# Konfigurieren von SNMP in der ACI

## Inhalt



# Einleitung

In diesem Dokument wird die Konfiguration des Simple Network Management Protocol (SNMP) und der SNMP-Traps in der ACI beschrieben.

# Voraussetzungen

## Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Fabric-Erkennung abgeschlossen
- In-Band-/Out-of-Band-Verbindungen zu Ihrem Application Policy Infrastructure Controller (APIC) und den Fabric-Switches

- Für SNMP-Datenverkehr konfigurierte In-Band-/Out-of-Band-Verträge (UDP-Ports 161 und 162)
- Für die APICs und Fabric-Switches unter dem Standard-Mgmt-Tenant konfigurierte statische Knoten-Managementadressen (ohne diese Konfiguration scheitert das Abrufen von SNMP-Informationen von einem APIC)
- Kenntnis des SNMP-Protokoll-Workflows

## Verwendete Komponenten

### Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- APIC
- Browser
- Application Centric Infrastructure (ACI) mit 5.2 (8e)
- Snmpwalk  command

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Die Cisco ACI bietet Unterstützung für SNMPv1, v2c und v3, einschließlich Management Information Bases (MIBs) und Benachrichtigungen (Traps). Der SNMP-Standard ermöglicht es allen Drittanbieteranwendungen, die die verschiedenen MIBs unterstützen, die ACI-Leaf- und Spine-Switches sowie die APIC-Controller zu verwalten und zu überwachen.

SNMP-Schreibbefehle (Set) werden von der ACI jedoch nicht unterstützt.

Die SNMP-Richtlinie wird unabhängig auf den Leaf- und Spine-Switches sowie auf den APIC-Controllern angewendet und ausgeführt. Da jedes ACI-Gerät über eine eigene SNMP-Einheit verfügt, d. h. mehrere APICs in einem APIC-Cluster müssen sowie die Switches separat überwacht werden. Die SNMP-Richtlinienquelle wird jedoch als Überwachungsrichtlinie für die gesamte ACI-Fabric erstellt.

Standardmäßig verwendet SNMP den **UDP**-Port **161** für Polling und Port **162** für TRAPs.

SNMP-Bereiche im Überblick

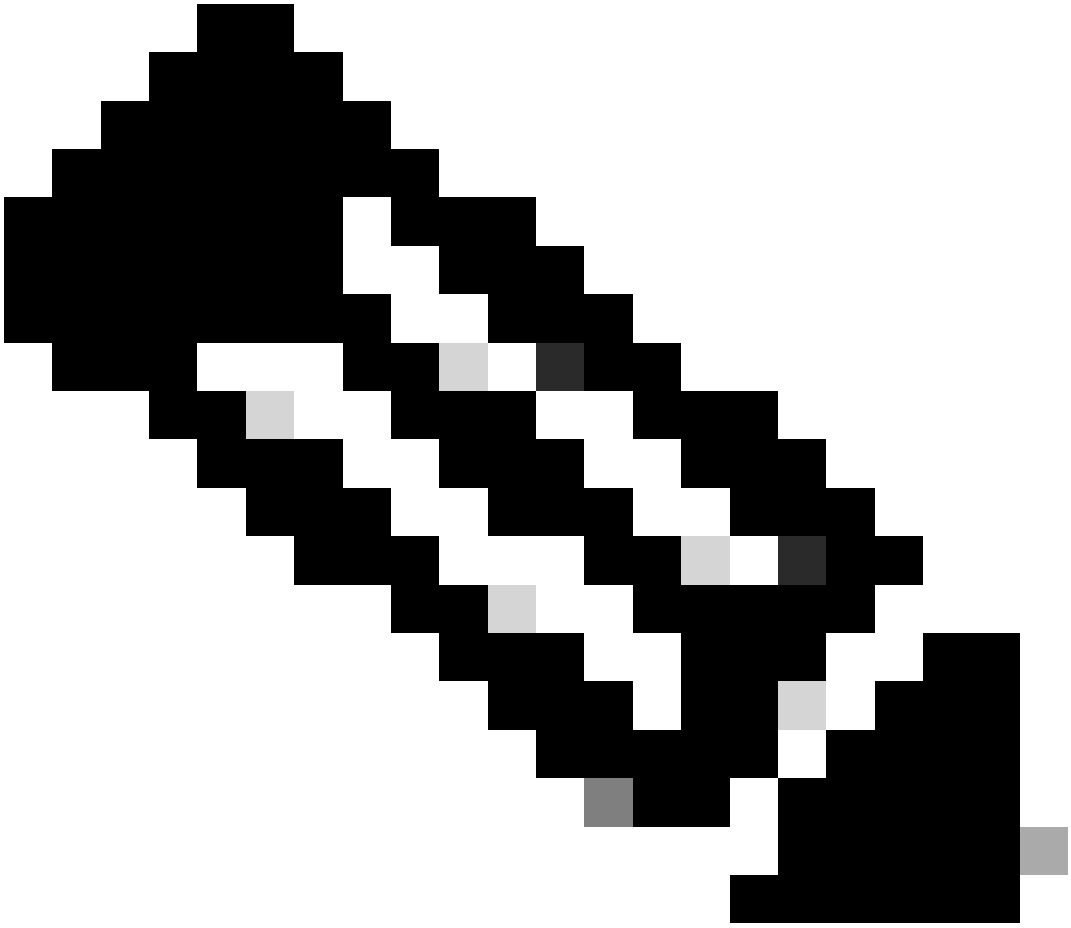
Ein Grundkonzept von SNMP in der ACI ist, dass SNMP-Informationen in zwei Bereichen abgerufen werden können:
1. Global
2. VRF-Kontext (Virtual Routing and Forwarding)

Der **globale Geltungsbereich** umfasst Chassis-MIBs, z. B. die Anzahl der Schnittstellen, Schnittstellenindizes, Schnittstellennamen, den Schnittstellenstatus usw. eines Leaf-/Spine-Knotens.

**VRF-Context-Scope**-spezifische MIBs rufen VRF-spezifische Informationen ab, z. B. IP-Adressen und Routing-Protokollinformationen.

Die Cisco ACI MIB Support List enthält eine vollständige Liste der unterstützten globalen und VRF-Kontext-MIBs für APIC und Fabric Switches.

---



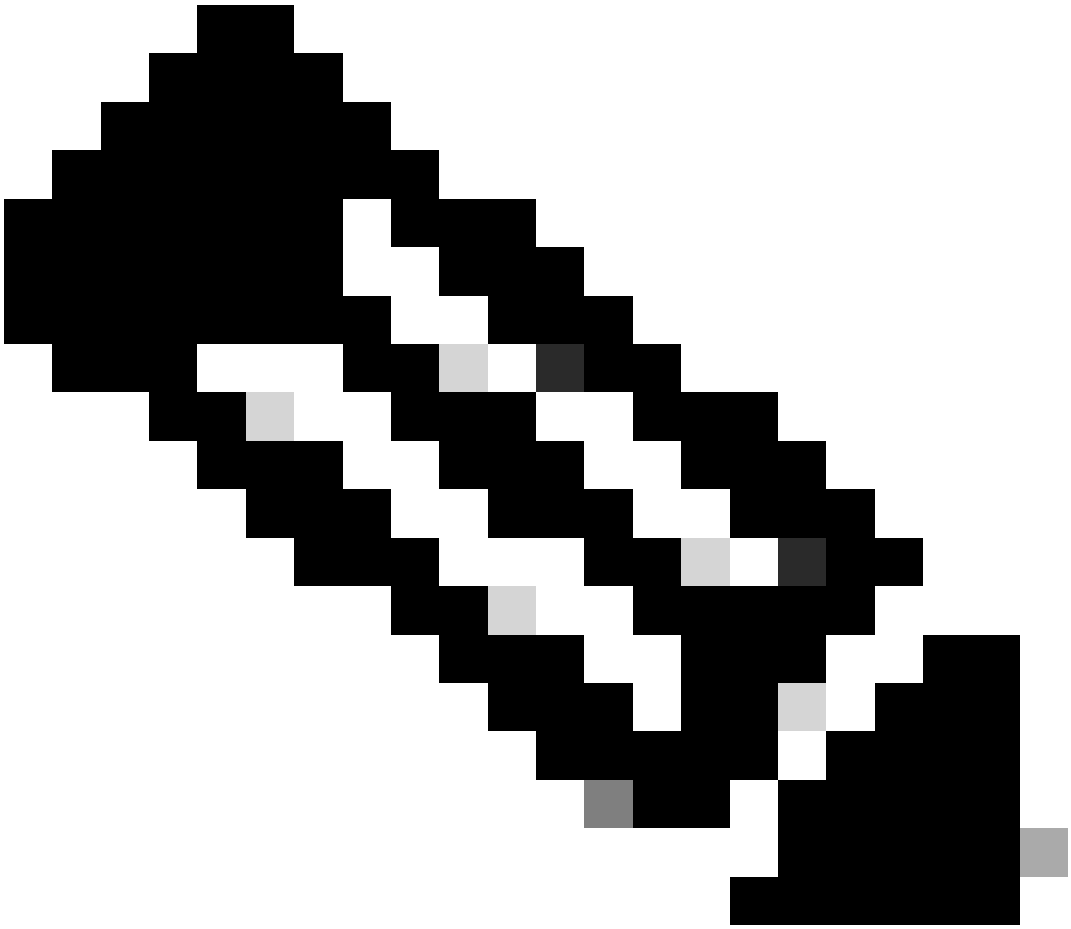
**Hinweis**: Eine MIB mit einem globalen Gültigkeitsbereich hat nur eine Instanz im System. Die Daten in einer globalen MIB beziehen sich auf das Gesamtsystem.

Eine MIB mit VRF-spezifischem Umfang kann pro VRF Instanzen im System aufweisen. Die Daten in einer VRF-spezifischen MIB beziehen sich nur auf diese VRF-Instanz.

---

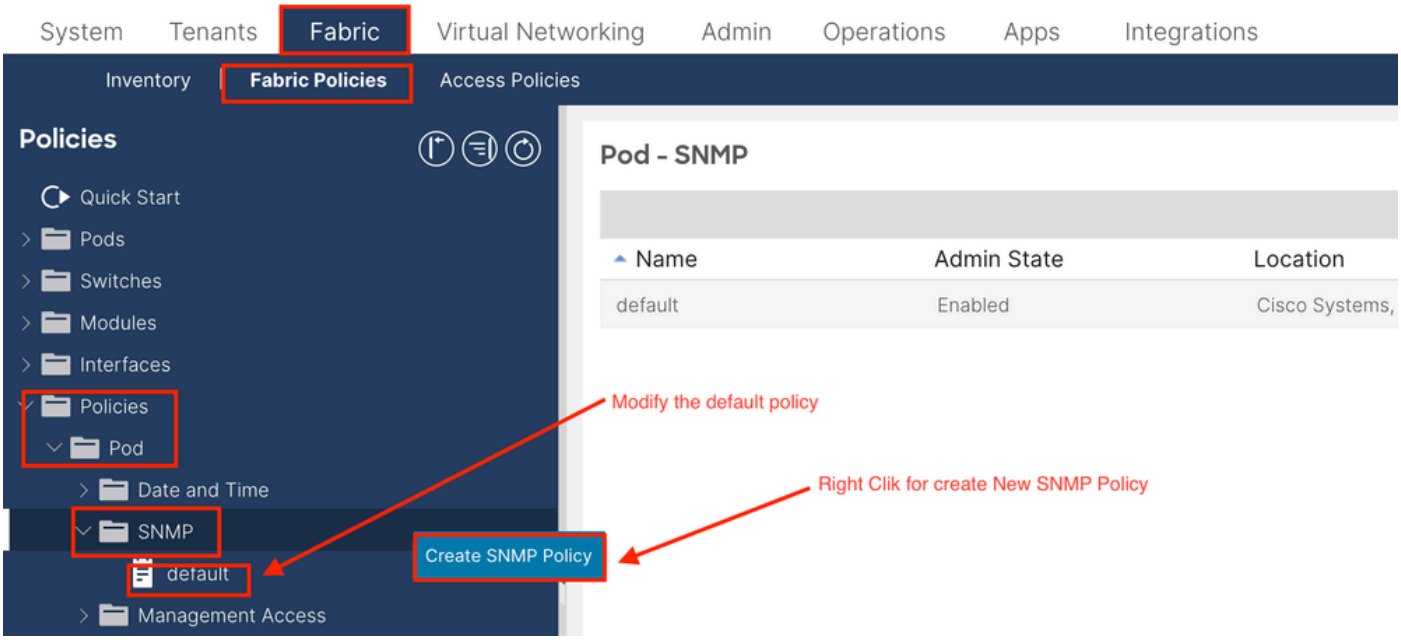
Konfigurationsschritte (für globale und VRF-Kontextbereiche)

Schritt 1: Konfigurieren der SNMP Fabric-Richtlinie



**Hinweis:** Hier werden SNMP-Einstellungen festgelegt, z. B. SNMP-Community-Richtlinien und SNMP-Client-Gruppen-Richtlinien.

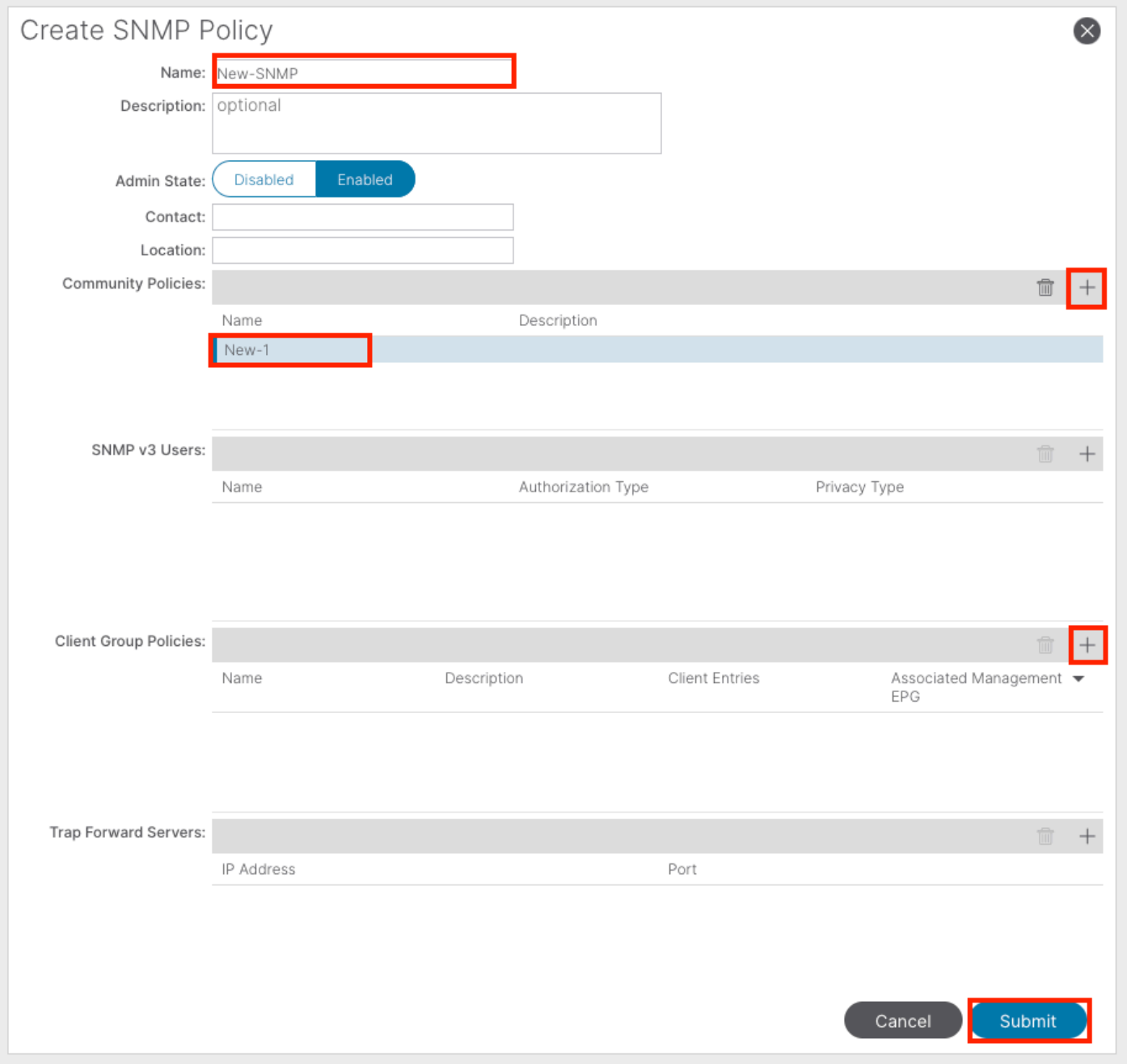
Der erste Schritt bei der Konfiguration des SNMP besteht in der Erstellung der erforderlichen SNMP Fabric-Richtlinien. Um die SNMP Fabric-Richtlinien zu erstellen, navigieren Sie zum Web-GUI-Pfad des APICFabric > Fabric Policies > Policies > Pod > SNMP.




Sie können eine neue SNMP-Richtlinie erstellen oder die Standard-SNMP-Richtlinie ändern.

Im Dokument wird die SNMP-Richtlinie als **New-SNMP** bezeichnet und verwendet die SNMP-Version v2c. Daher sind hier nur die Community-Richtlinien und die Client-Gruppen-Richtlinien erforderlich.

Das Feld "Community Policy Name" (Name der Community-Richtlinie) definiert den zu verwendenden SNMP Community String. In unserem Fall **New-1**. Sie sehen, wo diese beiden Community Strings später hineinkommen.




Name - der Name der SNMP-Richtlinie. Dieser Name muss zwischen 1 und 64 alphanumerische Zeichen lang sein.

Beschreibung - die Beschreibung der SNMP-Richtlinie. Die Beschreibung kann 0 bis 128 alphanumerische Zeichen enthalten.

Admin State (Admin-Status): Der administrative Status der SNMP-Richtlinie. Der Status kann aktiviert oder deaktiviert werden. Die Bundesstaaten sind:

- enabled - Der Admin-Status ist aktiviert.
- disabled (Deaktiviert): Der Admin-Status ist deaktiviert

Standardmäßig ist diese Option **deaktiviert**.

Kontakt - Die Kontaktinformationen für die SNMP-Richtlinie.

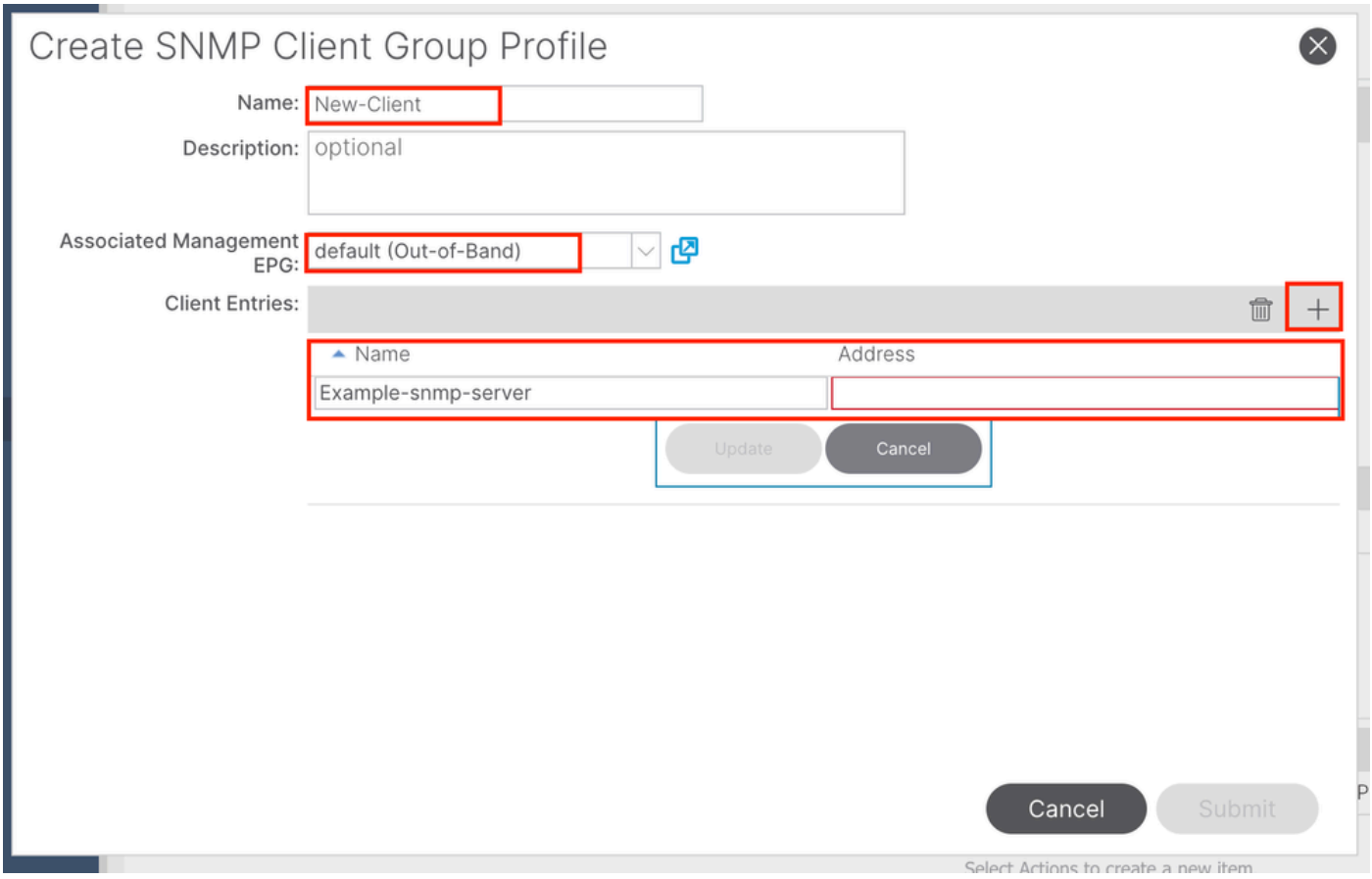
Speicherort - Der Speicherort für die SNMP-Richtlinie.

SNMP v3-Benutzer - Das SNMP-Benutzerprofil dient dazu, Benutzer mit SNMP-Richtlinien für Überwachungsgeräte in einem Netzwerk zu verknüpfen.

Community-Richtlinien - Das SNMP-Community-Profil ermöglicht den Zugriff auf die Router- oder Switch-Statistik für die Überwachung.

Client-Gruppenrichtlinien:

Der nächste Schritt besteht darin, die Richtlinie/das Profil der Client-Gruppe hinzuzufügen. Der Zweck der Richtlinie/des Profils für Client-Gruppen besteht darin, festzulegen, welche IPs/Subnetze SNMP-Daten von APICs und Fabric-Switches abrufen können:




Name: Der Name des Client-Gruppenprofils. Dieser Name muss zwischen 1 und 64 alphanumerische Zeichen lang sein.

Beschreibung - die Beschreibung des Client-Gruppenprofils. Die Beschreibung kann 0 bis 128 alphanumerische Zeichen enthalten.

Associated Management End Point Group (EPG) - der Distinguished Name einer Endpunktgruppe, über die auf die VRF-Instanz zugegriffen werden kann. Die maximal unterstützte Zeichenfolgenlänge beträgt 255 ASCII-Zeichen. Die Standardeinstellung ist die Verwaltungs-Tenant-EPG für den Out-of-Band-Verwaltungszugriff.

Clienteinträge - die IP-Adresse des SNMP-Clientprofils.

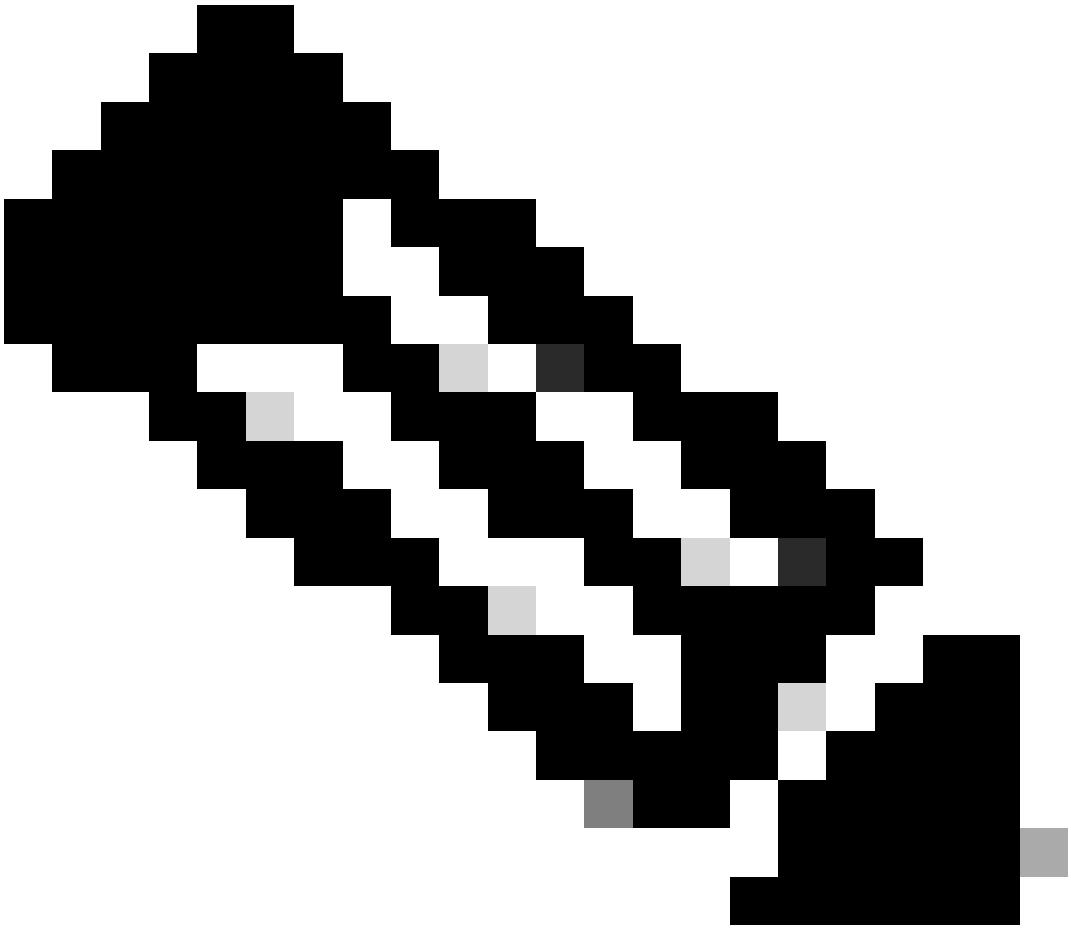
Im Dokument wird die Client-Gruppenrichtlinie/-profil als **Neuer Client** bezeichnet.

In der Client Group Policy/Profile (Client-Gruppenrichtlinie/Profil) müssen Sie die bevorzugte Management-EPG zuordnen. Sie müssen sicherstellen, dass die ausgewählte Management-EPG über die erforderlichen Verträge für SNMP-Datenverkehr verfügt (UDP-Ports 161 und 162). Die standardmäßige Out-of-Band-Verwaltungs-EPG wird im Dokument zu Demonstrationszwecken verwendet.

Der letzte Schritt besteht darin, Ihre **Clienteinträge** zu definieren, damit bestimmte IPs oder ganze Subnetze auf ACI-SNMP-Daten zugreifen können. Es gibt eine Syntax zum Definieren einer bestimmten IP oder eines gesamten Subnetzes:

- Spezifische Host-IP: 192.168.1.5
- Gesamtes Subnetz: 192.168.1.0/24

---



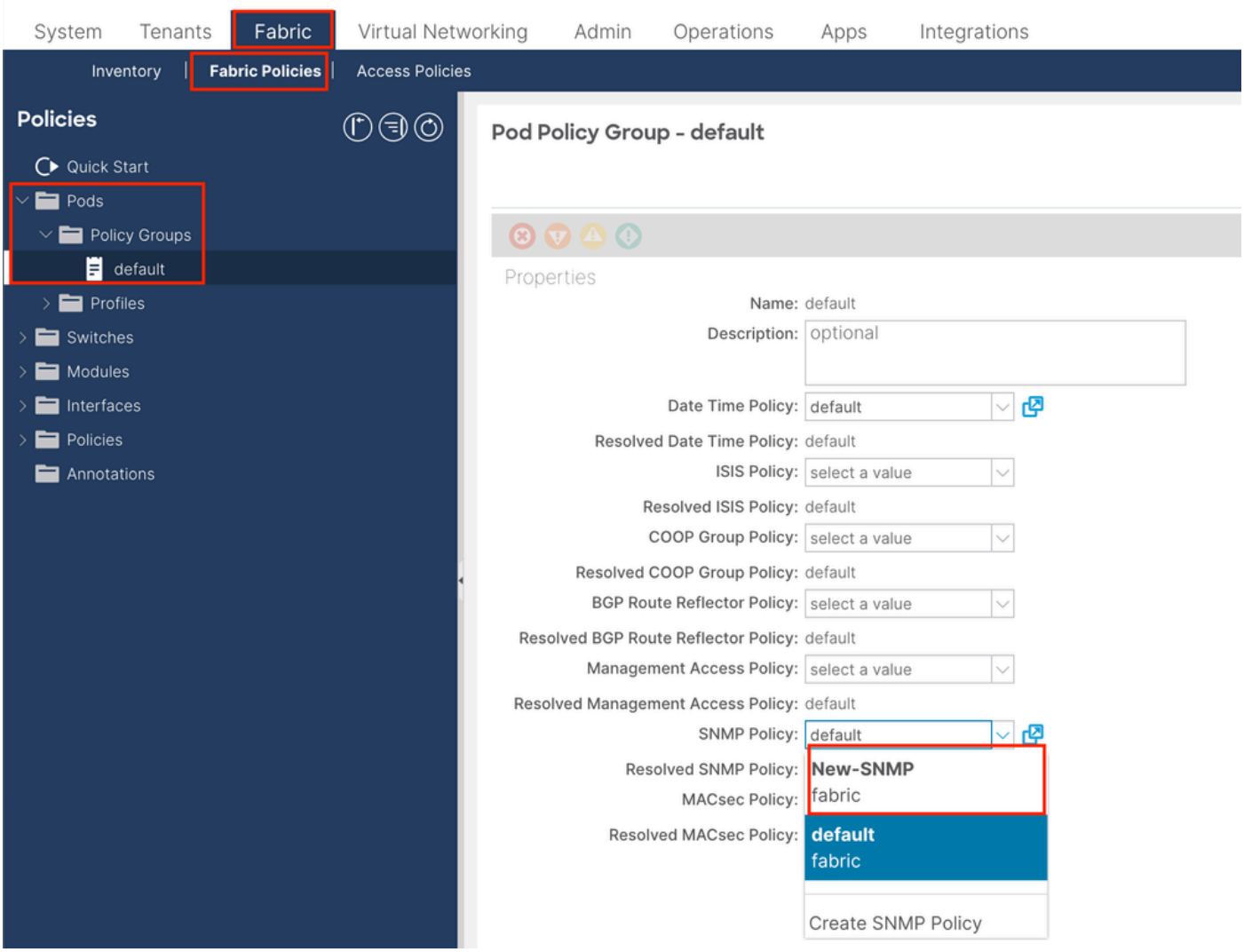
**Hinweis:** Sie können 0.0.0.0 im Clienteintrag nicht verwenden, um alle Subnetze zuzulassen (wenn Sie allen Subnetzen den Zugriff

---

auf SNMP MIB erlauben möchten, lassen Sie die Clienteinträge leer).

Schritt 2: SNMP-Richtlinie auf Pod Policy Group (Fabric Policy Group) anwenden

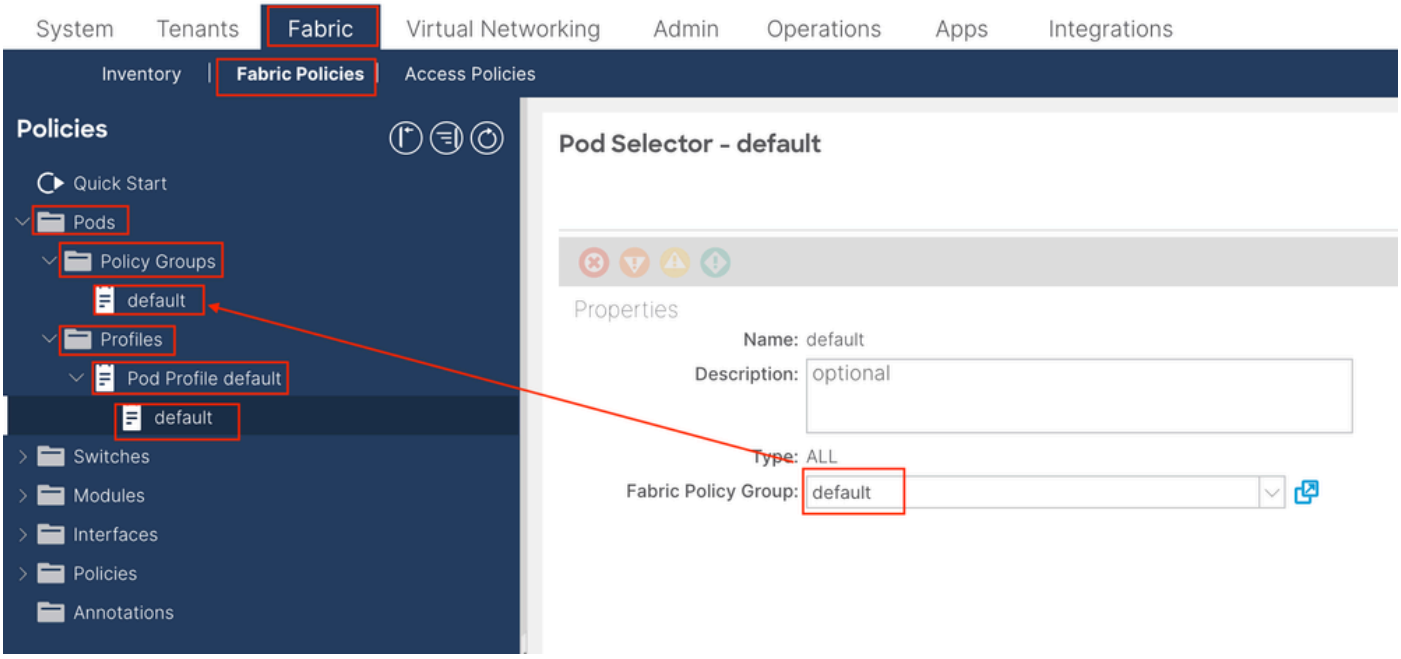
Um diese Konfiguration anzuwenden, navigieren Sie zum Pfad der Web-GUI des APICFabric > Fabric Policies > Pods > Policy Groups > POD_POLICY_GROUP (Standardeinstellung im Dokument).




Im rechten Fensterbereich sehen Sie ein Feld für die SNMP-Richtlinie. Wählen Sie aus dem Dropdown-Menü Ihre neu erstellte SNMP-Richtlinie aus, und senden Sie Ihre Änderungen.

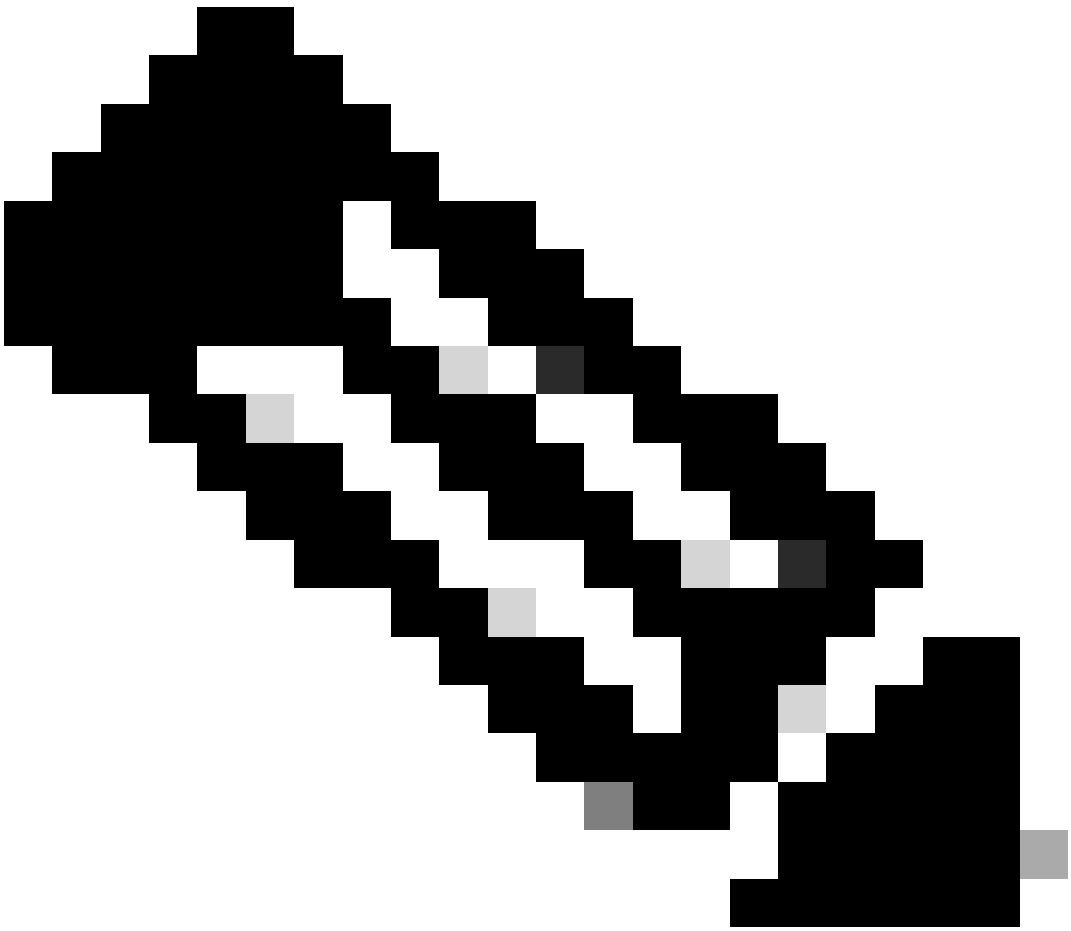
Schritt 3: Zuweisung der Pod-Richtliniengruppe zum Pod-Profil

Verwenden Sie im Dokument zur Vereinfachung das Standard-POD-Profil. Navigieren Sie dazu zum Pfad der Web-GUI des APICFabric > Fabric Policies > Pods > Profiles > POD_PROFILE (Standardeinstellung im Dokument).




Konfigurieren Sie in dieser Phase das grundlegende SNMP für globale MIBs.

---



---

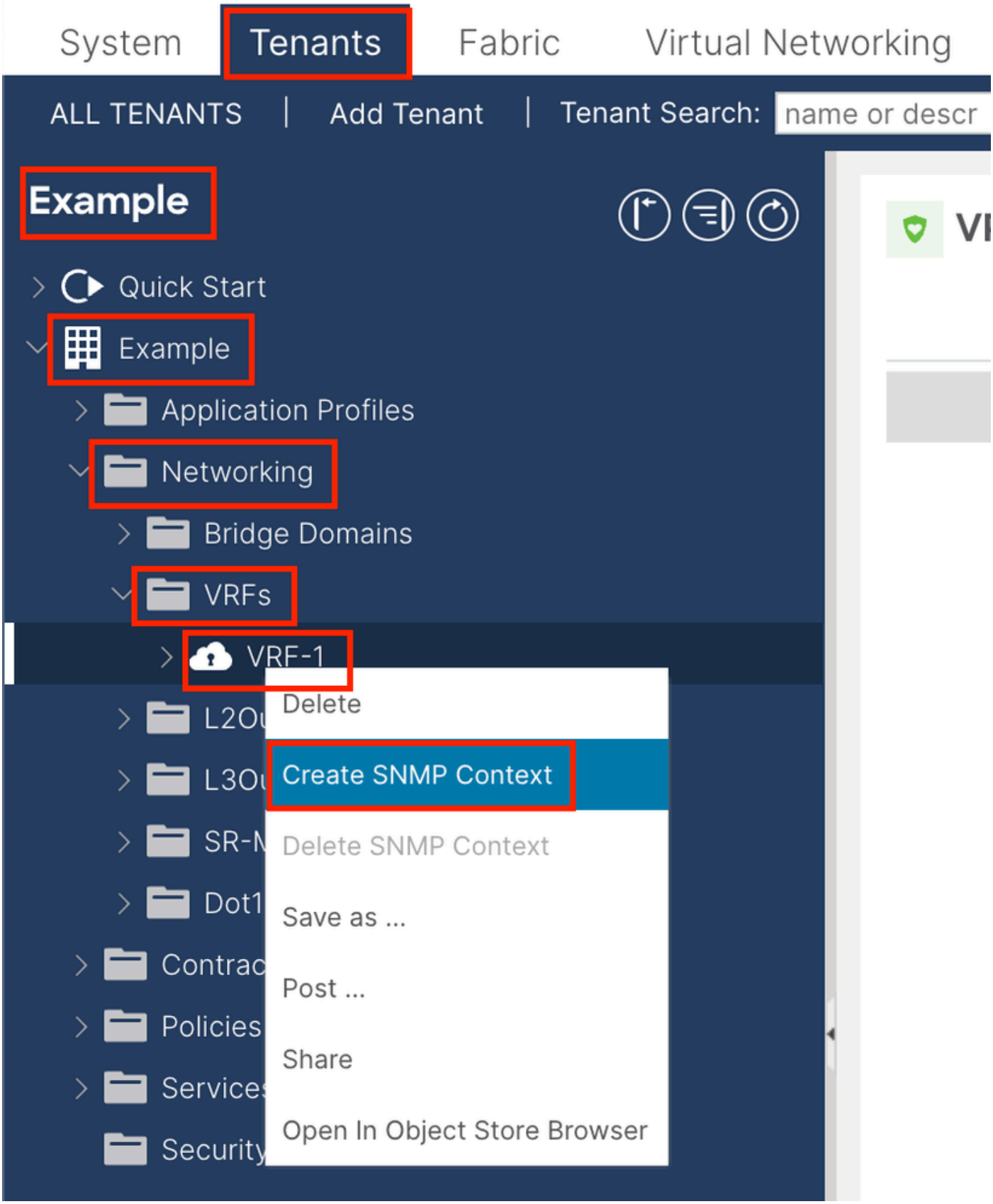
**Hinweis**: Zu diesem Zeitpunkt sind alle erforderlichen Schritte (Schritte 1-3) für die SNMP-Konfiguration abgeschlossen, und der globale MIB-Bereich wurde implizit verwendet. Auf diese Weise kann ein SNMP Walk für jeden ACI-Knoten oder APIC durchgeführt werden.

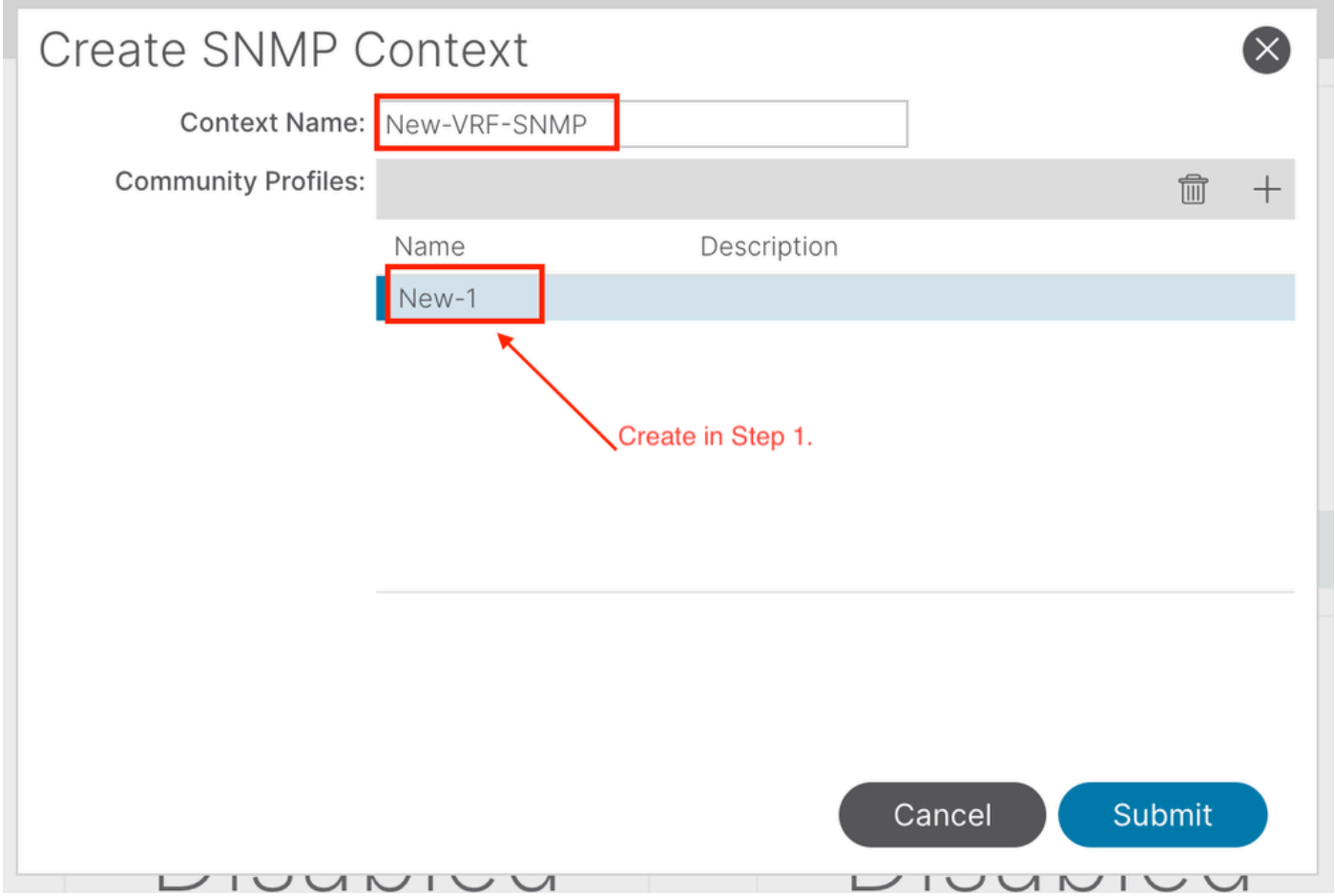
---

Schritt 4: Konfigurieren von VRF-Kontextbereichen

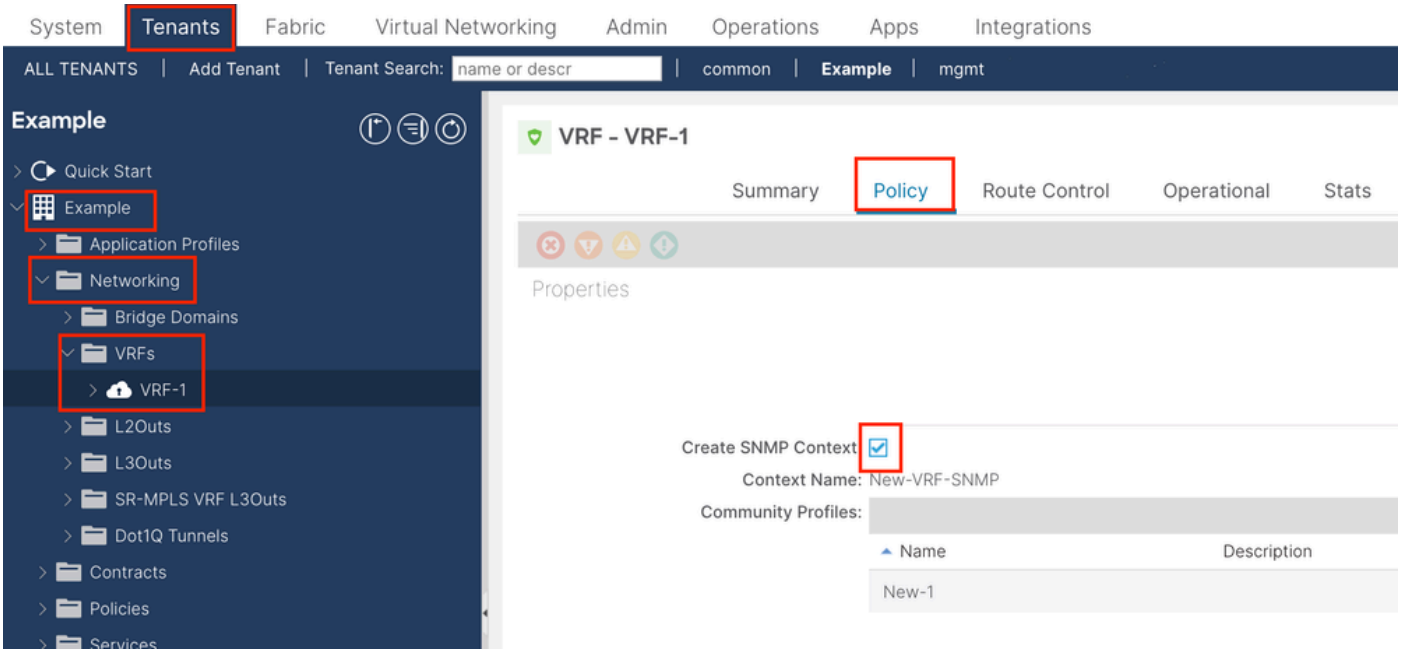
Wenn Sie einen Community String einem VRF-Kontext zugeordnet haben, kann dieser spezielle Community String nicht zum Abrufen von SNMP-Daten des globalen Bereichs verwendet werden. Wenn Sie SNMP-Daten sowohl für den globalen Bereich als auch für den VRF-Kontext abrufen möchten, müssen Sie daher zwei SNMP Community Strings erstellen.

In diesem Fall verwenden die zuvor erstellten Community-Strings (in Schritt 1.), und zwar (**New-1)**, **New-1** für den VRF-Kontextbereich und **VRF-1** benutzerdefiniertes VRF in **Beispiel eines** benutzerdefinierten Tenants. Navigieren Sie dazu zum Web-GUI-Pfad des APICTenants > Example > Networking > VRFs > VRF-1 (right click) > Create SNMP Context .


System
Tenants
Fabric
Virtual Networking
ALL TENANTS
Add Tenant
Tenant Search:
name or descr
Example
Quick Start
Example
Application Profiles
Networking
Bridge Domains
VRFs
VRF-1
Delete
Create SNMP Context
Delete SNMP Context
Save as ...
Post ...
Share
Open In Object Store Browser




Nach dem Absenden der Konfiguration können Sie die angewendete SNMP-Kontextkonfiguration überprüfen, indem Sie mit der linken Maustaste auf die VRF-Instanz klicken, zur Registerkarte Policy (Richtlinie) der VRF-Instanz navigieren und einen Bildlauf nach unten zum unteren Rand des Bereichs durchführen:



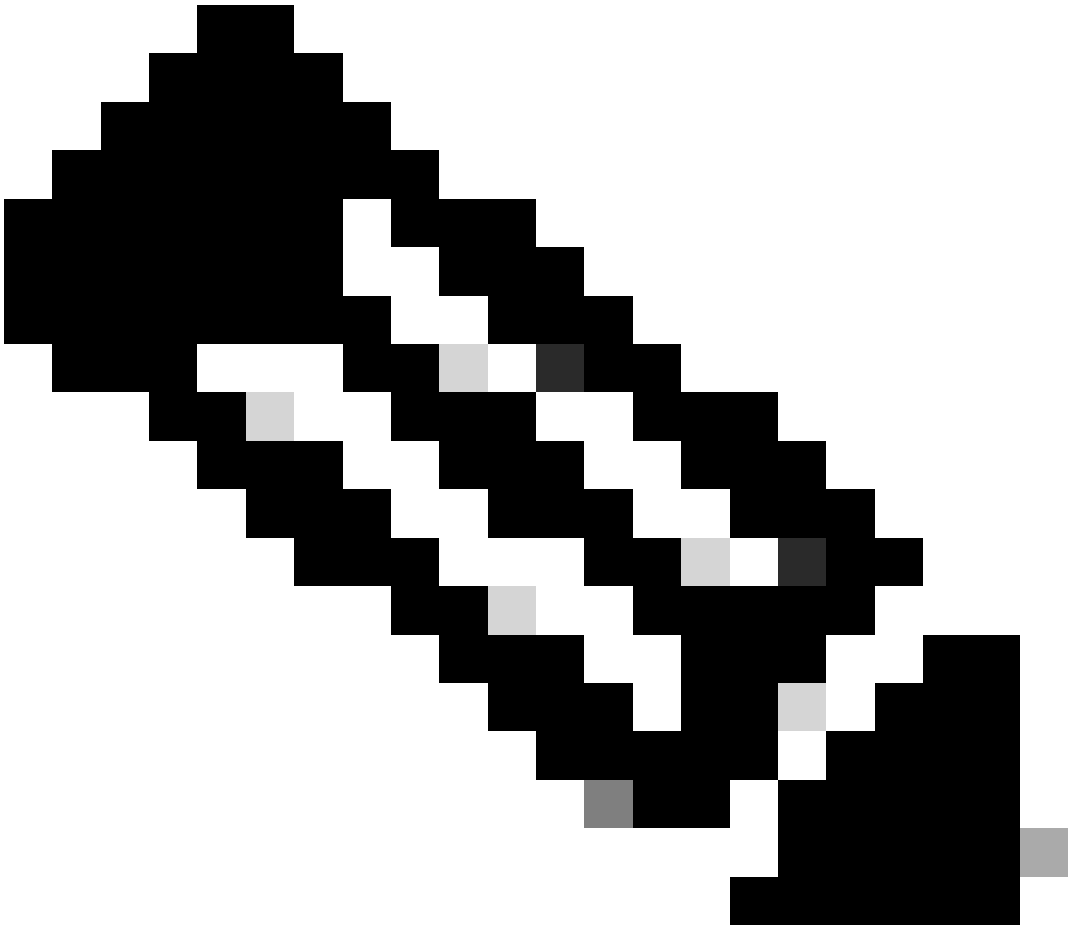

Um einen SNMP-Kontext auf einer VRF zu deaktivieren, können Sie das Kontrollkästchen **SNMP-Kontext erstellen** deaktivieren (siehe Screenshot) oder mit der rechten Maustaste auf die VRF-Instanz klicken und **SNMP-Kontext löschen** auswählen.

Konfiguration von SNMP-TRAPs über die Benutzeroberfläche

SNMP-TRAPs werden ohne Polling an den SNMP-Server (SNMP-Ziel-/Netzwerkmanagementsysteme (NMS)) gesendet, und der ACI-Knoten/APIC sendet SNMP-TRAP, sobald der Fehler bzw. das Ereignis (eine definierte Bedingung) auftritt.

SNMP-Traps werden je nach Richtlinienbereich unter Zugriffs-/Fabric-/Tenant-Überwachungsrichtlinien aktiviert. Die ACI unterstützt maximal 10 Trap-Empfänger.

---



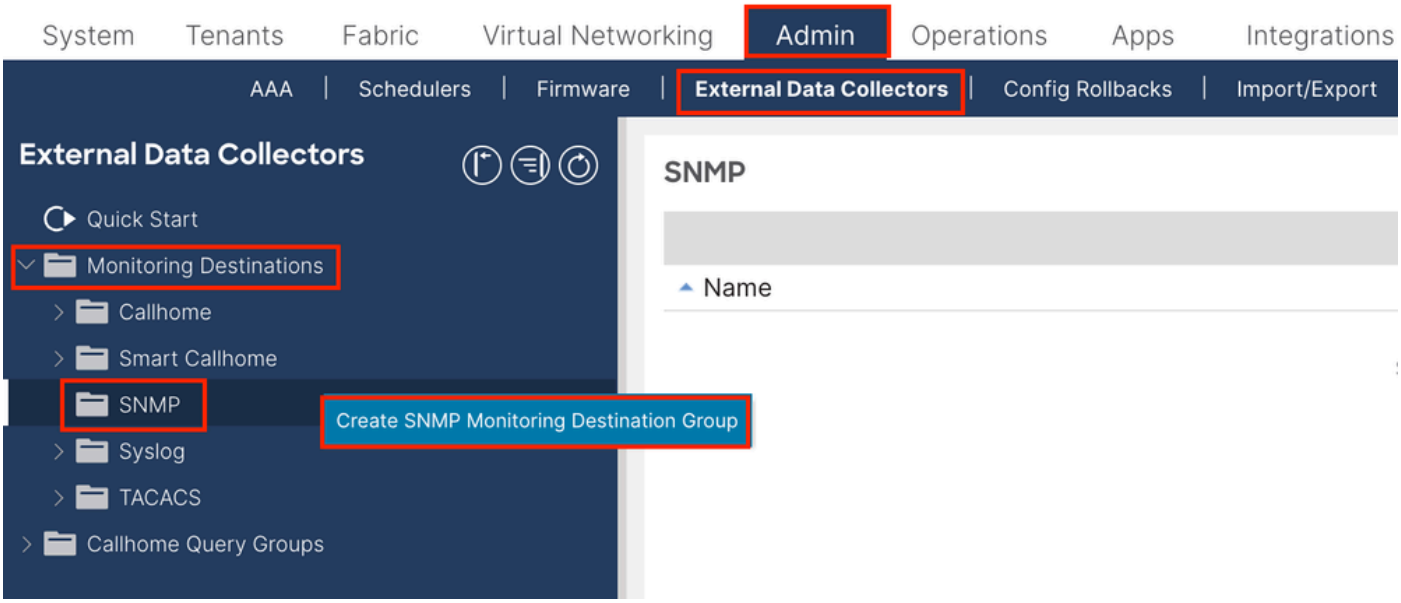
**Hinweis**: Ohne die Schritte 1-3 aus dem vorherigen Abschnitt ist die Konfiguration von SNMP TRAPs nicht ausreichend. Schritt 2. in der SNMP-TRAP-Konfiguration bezieht sich auf Überwachungsrichtlinien für (Zugriff/Fabric/Tenant).

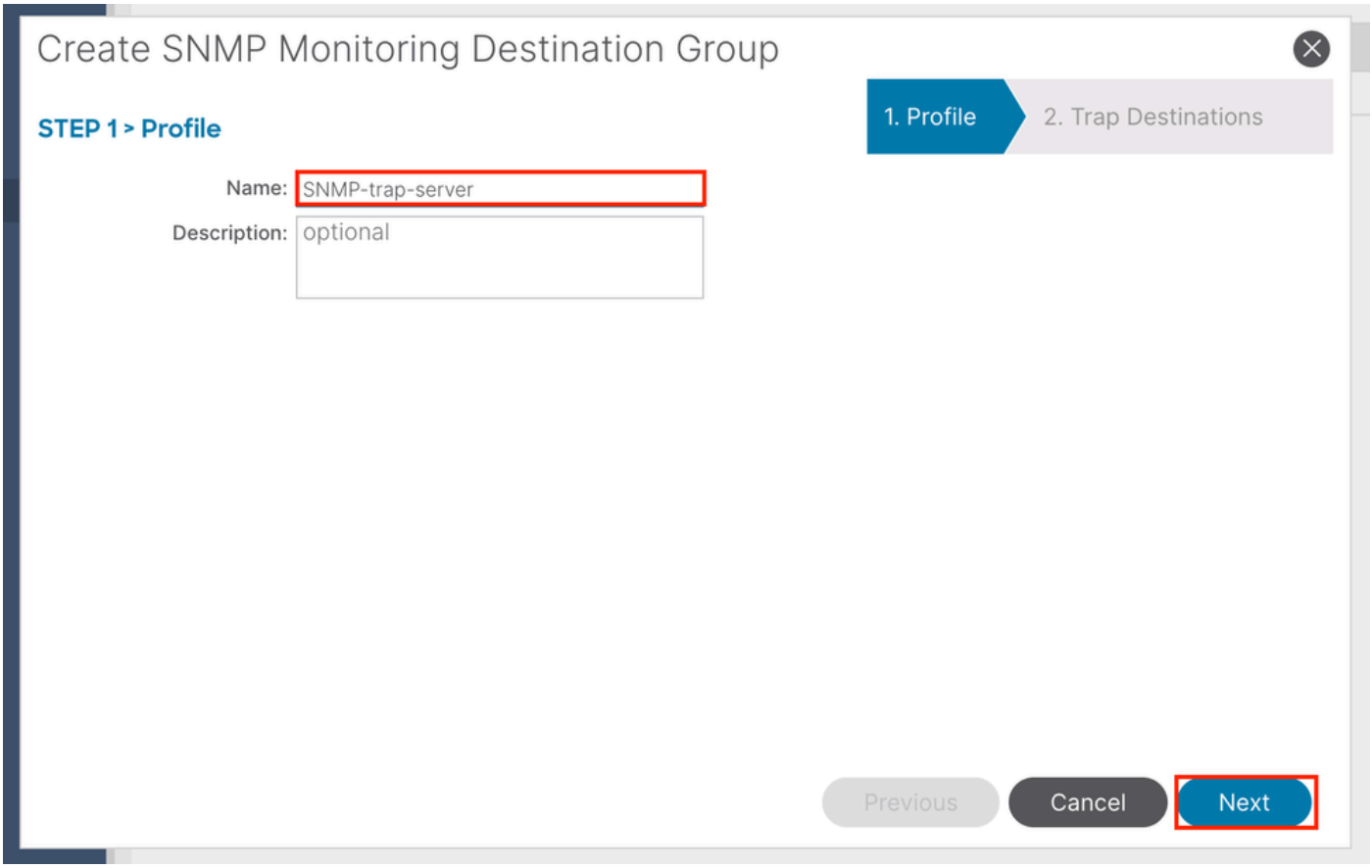
---

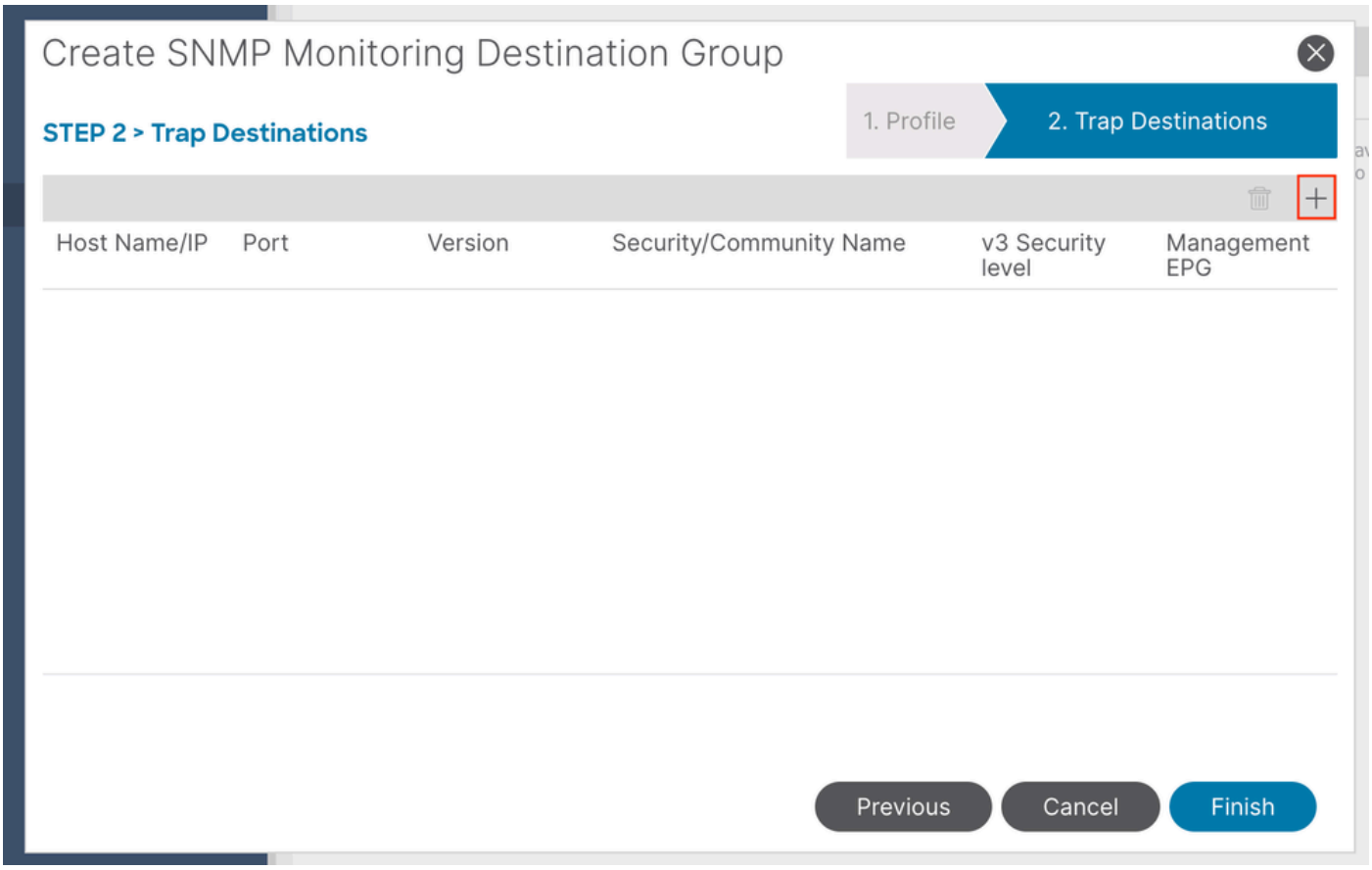
Zur Konfiguration von SNMP TRAPs in der ACI sind neben den Schritten 1, 2 und 3 im vorherigen Abschnitt zwei weitere Schritte erforderlich.

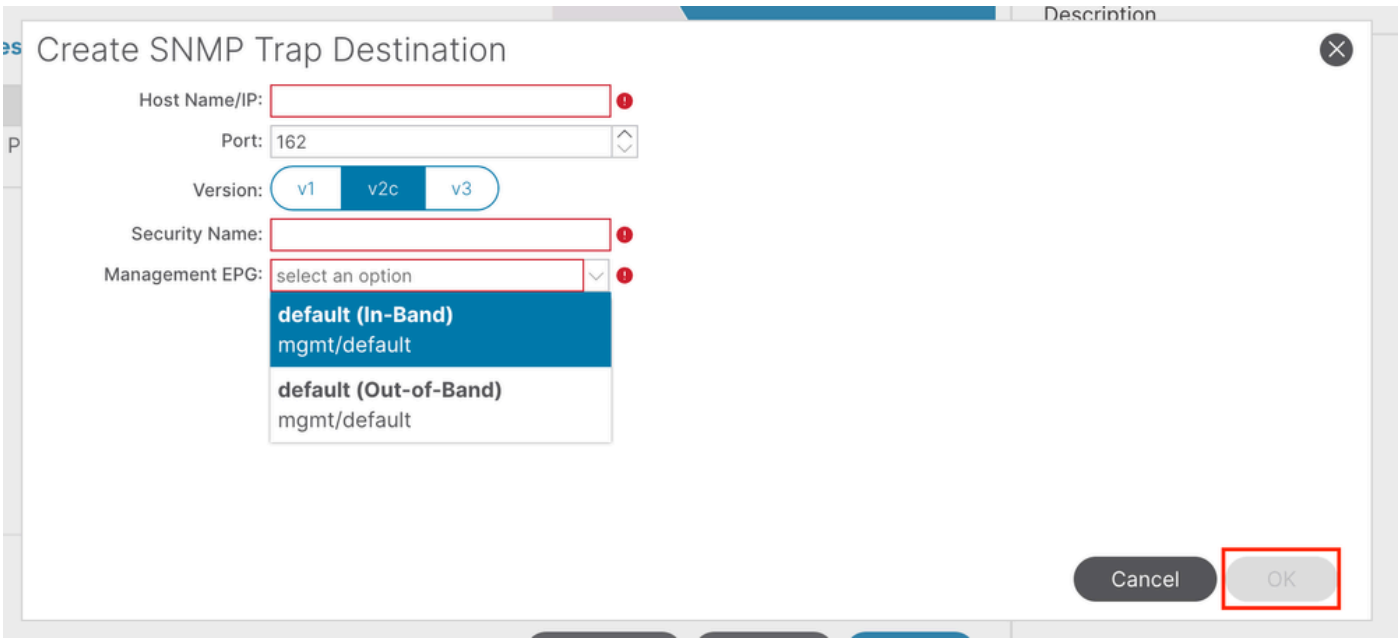
Schritt 1: SNMP-TRAP-Server konfigurieren

Navigieren Sie dazu zum Web-GUI-Pfad des APICAdmin > Eternal Data Collectors > Monitoring Destinations > SNMP.






Hostname/IP - der Host für das SNMP-Trap-Ziel.

Port - der Service-Port des SNMP-Trap-Ziels Der Bereich liegt zwischen 0 (nicht angegeben) und 65535; der Standardwert ist 162.

Version - Die unterstützte CDP-Version für das SNMP-Trap-Ziel. Die Version kann wie folgt aussehen:

- v1: Verwendet einen Community-String-Abgleich für die Benutzerauthentifizierung.

- v2c - Verwendet einen Community-String-Abgleich für die Benutzerauthentifizierung.

- v3 - ein interoperables, standardbasiertes Protokoll für die Netzwerkverwaltung, das einen sicheren Zugriff auf Geräte ermöglicht, indem Frames über das Netzwerk authentifiziert und verschlüsselt werden.

Der Standardwert ist "**v2c"**.

Sicherheitsname - der Zielsicherheitsname des SNMP-Traps (Communityname). Es darf nicht das Symbol **@** enthalten.

v.3 Sicherheitsstufe - Die SNMPv3-Sicherheitsstufe für den SNMP-Zielpfad. Die Ebene kann wie folgt lauten:

- verfassen

- Naute

- Priv

Der Standardwert ist "**noauth"**.

Management-EPG - der Name der Management-Endpunktgruppe für das SNMP-Ziel, über das der Remote-Host erreichbar ist.

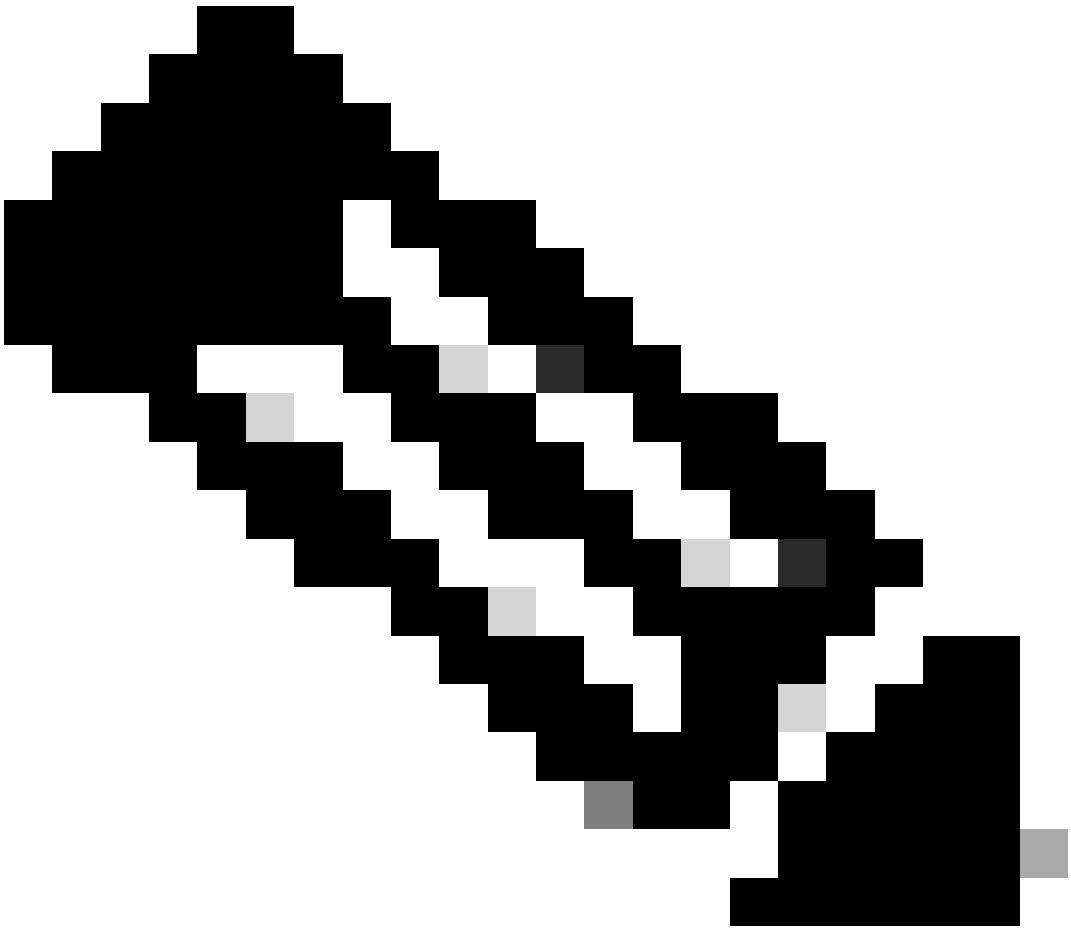
Schritt 2: Konfigurieren der SNMP-TRAP-Quelle unter der Überwachungsrichtlinie (Access/Fabric/Tenant)

Sie können Überwachungsrichtlinien mit den drei Bereichen erstellen:

- Zugriff - Access-Ports, FEX, VM-Controller
- Fabric: Fabric-Ports, Karten, Chassis, Lüfter

- Tenant - EPGs, Anwendungsprofile, Services

---

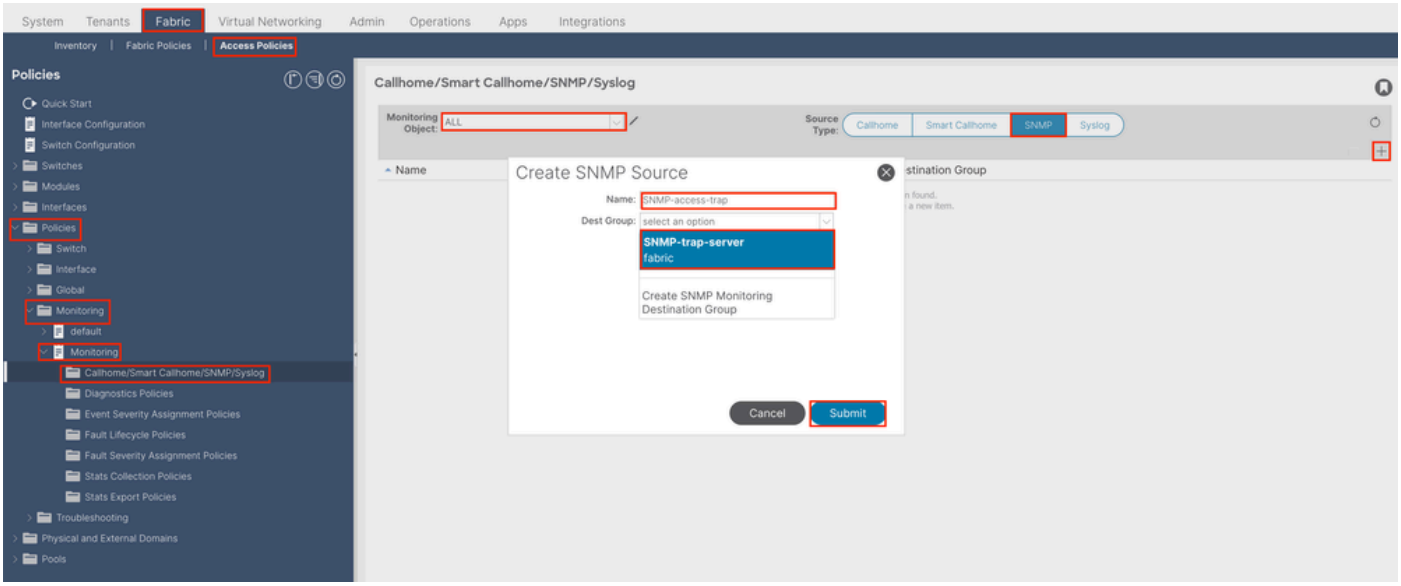


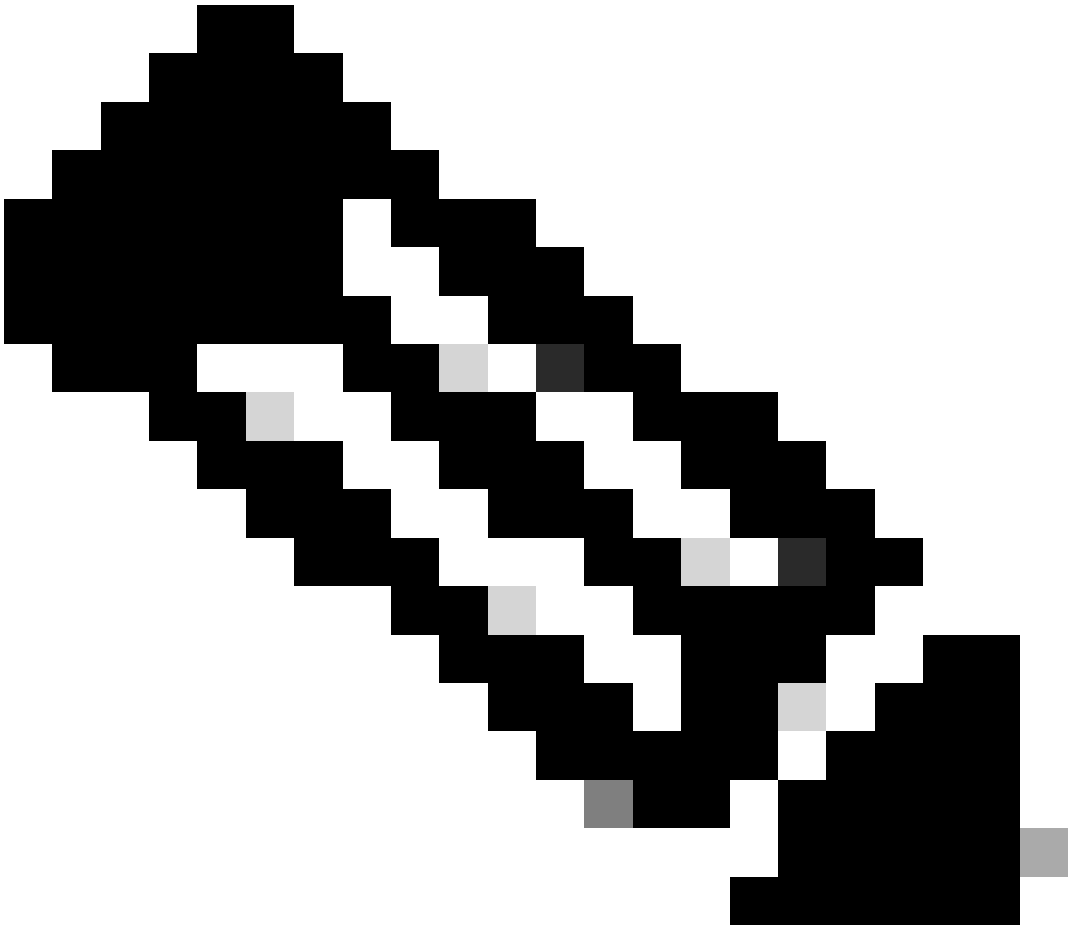
**Hinweis**: Sie können eine oder eine beliebige Kombination auswählen, um sie entsprechend Ihren Anforderungen zu konfigurieren.

---

Option 1: SNMP-Quelle unter Zugriffsrichtlinien definieren

Navigieren Sie dazu zum Web-GUI-Pfad des APICFabric > Access Polices > Polices > Monitoring > Default > Callhome/Smart Callhome/SNMP/Syslog/TACACS.

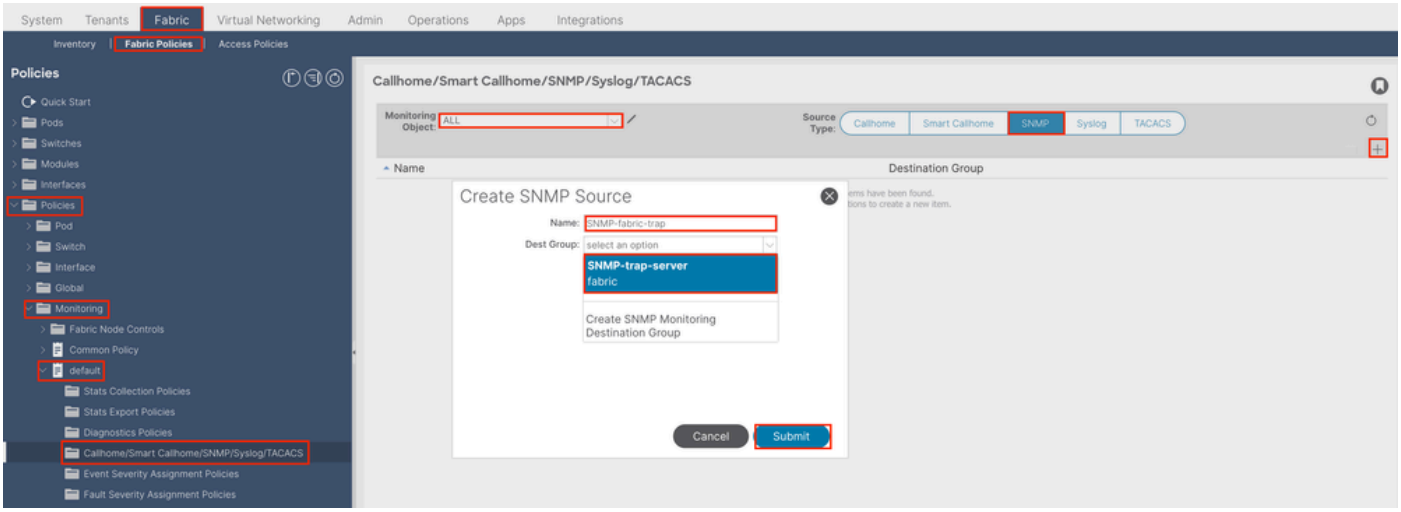

System
Tenants
Fabric
Virtual Networking
Admin
Operations
Apps
Integrations
Inventory
Fabric Policies
Access Policies
Policies
Quick Start
Interface Configuration
Switch Configuration
Switches
Modules
Interfaces
Policies
Switch
Interface
Global
Monitoring
default
Monitoring
Callhome/Smart Callhome/SNMP/Syslog
Diagnostics Policies
Event Severity Assignment Policies
Fault Lifecycle Policies
Fault Severity Assignment Policies
Stats Collection Policies
Stats Export Policies
Troubleshooting
Physical and External Domains
Pools
Callhome/Smart Callhome/SNMP/Syslog
Monitoring Object:
ALL
Source Type:
Callhome
Smart Callhome
SNMP
Syslog
Name
Create SNMP Source
Name:
SNMP-access-trap
Dest Group:
select an option
SNMP-trap-server
fabric
Create SNMP Monitoring Destination Group
Cancel
Submit



**Hinweis**: Sie können eine benutzerdefinierte Überwachungsrichtlinie (sofern konfiguriert) anstelle der Standardrichtlinie verwenden. Verwenden Sie hierzu die Standardrichtlinie. Sie können angeben, welches Überwachungsobjekt überwacht werden soll. Alle wurden hier verwendet.

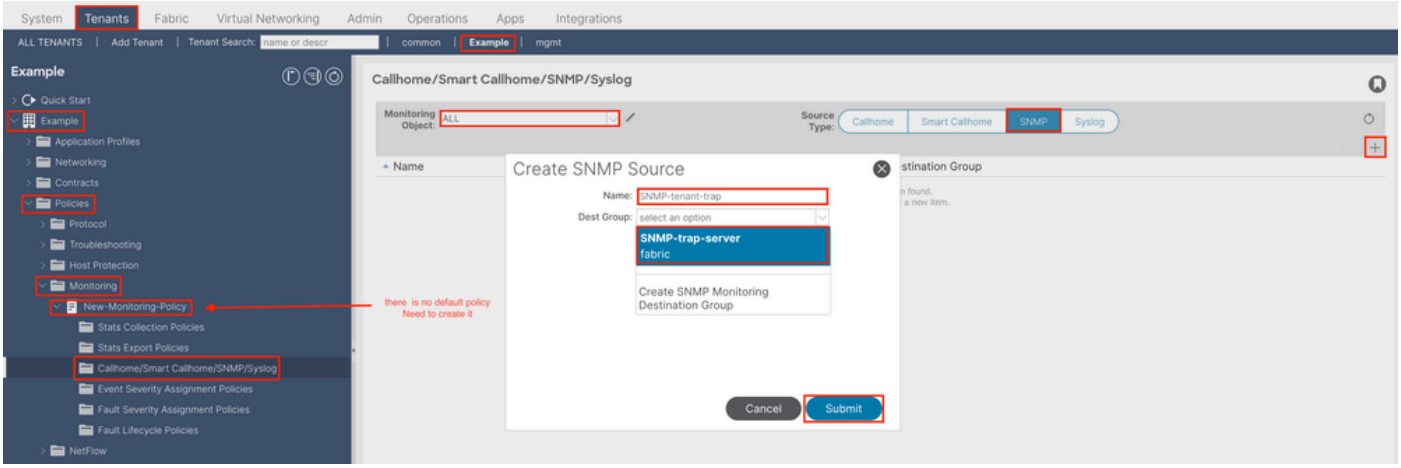
Option 2: SNMP-Quelle unter Fabric-Richtlinien definieren

Navigieren Sie dazu zum Web-GUI-Pfad des APICFabric > Fabric Polices > Polices > Monitoring > Default > Callhome/Smart Callhome/SNMP/Syslog/TACACS.




Option 3. SNMP-Quelle unter Tenant-Richtlinien definieren

Navigieren Sie dazu zum Web-GUI-Pfad des APICTenant > (Tenant Name) > Polices > Monitoring > (Custom monitoring policy) > Callhome/Smart Callhome/SNMP/Syslog/TACACS.




Überprüfung

Verwenden Sie den Befehl snmpwalk zur Überprüfung

Sehen Sie sich zunächst an, wie Sie SNMP-Daten aus der globalen Reichweite eines Leaf-Switches abrufen können. Mit dem Befehl snmpwalk

kann man genau das tun; snmpwalk -v 2c -c New-1 x.x.x.x.

Dieser aufgeschlüsselte Befehl stellt Folgendes dar:

snmpwalk = Die ausführbare Datei snmpwalk installiert unter MacOS/Linux/Windows

-v = Gibt die gewünschte SNMP-Version an

2c= Gibt an, dass SNMP Version 2c verwendet wird.

-c= Gibt an, dass eine bestimmte Community-Zeichenfolge

New-1= Der Community-String wird zum Abrufen der SNMP-Daten des globalen Bereichs verwendet.

x.x.x.x= Die Out-of-Band-Management-IP-Adresse meines Leaf-Switches

Befehlsergebnis:

```
$ snmpwalk -v 2c -c New-1 x.x.x.x SNMPv2-MIB::sysDescr.0 = STRING: Cisco NX-OS(tm) aci, Software (aci-n
```

In der Ausgabe des ausgeschnittenen Befehls können Sie sehen, dass der snmpwalk erfolgreich ist und hardwarespezifische Informationen abgerufen wurden. Wenn Sie den snmpwalk fortsetzen, werden die Namen der Hardware-Schnittstelle, Beschreibungen usw. angezeigt.

Fahren Sie nun mit dem Abrufen der SNMP-Daten für den VRF-Kontext, zuvor erstellte SNMP-Kontexte, **New-VRF-SNMP** für VRFs unter Verwendung des SNMP-Community-Strings **New-1 fort**.

Da der gleiche Community-String, **New-1,** für zwei verschiedene SNMP-Kontexte verwendet wird, müssen Sie angeben, von welchem SNMP-Kontext die SNMP-Daten abgerufen werden sollen. Es gibt die snmpwalk-Syntax, die Sie verwenden müssen, um einen bestimmten SNMP-Kontext anzugeben; snmpwalk -v 2c -c New-1@New-VrF-SNMP 10.x.x.x.

Wie Sie sehen, verwenden Sie zum Abrufen aus einem bestimmten SNMP-Kontext das folgende Format: COMMUNITY_NAME_HERE@SNMP_CONTEXT_NAME_HERE .

Verwenden von CLI Show-Befehlen

Im APIC:

```
show snmp show snmp policy <SNMP_policy_name> show snmp summary show snmp clientgroups show snmp commun
```

Auf Switch:

```
show snmp show snmp | grep "SNMP packets" show snmp summary show snmp community show snmp host show snm
```

Verwenden von CLI-Moquery-Befehlen

APIC/Switch:

```
moquery -c snmpGroup #The SNMP destination group, which contains information needed to send traps or in
```

Verwenden von CLI-CAT-Befehlen

Im APIC:

```
cat /aci/tenants/mgmt/security-policies/out-of-band-contracts/summary cat /aci/tenants/mgmt/security-po
```

Fehlerbehebung

SNMP-Prozess überprüfen

Auf Switch:

```
ps aux | grep snmp pidof snmpd
```

Im APIC:

```
ps aux | grep snmp
```

Wenn der Prozess normal ist, wenden Sie sich an Cisco TAC, um weitere Unterstützung zu erhalten.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.