente}]]}{[[\text{Geschlossene angreifbare Elemente}]]}$$

Summierte Dauer geschlossener angreifbarer OT-Elemente

Summierte Anzahl der OT-Dauer der geschlossenen angreifbaren Elemente in der Datenquelle „OTVI.Closed“, welche die Tabelle „sn_vul_vulnerable_item“ verwendet. Das Ziel besteht darin, die Gesamtdauer der geschlossenen angreifbaren Elemente in Ihrem System zu minimieren.

Operational Technology Vulnerability Response (PA) Dashboard-Aufgliederungen

Operational Technology Vulnerability Response verwendet Aufgliederungen, um die gesammelten Datensätze zu filtern und zu gruppieren.

Die folgenden Aufgliederungen gelten für die -Indikatoren im Dashboard.

Alter

Alter des angreifbaren Elements, das im Format „Tage/Stunden/Minuten“ angezeigt wird.

Geschlossen mit Alter

Alter des angreifbaren Elements, wenn sich sein Status in „Geschlossen“ ändert.

Zuweisungsgruppe

Zuweisungsgruppe des angreifbaren Elements oder der Korrekturaufgabe.

CI-Manager

Manager für angreifbare Konfigurationselemente (CIs).

Aufschiebungsgrund

Grund, warum die Korrektur eines angreifbaren Elements zurückgestellt wird.

Exploit-Angriffsvektor

Verwundbarster Angriffsvektor der Exploits für eine Schwachstelle.

Exploit vorhanden

Exploit, das mit einer Schwachstelle verbunden ist.

Exploit-Kompetenzniveau

Niedrigste Kompetenzstufe, die zum Ausnutzen einer Schwachstelle erforderlich ist.

Korrekturzielregel

Erwarteter Zeitrahmen für die Korrektur eines angreifbaren Elements.

Nachbesserungszielstatus

Aktualisiert den Status eines angreifbaren Elements mit einem Korrekturzieldatum.

Nachbesserungszielstatus (geschlossen)

Aktualisiert den Status eines angreifbaren Elements, wenn das Zieldatum für die Korrektur erfüllt ist.

Risikobewertung

Quantifizierte Risikopunktzahl, die angreifbare Elemente in „Kritisch“, „Hoch“, „Mittel“, „Niedrig“ und „Keine“ unterteilt.

Schweregrad

Normalisierter Schweregrad einer Schwachstelle.

Status

Status eines angreifbaren Elements oder einer Korrekturaufgabe.

Die folgenden Aufgliederungsquellen gelten für die -Indikatoren im Dashboard für Berichte zu angreifbaren Elementen, Korrekturaufgabenberichten oder beiden Arten von Berichten.

Zuweisungsgruppe

Berichte zu angreifbaren Elementen und Korrekturaufgaben.

Zurückgestellt.Grund.Nicht.Geschlossen

Berichte zu angreifbaren Elementen.

Exploit-Angriffsvektor

Berichte zu angreifbaren Elementen.

Exploit vorhanden

Berichte zu angreifbaren Elementen.

Exploit-Kompetenzniveau

Berichte zu angreifbaren Elementen.

OT-Altersbereich

Berichte zu angreifbaren Elementen.

Korrekturzielstatus

Berichte zu angreifbaren Elementen und Korrekturaufgaben.

Korrekturzielstatus (Geschlossen)

Berichte zu angreifbaren Elementen und Korrekturaufgaben.

Korrektur.Ziel.Regel

Berichte zu angreifbaren Elementen und Korrekturaufgaben.

Risikobewertung

Berichte zu angreifbaren Elementen und Korrekturaufgaben.

Schweregrad

Berichte zu angreifbaren Elementen und zu Korrekturaufgaben.

Status

Berichte zu angreifbaren Elementen und Korrekturaufgaben.

Schwachstelle.Element.CI.Manager

Berichte zu angreifbaren Elementen.

Operational Technology Vulnerability Response (PA) Dashboard-Sammlungsaufträge

Das Dashboard Operational Technology Vulnerability Response (PA) verwendet Erfassungsaufgaben, um die im Dashboard angezeigten Daten zu sammeln.

Die folgenden Erfassungsaufgaben erfassen die Daten, die im Dashboard Operational Technology Vulnerability Response (PA) angezeigt werden:

[PA OT VR] Sammlung historischer Schwachstellendaten

Sammlungsaufgabe für die Verlaufsdaten vorhandener Datensätze.

** Hinweis:**

Die Sammlung historischer Schwachstellendaten ist eine bedarfsgesteuerte Aufgabe, die nur einmal ausgeführt werden muss. Nachdem die Verlaufsdaten gesammelt wurden, werden die täglichen Datensammlungsaufgaben jeden Tag zu einer geplanten Zeit ausgeführt. Weitere Informationen finden Sie unter [Collect historical data](#) .

[PA OT VR] Tägliche Sammlung für Korrekturaufgaben

Sammlungsauftrag für die täglich anfallenden Korrekturaufgabendaten.

[PA OT VR] Tägliche Sammlung für angreifbare Elemente 1

Sammlungsaufgabe, die täglich für nicht zurückgestellte überfällige kritische angreifbare Elemente, zurückgestellte angreifbare Elemente, angreifbare Elemente und kritische angreifbare Elemente auftritt.

[PA OT VR] Tägliche Sammlung für angreifbare Elemente 2

Sammlungsauftrag, der täglich für nicht zugewiesene angreifbare Elemente, geschlossene angreifbare Elemente, Gesamtdauer geschlossener angreifbarer Elemente und kritische zurückgestellte angreifbare Elemente ausführt.

Im Dashboard Operational Technology Vulnerability Response (PA) verwendete Datenvisualisierungen

Das Dashboard Operational Technology Vulnerability Response (PA) verwendet Datenvisualisierungen, um Ihre OT-Schwachstellendaten anzuzeigen.

Die folgenden Tabellen beschreiben die im Dashboard Operational Technology Vulnerability Response (PA) angezeigten Datenvisualisierungen.

Datenvisualisierungen der Registerkarte „Angreifbare Elemente“.

Name	Typ	Beschreibung
Angreifbare OT-Elemente insgesamt	Balkendiagramm	Balkendiagramm, das die aktiven (nicht geschlossenen) angreifbaren OT-Elemente nach Gerätetyp gruppiert anzeigt.
Neue angreifbare OT-Elemente	Kreisdiagramm	Kreisdiagramm, das die neuen angreifbaren OT-Elemente anzeigt, die in Ihrem System gefunden wurden, gruppiert nach Gerätetyp.
Nicht zugewiesene angreifbare OT-Elemente	Kreisdiagramm	Kreisdiagramm, das die nach Gerätetyp gruppierten angreifbaren OT-Elemente anzeigt, die offen sind und keinem Benutzer zugewiesen wurden.
Angreifbare OT-Elemente nach Status	Balkendiagramm	Balkendiagramm, das alle angreifbaren Elemente nach Status geordnet anzeigt. Sie können interpretieren, wie

Datenvisualisierungen der Registerkarte „Angreifbare Elemente“. (Fortsetzung)

Name	Typ	Beschreibung
		viele Schwachstellen behoben werden und wie viele weitere Untersuchungen erfordern. Wenn beispielsweise die Kategorie „Wird untersucht“ relativ hoch ist, können Sie diese Elemente priorisieren, indem Sie zuerst die angreifbaren Elemente behandeln.
Angreifbare OT-Elemente nach Risikobewertung	Balkendiagramm	Anzahl der aktiven angreifbaren OT-Elemente, die nach der Risikobewertung für die ausgewählte Zeitspanne gruppiert sind.
OT-VIs mit erfülltem Korrekturziel	Einzelne Punktzahl	Prozentsatz der geschlossenen angreifbaren OT-Elemente, deren Nachbesserungszieldaten im aktuellen und vorherigen Quartal eingehalten wurden. Korrekturziele werden aus dem Datum der letzten Öffnung plus der Anzahl der Tage seit dem Datum der letzten Öffnung (gemessen in 24-Stunden-Schritten) berechnet.
Durchschnittliche Zeit bis zur Korrektur für OT-VI (MTTR)	Einzelne Punktzahl	Durchschnittliche Zeit für die Korrektur (Schließung) eines angreifbaren OT-Elements, angezeigt als laufender 30-Tage-Durchschnitt. i Hinweis: Der Wert für „Alter geschlossen“ wird berechnet, wenn die Daten erfasst werden. Der Wert ist die Differenz zwischen dem Datum „last_opened“ und dem Datum und der Uhrzeit der Erfassungsaufgabe.
OT AE nach Alter	Balkendiagramm	Balkendiagramm, das die aktiven angreifbaren OT-Elemente nach Alter gruppiert (in Tagen) anzeigt.
Geschlossene angreifbare OT-Elemente nach Korrekturzielstatus	Balkendiagramm	Anzahl der geschlossenen angreifbaren OT-Elemente, die nach dem Korrekturzielstatus für die ausgewählte Zeitspanne gruppiert sind.

Datenvisualisierungen der Registerkarte „Angreifbare Elemente“. (Fortsetzung)

Name	Typ	Beschreibung
		 Hinweis: Der Wert für „Alter geschlossen“ wird berechnet, wenn die Daten erfasst werden. Der Wert ist die Differenz zwischen dem Datum „last_opened“ und dem Datum und der Uhrzeit der Erfassungsaufgabe.
Kritisches angreifbares OT-Element nach Zuweisungsgruppe	Indikator-Bewertungsliste	Kritische VIs nach Zuweisungsgruppe geordnet.
Überfällige kritische angreifbare OT-Elemente nach Zuweisungsgruppe	Indikator-Bewertungsliste	Kritische VIs, die überfällig sind, organisiert nach Zuweisungsgruppe.

Datenvisualisierungen der Registerkarte „Nachbesserung“.

Name	Typ	Beschreibung
OT-Korrekturaufgaben	Einzelne Punktzahl	Anzahl der aktiven (nicht geschlossenen) OT-Korrekturaufgaben.
Kritische OT-Korrekturaufgaben kurz vor der Fälligkeit	Einzelne Punktzahl	Anzahl der aktiven OT-Korrekturaufgaben, deren Korrekturzieldatum näher rückt. Das Korrekturzieldatum einer OT-Korrekturaufgabe wird auf das nächstgelegene Fälligkeitsdatum festgelegt, das zu einem aktiven angreifbaren Element in der Gruppe gehört. Die Korrekturziele werden anhand des Datums von „Zuletzt geöffnet“ plus der Anzahl der Tage (gemessen in 24-Stunden-Schritten) berechnet. Dieser Bericht schließt die zurückgestellten OT-Korrekturaufgaben aus.
OT-Korrekturaufgabe nach Risikobewertung	Balkendiagramm	Balkendiagramm, das die aktiven OT-Korrekturaufgaben gruppiert nach Risikobewertung anzeigt.

Datenvisualisierungen der Registerkarte „Nachbesserung“. (Fortsetzung)

Name	Typ	Beschreibung
OT-Korrekturaufgabe nach Zielstatus	Balkendiagramm	Balkendiagramm, das die aktiven OT-Korrekturaufgaben gruppiert nach Status des Korrekturziels anzeigt. Dieser Bericht schließt die zurückgestellten angreifbaren OT-Elemente aus.
OT-Korrekturaufgabe nach Status	Balkendiagramm	Balkendiagramm, das alle Korrekturaufgaben nach Status anzeigt. Sie können den Fortschritt Ihrer Korrekturaufgaben interpretieren.
Nicht zugewiesene OT-Korrekturaufgaben	Einzelne Punktzahl	Anzahl der aktiven OT-Korrekturaufgaben ohne einen Beauftragten oder eine Zuweisungsgruppe.
Kritische OT-Korrekturaufgabe nach Zuweisungsgruppe	Indikator-Bewertungsliste	Kritische Korrekturaufgaben nach Zuweisungsgruppe organisiert.
Überfällige kritische OT-Korrekturaufgabe nach Zuweisungsgruppe	Indikator-Bewertungsliste	Kritische Korrekturaufgaben, die überfällig sind, organisiert nach Zuweisungsgruppe.

Datenvisualisierungen der Registerkarte „Ausnahme“.

Name	Typ	Beschreibung
Zurückgestellte angreifbare OT-Elemente nach Grund	Balkendiagramm	Anzahl der zurückgestellten angreifbaren OT-Elemente, die nach dem Zurückstellungsgrund gruppiert sind.
OT-Ausnahmen für kritische angreifbare Elemente nach Zuweisungsgruppe	Indikator-Bewertungsliste	Ausnahmen für kritische VIs nach Zuweisungsgruppe geordnet.

Zeigen Sie eine Operational Technology Einheitliche Übersicht an

Zeigen Sie eine einheitliche Übersicht Operational Technology (OT) in Industrial Workspace an, welche die Beziehungen zwischen Geräten und anderen CIs anzeigt.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Sie können an den folgenden Stellen in Industrial Workspace auf die einheitliche OT-Übersicht zugreifen.

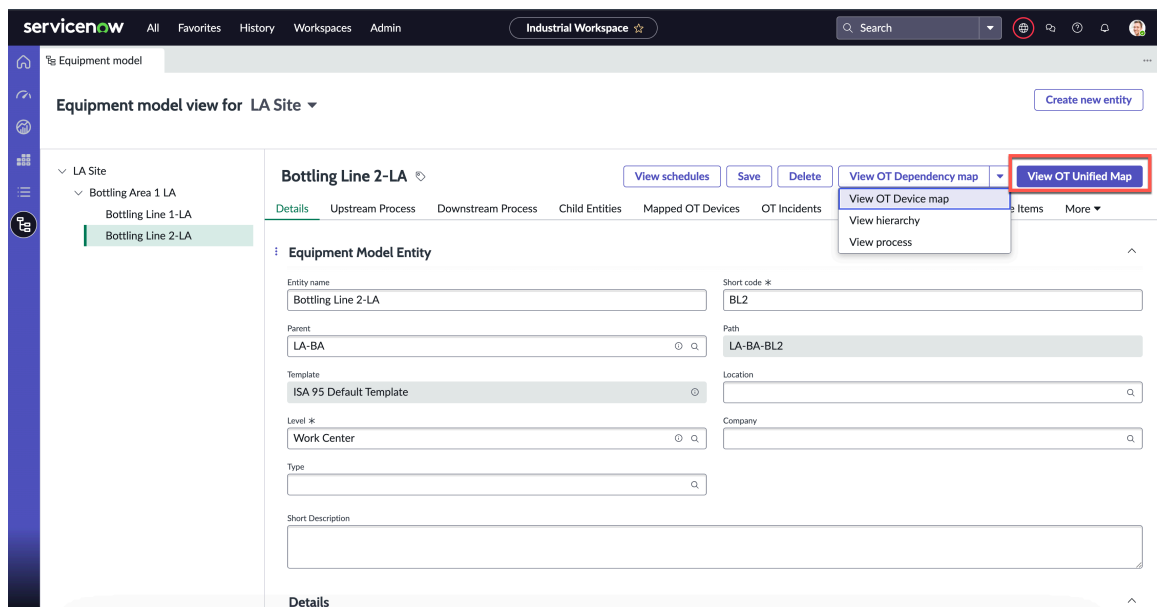
- ISA-Datensatz im Anlagenmodell-Manager
- OT-Incident-Datensatz
- OT-Change-Datensatz

Prozedur

1. Navigieren zu **Alle > Industrial Workspace**.

2. Führen Sie die folgenden Aktionen aus, um in einem Anlagenmodell-Entitätsdatensatz auf die einheitliche OT-Übersicht zuzugreifen.

- Öffnen Sie den Anlagenmodell-Manager, indem Sie das Symbol „Anlagenmodell“ () wählen.
- Öffnen Sie den Datensatz der Anlagenmodell-Entität, für den Sie die Einheitliche Übersicht anzeigen möchten.
- Wählen Sie die Schaltfläche **Einheitliche OT-Übersicht anzeigen**.



3. Um in einem zugehörigen Datensatz, z. B. einem OT-Incident-Datensatz oder Change-Datensatz, auf die einheitliche Übersicht von OT zuzugreifen, führen Sie die folgenden Aktionen aus.

- Öffnen Sie die Listenansicht Industrial Workspace, indem Sie das Symbol Liste () wählen.
- Wählen Sie den Datensatz aus, für den Sie die einheitliche Übersicht anzeigen möchten.

Wenn Sie beispielsweise die Einheitliche Übersicht für einen OT Incident-Datensatz anzeigen möchten, wählen Sie eine der verfügbaren Listen im Modul **OT Incidents** aus, und öffnen Sie den Datensatz.

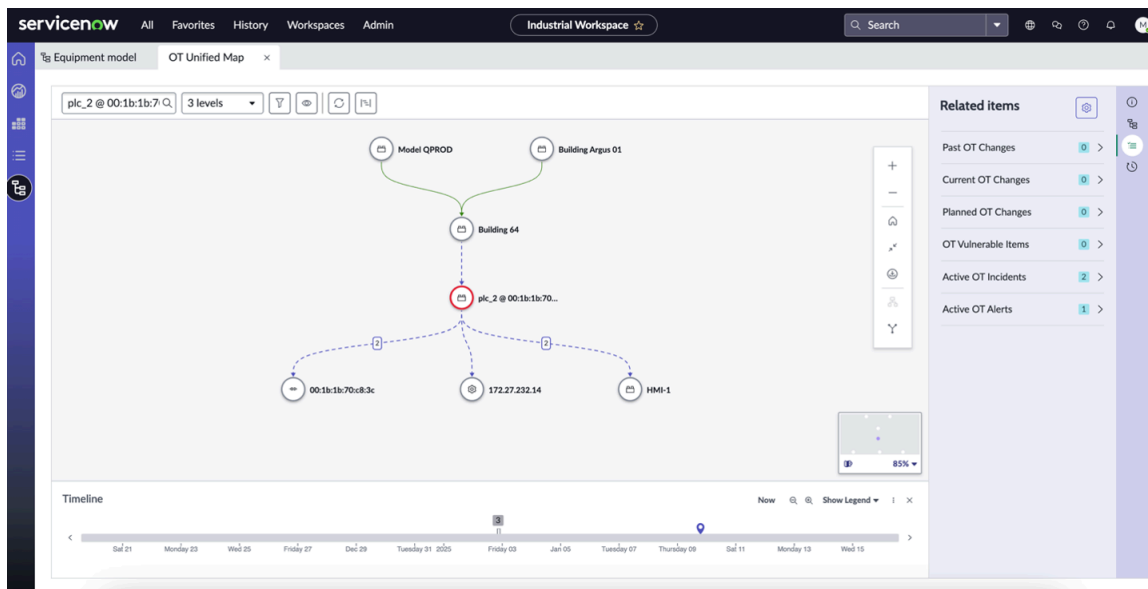
- c. Um die Zuordnung in einem neuen Fenster zu öffnen, wählen Sie die Schaltfläche **Einheitliche OT-Übersicht anzeigen**.
- d. Um die Zuordnung im Seitenbereich des Datensatzes zu öffnen, wählen Sie das Symbol **Prozessintegrität Industrie** ().

Nächste Maßnahme

Sie können jetzt die einheitliche OT-Übersicht anzeigen. In der einheitlichen Übersicht können Sie auch die hervorgehobenen Knoten der folgenden zugehörigen Elemente sehen.

- Bisherige OT-Changes
- Aktuelle OT-Changes
- Geplante OT-Changes
- Aktive OT-Incidents
- Aktive OT-Warnungen
- Angreifbare OT-Elemente

Die folgende Abbildung zeigt ein Beispiel für eine einheitliche OT-Übersicht.



Verwenden Sie und im Menü Bewertung von Hardware-Schwachstellen in Industrial Workspace

Das Menü *Bewertung von Hardware-Schwachstellen* enthält Informationen zu allen Schwachstellen im Bestand Operational Technology (OT), die vollständig oder teilweise mit den in der National Vulnerability Database (NVD) eingetragenen Schwachstellen übereinstimmen. .

Vorbereitungen

Erforderliche Rolle: sn_otvr.vul_event_manager

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *Industrial Workspace* > *Bewertung von Hardware-Schwachstellen*. **Wählen Sie das Menüsymbol** ().
2. Führen Sie auf den **Registerkarten Vollständig abgegliche Bewertungen, Teilweise abgegliche Bewertungen, Angreifbare Elemente, Ignorierte Bewertungen** und **Warten auf Normalisierung** nach Bedarf die folgenden Aktionen aus:
 - a. Wählen Sie zusätzliche Spalten, und zeigen Sie sie an, um weitere Informationen zur Bewertung durchzu erhalten, indem Sie update pPersonalisiert list Symbol () wählen.).
 - b. Wählen Sie  aus, um die angezeigte Liste der Bewertungen zu aktualisieren.
 - c. Wählen Sie  um Bewertungsinformationen auf der Registerkarte gemäß den zusätzlichen Filterbedingungen anzuzeigen , die Sie wählen.
 - d. Wählen Sie **Filter auswählen**, um eine schnelle Filterung von Bewertungen durchzuführen.
3. Wählen Sie die Registerkarten **Vollständig abgegliche Bewertungen** und **Teilweise abgegliche Bewertungen** aus, um die Bewertungsdatensätze anzuzeigen.
 - a. Wählen Sie einen oder mehrere Bewertungsdatensätze aus, und wählen Sie **Angreifbare Elemente erstellen**, um manuell angreifbare Elemente für die Bewertungsdatensätze zu erstellen, die Sie aus der angezeigten Liste auswählen.
 - b. Wählen Sie **Ignorieren** aus, um die Bewertungsdatensätze zu ignorieren, die Sie aus der angezeigten Liste auswählen. Die von Ihnen ignorierten Bewertungen sind unter oder auf der Registerkarte **Ignorierte Bewertungen** verfügbar.
4. Oauf der Registerkarte **Ignorierte Bewertungen** :
 - a. Wählen Sie **Rückgängig machen**, um Bewertungen für die OT-Geräte durchzuführen, die Sie zuvor ignoriert haben.
 - b. Wählen Sie **Angreifbare Elemente erstellen**, um manuell angreifbare Elemente für die Bewertungen zu erstellen, die Sie aus der angezeigten Liste auswählen.
5. Wählen Sie die Registerkarte **Angreifbare Elemente**.

Auf dieser Registerkarte wird die Liste der angreifbaren Elemente angezeigt, die basierend auf den Bewertungsdatensätzen erstellt werden, die auf den Registerkarten **Vollständig abgegliche Bewertungen, Teilweise abgegliche Bewertungen** und **Ignorierte Bewertungen** erstellt wurden.
6. Wählen Sie die Registerkarte **Warten auf Normalisierung** aus, um die OT-Gerät-Daten anzuzeigen, die nicht für die Bewertung verwendet wurden. Der Normalisierungsstatus lautet:

- **Neu**
- **Übereinstimmung nicht gefunden**
- **Herausgeber normalisiert**



Wichtig:

Aktivieren Sie die Opt-in-Funktion in Enterprise Asset Management, die OT-Geräte für die Normalisierung verfügbar macht. Weitere Informationen finden Sie unter [Opt-in to Enterprise Asset Management Content Service](#) .

Zugehörige Informationen

[Operational TechnologyBewertung von Hardware-Schwachstellen](#)

[Richten Sie ein und richten Sie die Bewertung von Hardware-Schwachstellen von Operational Technology -Geräten mithilfe des geführten Setups ein](#)

Domänentrennung und Operational Technology

Domänentrennung wird für Operational Technology 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: Basis

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

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

Weitere Informationen zu den Supportstufen finden Sie unter [Anwendungssupport für die Domänentrennung](#) .

Operational Technology Übersicht über Domain Separation

Operational Technology erbt die Domänentrennungsfunktionen der abhängigen Anwendungen. Da jede Anwendung ihre eigene Domain Separation-Beziehung haben kann, gibt es keine bestimmte Supportstufe, die mit Operational Technology verknüpft werden kann. Weitere Informationen finden Sie unter [Domain separation and Workflow Studio](#) .

In der folgenden Tabelle werden die Supportstufen für Domain Separation und die Anwendungsfälle für die einzelnen Operational Technology -Anwendungen beschrieben.

Supportstufen nach Anwendung

Anwendung	Support-Stufe
Operational Technology Manager	Standard
Prozessmanager Industrie	Standard
Operational Technology Vulnerability Response	Standard
Operational Technology	Standard
Change-Management für operative Technologie	Standard
Knowledge Management für operative Technologie	Standard
Anforderungsmanagement für operative Technologie	Standard

[store-future: BEGIN review]

Domänengetrennte Tabellen

Liste einfügen.

[End]

Zugehörige Informationen

[Domänentrennung für Service Provider](#)