



# Yokohama Telecommunications Service Operations 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](http://www.servicenow.com/terms-of-use.html)

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

# Inhaltsverzeichnis

<b>Telecommunications Service Operations Management.....</b>	<b>4</b>
Verarbeitet die externen Ereignisse mithilfe von Benachrichtigungen der Telekommunikations-API.....	4
Thema erstellen.....	6
Erstellen Sie ein -Themenabonnement.....	7
Aktivieren Sie den Endpunkt der Open API-Verbindung von Telecommunications Alarm Management.....	8
Anwenderrollen für Telekommunikations-API-Benachrichtigungen.....	9
TSOM-Transparenz.....	10
Discovery für die Telekommunikation.....	14
Identifizierung und Abgleich von Telekommunikationsdiskrepanzen.....	51

# Telecommunications Service Operations Management

---

Überwachen Sie proaktiv die Integrität Ihrer Netzwerke und Services, um potenzielle Ausfallzeiten zu vermeiden. Optimieren Sie Ihre Antwort mit ServiceNow® Ereignismanagement und Metrikdaten.

ServiceNow® Telecommunications Service Operations Management (TSOM) ist in Überwachungstools wie Ereignismanagement und Metrikdaten integriert, um Vorgänge zu vereinfachen, und bietet eine End-to-End-Serviceansicht über alle Telekommunikationstechnologiedomänen hinweg. Das TSOM verwendet die TM Forum Alarm Management API, um die Erfassung, Korrelation und Analyse umfangreicher Netzwerkereignisdaten über verschiedene Domänen hinweg zu automatisieren. Sie bietet Front-Office- und Back-Office-Teams eine zentrale End-to-End-Serviceintegritätsansicht.

## Verarbeitet die externen Ereignisse mithilfe von Benachrichtigungen der Telekommunikations-API

Verwenden Sie die Benachrichtigung der Telecommunications API, um die externen Ereignisse zu empfangen, die im Kundennetzwerksystem auftreten, damit Sie in Now Plattformumgehend darauf reagieren können.

### Übersicht

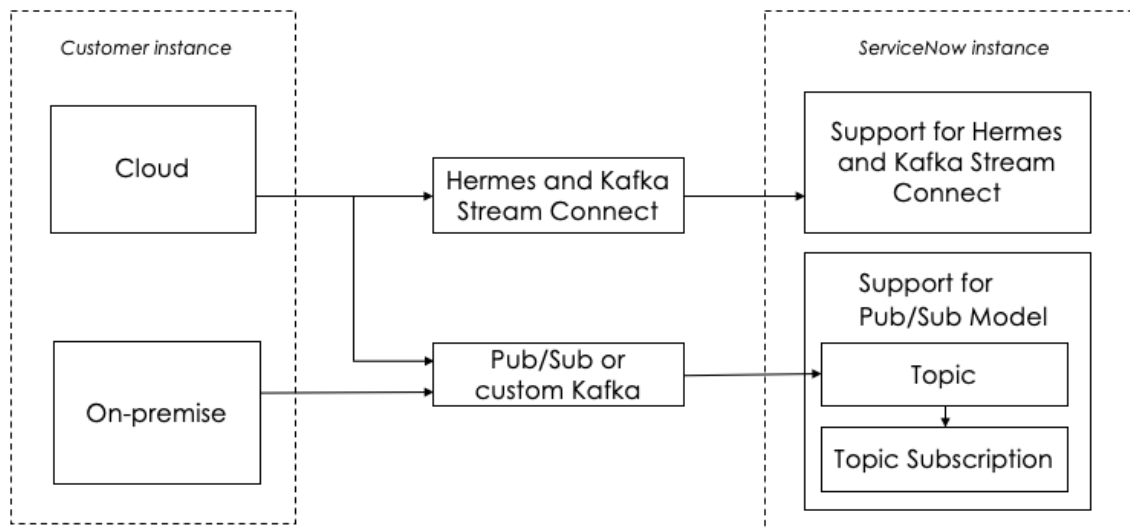
Die API-Benachrichtigung für die Telekommunikation ist eine Funktion, die in der Anwendung Telecommunications Alarm Management Open API verfügbar ist. Mit der Benachrichtigung der Telecommunications API kann ServiceNow die eingehenden Benachrichtigungen empfangen, die im externen Netzwerksystem auftreten, und rechtzeitig darauf reagieren. Sie ermöglicht die Übertragung von Ereignissen an externe Systeme über Plattformfunktionen, da keine Punkt-zu-Punkt-Verbindungen erforderlich sind.

Die Telekommunikations-API-Benachrichtigung empfängt eingehende Benachrichtigungen von den externen Systemen, die in Ihrem Netzwerk abonniert sind. Wenn die Benachrichtigungen vom externen System empfangen werden, können Sie die Ereignisse für die Antworten mithilfe der Anwendung Ereignismanagement erstellen. Basierend auf den gesammelten Informationen stellt Ereignismanagement Dashboards bereit, die eine konsolidierte Ansicht aller Ereignisse zeigen, die sich auf den Service auswirken.

### Benachrichtigungsdatenmodell der Telekommunikations-API

Das folgende Diagramm zeigt die Komponenten im Datenmodell für die Telecommunications API-Benachrichtigung.

## API-Benachrichtigungsdatenmodell



Die -Telekom-API-Benachrichtigung ermöglicht ServiceNow, eingehende Benachrichtigungen über ereignisgesteuerte Architekturen wie das Publisher/Subscriber-Abonnementmodell (Pub/Sub), Hermes und Kafka Stream Connect zu empfangen. Während Cloud-Kunden die Flexibilität haben, zwischen beiden Architekturen zu wählen, sind On-Premise-Kunden auf die Verwendung ihres eigenen Kafka- oder Pub/Sub-Abonnementmodells beschränkt.

- Weitere Informationen zu Stream Connect für Apache Kafka Stream finden Sie unter [Using Stream Connect for Apache Kafka](#) .
- Weitere Informationen zum Hermes Messaging Service finden Sie unter [Hermes Messaging Service](#) .

Im Pub/Sub-Modell werden eingehende Benachrichtigungen in Themen kategorisiert. Sie verwenden ServiceNow, um die eingehenden Benachrichtigungen zu diesen Themen zu veröffentlichen, und Abonnenten (Kunden) können die Themen auswählen, die sie abonnieren möchten. Mit diesem Prozess können Abonnenten nur die Nachrichten auswählen, die ihren Interessen entsprechen. Wenn beispielsweise 10 -Themen für eingehende Nachrichten aus dem externen System vorhanden sind, kann ein Kunde je nach Anforderung zwei davon abonnieren. Daher werden bei Empfang von Benachrichtigungen vom externen System Ereignisse speziell für die beiden Themen generiert, die der Kunde abonniert hat.

## Modellierung des Benachrichtigungs-Workflows der Telekommunikations-API

Die folgenden Schritte helfen beim Konfigurieren der Telekommunikations-API-Benachrichtigung in der Instanz ServiceNow.

- 1. Thema erstellen:** Sie können Themen erstellen, indem Sie die externen Nachrichtendetails manuell eingeben oder die verfügbaren Themen automatisch aus dem externen System erfassen.
- 2. Erstellen Sie ein -Themenabonnement:** Je nach Kundeneinstellung abonnieren Sie die verfügbaren Themen für eingehende Benachrichtigungen aus dem externen System. Außerdem generieren Sie die Rückruf-URL und registrieren das Abonnement.
- 3. Aktivieren Sie den Endpunkt der Open API-Verbindung von Telecommunications Alarm Management:** Um Antworten vom externen System zu erhalten, aktivieren Sie die abonnierten Endpunkte der Open API-Verbindung von Telecommunications Alarm Management in Workflow-Studio.

4. Stellen Sie dem externen System die Rückruf-URL für den Empfang von Benachrichtigungen bereit. Der Kunde kann die Rückruf-URL auch wiederverwenden. Wenn Anforderungen von TMF 688 auf die Rückruf-URL treffen, wird der Flow „Standard-Alarmereignis-Benachrichtigungsauslöser“ initiiert, um ein Ereignis zu erstellen.

Weitere Informationen zu den Funktionen zur Verarbeitung von Anforderungen der Event Notification Management Open API, die durch externe Auslöserdefinitionen zum Erstellen, Aktualisieren und Löschen von Ereignissen ausgelöst werden, finden Sie unter [Event Notification Management Open API](#) und [TMFTopicEventAPIUtilOOB - Scoped](#).

Dieser Workflow erstellt ein Ereignis in der Anwendung Ereignismanagement. Weitere Informationen zur Verwendung von Ereignismanagement finden Sie unter [Ereignismanagement](#).

## Thema erstellen

Erstellen Sie ein Thema, und veröffentlichen Sie die eingehenden Benachrichtigungen aus dem externen System im Thema. Durch das Erstellen der Themen können Abonnenten die Themen auswählen, die sie abonnieren möchten.

### Vorbereitungen

Stellen Sie sicher, dass die Anwendung Telecommunications Alarm Management Open API (sn\_ind\_tmf642) mit Now Plattform installiert ist.

Erforderliche Rolle: admin, sn\_api\_notif\_mgmt.topic\_creator

### Warum und wann dieser Vorgang ausgeführt wird

Sie können Themen erstellen, indem Sie die externen Nachrichtendetails manuell eingeben oder die verfügbaren Themen automatisch aus dem externen System erfassen. Wenn Sie ein Thema erstellen, wird ein Datensatz in der Tabelle „Thema“ [sn\_api\_notif\_mgmt\_topic] erstellt.

### Prozedur

#### 1. Alle > Telecom-API-Benachrichtigung > Themen.

#### 2. Wählen Sie **Neu**.

Bei der Integration mit einem externen System können Sie **Themen abrufen** auswählen, um die verfügbaren Themen automatisch abzurufen. Diese Aktion löst den Subflow *der API für Ereignisalarmbenachrichtigungen* aus. Weitere Informationen zu den Funktionen, mit denen Sie Datensätze im Thema abfragen und bearbeiten können, finden Sie unter [TopicUtilOOB - Scoped](#).

#### 3. Füllen Sie die Felder des Formulars aus.

#### Formular „Thema“

Feld	Beschreibung
Themen-ID	Eindeutige Themen-ID.
Themenname	Der Name des Themas.
Typ	Typ des Themas. Wählen Sie eine der folgenden Optionen aus:

Feld	Beschreibung
	<ul style="list-style-type: none"> <li>○ Eingehend: Option für eingehende Benachrichtigungen.</li> <li>○ Ausgehend: Option für ausgehende Benachrichtigung.</li> </ul>
Header-Abfrage	<p>Codierte Header-Abfrageparameter.</p> <p>Weitere Informationen zu den Abfrageparametern, die auf die TMF688-Standards folgen, finden Sie im <a href="#">TM-Forum</a> .</p>
Inhaltsabfrage	<p>Abfrageparameter für codierten Inhalt.</p> <p>Weitere Informationen zu den Abfrageparametern, die auf den TMF 688-Standard von [ folgen, finden Sieim <a href="#">TM-Forum</a> .</p>
Beschreibung	Eine kurze Beschreibung des Themas.

**4. Wählen Sie Absenden.**

**Ergebnisse**

Ein Thema wird erstellt.

**Nächste Maßnahme**

Sie können das Themenabonnement gemäß den Kundenanforderungen erstellen.

**Erstellen Sie ein -Themenabonnement**

Abonnieren Sie das Thema in Now Platform, mit dem Sie auf die eingehende Benachrichtigung vom externen System antworten möchten. Durch das Abonnieren des Themas erhält der Abonnent die Benachrichtigungen basierend auf den Themen, die Sie abonnieren.

**Vorbereitungen**

- Stellen Sie sicher, dass die Anwendung Telecommunications Alarm Management Open API (sn\_ind\_tmf642) mit Now Platforminstalliert ist.
- Erstellen Sie Themen für die eingehenden Benachrichtigungen.

Erforderliche Rolle: admin, sn\_api\_notif\_mgmt.subscription\_creator

**Warum und wann dieser Vorgang ausgeführt wird**

Abhängig von den Kundeneinstellungen abonnieren Sie die verfügbaren Themen für eingehende Benachrichtigungen aus dem externen System. Sie generieren die Rückruf-URL, um sie für die Kunden freizugeben. Wenn eine Anforderung von einem externen System auf die Rückruf-URL trifft, wird die Erstellung eines Ereignisses in der Anwendung Ereignismanagement initiiert.

Darüber hinaus registrieren Sie das -Themenabonnement, um die eingehenden Benachrichtigungen zu erhalten. Wenn Sie ein Themenabonnement erstellen, wird ein Datensatz in der Tabelle „Themenabonnement“ [sn\_api\_notif\_mgmt\_subscription] erstellt.

Weitere Informationen zu den Methoden zum Abfragen und Bearbeiten von Datensätzen im Themenabonnement finden Sie unter [TopicSubscriptionUtilOOB - Scoped](#) .

**Prozedur**

1. **Alle > Telecom-API-Benachrichtigung > Abonnement.**
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular aus.

**Formular „Themenabonnement“.**

Feld	Beschreibung
Thema	Thema, das Sie abonnieren möchten.
CallbackURL	Die Rückruf-URL, die Sie für das externe System freigeben, um die eingehende Benachrichtigung zu erfassen. Die URL wird automatisch generiert, wenn Sie <b>CallbackURL generieren</b> auswählen.
Abfrage filtern	Codierte Inhaltsabfrageparameter aus dem Thema. Sie können auch die Filterabfrage ändern.  Weitere Informationen zu den Abfrageparametern, die auf den TMF 688-Standard von [ folgen, finden Sie im <a href="#">TM-Forum</a> .
Registrierungsstatus	Status der Themenregistrierung beim externen System. Standardmäßig ist dies <b>Unregistriert</b> . Wenn der Prozess erfolgreich ist, ändert sich der Feldwert in <b>Registriert</b> . Andernfalls ist es <b>Fehler</b> .
Registrierungsnachricht	Registrierungsstatusnachricht vom externen System.
Abonnement-ID	Eindeutige Abonnement-ID aus dem externen System.

4. Rufen Sie die Rückruf-URL ab, indem Sie durch Auswahl **von CallbackURL generieren** auswählen.
5. Registrieren Sie das Abonnement, indem Sie wählen, indem Sie **Registrieren** wählen.

**Ergebnisse**

Für die Rückruf-URL wird eine Auslöserdefinition erstellt, und das Thema wird im externen System registriert.

**Nächste Maßnahme**

In Workflow-Studio aktivieren Sie die Endpunkte der Open API-Verbindung von Telecommunications Alarm Management.

**Aktivieren Sie den Endpunkt der Open API-Verbindung von Telecommunications Alarm Management**

Aktivieren Sie den Endpunkt der Open API-Verbindung von Telecommunications Alarm Management. Durch Aktivieren des Endpunkts erhalten Sie die eingehenden Benachrichtigungen vom externen System für das von Ihnen registrierte Thema.

Automatische Übersetzung

## Vorbereitungen

- Erstellen Sie das -Thema, und abonnieren Sie es, um die eingehenden Benachrichtigungen zu erhalten.
- Generieren Sie eine Rückruf-URL, und registrieren Sie das -Themenabonnement.

Erforderliche Rolle: Administrator

## Warum und wann dieser Vorgang ausgeführt wird

Sie aktivieren die abonnierten Endpunkte der Open API-Verbindung des Telecommunications Alarm Management in Workflow-Studio, um Antworten vom externen System zu erhalten.

## Prozedur

1. Navigieren zu **Alle > Prozessautomatisierung > Flow Designer**.
2. Wählen Sie auf der Registerkarte **Verbindungen** die **Option Telecommunications Alarm Management Open API aus**.
3. Öffnen Sie den Endpunktdatensatz, den Sie aktivieren möchten.
4. Wählen Sie **Aktivieren**.

## Anwenderrollen für Telekommunikations-API-Benachrichtigungen

Administratoren können Anwenderrollen zuweisen, um Zugriff auf die Tabellen der API-Benachrichtigungsdatenbank zu gewähren. Die folgenden Standardrollen für die Tabellen „Thema“ [sn\_api\_notif\_mgmt\_topic] und „Themenabonnement“ [sn\_api\_notif\_mgmt\_subscription] sind im System ServiceNow enthalten.

### Benachrichtigungsrollen für die Telekommunikations-API

Rolle	Beschreibung
sn_api_notif_mgmt.topic_subscription_viewer	Rolle, die mit Lesezugriff auf die Tabellen „Thema“ und „Themenabonnement“ verfügt.
sn_api_notif_mgmt.topic_creator	Rolle, die mit Erstellungs-, Lese- und Bearbeitungszugriff auf die Thementabelle ermöglicht.
sn_api_notif_mgmt.subscription_creator	Rolle, die mit Erstellungs- und Lesezugriff auf die Tabelle „Themenabonnement“ aktiviert ist.
sn_api_notif_mgmt.subscription_admin	Rolle, die mit den folgenden Berechtigungen aktiviert: <ul style="list-style-type: none"> <li>• Erstellen Sie und lesen Sie Zugriff auf die Tabellen „Thema“ und „Themenabonnement“.</li> <li>• Ändern Sie den Status der Registrierung, um die Registrierung eines -Themenabonnements aufzuheben.</li> </ul>

# TSOM-Transparenz

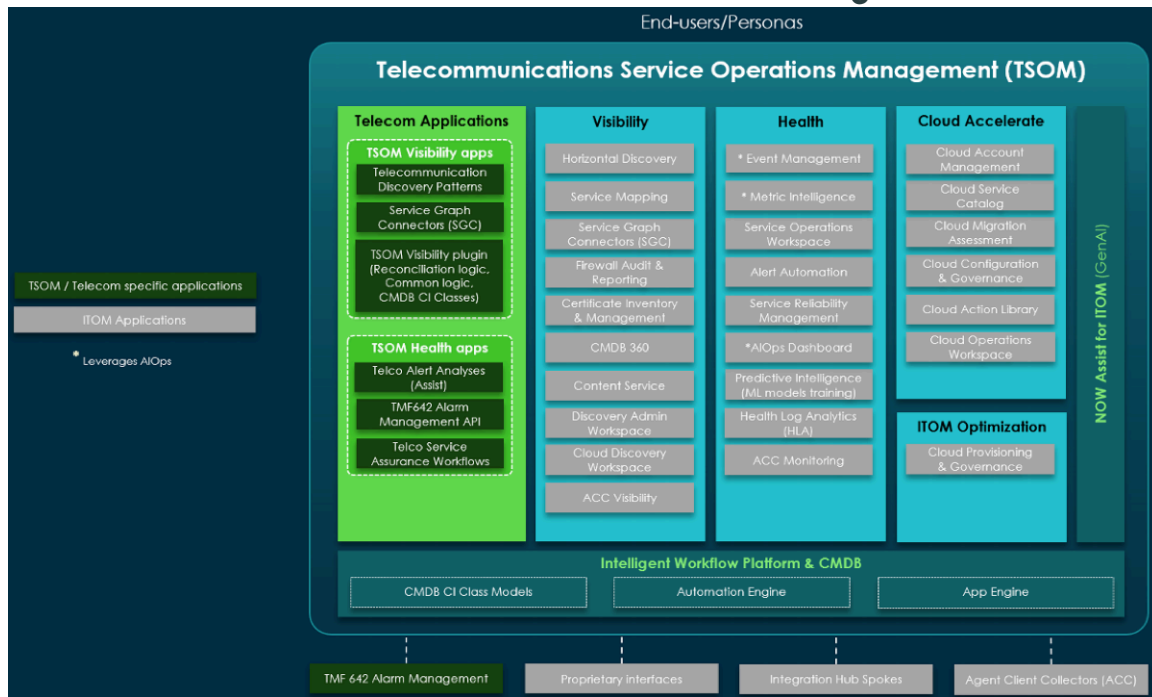
Die Lösung TSOM Visibility basiert auf den Grundprinzipien von ITOM Visibility und nutzt deren bewährte Frameworks für die Erkennung und Zuordnung von IT-Ressourcen.

Zusätzlich zu den Kernfunktionalitäten von ITOM Visibility führt TSOM Visibility eine einzigartige Telekommunikations-spezifische Ebene mit maßgeschneiderten Anwendungen ein. Dazu gehören Telecom Discovery, das die Anwendungen Horizontal Discovery und Telecommunications Discovery Patterns nutzt, Service Graph Connectors (SGC) und Telecom Diskrepanz Identifizierung und Abgleich, die durch das TSOM Visibility-Plugin eingeführte Telekommunikations-spezifische Logik enthalten. Alle Komponenten sind so konzipiert, dass sie die eindeutigen Hierarchie- und Ressourcenstrukturen des Telekommunikationsdatenmodells unterstützen. Diese Kombination verbessert die Erkennung, den Abgleich und die Verwaltung von Telekommunikationsinfrastruktur und -services in komplexen Netzwerken mit mehreren Lieferanten und Technologien sowie in IT- und Cloud-Umgebungen.

**i Hinweis:**

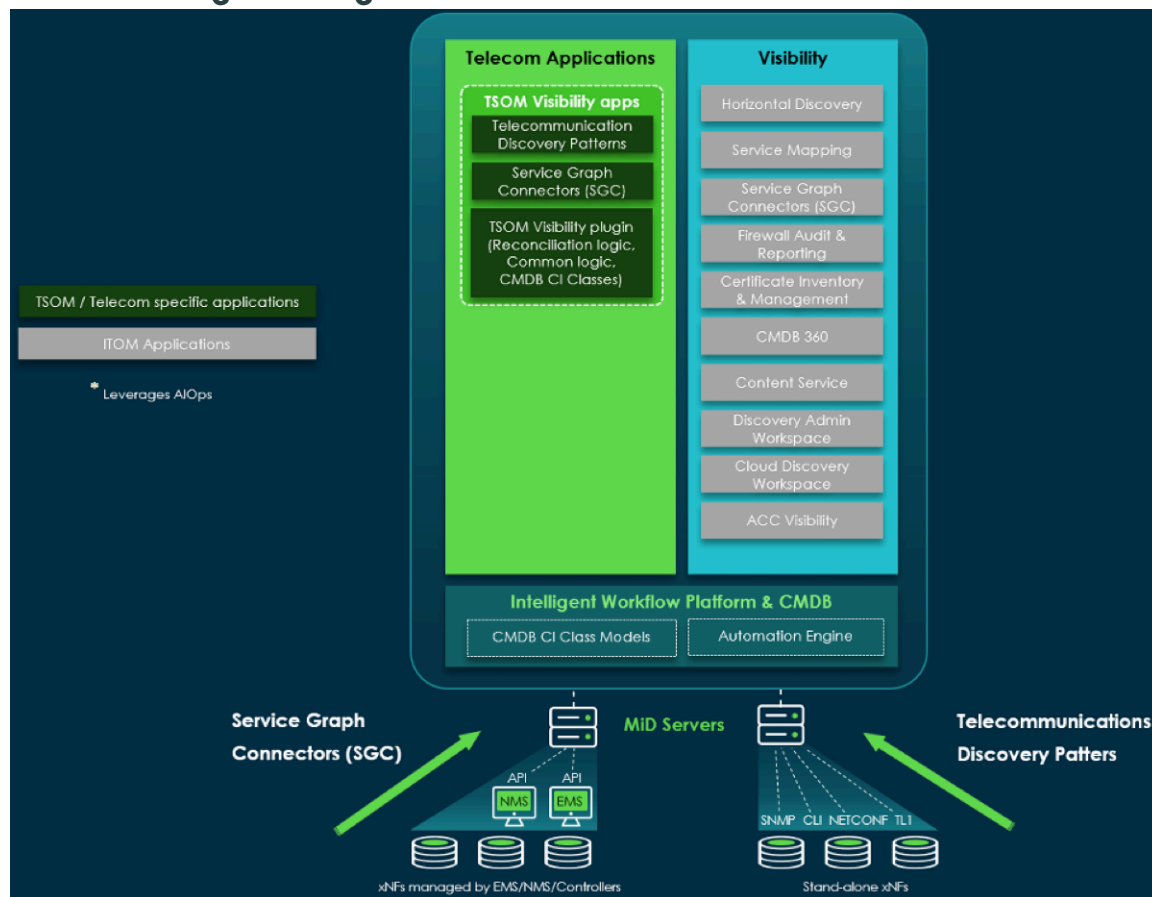
Zusätzliche TSOM-Anwendungen und APIs im Zusammenhang mit TSOM Health und AIOps fallen nicht in den Umfang der TSOM-Transparenz-Lösung und werden separat behandelt.

## TSOM: Architektur- und Telekommunikationsanwendungen



Automatische Übersetzung

## TSOM-Transparenz: Telekommunikations-Discovery und Diskrepanz-Identifizierung und -Abgleich



### Horizontal-Discovery und Telekommunikations-Discovery-Muster

Horizontal-Discovery ist ein automatisierter Prozess, der alle Komponenten innerhalb der Netzwerkinfrastruktur kontinuierlich scannt und identifiziert. Es spielt eine entscheidende Rolle für die Aufrechterhaltung einer genauen und aktuellen CMDB und TNI mit den Informationen im Netzwerk.

In Telecom Discovery verwenden wir die Discovery-Muster für Horizontal Discovery and Telecommunication (TSOM) (sn\_tsom\_patterns), um eigenständige xNFs mithilfe der Protokolle SNMP und CLI zu erkennen.

Weitere Informationen zu den TSOM-Mustern finden Sie unter [Telekommunikations-Discovery mithilfe von Telekommunikations-Discovery-Mustern](#).

Weitere Informationen zur Anwendung Horizontal Discovery finden Sie unter [Horizontal discovery process flow with patterns](#) .

### Service Graph Connectors (SGC)

Die Service Graph Connectors (SGC) sind vordefinierte Integrationen, die Daten aus Drittanbieterquellen in die Configuration Management Database (CMDB) erfassen. Sie können zusammen mit allen vorhandenen Service Graph Connectors verwendet werden, z. B. für Sicherheit, Server, Software, Überwachung, Internet der Dinge (IoT) und Cloud.

In Telecom Discovery verwenden wir Service Graph Connectors, um Netzwerkressourcen über Northbound-APIs von EMS/NMS/Controllern zu erkennen, die verschiedene xNFs verwalten.

Weitere Informationen zu Telecom-SGS finden Sie unter [Telecom-Discovery mit Service Graph Connectors \(SGC\)](#).

## TSOM-Transparenz-Anwendungen

- Service Graph Connectors (TSOM SGCs): Diese neuen Plugins ermöglichen die Discovery von Daten aus vorhandenen Netzwerkverwaltungssystemen (z. B. EMS/NMS/Controller).
- Plugin-Name: sn\_sgc\_altiplano\_connector
- Plugin-Beschreibung: Service Graph Connector für Nokia Altiplano

Weitere Informationen finden Sie unter [Telecom-Discovery mit Service Graph Connectors \(SGC\)](#).

- Telecommunications Discovery Patterns (TSOM Patterns) – Diese neuen Plugins enthalten Muster für die Discovery von standardmäßigen SNMP-basierten eigenständigen xNFs (z. B. Telekommunikationsrouter/-Switches ohne Verwaltungssystem oder solche, die direkt durch Umgehung ihrer Verwaltungssysteme erkannt werden sollen). Sie enthalten auch anwenderdefinierte Muster für die Überprüfung bestimmter Cisco- und Juniper-Geräte durch Nutzung der SNMP- und CLI-Zugänglichkeiten.
- Plugin-Name: sn\_tsom\_patterns
- Plugin-Beschreibung: Telekommunikations-Discovery-Muster

Weitere Informationen finden Sie unter [Telekommunikations-Discovery mithilfe von Telekommunikations-Discovery-Mustern](#).

- TSOM Visibility (Plugin) – Dieses Plugin aktiviert die TSOM Visibility-Anwendungen. Sie enthält eine Logik, die unserer Lösung Telecom Discovery und Telecom Diskrepanz Identifizierung und Abgleich gemeinsam ist. Es enthält telekommunikationsspezifische Logik zur Identifizierung und Behebung von Diskrepanzen sowie andere gängige Logik, die wir derzeit für die Verwendung in der gesamten Anwendung erstellen oder erstellen werden.
- Plugin-Name: sn\_tsom\_core
- Plugin-Beschreibung: TSOM Visibility (Plugin)

Weitere Informationen finden Sie unter [Identifizierung und Abgleich von Telekommunikationsdiskrepanzen](#).

## CMDB 360

CMDB 360 speichert einen vollständigen Verlauf der Discovery-Quellen und vorgeschlagenen Werte, die an Aktualisierungen von CI-Attributen beteiligt sind. Verwenden Sie CMDB 360-Daten, um nachzuerfolgen, wie die CMDB von verschiedenen Discovery-Quellen auf CI-Attributsebene gefüllt wird. Sie können auch CI-Aktualisierungen aus einer bestimmten Discovery-Quelle rückgängig machen oder Attributwerte mithilfe aktualisierter Abgleichsregeln neu berechnen.

Die CMDB 360-Ansicht bietet Zusammenfassungen und Analysen von CMDB 360-Daten, die zur Nachverfolgung von Aktivitäten und zur Identifizierung potenzieller Probleme mit Discovery-Quellen verwendet werden können. Darüber hinaus können Sie anwenderdefinierte Abfragen, Zeitpläne und Berichte zur Untersuchung von CMDB-Daten erstellen.

Weitere Informationen zu CMDB 360 finden Sie unter [CMDB 360/Multisource CMDB](#) .

## Discovery-Administratorarbeitsbereich

Der Discovery-Administratorarbeitsbereich dient als zentraler Ort für die Überwachung, Nachverfolgung und Durchführung von Discovery-bezogenen Aufgaben. Profitieren Sie von einem optimierten Discovery-Prozess und höherer Effizienz durch die Integration von Zeitplänen, Diagnosen, Optimierungen und mehr in diesem Arbeitsbereich.

Weitere Informationen zum Discovery-Administratorarbeitsbereich finden Sie unter [Discovery Admin Workspace](#) .

## Benutzer der TSOM-Transparenz

Mit TSOM Visibility können Telekommunikationsbetreiber, Communication Service Provider (CSP) und Platform-as-Service-Anbieter ihre Netzwerkressourcen erkennen.

Die ServiceNow® Configuration Management Database (CMDB) und Telecom Network Inventory (TNI) sind keine operativen Tools. Sie sind in der heutigen IT- und Telekommunikationslandschaft von strategischer Bedeutung. Die Pflege einer genauen und vollständigen CMDB/TNI bietet die Grundlage für die Bereitstellung kritischer Services und fördert mehrere Ergebnisse, die für den Telekommunikationsbetrieb wichtig sind, z. B. Auftrags-/Serviceerfüllung, Bestands-/Asset-Verwaltung und Qualitätssicherung. Ein aktueller CMDB-/Netzwerkbestand ist entscheidend für die Ermöglichung eines hohen Maßes an Autonomous Network Operations (NO) und wichtig für Echtzeitentscheidungen, Automatisierung und Abläufe im geschlossenen Kreislauf.

## Haftungsausschluss für die TSOM-Transparenz-Installation

Zur Unterstützung der TSOM-Transparenz-Lösung haben wir die Store-Anwendung [CMDB CI Class Models](#) geändert und die IRE-Identifizierungsregeln für die folgenden Telekommunikations-CIs aktualisiert:

- Schnittstellenkarten
- Steckplätze
- Untersteckplätze
- Netzwerkschnittstellen

TSOM Visibility erfordert CMDB CI Class Models Version 1.69.0 (sn\_cmdb\_ci\_class).

Wenn Sie eine der TSOM-Transparenz-Anwendungen (sn\_sgc\_altiplano\_connector, sn\_tsom\_patterns oder das Plugin sn\_tsom\_core) installieren, wird die Store-Anwendung CMDB CI Class Models (CMDB-CI-Klassenmodelle) automatisch auf Version 1.69.0 aktualisiert (oder installiert).

### **i Hinweis:**

Ein Administrator kann die Store-Anwendung „CMDB CI Class Models“ weiterhin nach seinem Ermessen auf Version 1.69.0 aktualisieren, unabhängig davon, ob seine Yokohama-Instanz über TSOM Visibility verfügt oder ob sich ihre Instanz auf einem Release vor Yokohama (z. B. Washington DC oder Xanadu) befindet ).

**WICHTIG!** Wenn ein Administrator CMDB CI-Klassenmodelle Version 1.69.0 bereitstellt – unabhängig davon, ob TSOM Visibility installiert ist oder nicht – können alle anwenderdefinierten IRE-Identifizierungsregeln betroffen sein, die auf eines oder mehrere der oben genannten Telekommunikations-CIs angewendet werden. Diese Regeln müssen sorgfältig validiert werden, um eine ordnungsgemäße Funktionalität sicherzustellen.

## Lizenzierung für die TSOM-Transparenz

Die Now Plattform verwendet ein Lizenzierungsmodell, bei dem Ihrer Organisation die Nutzung von TSOM-Transparenz-Anwendungen in Rechnung gestellt wird. Telecom-Discovery, Telecom-Diskrepanz-Identifizierung und -Abgleich und TSOM-Transparenz (Plugin) sind Komponenten von TSOM-Transparenz. Um die TSOM-Transparenz zu verwenden, muss Ihre Organisation TSOM abonnieren.

### **i Hinweis:**

Die Produktdokumentation von ServiceNow enthält keine Details zu Preisgestaltung, Verpackung oder anderen Besonderheiten, da diese durch den Kundenvertrag Ihres Unternehmens festgelegt werden.

## Discovery für die Telekommunikation

ServiceNow® Telecom Discovery (auch bekannt als TSOM Discovery) ist eine Speziallösung innerhalb des breiteren ServiceNow-Ökosystems, die auf die besonderen Anforderungen von Telekommunikationsanbietern (CSPs) bei der Erkennung und Verwaltung ihrer Telekommunikationsnetzwerk-Assets zugeschnitten ist.

Diese Lösung bietet Einblick in komplexe Telekommunikationsinfrastrukturen und ermöglicht es CSPs, verschiedene Netzwerkgeräte, Services und Konfigurationen in ihren Umgebungen mit mehreren Lieferanten automatisch zu identifizieren, zuzuordnen und zu verwalten und Datensätze in der CMDB/TNI mit einem Echtzeit-Snapshot von Netzwerkressourcen zu aktualisieren.

Diese Fähigkeit ist eine der wichtigsten Voraussetzungen für die Automatisierung und stimmt mit dem TM Forum Autonomous Network Operations-Framework (NO) überein.

IT Discovery ITOM Visibility	VS	Telecom Discovery TSOM Visibility
<ul style="list-style-type: none"> <li>• Flat, simple or no hierarchy</li> <li>• Basic attributes</li> <li>• Network is the trusted source of truth</li> <li>• Simple CI identification and reconciliation</li> <li>• Populates the CMDB with the CIs found in the network (everything found is written into the CMDB)</li> </ul>		<ul style="list-style-type: none"> <li>• Hierarchical, alignment to telecom models</li> <li>• Advanced attributes</li> <li>• Inventory/CMDB design is the trusted source of truth</li> <li>• Complex telecom CI identification and reconciliation</li> <li>• Validates that the network implementation is in sync with CMDB/TNI records as designed/planned</li> </ul>

TSOM und ITOM Discovery können zusammenarbeiten, um eine ganzheitliche Transparenz und Verwaltung in Telekommunikations- und IT-Umgebungen zu bieten.

Weitere Informationen zu Telecom Discovery finden Sie unter den folgenden Links:

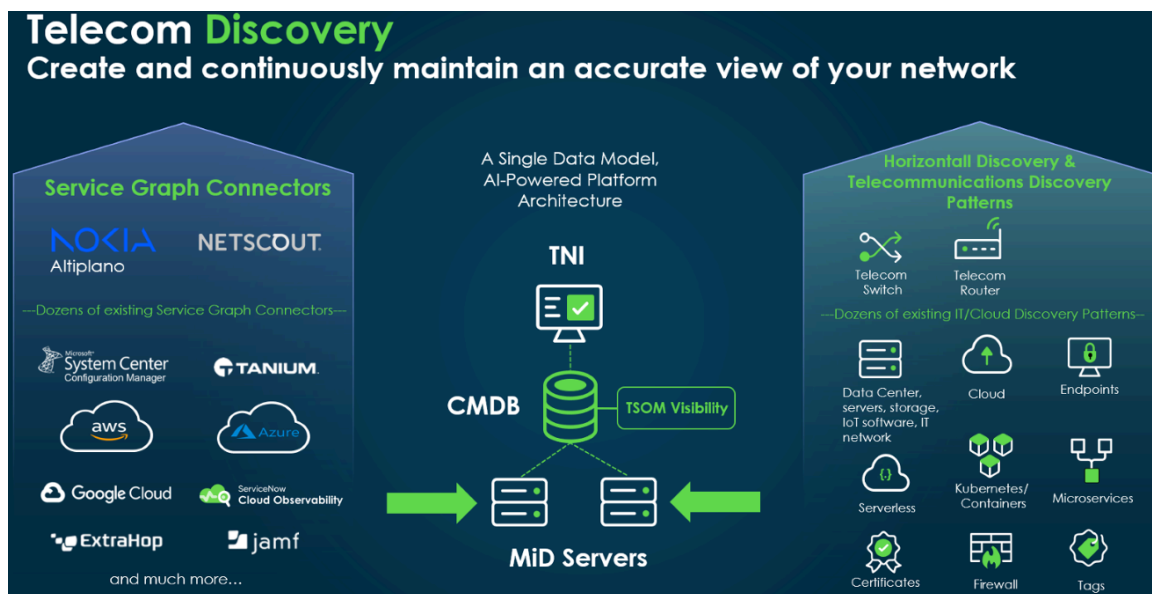
- [Telecom Discovery erkunden](#)
- [Telecom-Discovery mit Service Graph Connectors \(SGC\)](#)
- [Telekommunikations-Discovery mithilfe von Telekommunikations-Discovery-Mustern](#)

## Discovery-Lizenzierung für Unternehmen

Now Platform verwendet ein Lizenzierungsmodell, bei dem Ihrer Organisation die Nutzung von TSOM-Transparenz-Anwendungen in Rechnung gestellt wird. Telecom-Discovery, Telecom-Diskrepanz-Identifizierung und -Abgleich und TSOM-Transparenz (Plugin) sind Komponenten von TSOM-Transparenz. Um die TSOM-Transparenz zu verwenden, muss Ihre Organisation TSOM abonnieren. Beachten Sie, dass die Produktdokumentation ServiceNow® keine Details zu Preisgestaltung, Verpackung oder anderen Einzelheiten enthält, da diese durch den Kundenvertrag Ihres Unternehmens festgelegt werden.

## Telecom Discovery erkunden

Die Lösung ServiceNow® Telecom Discovery basiert auf bewährten Technologien der Plattform ServiceNow® und nutzt leistungsstarke Funktionen wie ITOM Visibility und Horizontal Discovery sowie Service Graph Connectors. Jede dieser Komponenten spielt eine Schlüsselrolle bei der Unterstützung Telekommunikationsspezifischer Anwendungsfälle, während gleichzeitig die Flexibilität für die allgemeine IT-/Cloud-Discovery gewahrt bleibt.



Die TSOM-Transparenz-Plugins können nahtlos zusammen mit ITOM-Transparenz verwendet werden, um die Erkennung und Transparenz der Infrastruktur zu verbessern. Durch die Integration dieser Plugins können Organisationen die erweiterten Telekommunikations-Discovery-Muster und Service Graph Connectors (SGC) von TSOM mit den Fähigkeiten von ITOM nutzen und eine umfassende Identifizierung und Zuordnung von Netzwerkkomponenten, Services und Konfigurationen ermöglichen. Dieser kombinierte Ansatz bestätigt eine genaue und angereicherte Datenmenge in der CMDB und bietet eine einheitliche und detaillierte Ansicht der IT- und Telekommunikationsnetzwerkressourcen.

### TSOM-Transparenz-Plugins:

#### Service Graph Connectors (SGC)

Dieses neue Plugin ermöglicht die Discovery von Daten aus vorhandenen Netzwerkverwaltungssystemen (z. B. EMS/NMS/Controller), wobei der Schwerpunkt in diesem Release auf der Integration der Funktion „Nokia Altiplano Access SDN Control“ über die REST API liegt. Es ist ein für Kunden sichtbares Plugin und muss einzeln installiert werden.

Plugin-Name: sn\_sgc\_altiplano\_connector.

Automatische Übersetzung

Plugin-Beschreibung: Service Graph Connector für Nokia Altiplano.

Weitere Informationen finden Sie unter [Telecom-Discovery mit Service Graph Connectors \(SGC\)](#).

### Discovery-Muster für die Telekommunikation (TSOM-Muster)

Dieses neue Plugin enthält Muster für die Discovery von standardmäßigen SNMP-basierten, eigenständigen xNFs (z. B. Telekommunikationsroutern und -Switches ohne Verwaltungssystem oder solche, die direkt durch Umgehung ihrer Verwaltungssysteme erkannt werden sollen) sowie anwenderdefinierte Muster zur Überprüfung bestimmter Cisco- und Juniper-Geräte durch Nutzung der SNMP- und CLI-Zugänglichkeit.

Plugin-Name: sn\_tsom\_patterns.

Plugin-Beschreibung: Telekommunikations-Discovery-Muster.

Weitere Informationen finden Sie unter [Telekommunikations-Discovery mithilfe von Telekommunikations-Discovery-Mustern](#).

### TSOM Visibility-Plugin

Dieses Plugin enthält eine Logik, die in unserer TSOM-Transparenz-Anwendung gleich ist. Es enthält telekommunikationsspezifische Diskrepanz- und Korrekturlogik sowie andere allgemeine Logik, die wir derzeit für die Verwendung in der gesamten Anwendung erstellen oder erstellen werden.

Plugin-Name: sn\_tsom\_core

Plugin-Beschreibung: Telecom Service Operations Core.

Weitere Informationen finden Sie unter [Identifizierung und Abgleich von Telekommunikationsdiskrepanzen](#).

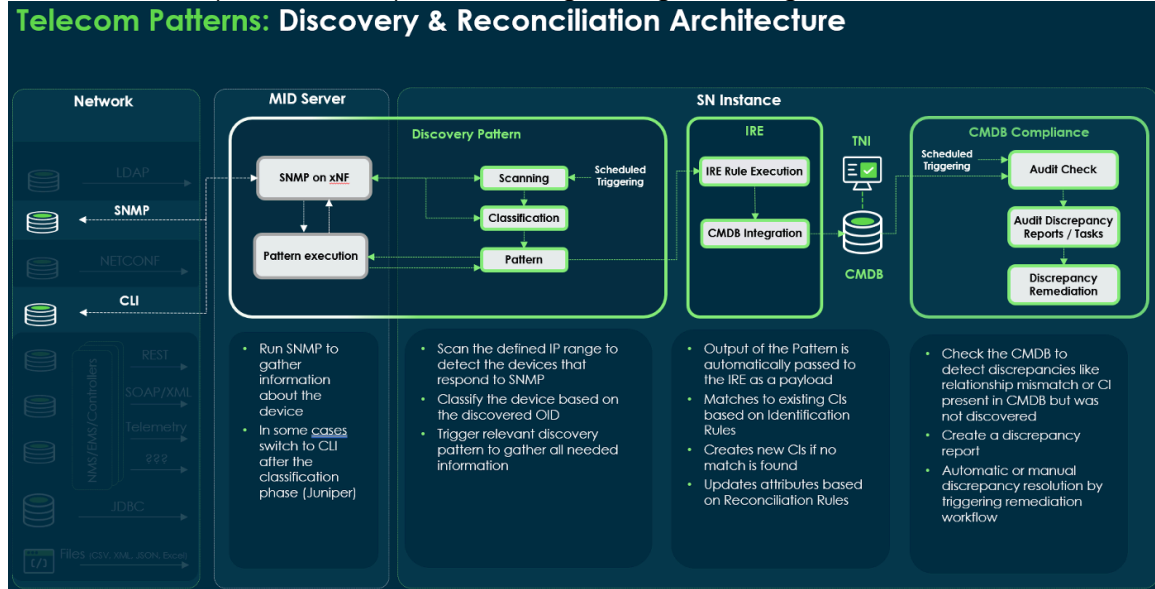
ServiceNow bietet Kunden und Partnern die Möglichkeit, Discovery-Muster für Service Graph Connectors und Telekommunikation zu erstellen und zu ändern. Um diesen Prozess zu vereinfachen, hat ServiceNow eine Reihe von **UI-basierten Designtools ohne Code/Low Code** entwickelt. Mit diesen Tools können Anwender Service Graph Connectors und Muster anpassen und erweitern, ohne dass dafür umfassende Kenntnisse in der Codierung erforderlich sind. Das bestätigt die Flexibilität und ermöglicht eine schnellere Bereitstellung maßgeschneiderter Lösungen für bestimmte Netzwerkumgebungen.

### Telekommunikations-Discovery mithilfe von Telekommunikations-Discovery-Mustern

Die neuen Telecommunication Discovery-Muster (auch bekannt als TSOM-Muster) enthalten Muster für die Erkennung eigenständiger xNFs und ermöglichen die Erkennung eigenständiger Netzwerkelemente ohne Verwaltungssystem mithilfe der Protokolle SNMP, CLI und NETCONF (Roadmap).

## Architektur mit Horizontal-Discovery und Telekommunikations-Discovery-Mustern

Dies ist ein Beispiel für die Implementierung für eigenständige SNMP- oder/und CLI-xNFs.



### Horizontal-Discovery-Anwendung

Die Anwendung „Horizont-Discovery“ in ServiceNow ist eine vielseitige und hoch skalierbare Discovery-Engine, die für den effektiven Betrieb in Netzwerk-, IT- und Cloud-Umgebungen entwickelt wurde und Daten über mehrere Ebenen sammelt, um eine ganzheitliche Ansicht der Infrastruktur zu bieten.

Weitere Informationen finden Sie unter [Horizontal discovery process flow with patterns](#).

### Discovery-Muster für die Telekommunikation (TSOM-Muster)

Ein Muster ist eine Folge von Befehlen, die Attribute eines Configuration Item (CI) und seiner ausgehenden Verbindungen erkennen sollen. Telecom Discovery stellt eine Reihe vorkonfigurierter Muster bereit, die eine Vielzahl von Netzwerkelementen abdecken. Die TSOM-Discovery-Muster fallen unter die Kategorie „Infrastruktur“, die von Horizontal-Discovery zum Generieren von Listen und der Ressourcenstruktur von xNFs verwendet werden.

Dieses Plugin führt Muster für die Erkennung eigenständiger xNFs ein, z. B. Telekommunikationsrouter und -schalter (mit Unterstützung für andere in der Zukunft geplante Gerätetypen), die nicht auf ein Verwaltungssystem angewiesen sind oder eine direkte Erkennung unter Umgehung ihres Verwaltungssystems erfordern. Darüber hinaus sind anwenderdefinierte Muster zum Überprüfen verschiedener Netzwerkgeräte enthalten. Dies ist ein für den Kunden sichtbares Plugin.

### MID-Server

MID-Server ist eine Java-Anwendung, die als Windows-Service oder UNIX-Daemon auf einem Server in Ihrem lokalen Netzwerk ausgeführt wird. ServiceNow® MID-Server erleichtert die Kommunikation und den Datentransfer zwischen einer ServiceNow-Instanz und externen Anwendungen, Datenquellen und Services.

Weitere Informationen finden Sie unter [MID Server](#).

## Identification and Reconciliation Engine (IRE)

IRE bietet ein zentralisiertes Framework zum Identifizieren und Abgleichen von Daten aus mehreren Quellen. Verifiziert die Integrität der CMDB und einiger Nicht-CMDB-Tabellen, wenn verschiedene Datenquellen zum Erstellen oder Aktualisieren von CI-Datensätzen verwendet werden.

Weitere Informationen finden Sie unter [Identifizierung und Abgleich von Telekommunikationsdiskrepanzen](#).

## Audits der CMDB-Compliance-Zertifizierung für die Identifizierung und den Abgleich von Telekommunikations-Diskrepanzen

CMDB-Compliance ist ein Toolset, mit dem Administratoren CMDB-Daten auf Richtigkeit prüfen und gefundene Diskrepanzen beheben können. In der Abteilung Identifizierung und Abgleich von Telekommunikationsdiskrepanzen verwenden wir die Funktion „Zertifizierungsaudits“, um Diskrepanzen in der CMDB zu erkennen und zu analysieren, Folgeaufgaben für die Zertifizierung zu generieren und Nachbesserungs-Workflows zu aktivieren.

Weitere Informationen zur Verwendung für Identifizierung und Abgleich von Diskrepanzen finden Sie unter [Identifizierung und Abgleich von Telekommunikationsdiskrepanzen](#).

## ITOM vs. TSOM – Discovery-Verhalten für eigenständige SNMP- und/oder CLI-xNFs

ITOM Discovery	TSOM Discovery (Telecom)
Basierend auf horizontalen Discovery-Mustern.	Basierend auf horizontalen Discovery-Mustern (für Telekommunikation).
Entdecken Sie Informationen zu Basisgeräten, die hauptsächlich für IT-Zwecke verwendet werden.	Entdecken Sie weitere Attribute und eine tiefere CI-Hierarchie basierend auf dem Anlagentyp.
Nur Standard-MIBs werden unterstützt.	Sowohl standardmäßige als auch herstellerspezifische MIBs werden unterstützt.
Keine Diskrepanzerkennung und -korrektur verfügbar OOB.	Diskrepanzerkennung und automatische oder manuelle Korrektur verfügbar OOB.

- Telecom Discovery basiert auf der Anwendung ITOM Discovery und nutzt die Nebula Discovery Language (NDL).
- Die Lösung enthält eine Reihe von für die Telekommunikation spezifischen Mustern und Systemeigenschaften.
- Benutzer können wählen, ob TSOM- oder ITOM-Muster ausgeführt werden sollen.
- Kunden können TSOM-Muster erweitern oder bei Bedarf eigene erstellen.
- Es gibt keine Abhängigkeit zwischen TSOM Visibility und Telecom Network Inventory (TNI).

## Logik wurde zu Telecom Discovery hinzugefügt

Benutzer können definieren, ob Telecommunications Discovery-Muster (auch als TSOM-Muster bezeichnet) mit ITOM-Mustern für die Ausführung von verwendet werden sollen. Standardmäßig führen alle in TSOM/Telecom Discovery erstellten Muster das ursprüngliche

ITOM-Muster aus (beispielsweise führt das Muster „Telco Router“ auch das Muster „Router“ aus). Kunden können jedoch auswählen, ob sie nur das TSOM-Muster ausführen und das ITOM-Muster ausschließen möchten.

Dieser Parameter wirkt sich nur auf die Muster aus, die als Teil der Anwendung „TSOM Patterns“ für Telco-Kunden entwickelt wurden. Wenn die Eigenschaft auf „true“ festgelegt ist (Standard), führt das TSOM-Muster auch bestimmte gemeinsam genutzte ITOM-Bibliotheken aus dem TSOM-Muster aus.

Diese Logik wird über die Systemeigenschaft `sn_tsom_patterns.itom_pattern_enabled` gesteuert.

**Entspricht dem TNI-Modell** – Discovery-Muster für die Telekommunikation folgen immer dem TNI-Datenmodell. Wenn Telecom Discovery also ein Karte-auf-Karte-Szenario identifiziert, wird dieses nicht als Karte-auf-Karte eingefügt. Stattdessen wird die Struktur geändert, indem ein Untersteckplatz auf der übergeordneten Karte synthetisiert und die untergeordnete Karte in diesen Untersteckplatz eingesetzt wird.

**TNI-Entitätserstellungslogik** – Immer wenn das System erkennt, dass der Kunde TNI installiert hat, erstellt es automatisch einen TNI-Entitätsdatensatz für alle erkannten Netzwerkdaten. Wenn TNI installiert ist, wird der IRE-Nutzlast für jedes Element eine Nutzlast wie die folgende hinzugefügt. Daher ist das erkannte CI in den Tabellen `cmdb_ci` und `tni_entity` enthalten.

### Telekommunikationsroutermuster

Die Anwendung ServiceNow® Telecom Discovery verwendet das Discovery-Muster „Telecom Router“, um SNMP-basierte Router im Netzwerk zu finden. Um einige dieser Ressourcen zu erkennen, müssen die Telecommunications Discovery Patterns (TSOM Patterns) aus dem ServiceNow Store aktualisiert werden.

Telecom Discovery verwendet die Discovery-Muster der Telekommunikation, um die Horizontal-Discovery auszuführen. Dieses Discovery-Muster für die Telekommunikation verwendet eine Reihe von SNMP-Anforderungen, um Netzwerkelemente zu suchen, zu klassifizieren und zu erkennen.

Das Muster „Telekom-Router“ ist Teil der Anwendung „Muster für die Telekommunikations-Discovery“ (`sn_tsom_patterns`), die Teil der TSOM-Transparenz ist.

### 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](#) .

### Voraussetzungen

- Abonnement für TSOM.
- Vergewissern Sie sich, dass Ihre Netzwerkroutergeräte SNMP-Zugriff haben.
- Konfigurieren Sie in der ServiceNow-Instanz die SNMP-Anmeldeinformationen. Weitere Informationen finden Sie unter [SNMP support for Discovery](#) .
- Informationen zum Einrichten von TSOM-Mustern finden Sie unter [Konfigurieren Sie TSOM-Muster \(Telecommunications Discovery-Muster\)](#)..

## Betroffene CMDB-CIs und CI-Beziehungen (Physische Ebene)

CI	CI-Beziehungen
IP-Router-CI	<p>Das IP-Routergerät wird durch das IP-Router-CI dargestellt.</p> <p>Tabellenname: <b>cmdb_ci_ip_router</b></p> <p>IP-Router-CI enthält Slots oder Netzwerkschnittstellen.</p>
Slot-CI	<p>Slots werden durch das Slot-CI dargestellt.</p> <p>Tabellenname: <b>cmdb_ci_container_slot</b></p> <p>Steckplatz ist im IP-Router enthalten.</p> <p>Steckplatz-CI enthält die Schnittstellenkarte.</p>
Subslot-CI	<p>Subslots werden durch das Subslot-CI dargestellt.</p> <p>Tabellenname: <b>cmdb_ci_container_subslot</b></p> <p>Subslot ist im Schnittstellenkarten-CI enthalten.</p> <p>Subslot-CI enthält das Schnittstellenkarten-CI.</p>
Schnittstellenkarten-CI	<p>Verschiedene Arten von Karten werden durch das Schnittstellenkarten-CI dargestellt.</p> <p>Lüfter und Netzteile werden auch durch das Karten-CI dargestellt.</p> <p>Tabellenname: <b>cmdb_ci_interface_card</b></p> <p>Schnittstellenkarten sind in Slots oder Subslots enthalten.</p> <p>Schnittstellenkarten können Netzwerkschnittstellen oder Subslots enthalten.</p>
Netzwerkschnittstellen-CI	<p>Jede Art von Netzwerkschnittstelle wird durch die Netzwerkschnittstellen-CI dargestellt.</p> <p>Tabellenname: <b>cmdb_ci_ni_interface</b></p>

Automatische Übersetzung

Clis	CI-Beziehungen
	Die Netzwerkschnittstelle ist in der Schnittstellenkarte, dem IP-Router, enthalten.

### Klassifizieren von xNFs für dieses Muster

Für den Zugriff auf eine vollständige Liste der OIDs, die klassifiziert werden.

### Vorbereitungen

Erforderliche Rolle: Administrator

Klassifizierername: **Standard-Netzwerkrouter**.

### Prozedur

1. Navigieren zu **Alle > Discovery-Definition > CI-Klassifizierung > SNMP**.
2. Wählen Sie in der Liste **Standard-Netzwerkrouter** aus.
3. Öffnen Sie die Registerkarte **SNMP-OID-Klassifizierungen**, und sehen Sie sich die Liste der OIDs an.

The screenshot shows the configuration page for an SNMP Classifier named 'Standard Network Router'. It includes fields for Name, Active status, Order, Table (IP Router), Match criteria (All), Manufacturer, and Model. Below these is a section for the classification script with a sample comment: '// This script gets run when something gets classified'. The bottom part of the image shows a table of 'SNMP OID Classifications' with columns for OID, Operator, Table, Manufacturer, Model, and Active status.

OID	Operator	Table	Manufacturer	Model	Active
1.3.6.1.4.1.141.1.1.3220	is	IP Router [cmdb_ci_ip_router]	NetScout Systems, Inc.	Packet Probe 3220	true
1.3.6.1.4.1.94.1.21.2.1.2	is	IP Router [cmdb_ci_ip_router]	Nokia	IP40x	true
1.3.6.1.4.1.91.1.2411	is	IP Router [cmdb_ci_ip_router]	Cisco Systems	ciscoNC55011	true
1.3.6.1.4.1.664.1.466	is	IP Router [cmdb_ci_ip_router]	Adtran	NETVANTA3205	true
1.3.6.1.4.1.43.1.6.4.2.12	is	IP Router [cmdb_ci_ip_router]	Hewlett-Packard	R6080	true
1.3.6.1.4.1.91.1.758	is	IP Router [cmdb_ci_ip_router]	Cisco Systems	1250	true
1.3.6.1.4.1.91.1.1448	is	IP Router [cmdb_ci_ip_router]	Cisco Systems	ciscoASAS15K73c	true
1.3.6.1.4.1.2636.1.1.2.24	is	IP Router [cmdb_ci_ip_router]	Juniper Networks	J2350	true
1.3.6.1.4.1.2636.1.1.2.5	is	IP Router [cmdb_ci_ip_router]	Juniper Networks	M5	true

### **i** Hinweis:

Weitere Informationen zum Hinzufügen zusätzlicher OIDs zum Klassifizierer finden Sie unter [Telekommunikations-Discovery mithilfe von Telekommunikations-Discovery-Mustern](#).

Für xNF verwendete MiB-Tabellen:

- SystemMIB
- EntityPhysicalMIB
- IfMIB
- IfXMIB
- IPMIB

### Telecom Cisco 7613 Routermuster

Die Anwendung ServiceNow Telecom Discovery verwendet das Discovery-Muster des Telecom Cisco 7613 Routers, um den SNMP-basierten Cisco 7613 im Netzwerk zu finden. Um einige dieser Ressourcen zu erkennen, müssen die Telecommunications Discovery Patterns (TSOM Patterns) aus dem ServiceNow Store aktualisiert werden.

Telecom Discovery verwendet die Discovery-Muster der Telekommunikation, um die Horizontal-Discovery auszuführen. Dieses Discovery-Muster für die Telekommunikation verwendet eine Reihe von SNMP-Anforderungen, um Netzwerkelemente zu suchen, zu klassifizieren und zu erkennen.

Das Muster für den Telecom Cisco 7613 Router ist Teil der Anwendung „Muster für die Telekommunikations-Discovery“ (sn\_tsom\_patterns), die Teil der TSOM-Transparenz ist.

### 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](#) .

### Voraussetzungen

- Abonnement für TSOM.
- Vergewissern Sie sich, dass Ihre Netzwerkroutergeräte SNMP-Zugriff haben.
- Konfigurieren Sie in der ServiceNow-Instanz die SNMP-Anmeldeinformationen. Weitere Informationen finden Sie unter [SNMP support for Discovery](#) .
- Informationen zum Einrichten von TSOM-Mustern finden Sie unter [Konfigurieren Sie TSOM-Muster \(Telecommunications Discovery-Muster\)](#)..

### Betroffene CMDB-CIs und CI-Beziehungen (Physische Ebene)

CI	CI-Beziehungen
IP-Router-CI	Das IP-Routergerät wird durch das IP-Router-CI dargestellt.  Tabellenname: <b>cmdb_ci_ip_router</b>  IP-Router-CI enthält Slots oder Netzwerkschnittstellen.
Slot-CI	Slots werden durch das Slot-CI dargestellt.  Tabellenname: <b>cmdb_ci_container_slot</b>  Steckplatz ist im IP-Router enthalten.  Steckplatz-CI enthält die Schnittstellenkarte.
Subslot-CI	Subslots werden durch das Subslot-CI dargestellt.

CI	CI-Beziehungen
	<p>Tabellenname: <b>cmdb_ci_container_subslot</b></p> <p>Subslot ist im Schnittstellenkarten-CI enthalten.</p> <p>Subslot-CI enthält das Schnittstellenkarten-CI.</p>
Schnittstellenkarten-CI	<p>Verschiedene Arten von Karten werden durch das Schnittstellenkarten-CI dargestellt.</p> <p>Lüfter und Netzteile werden auch durch das Karten-CI dargestellt.</p> <p>Tabellenname: <b>cmdb_ci_interface_card</b></p> <p>Schnittstellenkarten sind in Slots oder Subslots enthalten.</p> <p>Schnittstellenkarten können Netzwerkschnittstellen oder Subslots enthalten.</p>
Netzwerkschnittstellen-CI	<p>Jede Art von Netzwerkschnittstelle wird durch die Netzwerkschnittstellen-CI dargestellt.</p> <p>Tabellenname: <b>cmdb_ci_ni_interface</b></p> <p>Die Netzwerkschnittstelle ist in der Schnittstellenkarte, dem IP-Router, enthalten.</p>

**Klassifizieren von xNFs für dieses Muster**

Für den Zugriff auf eine vollständige Liste der OIDs, die klassifiziert werden.

**Vorbereitungen**

Erforderliche Rolle: Administrator

Klassifizierername: **Standard-Netzwerkrouter**.

**Prozedur**

1. Navigieren zu **Alle > Discovery-Definition > CI-Klassifizierung > SNMP**.
2. Wählen Sie in der Liste **Standard-Netzwerkrouter**aus.

3. Öffnen Sie die Registerkarte **SNMP-OID-Klassifizierungen**, und sehen Sie sich die Liste der OIDs an.

After the Sensor processes the results of the SNMP - Classify Probe, secondary to SNMP System OIDs, each SNMP Classification defines the order, match criteria, and Probes to trigger. [More Info](#)

Name: Standard Network Router  
 Active:   
 Order: 20  
 Table: IP Router  
 Match criteria: All  
 Manufacturer:   
 Model:   
 On classification script: 

```
1 // This script gets run when something gets classified
```

Update Delete  
 Related Links  
 Run Print Scan  
 Classification Criteria (1) **SNMP OID Classifications (199)** Triggers probes (3) Versions (8)  
 Search for text Search Actions on selected rows... New Sync Candidates Sync From CDS

OID	Operator	Table	Manufacturer	Model	Active
1.3.6.1.4.1.141.1.1.3220	Is	IP Router [cnmdb_ci_ip_router]	NetScout Systems, Inc.	Packet Probe 3220	true
1.3.6.1.4.1.94.1.212.1.2	Is	IP Router [cnmdb_ci_ip_router]	Nokia	IP4xx	true
1.3.6.1.4.1.9.1.2411	Is	IP Router [cnmdb_ci_ip_router]	Cisco Systems	ciscoNCS5011	true
1.3.6.1.4.1.664.1.466	Is	IP Router [cnmdb_ci_ip_router]	Adtran	NETVANTA3205	true
1.3.6.1.4.1.43.1.16.4.2.12	Is	IP Router [cnmdb_ci_ip_router]	Hewlett-Packard	R6080	true
1.3.6.1.4.1.9.1.758	Is	IP Router [cnmdb_ci_ip_router]	Cisco Systems	1250	true
1.3.6.1.4.1.9.1.1448	Is	IP Router [cnmdb_ci_ip_router]	Cisco Systems	ciscoASA5515K7xc	true
1.3.6.1.4.1.2636.1.1.1.2.24	Is	IP Router [cnmdb_ci_ip_router]	Juniper Networks	J2350	true
1.3.6.1.4.1.2636.1.1.1.2.5	Is	IP Router [cnmdb_ci_ip_router]	Juniper Networks	M5	true

**Hinweis:**

Weitere Informationen zum Hinzufügen zusätzlicher OIDs zum Klassifizierer finden Sie unter [Telekommunikations-Discovery mithilfe von Telekommunikations-Discovery-Mustern](#).

Die Liste der spezifischen OIDs zum Aufrufen dieses Musters:

Lieferant	Modell	OID	Muster
Cisco	7613	1.3.6.1.4.1.9.1.528	Telecom Cisco 7613 Router

Für xNF verwendete MIB-Tabellen:

- SystemMIB
- EntityPhysicalMIB
- IfMIB
- IfXMIB
- IPMIB

**SSH-Routermuster für Telecom Juniper Cross**

Die Anwendung ServiceNow® Telecom Discovery verwendet das Discovery-Muster Telecom Juniper MX SSHRouter, um SNMP- und CLI-basierte Router der Juniper-MX-Serie im Netzwerk zu finden. Um einige dieser Ressourcen zu erkennen, müssen die Telecommunications Discovery Patterns (TSOM-Muster) aus dem Store ServiceNow® aktualisiert werden.

Telecom Discovery verwendet die Discovery-Muster der Telekommunikation, um die Horizontal-Discovery auszuführen. Dieses Discovery-Muster für die Telekommunikation verwendet eine Reihe von SNMP-Anforderungen, um CLI über SSH zu finden und zu klassifizieren, um Netzwerkelemente zu erkennen.

Das Muster „Telecom Juniper CX SSH-Router“ ist Teil der Anwendung „Muster für die Telekommunikations-Discovery“ (sn\_tsom\_patterns), die Teil der TSOM-Transparenz ist.

## 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](#).

## Voraussetzungen

- Abonnement für TSOM.
- Vergewissern Sie sich, dass Ihre Netzwerkroutergeräte SNMP-Zugriff haben.
- Konfigurieren Sie in der ServiceNow-Instanz die SNMP-Anmeldeinformationen. Weitere Informationen finden Sie unter [SNMP support for Discovery](#).
- Informationen zum Einrichten von TSOM-Mustern finden Sie unter [Konfigurieren Sie TSOM-Muster \(Telecommunications Discovery-Muster\)](#).

## Betroffene CMDB-CIs und CI-Beziehungen (Physische Ebene)

CI	CI-Beziehungen
IP-Router-CI	<p>Das IP-Routergerät wird durch das IP-Router-CI dargestellt.</p> <p>Tabellenname: <b>cmdb_ci_ip_router</b></p> <p>IP-Router-CI enthält Slots oder Netzwerkschnittstellen.</p>
Slot-CI	<p>Slots werden durch das Slot-CI dargestellt.</p> <p>Tabellenname: <b>cmdb_ci_container_slot</b></p> <p>Steckplatz ist im IP-Router enthalten.</p> <p>Steckplatz-CI enthält die Schnittstellenkarte.</p>
Subslot-CI	<p>Subslots werden durch das Subslot-CI dargestellt.</p> <p>Tabellenname: <b>cmdb_ci_container_subslot</b></p> <p>Subslot ist im Schnittstellenkarten-CI enthalten.</p> <p>Subslot-CI enthält das Schnittstellenkarten-CI.</p>
Schnittstellenkarten-CI	<p>Verschiedene Arten von Karten werden durch das Schnittstellenkarten-CI dargestellt.</p>

CIs	CI-Beziehungen
	<p>Lüfter und Netzteile werden auch durch das Karten-CI dargestellt.</p> <p>Tabellenname: <b>cmdb_ci_interface_card</b></p> <p>Schnittstellenkarten sind in Slots oder Subslots enthalten.</p> <p>Schnittstellenkarten können Netzwerkschnittstellen oder Subslots enthalten.</p>
Netzwerkschnittstellen-CI	<p>Jede Art von Netzwerkschnittstelle wird durch die Netzwerkschnittstellen-CI dargestellt.</p> <p>Tabellenname: <b>cmdb_ci_ni_interface</b></p> <p>Die Netzwerkschnittstelle ist in der Schnittstellenkarte, dem IP-Router, enthalten.</p>

**Klassifizieren von xNFs für dieses Muster**

Für den Zugriff auf eine vollständige Liste der OIDs, die klassifiziert werden.

**Vorbereitungen**

Erforderliche Rolle: Administrator

Klassifizierername: **Standard-Netzwerkrouter**.

**Prozedur**

1. Navigieren zu **Alle > Discovery-Definition > CI-Klassifizierung > SNMP**.
2. Wählen Sie in der Liste **Standard-Netzwerkrouter** aus.

### 3. Öffnen Sie die Registerkarte **SNMP-OID-Klassifizierungen**, und sehen Sie sich die Liste der OIDs an.

After the Sensor processes the results of the SNMP - Classify Probe, secondary to SNMP System OIDs, each SNMP Classification defines the order, match criteria, and Probes to trigger. [More Info](#)

Name: Standard Network Router  
 Active:   
 Order: 20  
 Table: IP Router  
 Match criteria: All  
 Manufacturer:   
 Model:

On classification script  

```
1 // This script gets run when something gets classified
```

Update Delete  
 Related Links  
 Run Point Scan

Classification Criteria (1) **SNMP-OID-Klassifizierung (1599)** Triggers probes (3) Versions (8)

Classifier - Standard Network Router

OID	Operator	Table	Manufacturer	Model	Active
1.3.6.1.4.1.141.1.1.3220	Is	IP Router [cndb_ci_ip_router]	NetScout Systems, Inc.	Packet Probe 3220	true
1.3.6.1.4.1.94.1.21.2.1.2	Is	IP Router [cndb_ci_ip_router]	Nokia	IP4xx	true
1.3.6.1.4.1.9.1.2411	Is	IP Router [cndb_ci_ip_router]	Cisco Systems	ciscoNC55011	true
1.3.6.1.4.1.6641.466	Is	IP Router [cndb_ci_ip_router]	Adtran	NETWANTA205	true
1.3.6.1.4.1.43.1.16.4.2.12	Is	IP Router [cndb_ci_ip_router]	Hewlett-Packard	R6080	true
1.3.6.1.4.1.9.1.758	Is	IP Router [cndb_ci_ip_router]	Cisco Systems	1250	true
1.3.6.1.4.1.9.1.1448	Is	IP Router [cndb_ci_ip_router]	Cisco Systems	ciscoASAS515K73c	true
1.3.6.1.4.1.2636.1.1.2.24	Is	IP Router [cndb_ci_ip_router]	Juniper Networks	J2350	true
1.3.6.1.4.1.2636.1.1.1.2.5	Is	IP Router [cndb_ci_ip_router]	Juniper Networks	M5	true

#### **Hinweis:**

Weitere Informationen zum Hinzufügen zusätzlicher OIDs zum Klassifizierer finden Sie unter [Telekommunikations-Discovery mithilfe von Telekommunikations-Discovery-Mustern](#).

Die Liste der spezifischen OIDs zum Aufrufen dieses Musters:

Lieferant	Modell	OID	Muster
Juniper	MX80	1.3.6.1.4.1.2636.1.1.1.2.57	SSH-Router Telecom Juniper
Juniper	MX104	1.3.6.1.4.1.2636.1.1.1.2.97	SSH-Router Telecom Juniper
Juniper	MX240	1.3.6.1.4.1.2636.1.1.1.2.29	SSH-Router Telecom Juniper
Juniper	MX480	1.3.6.1.4.1.2636.1.1.1.2.25	SSH-Router Telecom Juniper

Auf einem xNF: SystemMIB verwendete MiB-Tabellen.

Verwendete CLI-Befehle.

- Gehäuse-Hardware anzeigen | nicht mehr | Anzeige-XML
- Schnittstellenmedien | anzeigen nicht mehr | Anzeige-XML

#### **Telekommunikations-Cisco-Switch-Muster**

Die Anwendung ServiceNow® Telecom Discovery verwendet das Discovery-Muster Telecom Cisco Switch, um SNMP-basierte Cisco-Switches im Netzwerk zu finden. Die Erkennung einiger dieser Ressourcen erfordert die Aktualisierung der Telecommunications Discovery Patterns (TSOM Patterns) aus dem ServiceNow® Store.

Telecom Discovery verwendet die Discovery-Muster der Telekommunikation, um die Horizontal-Discovery auszuführen. Dieses Discovery-Muster für die Telekommunikation verwendet eine Reihe von SNMP-Anforderungen, um Netzwerkelemente zu suchen, zu klassifizieren und zu erkennen.

Das Muster Telecom Cisco Switch ist Teil der Anwendung Telecommunications Discovery Patterns (sn\_tsom\_patterns), die Teil der TSOM-Transparenz ist.

## 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](#).

## Voraussetzungen

- Abonnement für TSOM.
- Vergewissern Sie sich, dass Ihre Netzwerkroutergeräte SNMP-Zugriff haben.
- Konfigurieren Sie die SNMP-Anmeldeinformationen in der ServiceNow®-Instanz. Weitere Informationen finden Sie unter [SNMP support for Discovery](#).
- Informationen zum Einrichten von TSOM-Mustern finden Sie unter [Konfigurieren Sie TSOM-Muster \(Telecommunications Discovery-Muster\)](#).

## Betroffene CMDB-CIs und CI-Beziehungen (Physische Ebene)

CIs	CI-Beziehungen
IP-Switch-CI	Das IP-Switch-Gerät wird durch das IP-Switch-CI dargestellt.  Tabellenname: <b>cmdb_ci_ip_change</b>  IP-Switch-CI enthält Slots oder Netzwerkschnittstellen.
Slot-CI	Slots werden durch das Slot-CI dargestellt.  Tabellenname: <b>cmdb_ci_container_slot</b>  Steckplatz ist im IP-Switch enthalten.  Steckplatz-CI enthält die Schnittstellenkarte.
Subslot-CI	Subslots werden durch das Subslot-CI dargestellt.  Tabellenname: <b>cmdb_ci_container_subslot</b>  Subslot ist im Schnittstellenkarten-CI enthalten.  Subslot-CI enthält das Schnittstellenkarten-CI.
Schnittstellenkarten-CI	Verschiedene Arten von Karten werden durch das Schnittstellenkarten-CI dargestellt.

CIs	CI-Beziehungen
	<p>Lüfter und Netzteile werden auch durch das Karten-CI dargestellt.</p> <p>Tabellenname: <b>cmdb_ci_interface_card</b></p> <p>Schnittstellenkarten sind in Slots oder Subslots enthalten.</p> <p>Schnittstellenkarten können Netzwerkschnittstellen oder Subslots enthalten.</p>
Netzwerkschnittstellen-CI	<p>Jede Art von Netzwerkschnittstelle wird durch die Netzwerkschnittstellen-CI dargestellt.</p> <p>Tabellenname: <b>cmdb_ci_ni_interface</b></p> <p>Die Netzwerkschnittstelle ist in der Schnittstellenkarte, dem IP-Switch, enthalten.</p>

**Klassifizieren von xNFs für dieses Muster**

Für den Zugriff auf eine vollständige Liste der OIDs, die klassifiziert werden.

**Vorbereitungen**

Erforderliche Rolle: Administrator

Klassifizierername: **Standard-Netzwerk-Switch.**

**Prozedur**

1. Navigieren zu **Alle > Discovery-Definition > CI-Klassifizierung > SNMP.**
2. Wählen Sie in der Liste **Standard-Netzwerk-Switch**aus.

3. Öffnen Sie die Registerkarte **SNMP-OID-Klassifizierungen**, und sehen Sie sich die Liste der OIDs an.

The screenshot shows the configuration page for a classification rule named 'StandardNetworkSwitch'. The configuration includes:
 

- Name: StandardNetworkSwitch
- Active:
- Order: 10
- Table: IP Switch
- Match criteria: All
- Manufacturer: (empty)
- Model: (empty)

 The 'On classification script' section contains the following code:
 

```
1 // This script gets run when something gets classified
```

 Below the configuration is a table of 'Classification Criteria (2)'. The table has columns for 'OID', 'Operator', 'Table', 'Manufacturer', 'Model', and 'Active'. The table lists various OIDs and their corresponding manufacturers and models, such as Extreme Networks, Airespace, Inc, Cisco Systems, Alcatel-Lucent Enterprise, Hewlett-Packard, and IBM.

**Hinweis:**

Weitere Informationen zum Hinzufügen zusätzlicher OIDs zum Klassifizierer finden Sie unter [Telekommunikations-Discovery mithilfe von Telekommunikations-Discovery-Mustern](#).

Die Liste der spezifischen OIDs zum Aufrufen dieses Musters:

Lieferant	Modell	OID	Muster
Cisco	Nexus 9000	1.3.6.1.4.1.9.12.3.1.3.1954	Telekommunikations-Cisco-Switch
Cisco	Nexus 3548	1.3.6.1.4.1.9.12.3.1.3.1666	Telekommunikations-Cisco-Switch

Für xNF verwendete MiB-Tabellen:

- SystemMIB
- EntityPhysicalMIB
- IfMIB
- IfXMIB
- IPMIB

**Telekommunikations-Switch-Muster**

Die Anwendung ServiceNow® Telecom Discovery verwendet das Discovery-Muster Telecom Switch, um SNMP-basierte Telekommunikations-Switches im Netzwerk zu finden. Die Erkennung einiger dieser Ressourcen erfordert die Aktualisierung der Telecommunications Discovery Patterns (TSOM Patterns) aus dem ServiceNow® Store.

Telecom Discovery verwendet die Discovery-Muster der Telekommunikation, um die Horizontal-Discovery auszuführen. Dieses Discovery-Muster für die Telekommunikation verwendet eine Reihe von SNMP-Anforderungen, um Netzwerkelemente zu suchen, zu klassifizieren und zu erkennen.

Das Muster „Telekom-Switch“ ist Teil der Anwendung „Muster für die Telekommunikations-Discovery“ (sn\_tsom\_patterns), die Teil der TSOM-Transparenz ist.

### 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](#) .

### Voraussetzungen

- Abonnement für TSOM.
- Vergewissern Sie sich, dass Ihre Netzwerkroutergeräte SNMP-Zugriff haben.
- Konfigurieren Sie die SNMP-Anmeldeinformationen in der ServiceNow®-Instanz. Weitere Informationen finden Sie unter [SNMP support for Discovery](#) .
- Informationen zum Einrichten von TSOM-Mustern finden Sie unter [Konfigurieren Sie TSOM-Muster \(Telecommunications Discovery-Muster\)](#)..

### Betroffene CMDB-CIs und CI-Beziehungen (Physische Ebene)

CI	CI-Beziehungen
IP-Switch-CI	Das IP-Switch-Gerät wird durch das IP-Switch-CI dargestellt.  Tabellenname: <b>cmdb_ci_ip_change</b>  IP-Switch-CI enthält Slots oder Netzwerkschnittstellen.
Slot-CI	Slots werden durch das Slot-CI dargestellt.  Tabellenname: <b>cmdb_ci_container_slot</b>  Steckplatz ist im IP-Switch enthalten.  Steckplatz-CI enthält die Schnittstellenkarte.
Subslot-CI	Subslots werden durch das Subslot-CI dargestellt.  Tabellenname: <b>cmdb_ci_container_subslot</b>  Subslot ist im Schnittstellenkarten-CI enthalten.  Subslot-CI enthält das Schnittstellenkarten-CI.
Schnittstellenkarten-CI	Verschiedene Arten von Karten werden durch das Schnittstellenkarten-CI dargestellt.

CIs	CI-Beziehungen
	<p>Lüfter und Netzteile werden auch durch das Karten-CI dargestellt.</p> <p>Tabellenname: <b>cmdb_ci_interface_card</b></p> <p>Schnittstellenkarten sind in Slots oder Subslots enthalten.</p> <p>Schnittstellenkarten können Netzwerkschnittstellen oder Subslots enthalten.</p>
Netzwerkschnittstellen-CI	<p>Jede Art von Netzwerkschnittstelle wird durch die Netzwerkschnittstellen-CI dargestellt.</p> <p>Tabellenname: <b>cmdb_ci_ni_interface</b></p> <p>Die Netzwerkschnittstelle ist in der Schnittstellenkarte, dem IP-Switch, enthalten.</p>

**Klassifizieren von xNFs für dieses Muster**

Für den Zugriff auf eine vollständige Liste der OIDs, die klassifiziert werden.

**Vorbereitungen**

Erforderliche Rolle: Administrator

Klassifizierername: **Standard-Netzwerk-Switch.**

**Prozedur**

1. Navigieren zu **Alle > Discovery-Definition > CI-Klassifizierung > SNMP.**
2. Wählen Sie in der Liste **Standard-Netzwerk-Switch**aus.

### 3. Öffnen Sie die Registerkarte **SNMP-OID-Klassifizierungen**, und sehen Sie sich die Liste der OIDs an.

The screenshot shows the configuration page for a 'Standard Network Switch' classifier. It includes fields for Name, Active status, Order, Table, Match criteria, Manufacturer, and Model. Below these is a section for the classification script. The second part of the screenshot shows a table of 'SNMP-OID Classifications (427)' with columns for Old, Operator, Table, Manufacturer, Model, and Active.

Old	Operator	Table	Manufacturer	Model	Active
1.3.6.1.4.1.1916.2.98	Is	IP Switch [cmdb_ci_ip_switch]	Extreme Networks	SUMMITX250-24XDC	true
1.3.6.1.4.1.14179.2.2.1.1.22.57	Is	IP Switch [cmdb_ci_ip_switch]	Airspace, Inc	Cisco 1830I Unified Access Point	true
1.3.6.1.4.1.9.1.1071	Is	IP Switch [cmdb_ci_ip_switch]	Cisco Systems	ciscoPwrC3900Poe	true
1.3.6.1.4.1.6527.6.2.1.2.1	Is	IP Switch [cmdb_ci_ip_switch]	Alcatel-Lucent Enterprise	7210 SAS-E	true
1.3.6.1.4.1.25506.1.246	Is	IP Switch [cmdb_ci_ip_switch]	Hewlett-Packard	H3C S3100-26TP-EI	true
1.3.6.1.4.1.25506.1.38	Is	IP Switch [cmdb_ci_ip_switch]	Hewlett-Packard	H3C S3600-52P-EI	true
1.3.6.1.4.1.9.1.1637	Is	IP Switch [cmdb_ci_ip_switch]	Cisco Systems	ciscoE140D	true
1.3.6.1.4.1.25506.1.654	Is	IP Switch [cmdb_ci_ip_switch]	H3C Technologies	S3100V2-16TP-SI	true
1.3.6.1.4.1.1991.1.3.39.1	Is	IP Switch [cmdb_ci_ip_switch]	Brocade Communications Systems	NetIron IMR 640 Switch	true
1.3.6.1.4.1.2.6.157	Is	IP Switch [cmdb_ci_ip_switch]	IBM	8275-416	true

#### **i Hinweis:**

Weitere Informationen zum Hinzufügen zusätzlicher OIDs zum Klassifizierer finden Sie unter [Telekommunikations-Discovery mithilfe von Telekommunikations-Discovery-Mustern](#).

Für xNF verwendete MiB-Tabellen:

- SystemMIB
- EntityPhysicalMIB
- IfMIB
- IfXMIB
- IPMIB

#### **Konfigurieren Sie TSOM-Muster (Telecommunications Discovery-Muster).**

In diesem Dokument werden die Abhängigkeiten, Anforderungen und Installationsschritte beschrieben, die zum Einrichten von Telecommunications Discovery Patterns (auch als TSOM-Muster bezeichnet) in TSOM Visibility in ServiceNow® erforderlich sind.

#### **Bevor Sie beginnen**

Zur Verwendung von Telecommunications Discovery Patterns benötigen Sie ein Abonnement für TSOM.

Erforderliche Rolle: Administrator

#### **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](#).

## Abhängigkeiten und Anforderungen

- Telecom Service Operations Core (sn\_tsom\_core)
- Discovery Core (com.snc.discovery.core), das automatisch von Discovery 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 [Request Discovery](#) .

## Haftungsausschluss für die TSOM-Transparenz-Installation

Unter [Haftungsausschluss für die TSOM-Transparenz-Installation](#) finden Sie wichtige Informationen und Anforderungen für den Installationsprozess.

## Installieren Sie Horizontal-Discovery und Telekommunikations-Discovery-Muster

Prozess zum Abrufen und Installieren der Telecommunications Discovery-Muster in TSOM

### Vorbereitungen

Erforderliche Rolle: Administrator

### Prozedur

1. Installieren Sie die Anwendung Horizontal Discovery.  
Weitere Informationen finden Sie unter [Discovery setup](#) , da dies die Grundlage für die Ausführung von Discovery-Mustern für die Telekommunikation darstellt.
2. Telecommunications Discovery Patterns abrufen und installieren:
  - a. Installieren Sie die Telecommunications Discovery Patterns (sn\_tsom\_patterns) aus dem ServiceNow® Store.
3. Richten Sie einen MID-Server und Synchronisierungsmuster ein:
  - a. Synchronisieren Sie die installierten Muster mit den entsprechenden MID-Servern, um zu bestätigen, dass sie zur Verwendung bereit sind:
    - i. Navigieren zu **Discovery > MID-Server**.
    - ii. Wählen Sie **Mustersynchronisierung mit MID** aus.

**i** **Hinweis:**  
Diese Aktion synchronisiert TSOM- und ITOM-Muster.

Weitere Informationen zum Konfigurieren eines MID-Servers finden Sie unter [Configuring MID Server](#) .
4. Konfigurieren Sie die TSOM-Systemeigenschaften:
  - a. Legen Sie die Systemeigenschaft sn\_tsom\_patterns.itom\_pattern\_enabled fest, um die Logik dafür zu definieren, ob nur das TSOM-Muster oder eine Kombination aus ITOM- und TSOM-Mustern verwendet werden soll.
    - i. Navigieren Sie zu **Alle > Systemeigenschaften > Alle Eigenschaften**.
    - ii. Wählen Sie **sn\_tsom\_patterns.itom\_pattern\_enabled** aus.
    - iii. Überprüfen Sie, ob der Wert auf „wahr“ (Standard) festgelegt ist.

Wenn TSOM nur TSOM-Muster ausführen und ITOM-Muster ausschließen soll, legen Sie den Wert auf **false** fest.

### **Hinweis:**

Standardmäßig ist die Verwendung von TSOM- und ITOM-Mustern konfiguriert.

5. Ermöglichen Sie das Ersetzen verschiedener ITOM-Muster durch TSOM-Muster auf einem bestimmten MID-Server:


Beispiel: Das Telecom-Router-Muster ersetzt das Netzwerkrouter-Muster für einen bestimmten MID-Server, wenn **mid.telecom.discovery.patterns.enabled** für diesen MID-Server auf „true“ festgelegt ist.

- a. Wechseln Sie zum **Filternavigator**, und geben Sie **ecc\_agent\_config.list** ein.
- b. Wählen Sie „**mid.telecom.discovery.patterns.enabled**“ aus (jeder MID-Server verfügt über diesen Parameter).
- c. Überprüfen Sie, ob der Wert auf **true** festgelegt ist.

Wiederholen Sie diese Konfiguration für jeden MID-Server, den Sie zum Ausführen von TSOM-Mustern verwenden möchten.

### **Haftungsausschluss für die TSOM-Transparenz-Installation**

Zur Unterstützung der TSOM-Transparenz-Lösung haben wir die Store-Anwendung „CMDB CI Class Models Models“ geändert und Updates an die IRE-Identifizierungsregeln für die folgenden Telekommunikations-CIs vorgenommen.

Weitere Informationen zur Store-Anwendung CMDB CI Class Models finden Sie unter [CMDB CI-Klassenmodelle](#) .

- **Schnittstellenkarten**
- **Steckplätze**
- **Untersteckplätze**
- **Netzwerkschnittstellen**

TSOM Visibility erfordert CMDB CI Class Models Version 1.69.0 (**sn\_cmdb\_ci\_class**).

Wenn Sie eine der TSOM-Transparenz-Anwendungen (**sn\_sgc\_altiplano\_connector**, **sn\_tsom\_patterns** oder das Plugin **sn\_tsom\_core**) installieren, wird die Store-Anwendung CMDB CI-Klassenmodelle automatisch auf Version 1.69.0 aktualisiert (oder installiert).

### **Hinweis:**

Ein Administrator kann die Store-Anwendung „CMDB CI Class Models“ weiterhin nach seinem Ermessen auf Version 1.69.0 aktualisieren, unabhängig davon, ob seine Yokohama-Instanz über TSOM Visibility verfügt oder ob sich ihre Instanz auf einem Release vor Yokohama (z. B. Washington DC oder Xanadu) befindet).

**WICHTIG!** Wenn ein Administrator CMDB CI-Klassenmodelle Version 1.69.0 bereitstellt – unabhängig davon, ob TSOM Visibility installiert ist oder nicht – können alle anwenderdefinierten IRE-Identifizierungsregeln betroffen sein, die auf eines oder mehrere der oben genannten Telekommunikations-CIs angewendet werden. Diese Regeln müssen sorgfältig validiert werden, um eine ordnungsgemäße Funktionalität sicherzustellen.

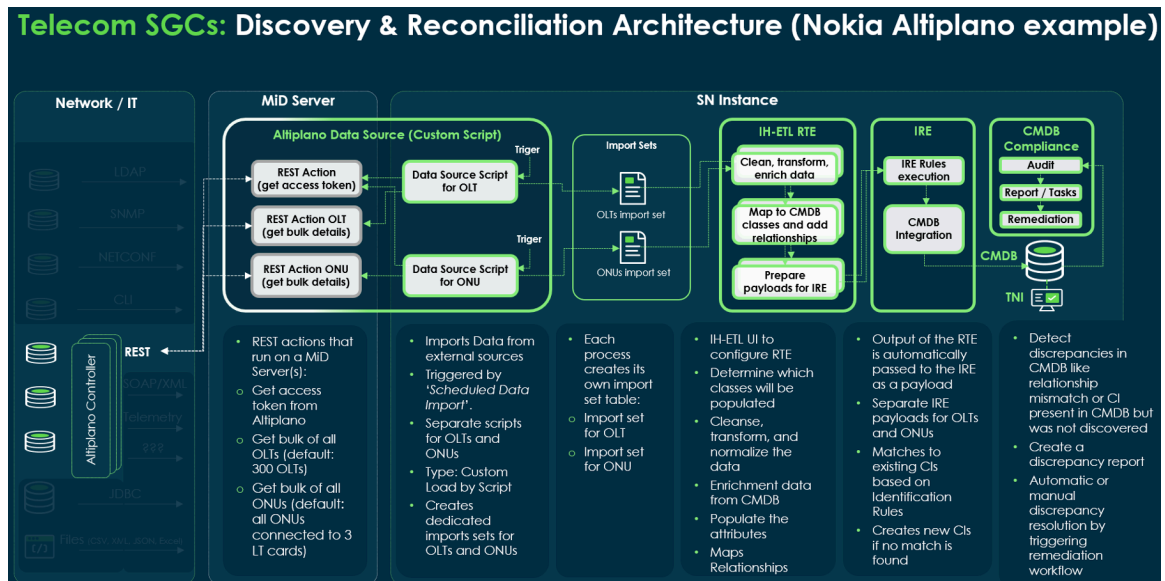
## Telecom-Discovery mit Service Graph Connectors (SGC)

Service Graph Connectors sind vordefinierte Integrationen, die Daten aus Drittanbieterquellen (z. B. Northbound-APIs von EMS/NMS/Controllern, die verschiedene xNFs verwalten) über verschiedene Netzwerkdomänen hinweg in die Configuration Management Database (CMDB) erfassen und gleichzeitig eine strukturierte, am Telekommunikationsmodell ausgerichtete Ansicht von Netzwerkressourcen und -services.

Sie können zusammen mit allen vorhandenen Service Graph Connectors verwendet werden, z. B. für Sicherheit, Server, Software, Überwachung, Internet der Dinge (IoT) und Cloud.

## Architektur mit Telecom Service Graph Connectors

Dies ist ein Beispiel für die -Implementierung für den Nokia Altiplano Service Graph Connector. Die Architektur anderer Connectors kann variieren.



Automatische Übersetzung

## IntegrationHub ETL (3.2)

Diese Store App zum Erstellen und Verwalten von ETL-Transformationszuordnungen, die Daten von Drittanbietern in die CMDB oder Nicht-CMDB-Tabellen integrieren, ohne die Integrität der Daten zu beeinträchtigen. IntegrationHub ETL bietet eine vereinfachte Anwenderoberfläche, die Sie durch den End-to-End-Integrationsprozess führt, einschließlich einer Testintegrationsausführung mit Beispieldaten.

Weitere Informationen finden Sie unter [IntegrationHub ETL](#) .

## Robuste Transformations-Engine (RTE)

Dieses Plugin wird verwendet, um Rohquelldaten, die in Bereitstellungstabellen gespeichert sind, in Daten umzuwandeln, die zugeordnet und in die CMDB integriert werden. RTE verwendet ETL-Transformationszuordnungen, die während der Datentransformation für die Integration erstellt wurden.

Weitere Informationen finden Sie unter [Create a robust import set transformer](#) .

## MID-Server

MID-Server ist eine Java-Anwendung, die als Windows-Service oder UNIX-Daemon auf einem Server in Ihrem lokalen Netzwerk ausgeführt wird. ServiceNow® MID-Server erleichtert die

Kommunikation und den Datentransfer zwischen einer ServiceNow-Instanz und externen Anwendungen, Datenquellen und Services.

Weitere Informationen finden Sie unter [MID Server](#) .

## Identification and Reconciliation Engine (IRE)

IRE bietet ein zentralisiertes Framework zum Identifizieren und Abgleichen von Daten aus mehreren Quellen. Bestätigt die Integrität der CMDB und einiger Nicht-CMDB-Tabellen, wenn verschiedene Datenquellen zum Erstellen oder Aktualisieren von CI-Datensätzen verwendet werden.

Weitere Informationen finden Sie im Abschnitt [CMDB Identification and Reconciliation \(IRE\)](#) .

## Audits der CMDB-Compliance-Zertifizierung für die Identifizierung und den Abgleich von Telekommunikations-Diskrepanzen

[CMDB Compliance](#) ist ein Toolset, mit dem Administratoren CMDB-Daten auf Richtigkeit prüfen und gefundene Diskrepanzen beheben können. In Telecom Diskrepancy Identification and Reconciliation verwenden wir die Funktion [Certification audits](#) , um Diskrepanzen in der CMDB zu erkennen und zu analysieren, [Certification follow-on tasks](#) zu generieren und Nachbesserungs-Workflows zu aktivieren.

Weitere Informationen zur Verwendung für Identifizierung und Abgleich von Diskrepanzen finden Sie unter [Identifizierung und Abgleich von Telekommunikationsdiskrepanzen](#).

## Erstellungslogik für TNI-Entitäten

Immer wenn das System erkennt, dass beim Kunden TNI installiert ist, erstellt es automatisch einen TNI-Entitätsdatensatz für alle erkannten Netzwerkdaten.

Wenn TNI installiert ist, wird der IRE-Nutzlast für jedes Element eine Nutzlast wie die folgende hinzugefügt (wobei „inventory\_category“ basierend auf dem Klassennamen ausgefüllt wird):

```
related = [{
  "className": "tni_entity",
  "values": {
    "inventory_category": ""
  }
}];
```

Daher ist das erkannte CI in den Tabellen cmdb\_ci und tni\_entity enthalten.

## Telecom Service Graph Connectors unterstützt

[Service Graph Connector für Nokia Altiplano](#).

Siehe andere verfügbare [Service Graph Connectors](#) .

## Unterstützte Versionen

Unterstützte ServiceNow® -Versionen: Yokohama und höher.

## Service Graph Connector für Nokia Altiplano

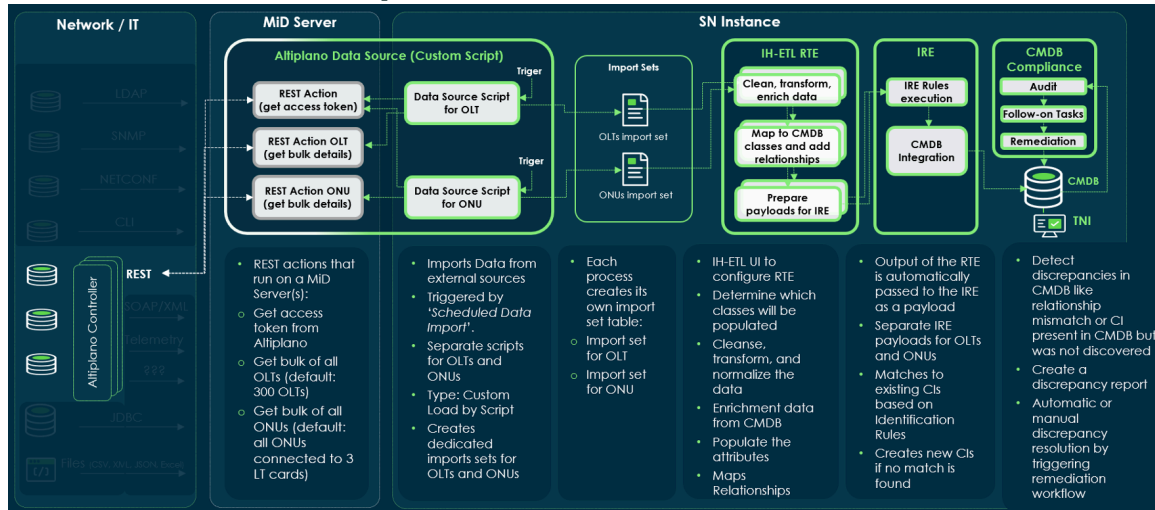
Verwenden Sie den SDN Controller für das Service Graph Connector für das Access Network von Nodi Plano, um Daten aus der Nodi Altiplano-Software mithilfe von REST APIs in Ihre ServiceNow-Instanz abzurufen.

Der Service Graphs Connector für Nodi Altiplano ruft Asset-Bestandsdaten (physische Netzwerkressourcen) aus der Nodi Altiplano-Datenbank ab.

## 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](#).

## Architektur von Nodi Altiplano SGC



Datenquelle wie folgt definiert:

- Anwenderdefiniertes Laden nach Skript
- Daten in einzelner Spalte

Eine allgemeine Übersicht über die Service Graph Connector-Technologie finden Sie unter [Getting started with Service Graph Connectors](#).

## Unterstützte Versionen

Mindestversionen des unterstützten Nokka Altiplano Controllers: 24.6.

## Anwendungsfälle

Im Folgenden finden Sie Beispiele für die Verwendung des Nowak Altiplano Service Graph Connector:

- **Der Nodi Altiplano Service Graph Connector** kann verwendet werden, um Daten vom Nodi Altiplano Access Controller über die REST API (über einen MID Server) abzurufen und zu bestätigen, dass die CMDB mit genauen, aktuellen Informationen zu physischen Netzwerkressourcen wie OLTs gefüllt ist und ONTs, unter anderem. Diese Integration bietet eine am Telekommunikationsmodell ausgerichtete Ansicht von Netzwerkressourcen und deren Beziehungen.
- **Zukünftige Fähigkeiten:** In den bevorstehenden Versionen des Weiteren werden die Fähigkeiten des Nodi Altiplano Service Graph Connector erweitert, um nicht nur physische Ressourcen, sondern auch logische Ressourcen und Services/Verbindungen zu erkennen. Dies ermöglicht eine umfassendere Ansicht der physischen und logischen Aspekte des Netzwerks. Außerdem wird die ereignisgesteuerte Erkennung unterstützt,

bei der der Altiplano-Controller die ServiceNow-Instanz (über den MID Server) über eine Änderung benachrichtigt und nacheinander eine Erkennungsaufgabe auslöst.

- Möglichkeit zum Konfigurieren und Speichern von Synchronisierungszeitplänen.

## Geführtes Setup

Das geführte Setup für Service Graphs Connector für Nokia Altiplano 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 Service Graph Connector für Nok Altiplano](#).

## Dashboard CMDB-Integrationen

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

## Importsätze

Die Importsätze sind die Eingabe für IntegrationHub ETL, wobei die Transformationszuordnungen Beziehungen erstellen und modellieren. Wenn Daten in den Importsatz geladen werden, wird der Transformationsprozess ausgelöst.

## Vorbereitungen

Erforderliche Rolle: Administrator

## Prozedur

Navigieren zu **Alle > System-Importsätze > Administration > Importsätze**.

Das Datenquellen-Skript erstellt automatisch Bereitstellungstabellen.

Number	Short description	State	Import set table	Data source	Created	Load completed	Load run time	Transaction ID	Created by
ISE000214	Specific on-demand discovery	Processed	SG-Altiplano OLT Inventory (sn_sgc_altiplano_bomn_olt)	SG-Altiplano OLT ON Demand	2025-01-02 00:35:25	2025-01-01 16:35:44			IsartAnnamanglic
ISE000213	Specific on-demand discovery	Loaded	SG-Altiplano OLT Inventory (sn_sgc_altiplano_bomn_olt)	SG-Altiplano OLT ON Demand	2025-01-01 07:40:52	2024-12-31 23:40:53			IsartAnnamanglic
ISE000212	Specific on-demand discovery	Loaded	SG-Altiplano OLT Inventory (sn_sgc_altiplano_bomn_olt)	SG-Altiplano OLT ON Demand	2025-01-01 07:36:14	2024-12-31 23:36:14			IsartAnnamanglic
ISE000211	Specific on-demand discovery	Loaded	SG-Altiplano OLT Inventory (sn_sgc_altiplano_bomn_olt)	SG-Altiplano OLT ON Demand	2025-01-01 07:34:17	2024-12-31 23:34:18			IsartAnnamanglic
ISE000210	Specific on-demand discovery	Loading	SG-Altiplano OLT Inventory (sn_sgc_altiplano_bomn_olt)	SG-Altiplano OLT ON Demand	2025-01-01 07:33:08				IsartAnnamanglic
ISE000209	Specific on-demand discovery	Loading	SG-Altiplano OLT Inventory (sn_sgc_altiplano_bomn_olt)	SG-Altiplano OLT ON Demand	2025-01-01 07:32:14				IsartAnnamanglic

## Datenzuordnung

Daten aus Datenquellen in der Software „Nokia Altiplano“ werden zugeordnet und mithilfe der Robust Transform Engine (RTE) in ServiceNow-CMDB-Tabellen umgewandelt. Daten werden mithilfe der Identification and Reconciliation Engine (IRE) in die ServiceNow-CMDB eingefügt.

Wenn Sie das geführte Setup abschließen, können Sie die Integration so konfigurieren, dass regelmäßig Daten aus der SolarWinds-Software abgerufen werden.

Die Daten werden in Bereitstellungstabellen geladen und dann in die folgenden CMDB-Zieltabellen mit den folgenden Beziehungen eingefügt:

## Zuordnung von CMDB-CIs und CI-Beziehungen (physische Ebene)

CI	CI-Beziehungen
OLT-CI	<p>Das OLT-Gerät wird durch das OLT-CI dargestellt.</p> <p>Tabellenname: <b>cmdb_ci_Optical_line_terminal</b></p> <p>OLT-CI enthält Slot-CIs.</p>
ONT-CI	<p>Das ONT-Gerät wird durch das ONT-CI dargestellt.</p> <p>Tabellenname: <b>cmdb_ci_optische_netzwerk_terminal</b></p> <p>ONT-CI enthält Netzwerkschnittstellen-CIs.</p> <p>ONT-Netzwerkschnittstellen-CIs sind im ONT-CI enthalten.</p>
Slot-CI	<p>Gehäuse-Steckplätze werden durch das Steckplatz-CI dargestellt.</p> <p>Tabellenname: <b>cmdb_ci_container_slot</b></p> <p>Slot-CI ist im OLT-CI enthalten.</p> <p>Steckplatz-CI enthält das Schnittstellenkarten-CI (LT-/NT-Karten, Lüfter-/Netzteileneinheiten).</p>
Subslot-CI	<p>LT-/NT-Kartenträger werden durch das Subslot-CI dargestellt.</p> <p>Tabellenname: <b>cmdb_ci_container_subslot</b></p> <p>Subslot-CI ist im CI der OLT-LT-Karte enthalten.</p> <p>Subslot-CI ist im CI der OLT-NT-Karte enthalten.</p> <p>Subslot-CI enthält das Schnittstellenkarten-CI (Transceiver-Karten).</p>
Schnittstellenkarten-CI	<p>LT- und NT-Karten werden durch das Schnittstellenkarten-CI dargestellt.</p> <p>Transceiverkarten werden durch die Schnittstelle Card CI dargestellt.</p> <p>Lüfter und Netzteile werden durch die Schnittstellenkarte CI dargestellt. (CI für</p>

CIs	CI-Beziehungen
	<p>spezielle Karten, Lüfter und Netzteile kann in den nächsten Releases geändert werden).</p> <p>Tabellenname: <b>cmdb_ci_interface_card</b></p> <p>LT-Karte enthält die Subslots-CIs.</p> <p>Die NT-Karte enthält die Subslots-CIs.</p> <p>CIs von NT-Karten enthalten Netzwerkschnittstellen-CIs</p> <p>CIs für LT/NT-Transceiverkarten enthalten Netzwerkschnittstellen-CIs.</p> <p>LT/NT-Karten-CI ist im LT/NT-Steckplatz-CI enthalten.</p> <p>Das CI der LT-Transceiver-Karte ist im Subslot-CI (LT-Karte) enthalten.</p> <p>Das CI der NT-Transceiver-Karte ist im Subslot-CI (NT-Karte) enthalten.</p>
Netzwerkschnittstellen-CI	<p>PON-Zugriffsports der LT-Karte sowie Netzwerkports der NT-Karte werden durch das Netzwerkschnittstellen-CI dargestellt.</p> <p>Tabellenname: <b>cmdb_ci_ni_interface</b></p> <p>Netzwerkschnittstellen-CIs, die in den CIs von LT-Transceiver/NT-Transceiver/NT-Karten enthalten sind.</p> <p>Das ONT-Netzwerkschnittstellen-CI ist in ONT-CIs enthalten.</p>

Sie können die Anwendung **IntegrationHub ETL** verwenden, um Datenzuordnungen anzuzeigen und zu verwalten.

Weitere Informationen finden Sie unter [IntegrationHub ETL](#) .

### Unterstützte xNFs

- Lightspan MF-2 (OLT)
- Lightspan ISAM FX-4 (OLT)
- Lightspan XS-010X-Q (ONT)
- Lightspan XS-010X-R (ONT)

### Spezielle Systemeigenschaften

Service Graph Connector für Nokia Altiplano installiert spezielle Systemeigenschaften, die verschiedene Verhaltensweisen der Anwendung steuern.

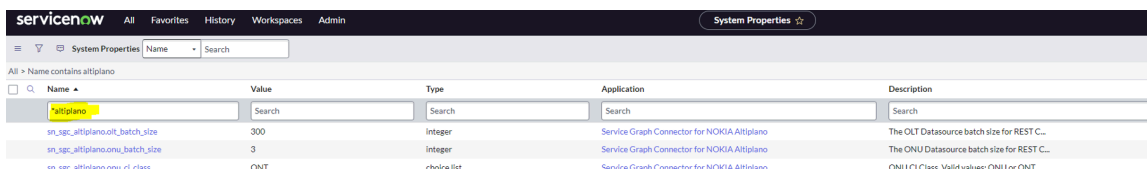
## Vorbereitungen

Erforderliche Rolle: Administrator

## Prozedur

Navigieren zu **Alle > Service Graph Connectors > Nokia Altiplano > Eigenschaften**.

Sie können auch auf diese Eigenschaften zugreifen, indem Sie `sys_properties.list` eingeben und nach dem Namen „\*altiplano“ filtern.



### Systemeigenschaften für SGC-Systeme von Nokia Altiplano

Eigenschaftsname	Empfohlener Wert/ Standardwert	Beschreibung
sn_sgc_altiplano.olt_batch_size	300	Die Batch-Größe der OLT-Datenquelle für REST-Aufrufe. Die Zahl stellt die Anzahl der Altiplano-Antwortentitäten dar. (Eine Erhöhung kann zu einem Fehler bei der Ausführung von REST-Aktionen führen.)
sn_sgc_altiplano.onu_batch_size	3	Batch-Größe der ONU-Datenquelle für REST-Aufrufe. Die Zahl stellt die Anzahl der ONU-Daten im Zusammenhang mit LT-Karten dar. (Eine Erhöhung kann zu einem Fehler bei der Ausführung von REST-Aktionen führen.)
sn_sgc_altiplano.onu_ci_class	ONT	ONU-CI-Klasse, gültige Werte: ONU oder ONT

### Beispiele für den Abruf von Daten aus dem Nokia Altiplano über die REST API

Beispiele für den Abruf von Daten aus dem Nokia Altiplano über die REST API.

### URL-Format

URL mit Versionsnummer: POST: `altiplano-indexsearch/latestcompleted-inv/_search`

### Example: Für OLT

```
{
  "_source": [
```

```

"deviceAVmetadata",
"inventorymetadata",
"inventorydata.ietf-hardware:hardware",
"inventorydata.ietf-hardware:hardware-state",
"inventorydata.nokia-state:state"
],
"sort": [{"_id": {"order": "asc"}}],
"from": 0,
"size": 300
}

```

### Example: Für ONU

```

{
  "query": {
    "bool": {
      "should": [
        {
          "exists": {
            "field":
"inventorydata.ietf-interfaces:interfaces-state.interface.bbf-xponvani:v-ani.onu-present-on-thi
s-olt.detected-serial-number"
          }
        }
      ]
    }
  },
  "_source": [
    "inventorydata.ietf-interfaces:interfaces-state.interface.bbf-xponvani:v-ani.onu-present-on-thi
s-olt.detected-serial-number",
    "inventorydata.bbf-fiber-onu-emulated-mount:onus.onu.root.ietf-hardware-mounted:hardware-
state",
    "inventorydata.bbf-fiber-onu-emulated-mount:onus.onu.name"
  ],
  "sort": [{"_id": {"order": "asc"}}],
  "from": 0,
  "size": 3
}

```

### Konfigurieren Sie Service Graph Connector für Nok Altiplano

In diesem Dokument wird erläutert, wie Sie Service Graph Connector für Nokia Altiplano mithilfe des geführten Setups konfigurieren, um Netzwerkressourcendaten vom Nokia Altiplano Access Controller (REST API) in die ServiceNow-CMDB zu integrieren. Sie enthält Schritte für Setup, Authentifizierung und Planung, um die genaue Integration von Netzwerkdaten zu bestätigen.

Zur Verwendung von Service Graph Connector für Google Altiplano benötigen Sie ein Abonnement für TSOM.

## 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](#).

## Abhängigkeiten und Anforderungen

- TSOM Visibility-Plugin (`sn_tsom_core`)
- Plugin „Discovery Core“ (`com.snc.discovery.core`), das automatisch von Discovery installiert wird.
- 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 [Request Discovery](#).

- Nur für Entwicklungsumgebung – IntegrationHub ETL (`sn_int_studio`).
- Nokia Altiplano Platform (Zugriff auf die zugehörige REST-API für den Nordübergang).

Erforderliche Rolle: admin

## Haftungsausschluss für die TSOM-Transparenz-Installation


Unter [Haftungsausschluss für die TSOM-Transparenz-Installation](#) finden Sie wichtige Informationen und Anforderungen für den Installationsprozess.

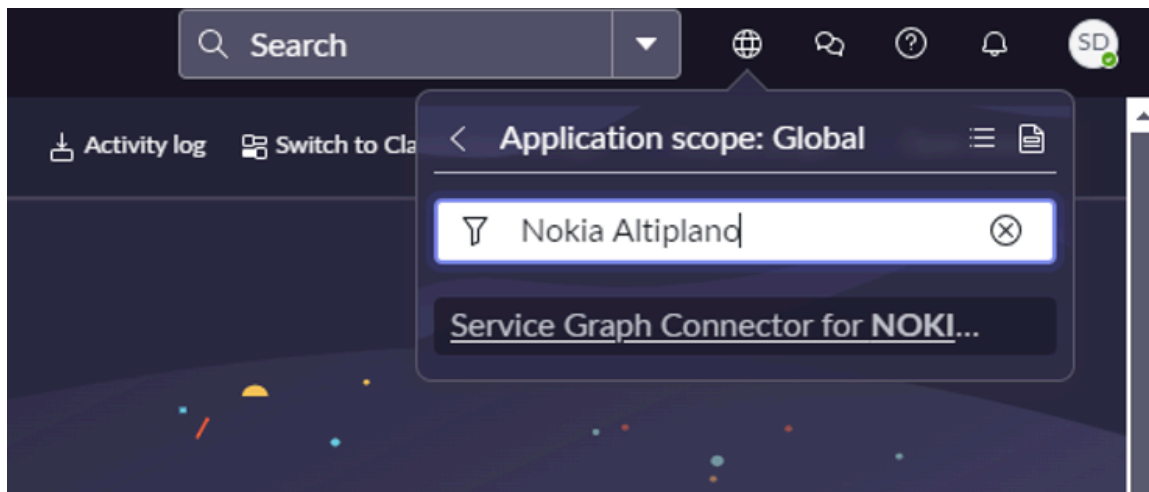
## Verfahren zur Ersteinrichtung

Dieses Verfahren gilt für die Ersteinrichtung des Nokia Altiplano.

## Vorbereitungen

Erforderliche Rolle: Administrator

Ändern Sie den Anwendungsbereich in „Service Graph Connector für Nokia Altiplano“, indem Sie  auswählen, nach „Nokia Altiplano“ suchen und den Eintrag auswählen.



## Prozedur

1. Navigieren zu **Alle > Service Graph Connectors > Nokia Altiplano > Setup.**
2. Wählen Sie auf der Seite „Erste Schritte “ **Erste Schritte** aus.
3. MID-Serverkonfigurieren:

- a. Wählen Sie **Konfigurieren**.
- b. Wenn ein MID-Server konfiguriert wurde, setzen Sie alle auf **Als abgeschlossen markieren**.

Weitere Informationen zur Installation und Konfiguration des MID-Servers finden Sie unter [Configuring MID Server](#) .

## 4. Konnektivität konfigurieren:

- a. Wählen Sie **Erste Schritte** aus.
- b. Konfigurieren Sie Aliasse für die Verbindungen und Anmeldeinformationen:
  - i. Wählen Sie **Konfigurieren**.
  - ii. Geben Sie im Feld Name den Namen der Geschäftspartner an.
  - iii. Behalten Sie für die restlichen Felder die Standardwerte bei, wählen Sie **Absenden** und dann **Als abgeschlossen markieren aus**.

The screenshot shows the 'Create Connection Aliases' form in ServiceNow. The 'Name' field is highlighted in yellow and contains the text 'yuri.altiplano.alias'. The form includes the following fields and options:

- Name:** yuri.altiplano.alias (highlighted)
- ID:** (empty)
- Application:** Service Graph Connector for NOKIA Altiplano
- Parent Alias:** (empty)
- Type:** Connection and Credential
- Connection type:** HTTP
- Support Multiple Active Connections:**
- Default Retry Policy:** Default HTTP Retry Policy
- Configuration Template:** (empty)
- Submit:** (button)

Dies ermöglicht die Verwendung der Verbindung nach Name und nicht direkt. Dadurch kann der Sammler alle aktiven Aliasse aus der CMDB extrahieren und die Datenerfassung über die daran gebundene HTTP-Verbindung starten.

- c. Erstellen Sie die Anmeldeinformationen für den Zugriff auf den Nokia Altiplano Controller:
  - i. Wählen Sie **Konfigurieren**.
  - ii. Geben Sie im Feld **Name** den Anwendernamen für Ihre Nokka Altiplano-Instanz an.
  - iii. Geben Sie im Feld **Passwort** Ihr Passwort für die Nokia Altiplano-Instanz an.


## **i** Hinweis:

Abhängig von den in Ihrer Nowak Altiplano-Instanz verwendeten Authentifizierungsmethoden sind möglicherweise andere Authentifizierungsfelder erforderlich. Standardmäßig verwenden wir [Basic authentication credentials](#) (als Teil des geführten Setups).

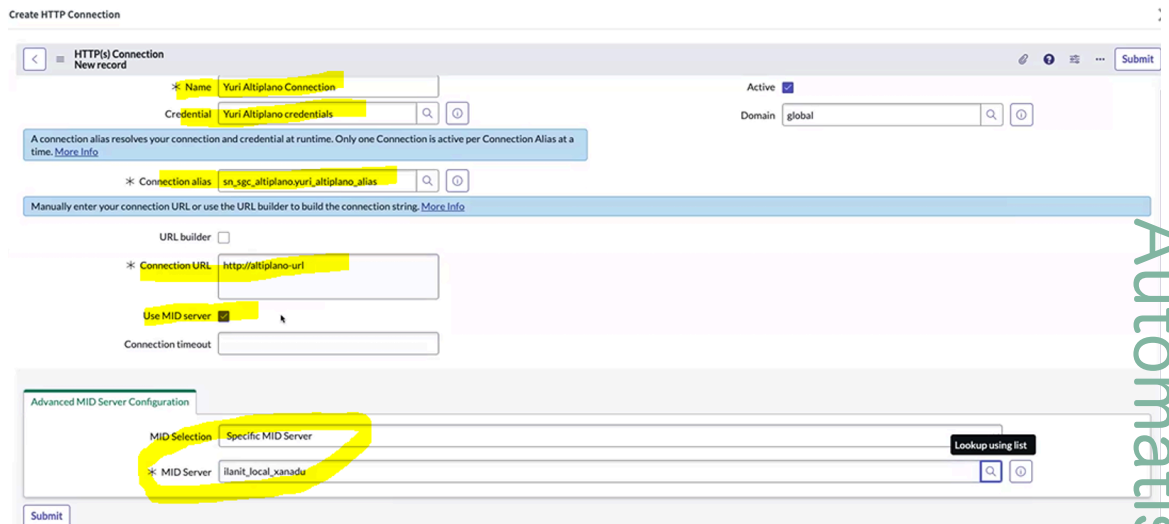
- iv.** Behalten Sie für die restlichen Felder die Standardwerte bei, wählen Sie **Absenden** und dann **Als abgeschlossen markieren aus**.

The screenshot shows the 'Basic Auth Credentials' form in ServiceNow. The 'Name' field is highlighted with a yellow circle and contains the text 'Nokia Altiplano Creds'. The 'User name' field contains 'Altiplano\_username' and the 'Password' field is masked with dots. The 'Order' field is set to '100'. Below the form is a blue informational banner and a 'Submit' button.

- d.** HTTP-Verbindung erstellen:

- i.** Wählen Sie **Konfigurieren**.
- ii.** Geben Sie im Feld **Name** den HTTP-Verbindungsnamen an.
- iii.** Wählen Sie im Feld **Anmeldeinformationen** das Lupensymbol aus, und wählen Sie die in Abschnitt 5.b definierten Anmeldeinformationen aus
- iv.** Wählen Sie im Feld **Verbindungsalias** das Symbol  aus, und wählen Sie die in Abschnitt 5.a definierten Verbindungspartner aus
- v.** Geben Sie im Feld „Verbindungs-URL“ die URL des Dokuments „Nokia Altiplano“ an.

- vi. Aktivieren Sie das Kontrollkästchen **MID-Server verwenden**, und wählen Sie den spezifischen MID-Server oder MID-Server-Cluster aus, von dem aus die Erkennung ausgeführt werden soll.
- vii. Behalten Sie für die restlichen Felder die Standardwerte bei, wählen Sie **Absenden** und dann **Als abgeschlossen markieren aus**.



## 5. Datensammlungszeitplan konfigurieren:

a. Wählen Sie **Erste Schritte** aus.

i. Wählen Sie **Konfigurieren**.

ii. Geben Sie im **Feld Name** den Planernamen an.

iii. Wählen Sie im Feld **Datenquelle** das Symbol  aus, und wählen Sie eine Datenquelle für die OLT-Erkennung aus:

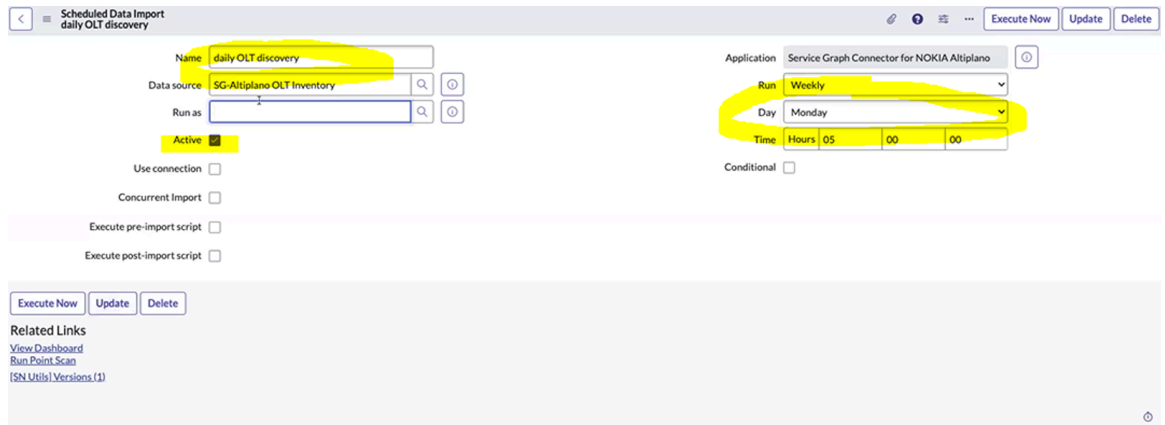
- **SG Altiplano OLT for All (SG Altiplano OLT für alle)**: Wählen Sie diese Option für alle Aliasse (Instanzen) von Nokia Altiplano aus.
- **SG Altiplano OLT [ALIAS\_NAME]**: Wählen Sie diese Option für den spezifischen Alias einer Altiplano-Instanz aus.

iv. Aktivieren Sie zum Aktivieren das Kontrollkästchen **Aktiv**.

Geben Sie an, wann dieser Zeitplan ausgeführt werden soll (täglich, wöchentlich, monatlich, regelmäßig, nach übergeordneter Ausführung, einmal).

v. Sie können es jetzt ausführen, indem Sie **Jetzt ausführen** auswählen.


vi. Behalten Sie für die restlichen Felder die Standardwerte bei, wählen Sie **Aktualisieren** und dann **Als abgeschlossen markieren aus**.



**b.** Datensammlung für ONU planen:

**i.** Wählen Sie **Konfigurieren**.

**ii.** Geben Sie im Feld **Name** den Planernamen an.

**iii.** Wählen Sie im Feld **Datenquelle**  aus, und wählen Sie eine Datenquelle für die ONU-Erkennung aus:

- **SG Altiplano ONU for All (SG Altiplano ONU für alle):** Wählen Sie diese Option für alle Aliasse (Instanzen) von Nokia Altiplano aus.
- **SG Altiplano ONU [ALIAS\_NAME]:** Wählen Sie diese Option für den spezifischen Alias einer Altiplano-Instanz aus.

**iv.** Aktivieren Sie zum Aktivieren das Kontrollkästchen **Aktiv**.

**i** **Hinweis:**

Geben Sie an, wann dieser Zeitplan ausgeführt werden soll (täglich, wöchentlich, monatlich, regelmäßig, nach übergeordneter Ausführung, einmal).

**v.** Sie können es jetzt ausführen, indem Sie **Jetzt ausführen** auswählen.

**vi.** Behalten Sie für die restlichen Felder die Standardwerte bei, klicken Sie auf **Aktualisieren** und dann auf **Als abgeschlossen markieren**.

**6.** Testen Sie die Verbindung mithilfe des zugehörigen Links **Testladen von 20 Datensätzen**.

Dieser Schritt testet die ausgewählte Datenquelle und bestätigt, dass die Daten in die Bereitstellungstabelle geladen werden. Eine erfolgreiche Verbindung zeigt an, dass die Verbindung mit der ausgewählten Datenquelle „Nokia Altiplano“ erfolgreich hergestellt wurde. Führen Sie diese Aktion für die Datenquellen „**SG-Altiplano OLT for all**“ und „**SG-Altiplano ONU for all**“ sowie für alle anderen von Ihnen erstellten Datenquellen aus.

**a.** Navigieren zu **Service Graph Connectors > Nokia Altiplano > Datenquellen**.

**7.** Wählen Sie die gewünschte Datenquelle aus.

**8.** Wählen Sie im Formular „Datenquelle“ unter „Zugehörige Links“ die Option **Testladen von 20 Datensätzen** aus.

9. Warten Sie, bis das Testergebnis „Abgeschlossen“ mit dem Abschlusscode „Erfolg“ lautet.

Progress	
Name	ImportProcessor
State	Complete
Completion code	Success
Message	Processed: 4, inserts 4, updates 0, errors 0, empty and ignored 0, ignored errors 0 (0:00:04.720)

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: sn\_sgc\_altiplano\_tsom\_olt
- [Run Robust Transform](#) Transform a loaded import set using a robust transform
- [Import log](#) View the import log

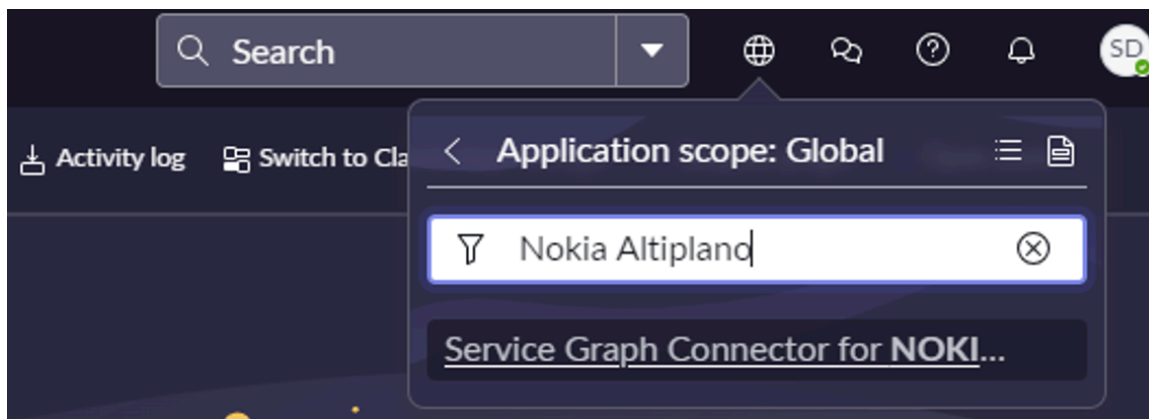
**Mehrinstanz-Setup**

Zweite Instanz eines Mobiltelefons und nachfolgende Instanzen hinzufügen.

**Vorbereitungen**

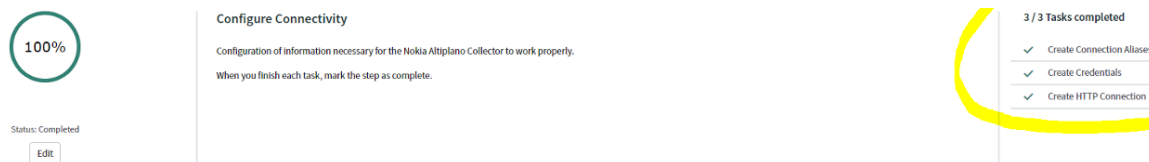
Erforderliche Rolle: Administrator

Ändern Sie den Anwendungsbereich in „Service Graph Connector fürNokia Altiplano“, indem Sie das Symbol  wählen, nach „Nokia Altiplano“ suchen und auswählen.



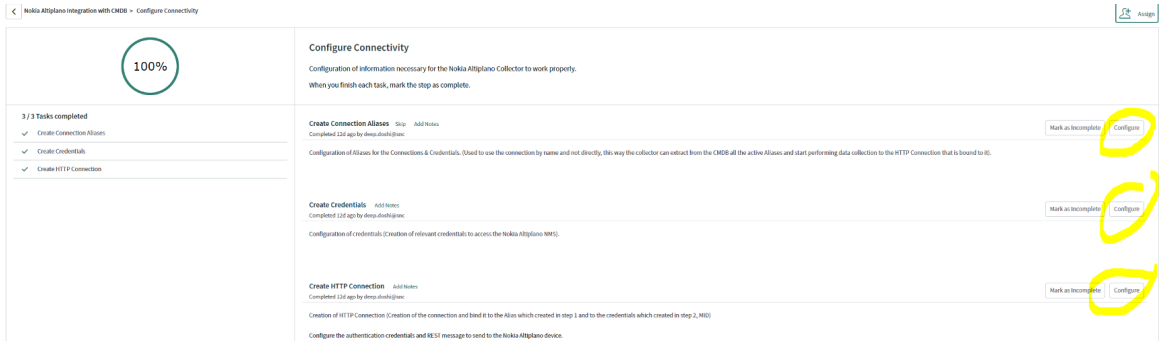
**Prozedur**

1. Navigieren zu **Alle > Service Graph Connectors > Nokia Altiplano > Setup.**
2. Wählen Sie auf der Seite „Erste Schritte “ **Erste Schritte** aus.  
Wiederholen Sie alle Schritte im Abschnitt Konfigurierte Konnektivität. Erstellt Konfigurationseinträge für die neue Instanz vonNokia Altiplano.



3. Wählen Sie **Verbindungsalias erstellen aus.**

4. Konfigurieren Sie „Verbindungsalias erstellen“, „Anmeldeinformationen erstellen“ und „HTTP-Verbindung erstellen“.

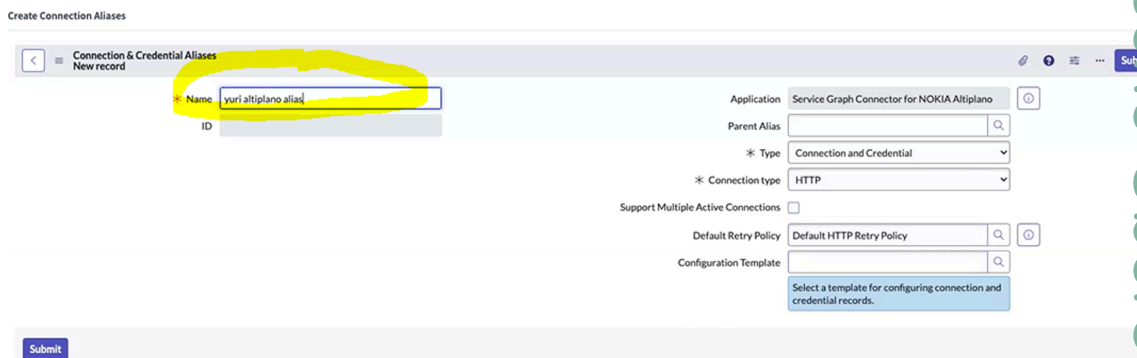


a. Konfigurieren Sie Aliasse für die Verbindungen und Anmeldeinformationen:

i. Wählen Sie **Konfigurieren**.

ii. Geben Sie im Feld **Name** den Namen der Geschäftspartner an.

iii. Behalten Sie für die restlichen Felder die Standardwerte bei, wählen Sie **Absenden** und dann **Als abgeschlossen markieren aus**.



Dies ermöglicht die Verwendung der Verbindung nach Name und nicht direkt. Dadurch kann der Sammler alle aktiven Aliasse aus der CMDB extrahieren und die Datenerfassung über die daran gebundene HTTP-Verbindung starten.

b. Erstellen Sie die relevanten Anmeldeinformationen für den Zugriff auf den Nokia Altiaplano Controller:

i. Wählen Sie **Konfigurieren**.

ii. Geben Sie im Feld **Name** den Anwendernamen für Ihre Nokka Altiaplano-Instanz an.

iii. Geben Sie im Feld **Passwort** Ihr Passwort für die Nokia Altiaplano-Instanz an.

**Hinweis:**

Abhängig von den in Ihrer Nowak Altiaplano-Instanz verwendeten Authentifizierungsmethoden sind möglicherweise andere Authentifizierungsfelder erforderlich.

iv. Behalten Sie für die restlichen Felder die Standardwerte bei, wählen Sie **Absenden** und dann **Als abgeschlossen markieren aus**.


Automatische Übersetzung

c. HTTP-Verbindung erstellen:

i. Wählen Sie **Konfigurieren**.

ii. Geben Sie im Feld **Name** den HTTP-Verbindungsnamen an.

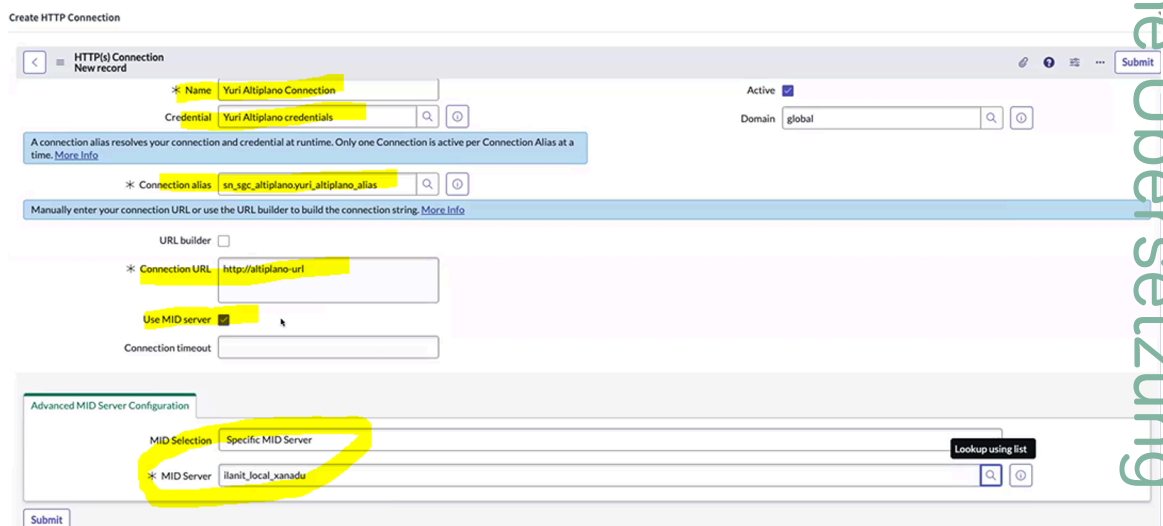
iii. Wählen Sie im Feld **Anmeldeinformationen** das Symbol  aus, und wählen Sie die in Abschnitt 5.b definierten Anmeldeinformationen aus

iv. Klicken Sie im Feld **Verbindungsalias** auf das Symbol , und wählen Sie die verbündeten Verbindungen aus.

v. Geben Sie im Feld „**Verbindungs-URL**“ die URL des Dokuments „Nokia Altiplano“ an.

vi. Aktivieren Sie das Kontrollkästchen **MID-Server verwenden**, und wählen Sie den spezifischen MID-Server oder MID-Server-Cluster aus, von dem aus die Discovery ausgeführt werden soll.

vii. Behalten Sie für die restlichen Felder die Standardwerte bei, wählen Sie **Absenden** und dann **Als abgeschlossen markieren** aus.



5. Testen Sie die Verbindung mithilfe des zugehörigen Links **Testladen von 20 Datensätzen**.

## Identifizierung und Abgleich von Telekommunikationsdiskrepanzen

Die Identifizierung und der Abgleich von Telekommunikationsdiskrepanzen bestätigt, dass die CMDB/TNI von ServiceNow den aktualisierten Status des Netzwerks genau wiedergibt und mit den geplanten oder entworfenen Bestandsressourcen synchronisiert bleibt.

Es vergleicht Netzwerkdaten kontinuierlich mit CMDB/TNI-CI-Datensätzen im Rahmen von Audits, identifiziert und behebt Diskrepanzen, um die Ausrichtung zwischen beiden

aufrechtzuerhalten. Dieser Prozess ist wichtig, um die Datenintegrität zu bestätigen, Inkonsistenzen zu vermeiden und die Synchronisierung von CMDB/TNI mit der tatsächlichen Netzwerkbereitstellung aufrechtzuerhalten.

Die Pflege zuverlässiger und genauer Daten in Ihrer CMDB/TNI ist eine wichtige Voraussetzung für eine nahtlose Auftrags- und Serviceerfüllung, Assurance, Sicherheit und Asset-Verwaltung. Diese Fähigkeit ist eine der wichtigsten Voraussetzungen für die Automatisierung und stimmt mit dem TM Forum Autonomous Network Operations-Framework (NO) überein.

## Identifizierung und Abgleich von Telekommunikationsdiskrepanzlichenzenzen

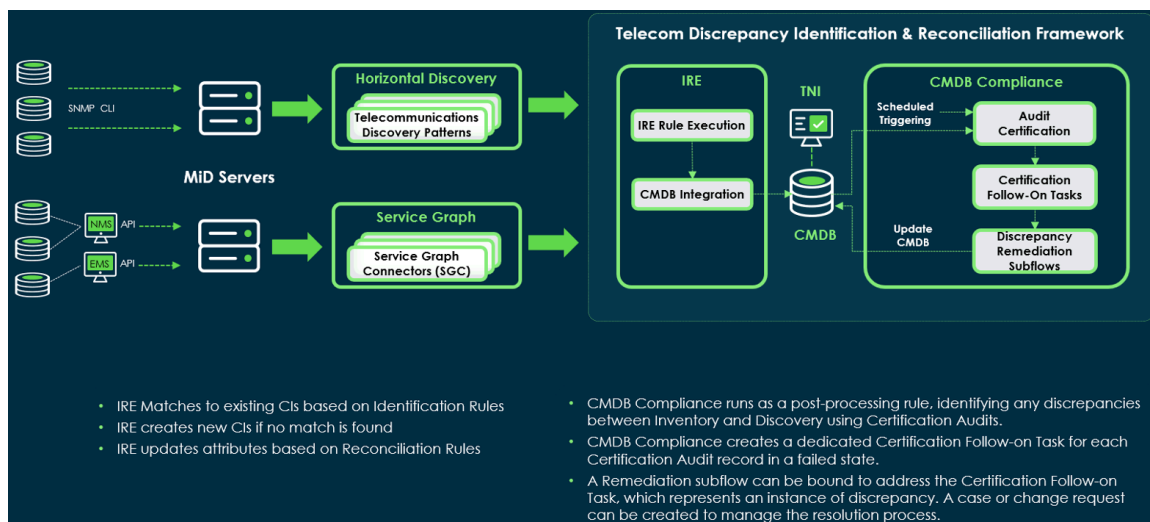
Die Now Platform verwendet ein Lizenzierungsmodell, bei dem Ihrer Organisation die Nutzung von TSOM-Transparenz-Anwendungen in Rechnung gestellt wird. Telecom-Discovery, Telecom-Diskrepanz-Identifizierung und -Abgleich und TSOM-Transparenz (Plugin) sind Komponenten von TSOM-Transparenz. Um die TSOM-Transparenz zu verwenden, muss Ihre Organisation TSOM abonnieren. Beachten Sie, dass die Produktdokumentation von ServiceNow keine Details zu Preisen, Verpackungen oder anderen Besonderheiten enthält, da diese durch den Kundenvertrag Ihres Unternehmens festgelegt werden.

## Erkunden der Identifizierung und des Abgleichs von Telekommunikationsdiskrepanzen

Die Lösung zur Identifizierung und Abgleich von Telekommunikations-Diskrepanzen wurde entwickelt, um die Genauigkeit und Konsistenz von Netzwerkressourcendaten zwischen Netzwerksystemen und Bestandsverwaltungsdatenbanken wie CMDB/TNI zu bestätigen.

Die Identifizierung und der Abgleich von Telekommunikationsdiskrepanzen nutzt Telekommunikations-Discovery und die Fähigkeiten der Plattform, um ihre Funktionen auszuführen.

## Telecom-Diskrepanzidentifizierung und -abgleich – Übersicht



## TSOM Visibility-Plugin

Die Logik für die Identifizierung und den Abgleich von Telekommunikations-Diskrepanzen ist eine Komponente des Plugins „TSOM Visibility“ (sn\_tsom\_core). Dieses Plugin umfasst gemeinsam genutzte Logik, die für die Prozesse Telecom Discovery und Telecom Diskrepanz Identifizierung und Abgleich unerlässlich ist. Sie enthält für die Telekommunikation spezifische Funktionen zur Erkennung und Korrektur von Diskrepanzen sowie andere

grundlegende Logik zur Unterstützung aktueller und zukünftiger Funktionalitäten von Telekommunikationsanwendungen.

## Identification and Reconciliation Engine (IRE)

IRE bietet ein zentralisiertes Framework zum Identifizieren und Abgleichen von Daten aus mehreren Quellen. Bestätigt die Integrität der CMDB und einiger Nicht-CMDB-Tabellen, wenn verschiedene Datenquellen zum Erstellen oder Aktualisieren von CI-Datensätzen verwendet werden.

- IRE gleicht vorhandene CIs basierend auf Identifizierungsregeln ab.
- IRE erstellt CIs, wenn keine Übereinstimmung gefunden wird.
- IRE-Aktualisierungen werden basierend auf den Abgleichsregeln zugeordnet.


Weitere Informationen finden Sie unter [CMDB Identification and Reconciliation \(IRE\)](#) .

## CMDB-Compliance und Identifizierung und Abgleich von Telekommunikations-Diskrepanzen

CMDB-Compliance ist ein Toolset, mit dem Administratoren CMDB-Daten auf Richtigkeit prüfen und Diskrepanzen identifizieren können, die bei Compliance-Audits erkannt wurden. Es kann auch automatisch Folgeaufgaben für fehlgeschlagene Audit-Datensätze generieren und zuweisen, die als Aufgaben zum Auslösen eines geeigneten Nachbesserungs-Subflows dienen, um Diskrepanzen zu korrigieren. CMDB-Compliance-Audits bilden die Grundlage für die Identifizierung und den Abgleich von Telekommunikations-Diskrepanzen.

- CMDB-Compliance führt Audits als Nachverarbeitungsregel durch, um Anomalien (Diskrepanzen) in der CMDB zu identifizieren.
- CMDB-Compliance erstellt für jeden Audit-Datensatz in einem fehlgeschlagenen Status eine Folgeaufgabe (der fehlgeschlagene Status ist das Ergebnis einer Audit-Ermittlung einer Anomalie oder Diskrepanz in der CMDB). Für jede Folgeaufgabe kann ein Nachbesserungs-Flow entworfen und ausgelöst werden, um die Diskrepanz zu beheben.

Die Logik für Telecom Diskrepancy Identification & Reconciliation sowie die Beispiel-Nachbesserungs-Subflows sind im Yokohama-Release enthalten und werden automatisch mit dem Plugin „TSOM Visibility“ installiert.

Weitere Informationen zum allgemeinen CMDB-Compliance-Toolset finden Sie unter [CMDB Compliance](#) .

## Szenarien der Diskrepanz-Identifizierung (mit Zertifizierungsaudits)


Es gibt zwei Hauptdiskrepanzkategorien, die zwischen Bestand (CMDB) und Discovery erkannt werden können und im Folgenden beschrieben werden:

- Entitäten, die im Bestand, aber nicht im Netzwerk vorhanden sind.
- Entitäten, die sowohl im Netzwerk als auch im Bestand vorhanden sind, sich jedoch in ihrer Hierarchie unterscheiden.

Die Diskrepanzidentifizierung in TSOM Visibility basiert auf der Verwendung von CMDB-Compliance (Zertifizierungsaudits) und wurde durch Hinzufügen einer spezifischen Logik erweitert, die Modellbeziehungen und Informationen verwendet, um Nichtübereinstimmungen zu identifizieren.

**i Hinweis:**

Der Schwerpunkt des aktuellen Release liegt auf der Identifizierung und dem Abgleich von Diskrepanzen auf Ebene physischer Ressourcen. Im anstehenden Release wird diese Funktionalität um Unterstützung für die logische Ressourcenebene und Attribute erweitert.

Weitere Informationen zur allgemeinen Funktion „Zertifizierungsaudits“ finden Sie unter [Certification audits](#) .

## Folgaufgabentypen, die für fehlgeschlagene Audit-Ergebnisdatensätze erstellt wurden

Die folgenden Diskrepanztypen (Audit-Ergebnisse) sind für übergeordnete CIs und untergeordnete CIs für jeden Beziehungsdatensatz in der CI-Beziehungstabelle (cmdb\_rel\_ci) zu finden, die den Bedingungen entsprechen, und die folgenden Folgeaufgaben können für jedes der fehlgeschlagenen Audits erstellt werden Ergebnisse:

1. Das neueste Discovery-Datum ist nicht festgelegt – wird generiert, wenn das Feld „Neuestes Discovery-Datum“ im CI fehlt.
2. Das neueste Discovery-Datum, das nicht innerhalb des konfigurierten Schwellenwerts liegt. Wird generiert, wenn die Differenz im Feld „Neuestes Discovery-Datum“ zwischen einem übergeordneten CI und einem untergeordneten CI mehr als 2,5 Tage beträgt.

Standardmäßig ist sie in der Systemeigenschaft `sn_tsom_core.discovered_date.diff.threshold.in.days` auf 2,5 Tage festgelegt und kann geändert werden.

3. CI-Modell nicht gefunden (Feld „Modell-ID“ nicht festgelegt oder Daten ungültig). Wird generiert, wenn kein entsprechendes CI-Modell gefunden wird. Wenn kein CI-Modell gefunden wird, sind die nächsten Validierungen (4–6) irrelevant, da sie auf CI-Modellen basieren. Falls ein CI-Modell gefunden wird, wird das Audit mit den nächsten Validierungen (4–6) fortgesetzt.
4. Diskrepanz bei belegten Steckplätzen: Wird generiert, wenn eine Karte eine falsche Anzahl von Steckplätzen belegt.
5. Modellbeziehungen nicht definiert – nur relevant, wenn TNI installiert ist. Wird generiert, wenn das Audit keine Beziehung zwischen übergeordneten und untergeordneten CI-Modellen in der Tabelle „Netzwerkmodellbeziehungen“ finden kann.
6. Falsche Anzahl von Beziehungen – nur relevant, wenn TNI installiert ist. Wird generiert, wenn beim Audit festgestellt wird, dass die Anzahl der erkannten untergeordneten CI-Datensätze die maximale Anzahl des entsprechenden übergeordneten CI-Datensatzes im Feld **Anzahl** der Modellbeziehung in der Beziehungstabelle des Netzwerkmodells überschreitet.

Weitere Informationen zur allgemeinen Funktion Folgeaufgaben finden Sie unter Subflows erstellen.

## Subflows zur Diskrepanzkorrektur

Sobald bei einem Audit eine Diskrepanz erkannt wird, wird dies als Folgeaufgabe protokolliert. Mit dem System können Benutzer einen Subflow für bestimmte Diskrepanzscenarien definieren, um zwischen verschiedenen Arten von Diskrepanzen zu unterscheiden und anwenderdefinierte Flows zu deren Behebung zu erstellen.

Weitere Informationen zum Erstellen von Subflows finden Sie unter [Building subflows](#) .

## Verwendungsbeispiel

Im Folgenden finden Sie ein Beispiel für ein bestimmtes Szenario zur Verwendung von Identifizierung und Abgleich von Telekommunikationsdiskrepanz:

Angenommen, ein Gerät wurde ursprünglich mit einer Karte (Card40) im Steckplatz (Slot40) erkannt. Im Laufe der Zeit wurde ein Problem mit Card40 identifiziert, und sie wurde durch Card41 ersetzt. Der Bestand (CMDB) enthält jedoch noch ein Card40-CI, während es im Netzwerk durch Card41 ersetzt wurde. Wenn der nächste Discovery-Auftrag ausgeführt wird, wird das Card41-CI erkannt und der CMDB im selben Slot (Slot40) hinzugefügt. Daher befinden sich zwei CIs (das alte – Card40 – und das neu erkannte – Card41) im selben Slot40.

Der Audit identifiziert diese Diskrepanz, erstellt eine Folgeaufgabe und ermöglicht einem Benutzer die Nachbesserung. (beheben Sie diese Diskrepanz, und nehmen Sie Card40 außer Betrieb).

Wenn das CMDB-Compliance-Audit für den Servicebetrieb ausgeführt wird, identifiziert es diese Diskrepanz und erstellt einen Audit-Datensatz mit dem Status „Fehlgeschlagen“ (in unserem Beispiel AUDR0001283).

1. Navigieren **Alle > Compliance > Audits > .**
2. Wählen Sie **Service Operations-CMDB Compliance-Audit aus.**
3. Wählen Sie **Audits ausführen aus,** um das Audit auszuführen.

Für jeden fehlgeschlagenen Audit-Datensatz wird automatisch eine Folgeaufgabe erstellt (in unserem Beispiel TASK0020215).

Created	Document	State	Column name	Desired value	Discrepancy value	Follow on task	Number	Template	Threshold	Stability
2024-11-26 04:34:33	Configuration Item: Card40	Failed	Most recent discovered date	Is not within threshold 2024-11-25 00:59:44	2024-11-22 00:59:45	TASK0020215	AUDR0001283	(empty)	Pending	Pending

4. Wählen Sie **TASK0020215** aus.

Die Folgeaufgabe enthält eine detaillierte Beschreibung der Diskrepanz. Wie Sie in der Beschreibung sehen können, weist das Card40-CI eine Diskrepanz auf.

**Hinweis:**

Dies ist ein Beispiel für die TASK0020215-Beschreibung, die für das Szenario „Ungültige Anzahl von Beziehungen“ erstellt wurde. Andere Szenarien und Umgebungen haben möglicherweise andere Beschreibungen.

Card40 wurde zuletzt vor mehr als 2,5 Tagen erkannt.

Beziehungen zwischen den folgenden CIs:

CI	Modell
Steckplatz40 (8b2beb4247ceda10f04f83ac416d4398)	DEMO 20532Baum (1ba577524c1b3110f8772646dabeb9bb)
Karte40 (0b2beb4247ceda10f04f83ac416d4399)	NOKIA 7360 FANT-F KARTENMODUL (3af9617de5928110f877657a333391e0)
Karte41 (832beb4247ceda10f04f83ac416d439a)	

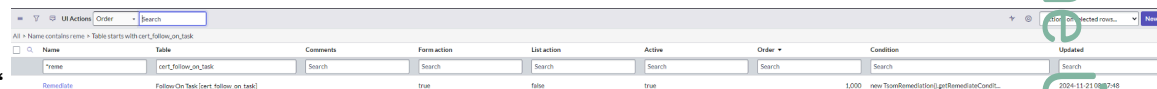
5. Wählen Sie zur Nachbesserung die Schaltfläche **Nachbessern**.

6. Hinweis: „Nachbessern“ ist eine UI-Aktion, auf die folgendermaßen zugegriffen werden kann:

7. **Alle > Systemdefinition > UI-Aktionen.**

8. Öffnen Sie die **zu beobachtende** UI-Aktion

„Nachbessern“.



Weitere Informationen zu UI-Aktionen finden Sie unter [Defining UI actions](#).

In diesem Beispiel ruft die UI-Aktion „Nachbessern“ (ausgelöst durch **Nachbessern**) den Subflow „TSOM CI-Außerbetriebnahme ausführen“ auf, um die in der Folgeaufgabe TASK0020215 angegebene Diskrepanz zu beheben und zu beheben. Außerdem müssen Sie eine alte Card40 außer Betrieb nehmen, die automatisch durch Aufrufen des Subflows „TSOM Decommission Card“ ausgeführt wird.

Sobald die Remediation erfolgreich abgeschlossen wurde, werden im Fenster „Folgeaufgabe“ (TASK0020215) Arbeitsnotizen mit den Remediationsergebnissen generiert.

Wie Sie in den Arbeitsnotizen sehen können, haben wir Card40 erfolgreich stillgelegt und die Beziehung Slot40 → Slot40 entfernt. Die Diskrepanz wurde erfolgreich behoben, und die CMDB-CI-Datensätze werden jetzt mit dem Netzwerkstatus synchronisiert.

SM Service-now: Yaron Nechushtan [maint...]

Work notes • 2024-11-26 04:37:39

TSOM CI Decommission  
 =====  
 Card: Card40

LCS set to 'End of life'  
 LCSS set to 'Retired'

Relationships removed:  
 Slot40 ==> Card40

SA System Administrator

Field Changes • 2024-11-26 04:34:33

Description Card40 was last discovered more than 2.5 days ago.  
 Relationships between the following CIs:  
 CI: Slot40 (8b2beb4247ceda10f04f83ac416d4398), Model: DEMO 20532Tree (1ba577524c1b3110f8772646dabeb9bb),  
 CI: Card40 (0b2beb4247ceda10f04f83ac416d4399), Model: Nokia 7360 FANT-F CARD MODULE  
 (3af9617de5928110f877657a333391e0),  
 CI: Card41 (832beb4247ceda10f04f83ac416d439a), Model: ()

SA System Administrator

Field Changes • 2024-11-26 04:34:32

Active true  
 Audit Service.Operation CMDB Compliance Audit  
 Configuration item Card40  
 Impact 3 - Low  
 Number TASK0020215  
 Opened by System Administrator  
 Priority 4 - Low  
 Short description Most recent discovery date not within configured threshold.  
 State Open

Dieser Beispiel-Subflow ist im Lieferumfang der Lösung enthalten. Benutzer können mit Flow Designer anwenderdefinierte Nachbesserungs-Subflows definieren.

### Systemeigenschaften, die sich auf die Identifizierung und den Abgleich von Telekommunikations-Diskrepanzen auswirken

Diese Systemeigenschaften sind Teil des Plugins „TSOM Visibility“ (sn\_tsom\_core) und steuern das Protokoll zur Identifizierung und Abgleich von Telekommunikations-Diskrepanzen (TSOM-CMDB-Audit). Das TSOM Visibility-Plugin dient als Befähiger für die TSOM Visibility-Anwendungen, die eine Logik enthalten, die von der Lösung Telecom Discovery und Telecom Diskrepanz Identifizierung und Abgleich gemeinsam genutzt wird.

### TSOM-Transparenz-Systemeigenschaften (Auswirkungen CMDB-Audit)

Eigenchaftsname	Empfohlener Wert/Standardwert	Beschreibung
<code>sn_tsom_core.audit.interface_card_tables</code>	cmdb_ci_interface_card	Wenig (d. h. Schnelligkeit TSOM-Diskrepanz-Abgleich)
<code>sn_tsom_core.audit.discovery_sources</code>	SG-Altiplano, ServiceNow	Das Audit-Diskrepanz-abgleich-Datensatz-Quelle oder Discovery-Zusätzliche Konfigurationen Versuchen
<code>sn_tsom_core.audit.relationship_types</code>	Enthält::Enthalten in	Das Audit-Diskrepanz-Abgleich-Diskrepanz

Automatische Übersetzung

**TSOM-Transparenz-Systemeigenschaften (Auswirkungen CMDB-Audit) (Fortsetzung)**

Eigenschaftsname	Empfohlener Wert/Standardwert	Beschreibung
		Beziehungs- Beziehungs- in“.
<code>sn_tsom_core.audit.slot_tables</code>	cmdb_ci_container_slot	Wert (d. h. Slot- CMD und A Disk
<code>sn_tsom_core.audit.log.level</code>	Info	Das (Idee Abg Disk der Prot <b>info</b>  Hinv Prot die l
<code>sn_tsom_core.audit.subslot_tables</code>	cmdb_ci_container_subslot	Wert ist (d die S vom (Idee Tele veran
<code>sn_tsom_core.audit.interface_tables</code>	cmdb_ci_ni_interface	Wert ist (d die S vom (Idee Tele veran
<code>sn_tsom_core.audit.equipment_tables</code>	<ul style="list-style-type: none"> <li>cmdb_ci_ni_telco_equipment</li> <li>cmdb_ci_ip_switch</li> <li>cmdb_ci_ip_router</li> </ul>	Wert ist (d die A vom (Idee Tele veran
<code>sn_tsom_core.audit.discovered_date.diff.threshold.in.days</code>	2,5	Das (Idee von 7 Disk Date Disc der S

Automatische Übersetzung

**TSOM-Transparenz-Systemeigenschaften (Auswirkungen CMDB-Audit) (Fortsetzung)**

Eigenschaftsname	Empfohlener Wert/Standardwert	Beschreibung
<code>sn_tsom_core.audit.max_number_of_records_to_process</code>	100000	Das (Idee) von ist f von Bezi fest 

Automatische Übersetzung

**Konfigurieren Sie den Abgleich**

Weitere Informationen finden Sie unter [Telekommunikations-Diskrepanzidentifizierung und -abgleich konfigurieren](#).

**Telekommunikations-Diskrepanzidentifizierung und -abgleich konfigurieren**

Dieser Leitfaden beschreibt die Schritte zum Konfigurieren der Identifizierung und des Abgleichs von Telekommunikationsdiskrepanzen (Teil von TSOM-Transparenz), um die genaue Erkennung und Behebung von Diskrepanzen in Telekommunikationsnetzwerkressourcen in Ihrer ServiceNow-CMDB-/TNI-Instanz zu bestätigen.

**Vorbereitungen**

Zur Verwendung von Telecom Diskrepancy Identification & Reconciliation benötigen Sie ein Abonnement für TSOM.

Erforderliche Rolle: Administrator

**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](#).

**Abhängigkeiten und Anforderungen**

Abhängigkeiten des TSOM-Transparenz-Plugins:

- CMDB-CI-Klassenmodelle für Telecom Service Operations Core (sn\_tsom\_core) (App-ID: sn\_cmdb\_ci\_class, Typ: Store)
- Anwendung „Erweitertes Modell und Assetklassen“ (App-ID: sn\_ent, Typ: Store)
- Sichtbarkeitsinhalt (App-ID: sn\_pattern\_design, Typ: Store)
- Integration Common for CMDB (App-ID: sn\_cmdb\_int\_util, Typ: Store)
- Installationsprogramm für ServiceNow IntegrationHub Starter Pack (Plugin-ID: com.glide.hub.integration, Typ: Familie)

Discovery Core (com.snc.discovery.core), das automatisch von Discovery installiert wird.  
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 [Request Discovery](#) .

## Installation

Das TSOM Visibility-Plugin (sn\_tsom\_core) wird automatisch mit Telecommunications Discovery Patterns (sn\_tsom\_patterns) oder mit dem Nokia Altiplano Service Graph Connector (sn\_sgc\_altiplano\_connector) installiert. Alle Logik- und Systemeigenschaften sind in Ihrer ServiceNow-Instanz installiert.

Informationen zur Installation des Plugins „TSOM Visibility“ finden Sie unter [Konfigurieren Sie TSOM-Muster \(Telecommunications Discovery-Muster\)](#). oder [Konfigurieren Sie Service Graph Connector für Nok Altiplano](#).

## Haftungsausschluss für die TSOM-Transparenz-Installation

Unter [Haftungsausschluss für die TSOM-Transparenz-Installation](#) finden Sie wichtige Informationen und Anforderungen für den Installationsprozess.

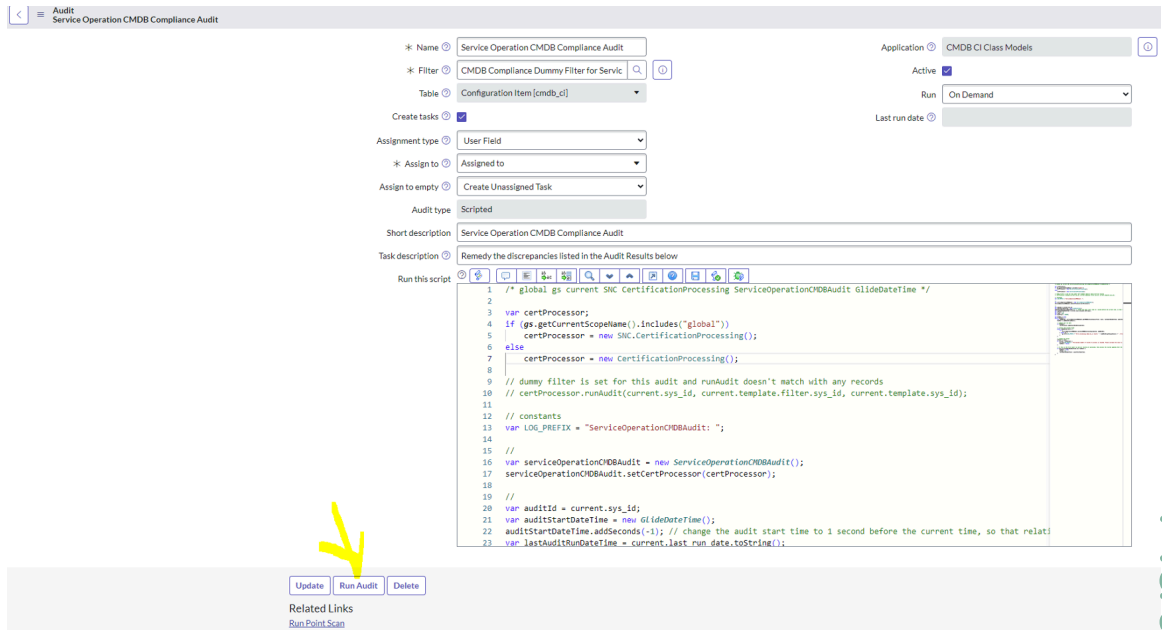
## Ausführung

Die Lösung zur Identifizierung und zum Abgleich von Telekommunikationsdiskrepanzen basiert auf CMDB-Integrität/Compliance, die Zertifizierungsaudits für ausgewählte Tabellen und Datensätze in der CMDB ausführt. Es wird unabhängig von Discovery ausgeführt und kann bei Bedarf oder geplant ausgeführt werden.

Weitere Informationen zur CMDB-Compliance finden Sie unter [CMDB Compliance](#) und [Certification audits](#) .

## Prozedur

1. Navigieren zu **Alle > Compliance > Audits > Audit der CMDB-Compliance für den Servicebetrieb (Tabelle „cert\_audit“)**.
2. Wählen Sie **Audit ausführen aus**.



Es führt verschiedene Skripts und Vorgänge aus.

### Audit-Logiken für Zertifizierung

Audit-Ergebnisse werden für jedes Audit erstellt, das für Datensätze ausgeführt wird, die der Auswahl entsprechen (siehe Übereinstimmungsbedingungen unter Audit-Ausführung der Erstzertifizierung).

Der Status des Ergebnisses kann „Zertifiziert“ oder „Fehlgeschlagen“ sein. Für jeden Audit-Ergebnisdatensatz mit dem Status „Fehlgeschlagen“ wird eine Folgeaufgabe erstellt.

### Audit-Ausführung der Erstzertifizierung

Bestimmte CMDB-Tabellen werden auf Anomalien validiert

Das CMDB-Compliance-Audit für den Servicebetrieb wird für die CI-Beziehungstabelle (cmdb\_rel\_ci) gestartet, jedoch nur für bestimmte Datensätze mit übereinstimmenden Bedingungen:

- Übergeordnete UND untergeordnete CI-Klassen sind unterstützte Klassen, einschließlich erweiterter Tabellen:

Slot (cmdb\_ci\_container\_slot), Subslot (cmdb\_ci\_container\_subslot), Karte (cmdb\_ci\_interface\_card), Schnittstelle (cmdb\_ci\_ni\_interface), Telekommunikationsgerät (cmdb\_ci\_ni\_telco\_equipment), IP-Switch (cmdb\_ci\_ip\_Switch) und IP-Router (cmdb\_ci\_ip\_router).

**i Hinweis:**

Diese Eigenschaften können über die Systemeigenschaften sn\_tsom\_core.audit.\* konfiguriert werden.

- Übergeordnetes ODER untergeordnetes Element wird von Discovery (discovery\_source = SG-Altiplano, ServiceNow) erstellt oder aktualisiert.

**i Hinweis:**

Diese Eigenschaft kann in der Systemeigenschaft sn\_tsom\_core.audit.discovery\_sources konfiguriert werden.

- Übergeordnete UND untergeordnete Lebenszyklusphase ist „Operativ“.
- Der CI-Beziehungstyp ist „Contains::Contained By“.

** Hinweis:**

Diese Eigenschaft kann in der Systemeigenschaft `sn_tsom_core.audit.relationship_types` konfiguriert werden.

## Nachfolgende Zertifizierungsaudit-Ausführungen

Verfolgt die gleiche Logik wie der Auditlauf der Erstzertifizierung, jedoch mit den folgenden zusätzlichen übereinstimmenden Auswahlkriterien:

Der Zeitstempel im Feld „Aktualisiert“ in der CI-Beziehungstabelle oder der Zeitstempel im Feld „Aktualisiert“ eines übergeordneten CI oder der Zeitstempel im Feld „Aktualisiert“ von untergeordneten CIs ist später als der Zeitstempel im Feld „Letztes Ausführungsdatum“ im Service Audit der CMDB-Compliance des Vorgangs (dies bedeutet, dass seit dem letzten Audit ein Change aufgetreten ist).