SNMP configureren in ACI

Inhoud

Inleiding

Dit document beschrijft de configuratie van Simple Network Management Protocol (SNMP) en SNMP-traps in ACI.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Fabric-detectie voltooid
- In-Band/Out-of-Band-connectiviteit met uw Application Policy Infrastructure Controller-controller (APIC) en fabric-switches
- In-band/out-of-band contracten geconfigureerd om SNMP-verkeer toe te staan (UDP-

poorten 161 en 162)
- Statische nodebeheeradressen geconfigureerd voor uw APIC's en fabric switches onder de standaardbeheerhuurder (zonder dit, het halen van SNMP-informatie uit een APIC mislukt)
- De SNMP-protocolworkflow begrijpen

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- APIC
- Browser
- Application Centric Infrastructure (ACI) met 5.2 (8e)
- Snmpwalk opdracht

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Cisco ACI biedt SNMPv1, v2c en v3-ondersteuning, inclusief Management Information Bases (MIB's) en meldingen (traps). De SNMP-standaard staat toepassingen van derden die de verschillende MIB's ondersteunen toe om de ACI-switches voor blad en wervelkolom en APIC-controllers te beheren en te bewaken.

SNMP-schrijfopdrachten (Set) worden echter niet ondersteund in ACI.

Het SNMP-beleid wordt toegepast en werkt onafhankelijk op de blad- en wervelkolom switches en op APIC-controllers. Aangezien elk ACI-apparaat zijn eigen SNMP-entiteit heeft, dat wil zeggen meerdere APIC's in een APIC-cluster moeten afzonderlijk worden bewaakt, evenals de switches. De SNMP-beleidsbron is echter gemaakt als monitoringbeleid voor de gehele ACI-structuur.

Standaard gebruikt SNMP **UDP**-poort **161** voor opiniepeiling en poort **162** voor TRAP's.

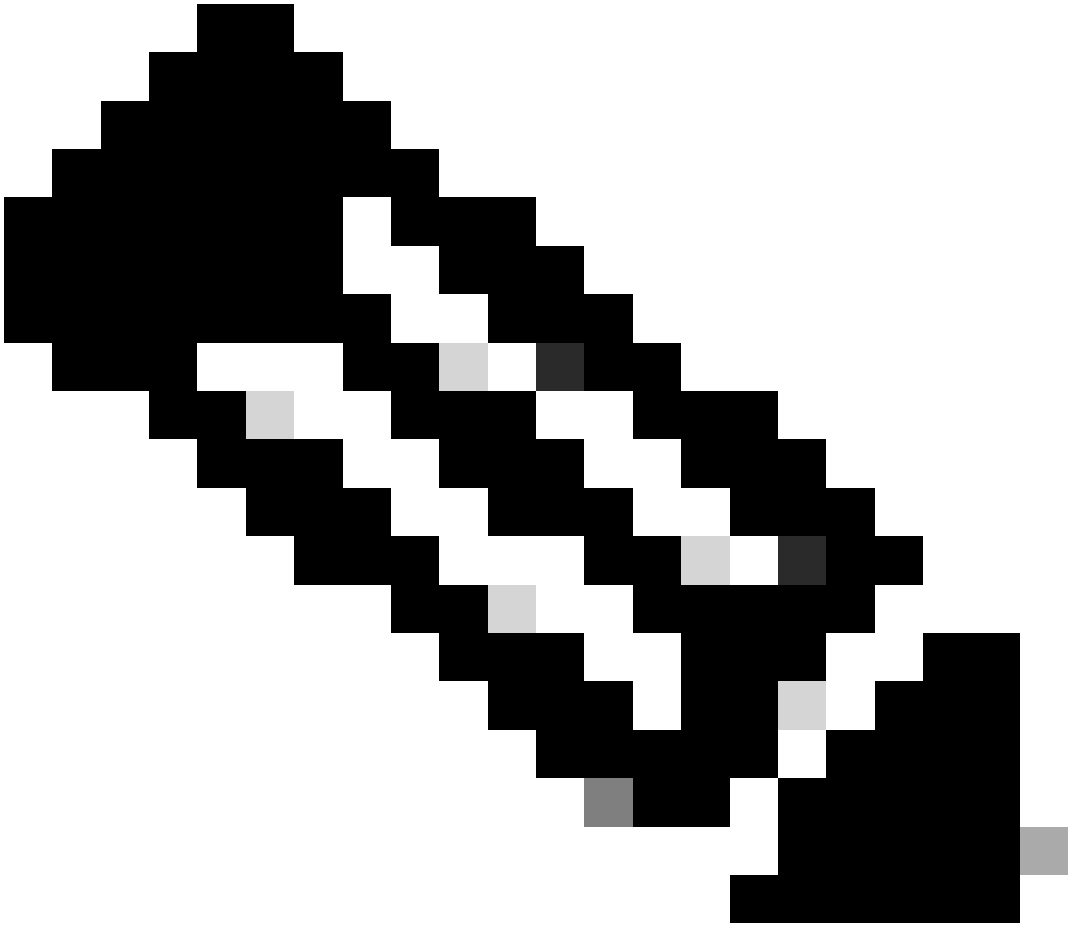
SNMP-gebieden begrijpen

Een snel fundamenteel concept van SNMP in ACI is dat er twee toepassingsgebieden zijn waar SNMP-informatie uit kan worden gehaald:
1. Wereldwijd
2. Virtual Routing and Forwarding (VRF)-context

Het **globale werkingsgebied** moet chassis MIBs zoals het aantal interfaces, interfaceindexen, interfacenamen, interfacestatus, etc. van een blad/wervelkolom trekken.

VRF-context Reikwijdte specifieke MIBs halen VRF-specifieke informatie op, zoals IP-adressen en routeringsprotocolinformatie.

Er is een volledige lijst met ondersteunde MIB's voor APIC- en fabric switch Global en VRF-context in de Cisco ACI MIB-ondersteuningslijst.

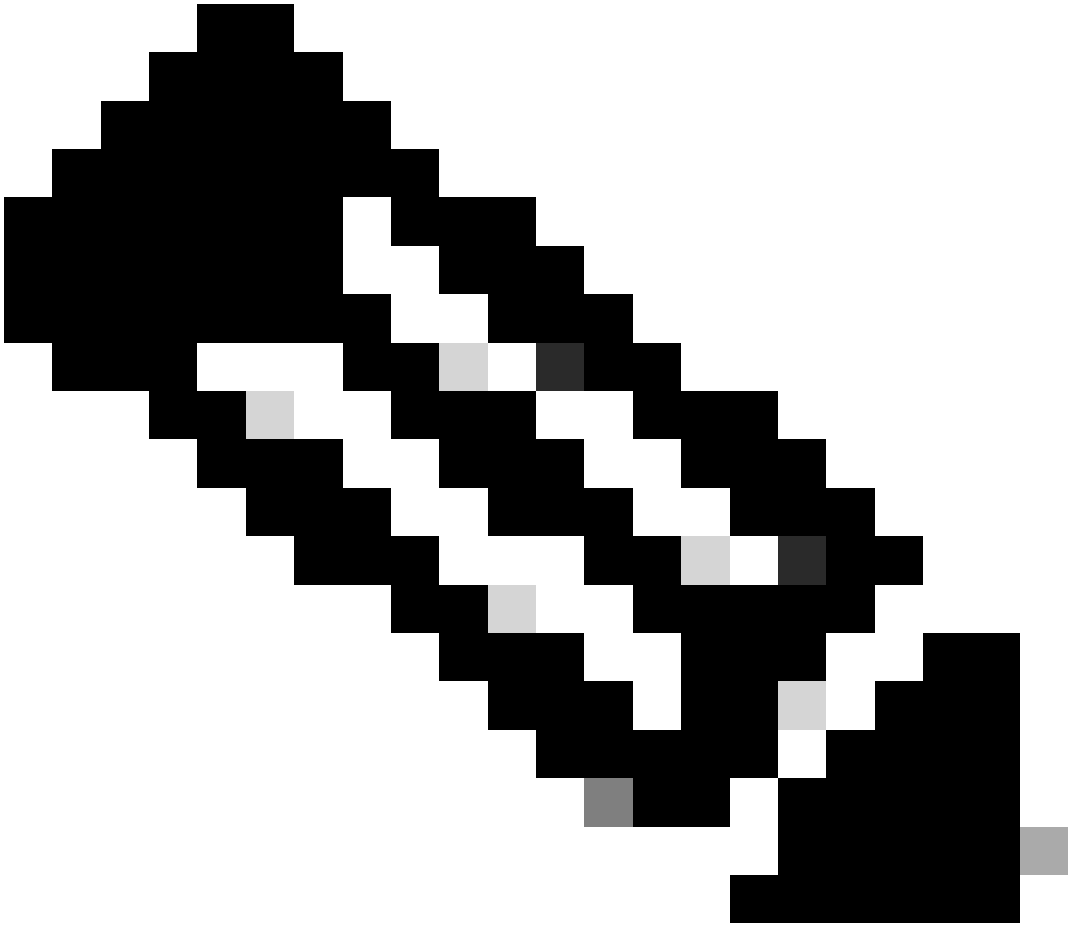


Opmerking: een MIB met een wereldwijde scope heeft slechts één instantie in het systeem. De gegevens in een mondiale MIB hebben betrekking op het gehele systeem.

Een MIB met VRF-specifiek bereik kan per-VRF-instanties in het systeem hebben. De gegevens in een VRF-specifieke MIB hebben alleen betrekking op die VRF.

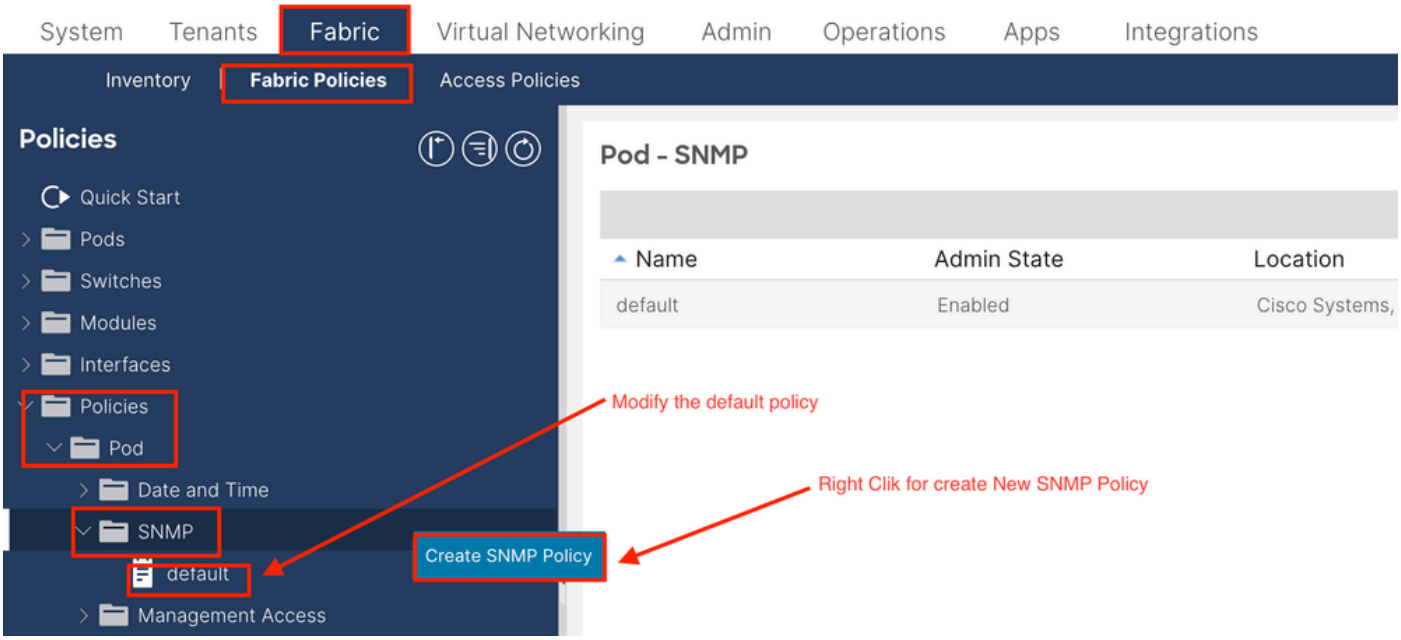
Configuratiestappen (voor zowel wereldwijde als VRF-contextgebieden)

Stap 1. SNMP-fabric-beleid configureren



Opmerking: hier worden SNMP-instellingen gespecificeerd zoals SNMP-communitybeleid en SNMP-clientgroepbeleid.

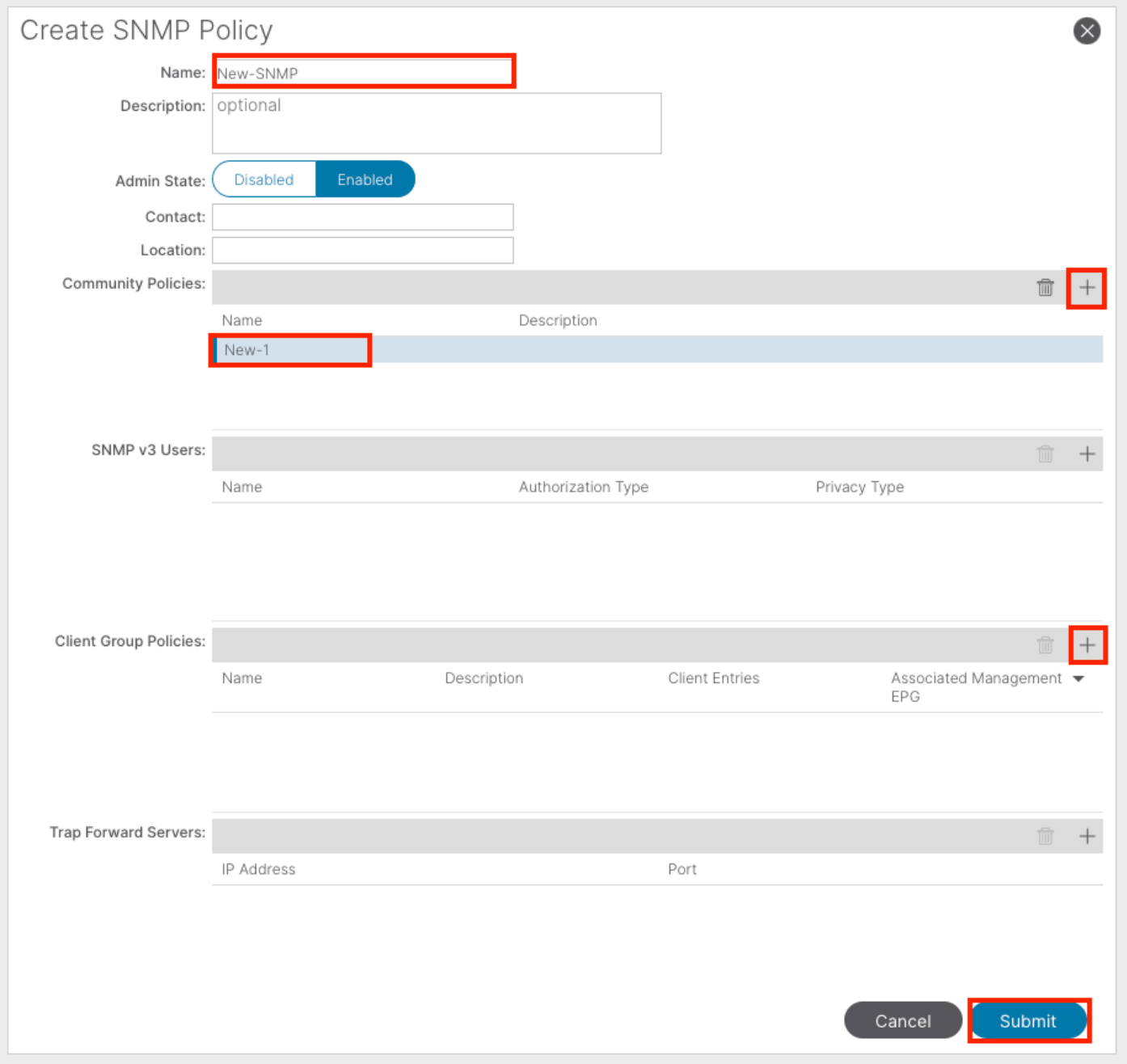
De eerste stap bij het configureren van SNMP is het aanmaken van het benodigde SNMP Fabric Policy. Om het SNMP Fabric Policies te maken, navigeer je naar het APIC web GUI pad; Fabric > Fabric Policies > Policies > Pod > SNMP.



U kunt een nieuw SNMP-beleid maken of het standaard SNMP-beleid wijzigen.

In het document wordt het SNMP-beleid **New-SNMP** genoemd en wordt SNMP versie v2c gebruikt. De enige velden die hier nodig zijn, zijn Community Policies en Client Group Policies.

In het veld Community Policy Name wordt de SNMP-community-string gedefinieerd die moet worden gebruikt. In ons geval, **New-1**. Je ziet waar deze twee gemeenschapsnaren later zijn.



Naam - de naam van het SNMP-beleid. Deze naam kan tussen 1 en 64 alfanumerieke tekens bevatten.

Beschrijving - de beschrijving van het SNMP-beleid. De beschrijving kan 0 tot 128 alfanumerieke tekens bevatten.

Admin State - de beheerstatus van het SNMP-beleid. De status kan worden in- of uitgeschakeld. De staten zijn:

- ingeschakeld - de beheerstatus is ingeschakeld
- uitgeschakeld - de beheerstatus is uitgeschakeld

De standaardinstelling is **uitgeschakeld**.

Contact - de contactinformatie voor het SNMP-beleid.

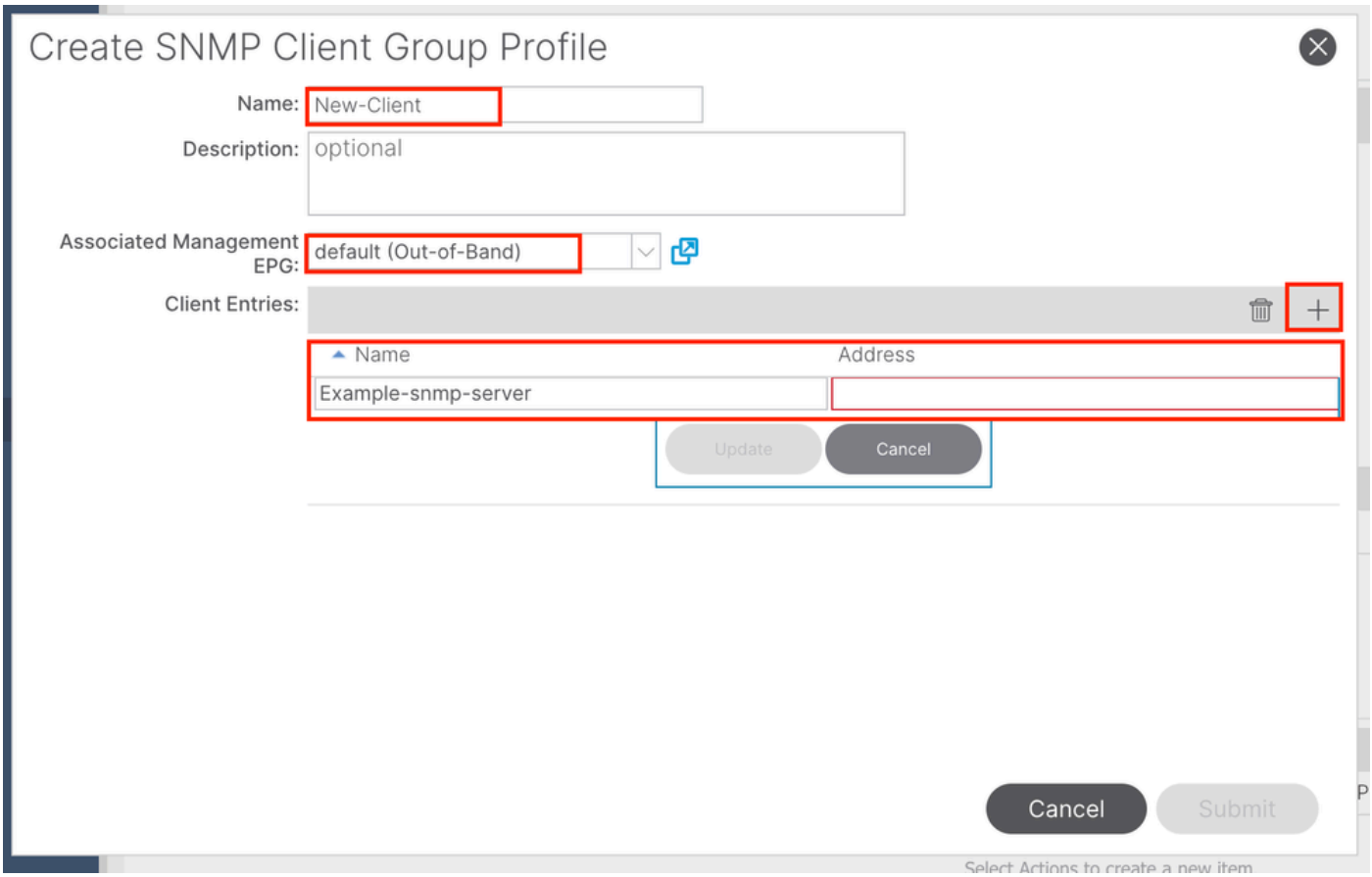
Locatie - de locatie voor het SNMP-beleid.

SNMP v3-gebruikers - het SNMP-gebruikersprofiel wordt gebruikt om gebruikers te koppelen aan SNMP-beleid voor het controleren van apparaten in een netwerk.

Community Policies - het SNMP-communityprofiel maakt toegang tot de router- of switch-statistieken voor bewaking mogelijk.

Beleidsregels clientgroep:

De volgende stap is het beleid/profiel van de Clientgroep toe te voegen. Het doel van het beleid/profiel van de Groep van de Cliënt is te bepalen welke IPs/subnets SNMP- gegevens van APICs en de switches van het weefsel kunnen trekken:



Naam - de naam van het profiel van de clientgroep. Deze naam kan tussen 1 en 64 alfanumerieke tekens bevatten.

Beschrijving - de beschrijving van het clientgroepprofiel. De beschrijving kan 0 tot 128 alfanumerieke tekens bevatten.

Associated Management End Point Group (EPG) - de voorname naam van een endpointgroep waartoe de VRF toegang heeft. De maximale ondersteunde tekenlengte is 255 ASCII-tekens. Het gebrek is de beheerhuurder out-of-band beheertoegang EPG.

Clientvermeldingen - het IP-adres van het SNMP-clientprofiel.

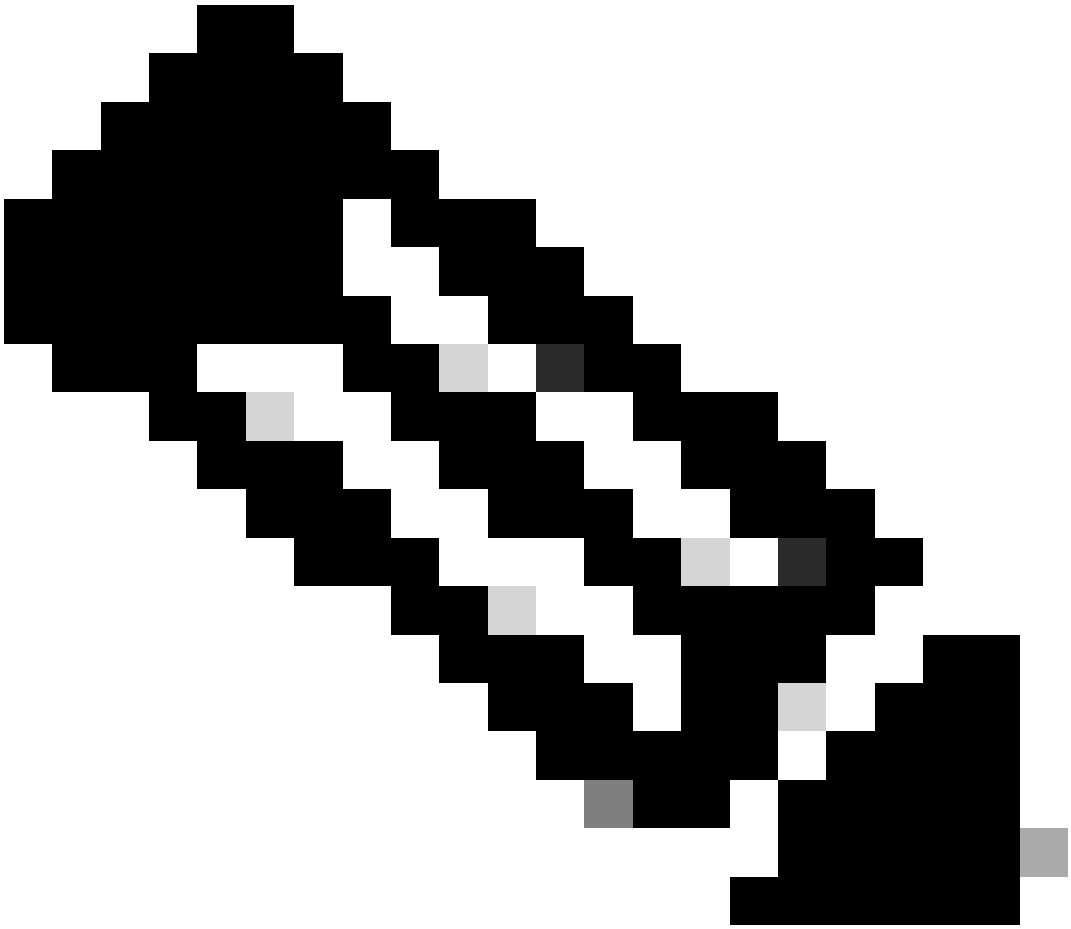
In het document wordt het beleid/profiel van de clientgroep **nieuwe client** genoemd.

In het beleid/profiel van de Clientgroep moet u het voorkeursbeheer EPG koppelen. U moet ervoor zorgen dat de door u gekozen Management

EPG over de nodige contracten beschikt om SNMP-verkeer toe te staan (UDP-poorten 161 en 162). Het standaard Out-of-Band Management EPG wordt in het document gebruikt voor demonstratiedoeleinden.

De laatste stap is het definiëren van uw **Client Entries** om specifieke IPs of volledige subnetten toegang te geven tot de pull ACI SNMP-gegevens. Er is een syntaxis voor het definiëren van een specifiek IP of een heel subnet:

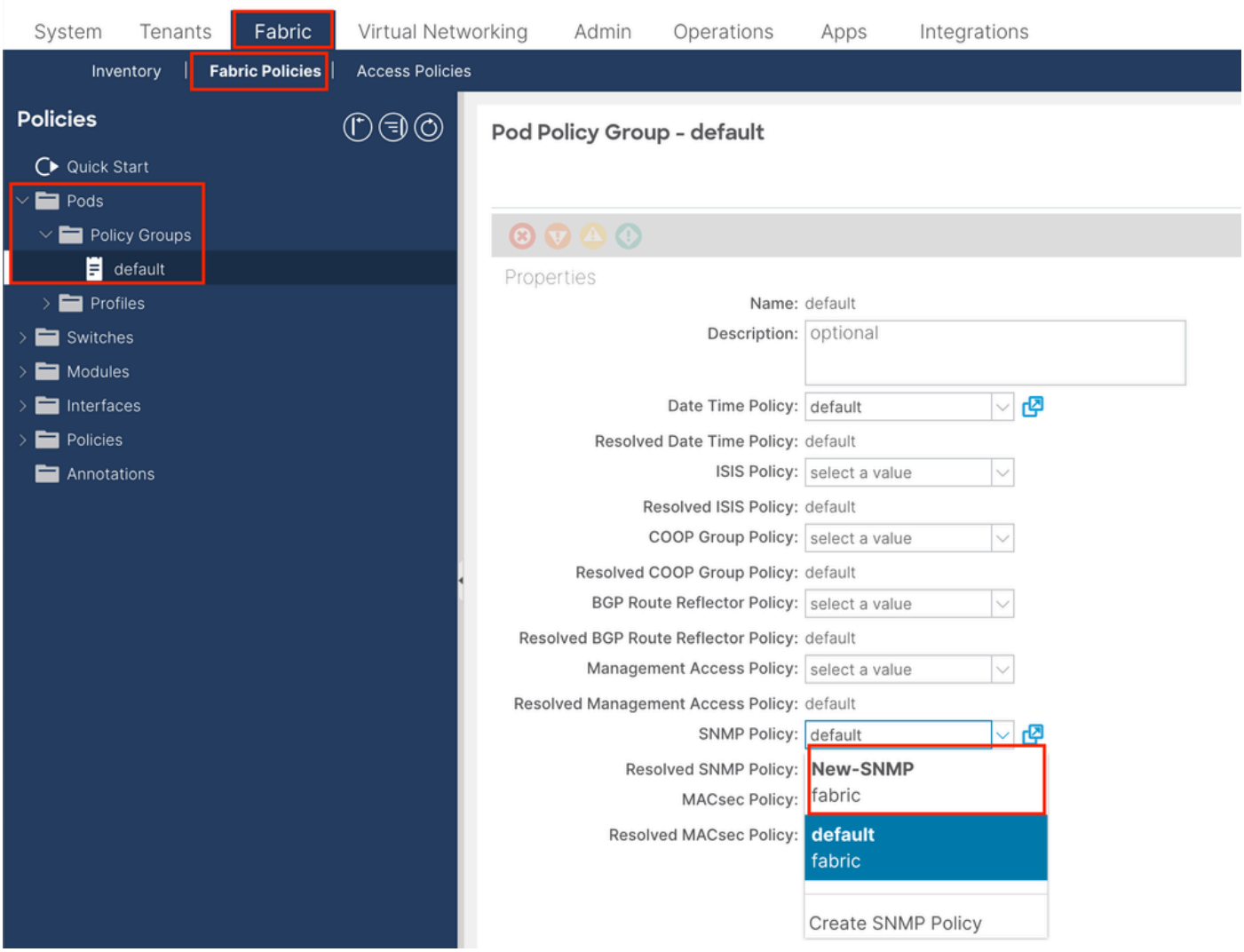
- Specifieke host IP: 192.168.1.5
- Gehele Subnet: 192.168.1.0/24



Opmerking: u kunt 0.0.0.0 niet gebruiken in het client-item om alle subnetten toe te staan (als u alle subnetten toegang tot SNMP MIB wilt geven, laat dan gewoon de client-vermeldingen leeg).

Stap 2. SNMP-beleid toepassen op de Pod Policy Group (Fabric Policy Group)

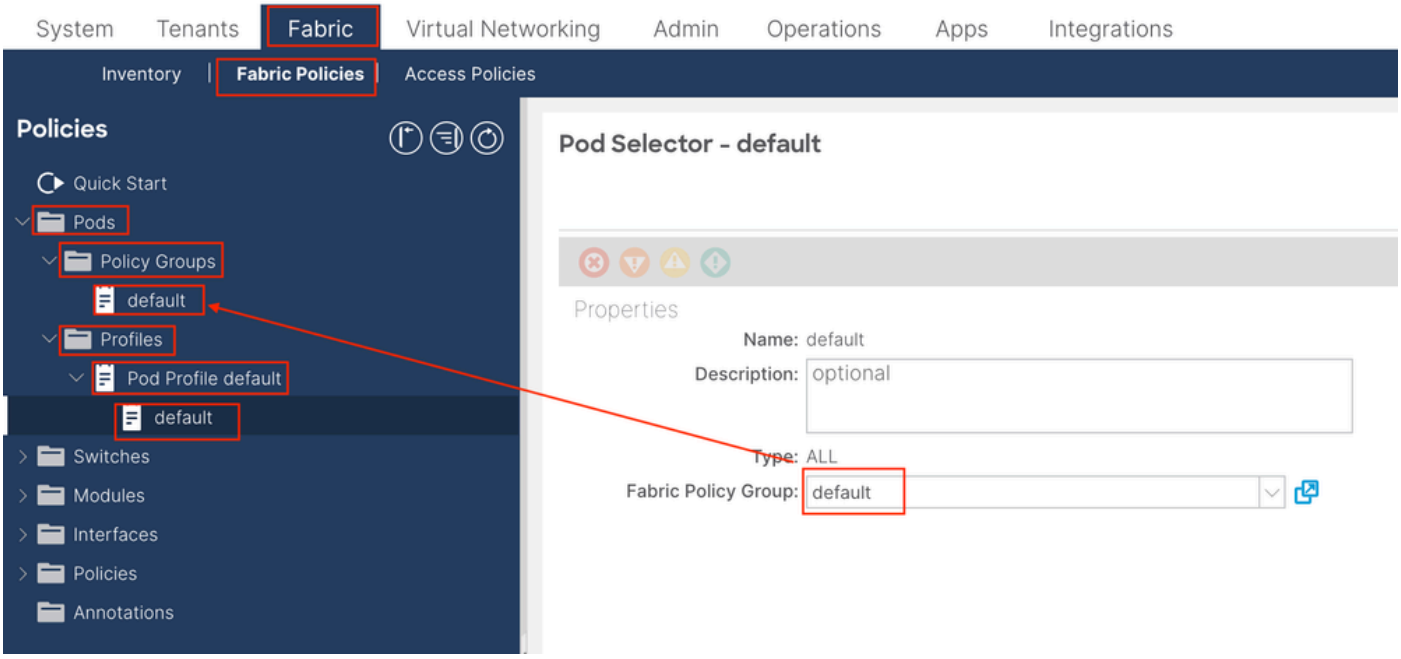
Om deze configuratie toe te passen, navigeer je naar het APIC web GUI pad; Fabric > Fabric Policies > Pods > Policy Groups > POD_POLICY_GROUP (standaard in het document).



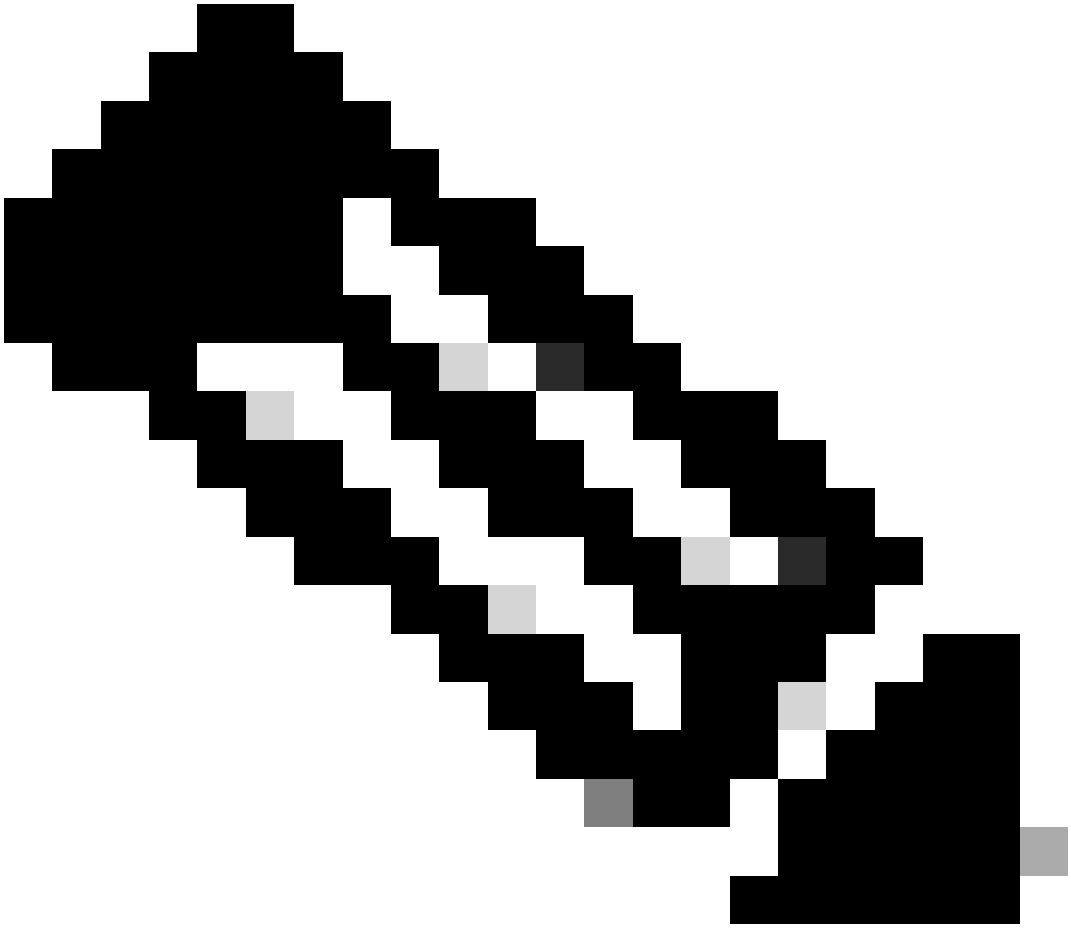
In het rechter deelvenster ziet u een veld voor SNMP-beleid. Kies in de vervolgkeuzelijst uw nieuwe SNMP-beleid en dien uw wijzigingen in.

Stap 3. Associeer de Groep van het Beleid van de Peul met het Profiel van de Peul

Gebruik in het document het standaard podprofiel voor eenvoud. Ga hiervoor naar het APIC web GUI-pad; Fabric > Fabric Policies > Pods > Profiles > POD_PROFILE (standaard in het document).



In deze fase moet u basis-SNMP voor wereldwijde MIB's configureren.

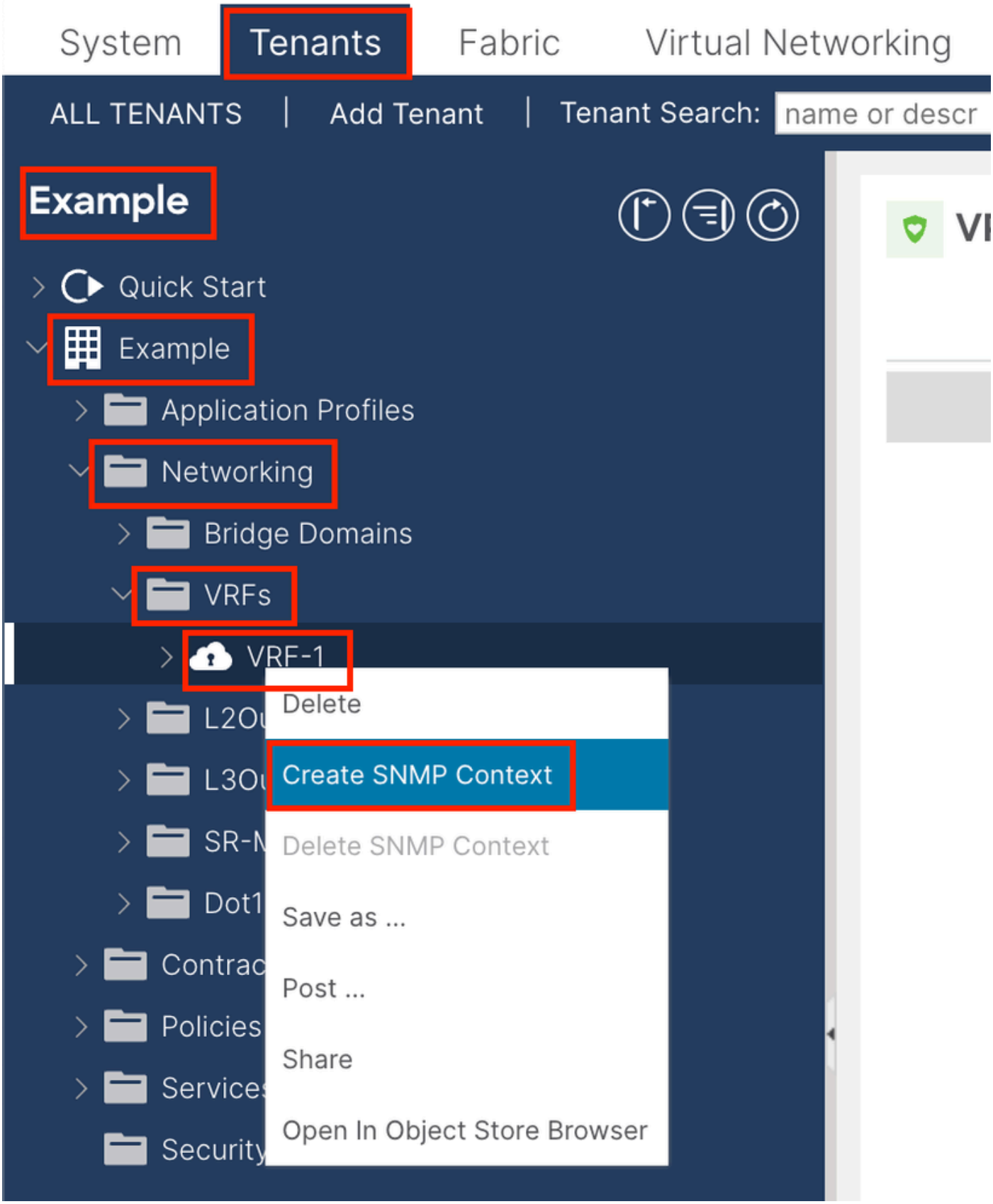


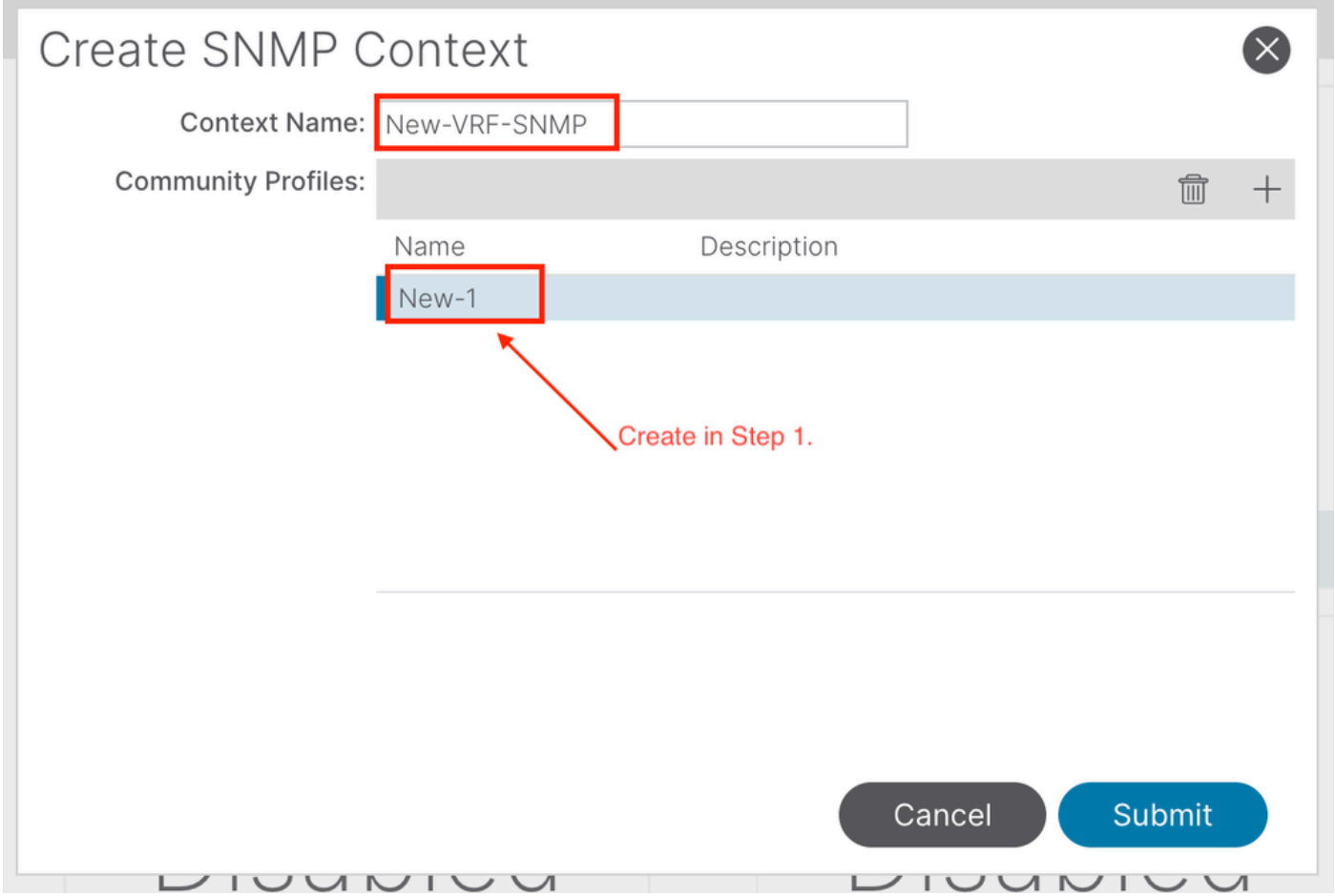
Opmerking: op dit punt zijn alle benodigde stappen (stappen 1-3) voor SNMP-configuratie voltooid en is het algemene MIB-bereik impliciet gebruikt. Hierdoor kan een SNMP-wandeling worden uitgevoerd voor elk ACI-knooppunt of APIC.

Stap 4. VRF-contextgebieden configureren

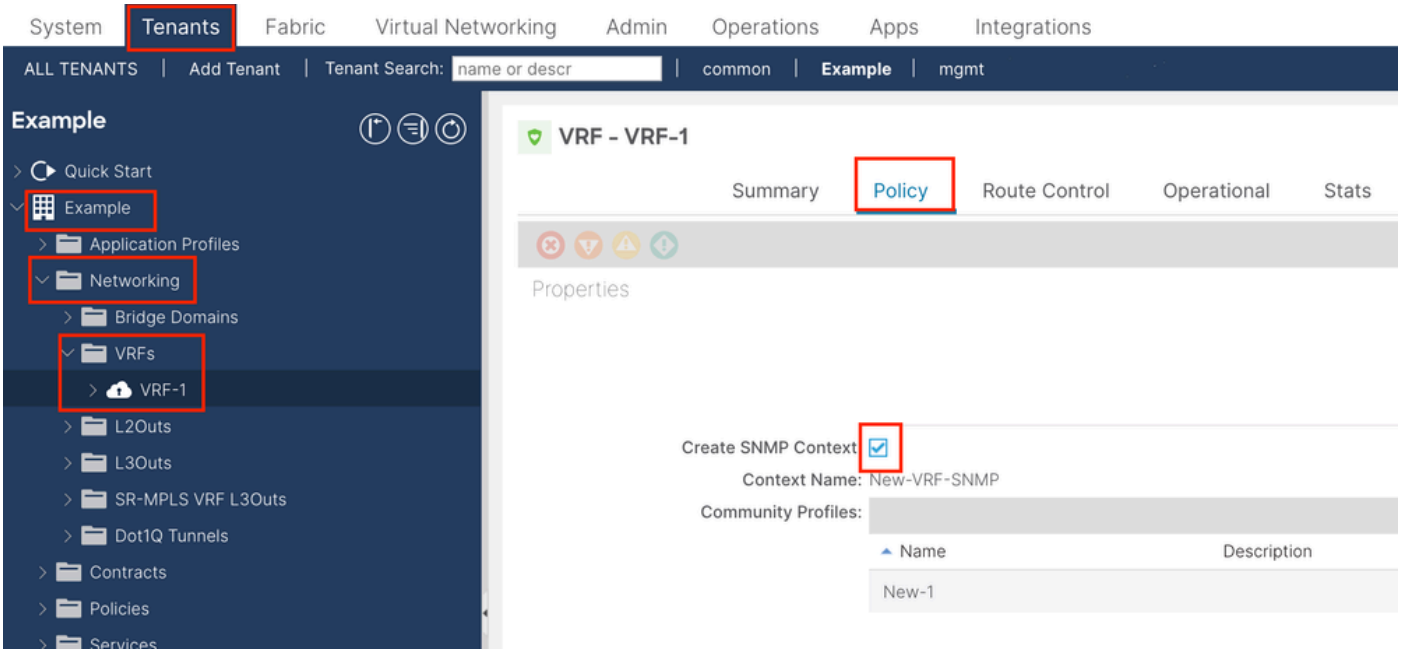
Zodra u een community-string aan een VRF-context koppelt, kan die specifieke community-string niet worden gebruikt om Global scope SNMP-gegevens te halen. Daarom is het nodig om twee SNMP community strings te maken als u zowel Global scope als VRF Context SNMP data wilt aantrekken.

In dit geval, de eerder gemaakte community strings (in Stap 1.) namelijk (**New-1**), gebruik **New-1** voor VRF context scope en **VRF-1** aangepaste VRF in **Voorbeeld** custom tenant. Ga daarom naar het APIC web GUI-pad; Tenants > 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



Nadat u de configuratie hebt ingediend, kunt u de configuratie van de SNMP-context controleren die u hebt toegepast door op de VRF met de rechtermuisknop te klikken, naar het tabblad Beleid op de VRF te navigeren en naar de onderkant van het deelvenster te bladeren:

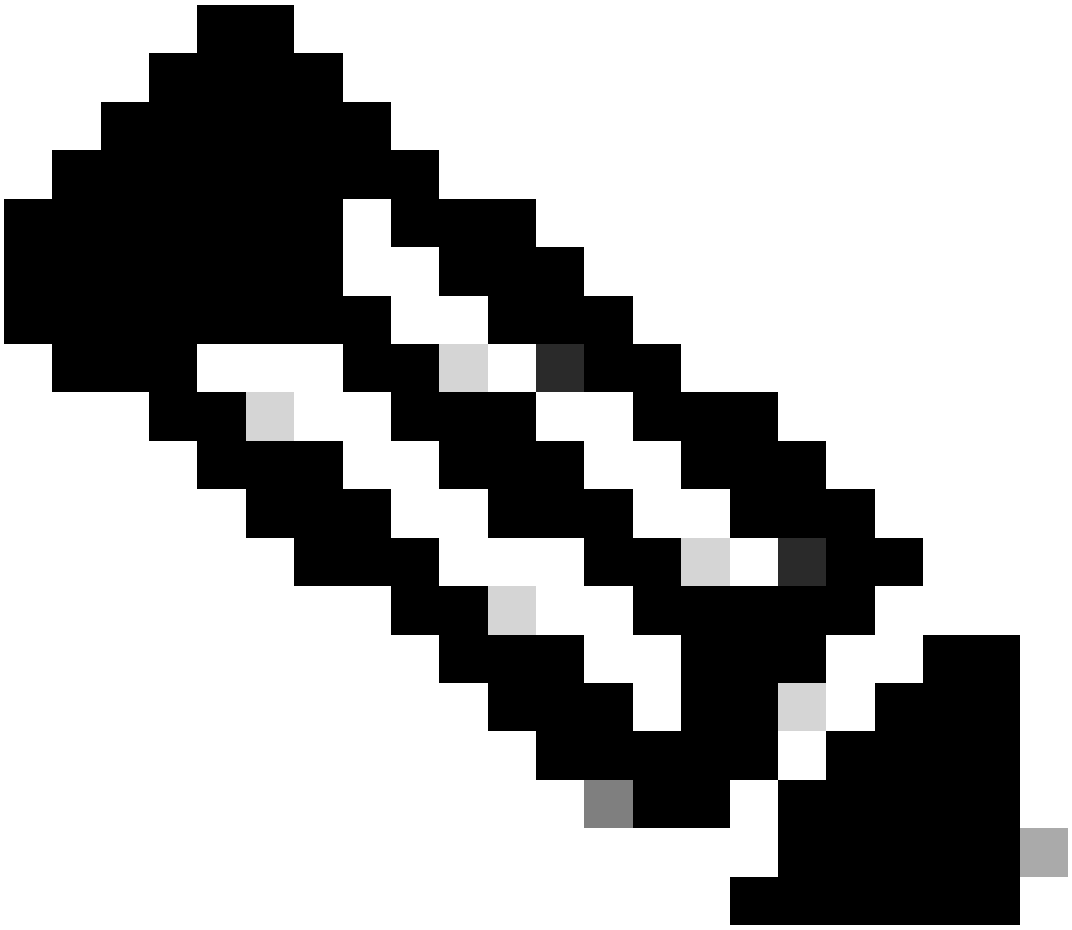


Als u een SNMP-context op een VRF wilt uitschakelen, deselecteert u het aankruisvakje **SNMP-context maken** (zie de screenshot) of klikt u met de rechtermuisknop op de VRF en kiest u **SNMP-context verwijderen**.

SNMP-TRAP's - configuratie met GUI

SNMP-TRAP's worden zonder enquête naar de SNMP-server (SNMP-bestemmingen/netwerkbeheersystemen) verzonden en de ACI-knooppunt/APIC verstuurt de SNMP-TRAP zodra de fout/gebeurtenis (gedefinieerde voorwaarde) optreedt.

SNMP-traps zijn ingeschakeld op basis van beleidsbereik onder beleid voor Access/Fabric/Tenant-bewaking. ACI ondersteunt maximaal 10 Trap-ontvangers.

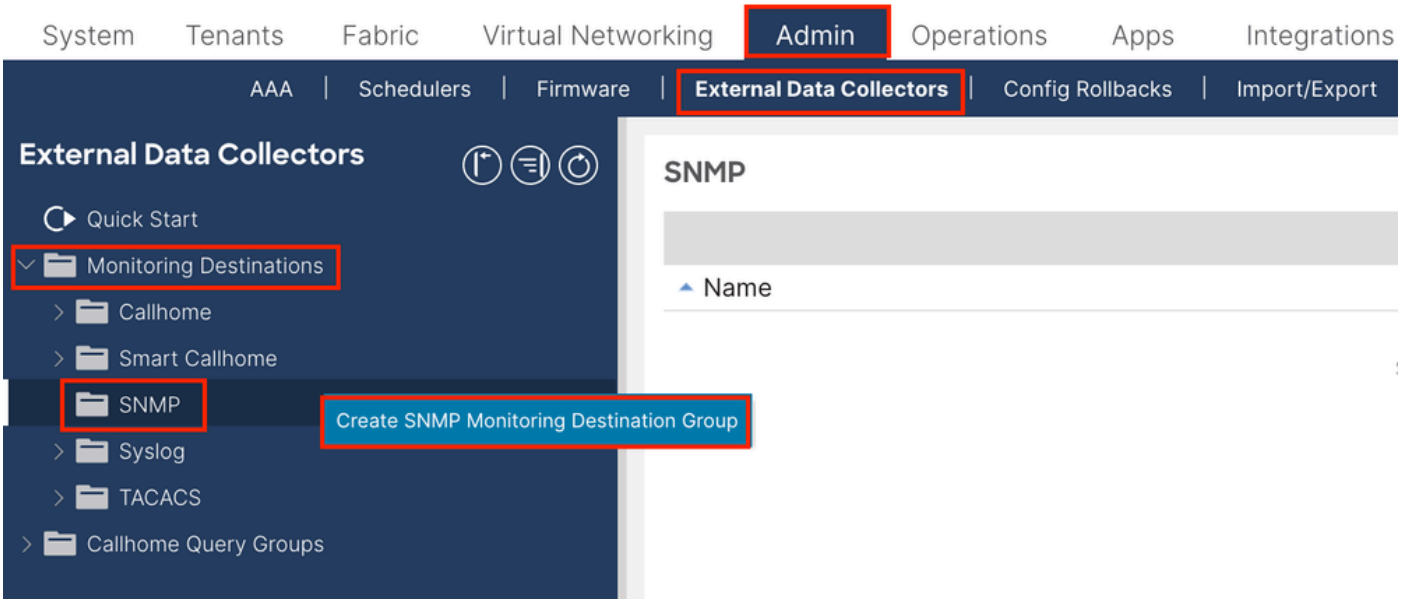


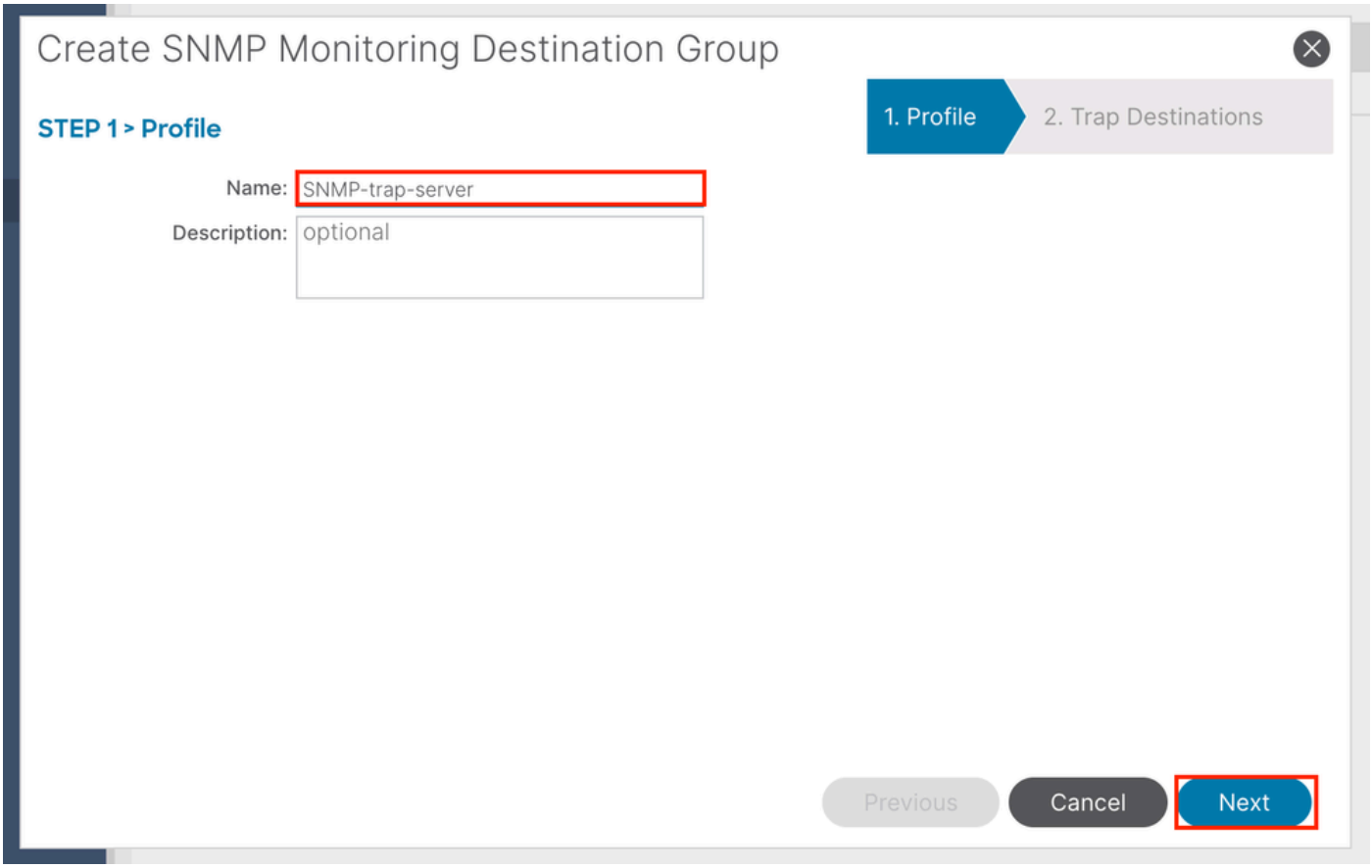
Opmerking: zonder stappen 1-3 van de vorige sectie is de SNMP TRAPs-configuratie niet genoeg. Stap 2. In SNMP-TRAP-configuratie is gerelateerd aan bewakingsbeleid voor (Access/Fabric/Tenant).

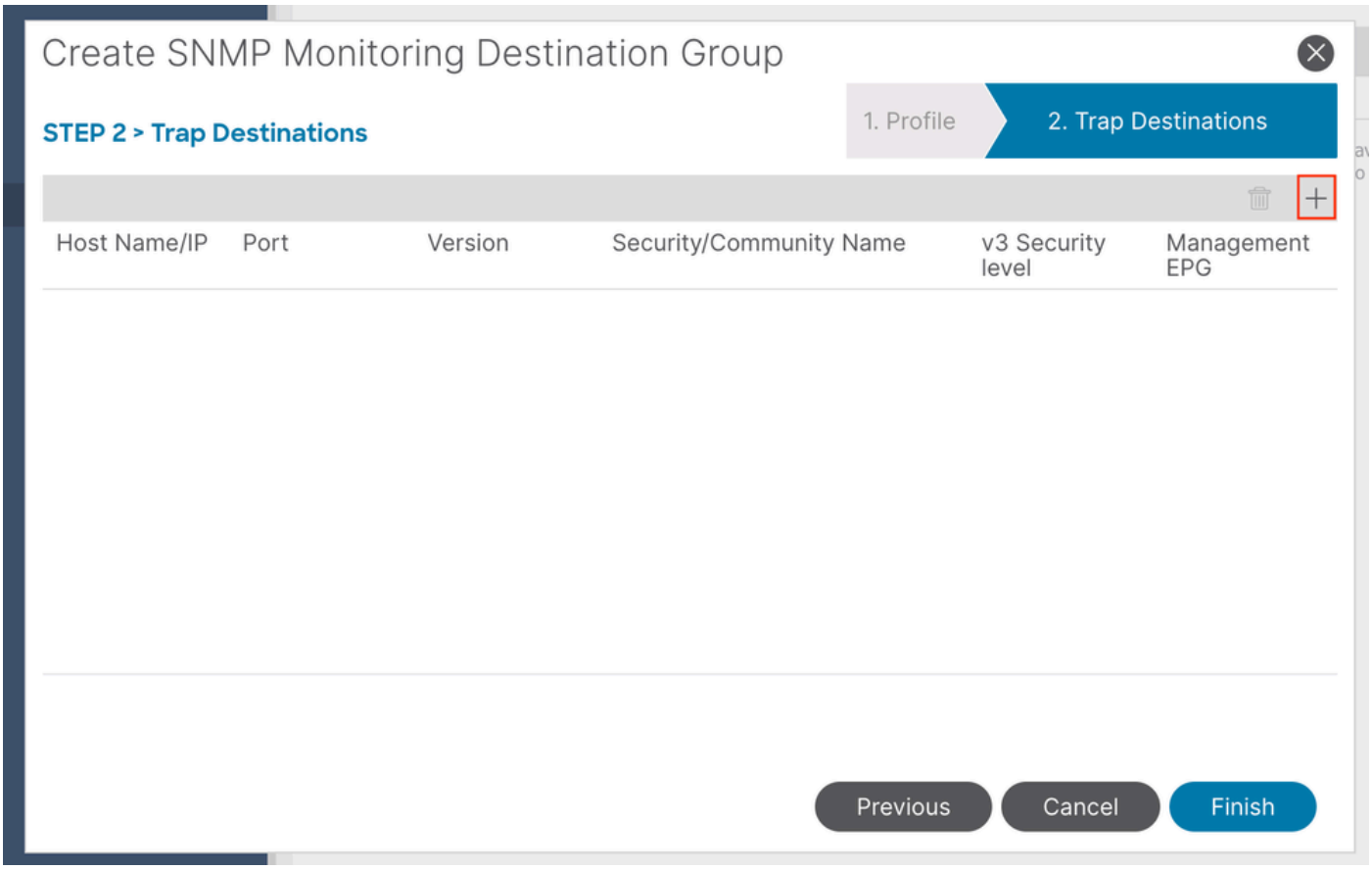
Om SNMP-TRAP's in ACI te kunnen configureren hebt u in de vorige sectie de twee stappen naast de stappen 1, 2 en 3 nodig.

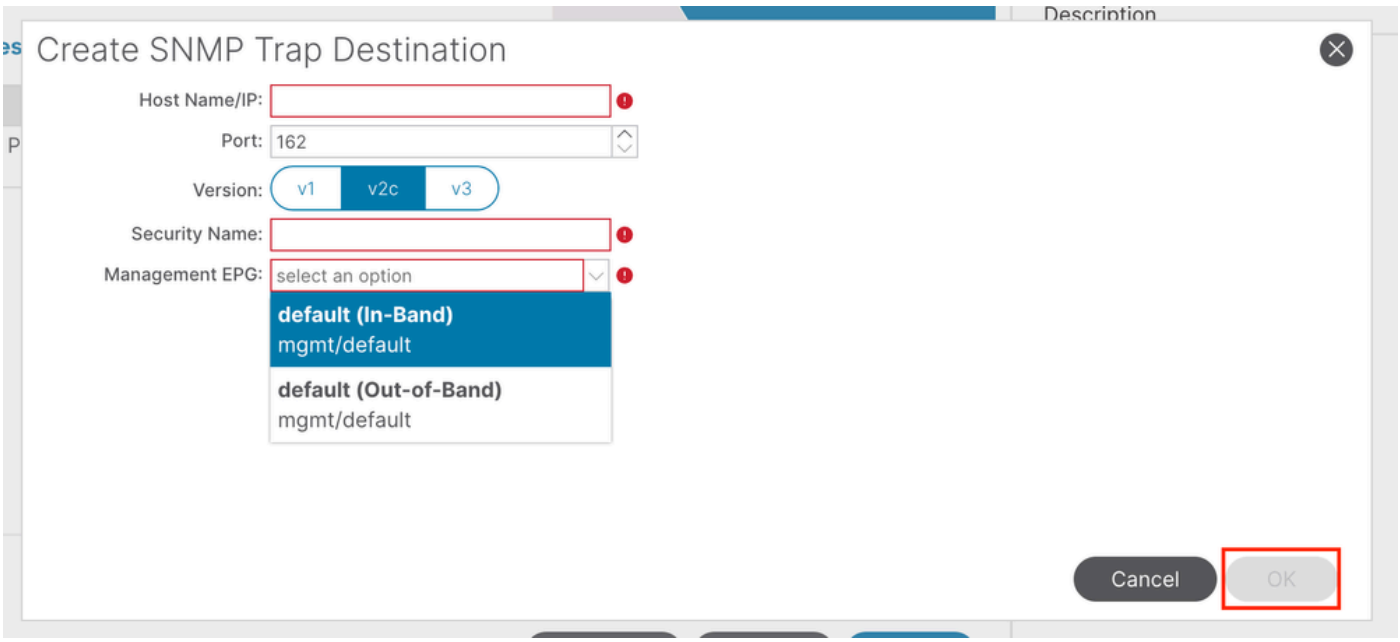
Stap 1. SNMP-TRAP server configureren

Ga daarom naar het APIC web GUI-pad; Admin > Eternal Data Collectors > Monitoring Destinations > SNMP.









Hostnaam/IP - de host voor de SNMP-trap-bestemming.

Port - de servicepoort van de SNMP-trap. Het bereik loopt van 0 (niet gespecificeerd) tot 65535; de standaardinstelling is 162.

Versie - de ondersteunde CDP-versie voor de SNMP-trap. De versie kan zijn:

-

v1 - gebruikt een community string match voor gebruikersverificatie.

- v2c - maakt gebruik van een community string match voor gebruikersverificatie.

- v3 - een interoperabel op standaarden gebaseerd protocol voor netwerkbeheer dat beveiligde toegang tot apparaten biedt door een combinatie van het authenticeren en versleutelen van frames via het netwerk.

De standaardinstelling is **v2c**.

Security Name - de naam van de doelbeveiliging van de SNMP-trap (community-naam). Het kan geen **@**symbool bevatten.

v.3 Beveiligingsniveau - het SNMPv3-beveiligingsniveau voor het SNMP-doelpad. Het niveau kan zijn:

- auth

- noauth

- priv

De standaardinstelling is **nul**.

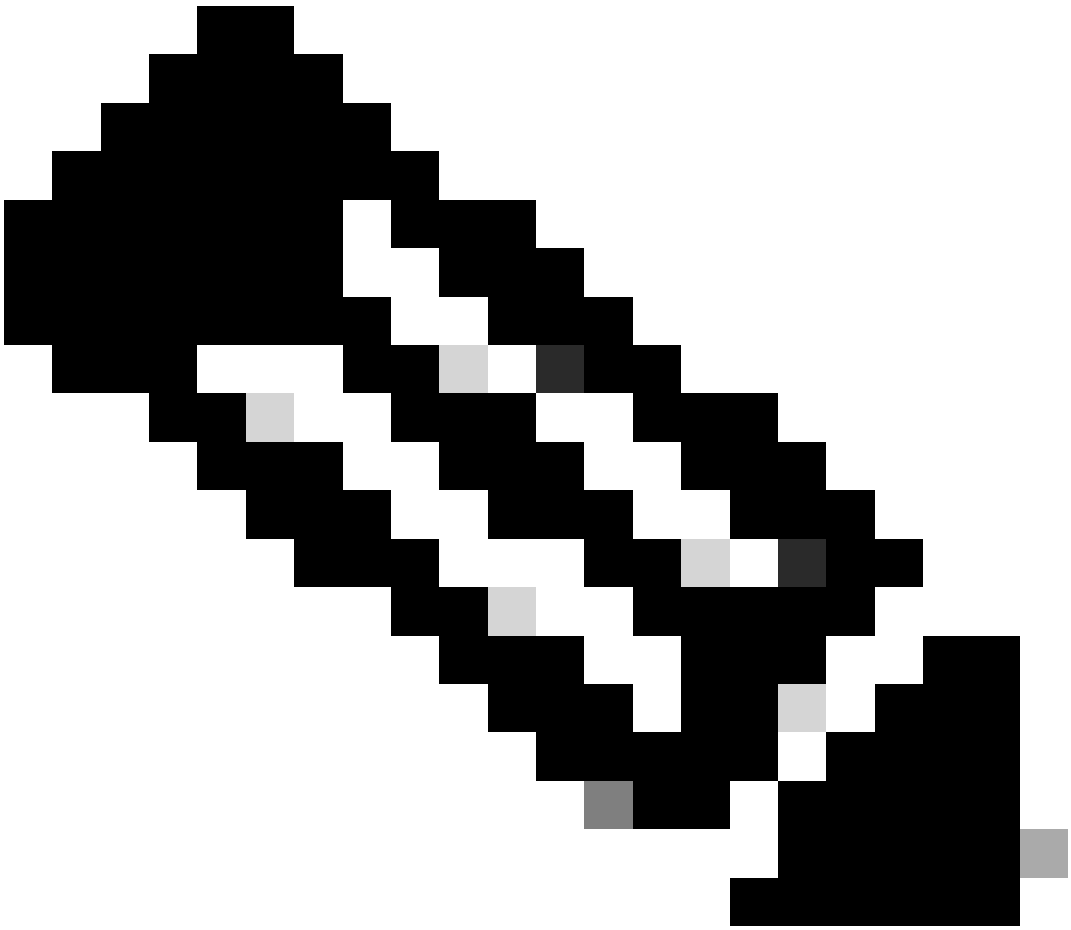
Beheer EPG - de naam van de beheerendpointgroep voor de SNMP-bestemming waarmee de externe host kan worden bereikt.

Stap 2. SNMP-TRAP-bron configureren onder bewakingsbeleid (Access/Fabric/Tenant)

U kunt een bewakingsbeleid maken met de drie toepassingsgebieden:

- Toegang - toegangspoorten, FEX, VM-controllers
- Fabric - fabricpoorten, kaarten, chassis, ventilatoren

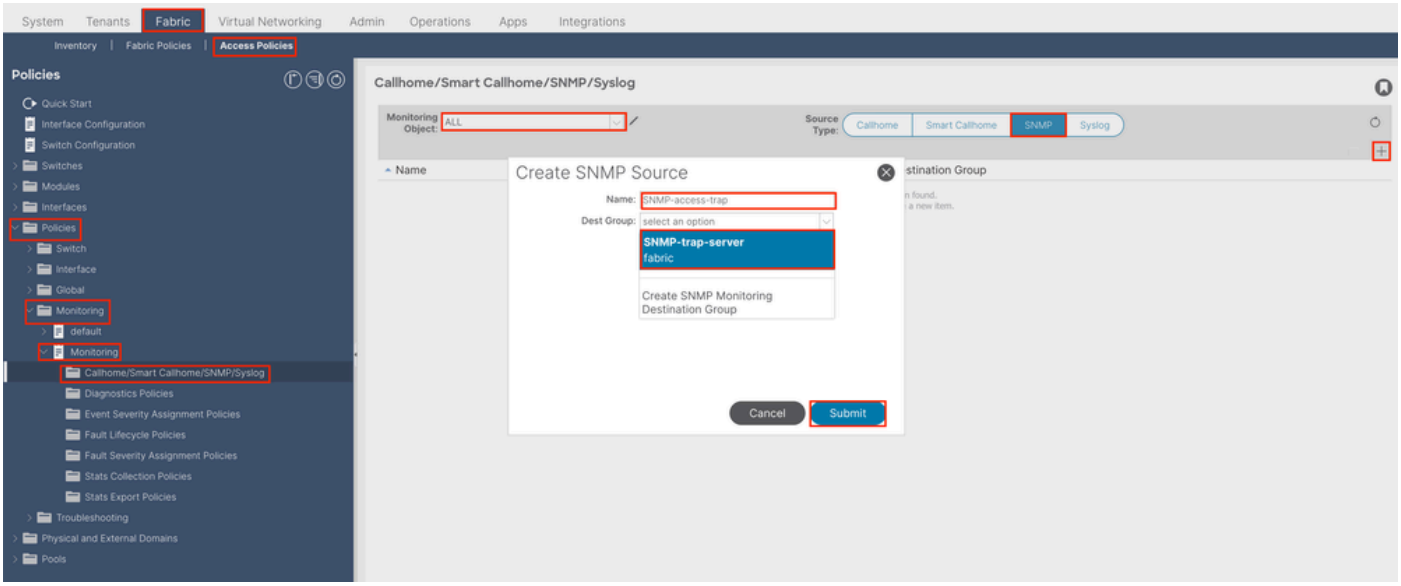
- Tenant - EPG's, toepassingsprofielen, diensten

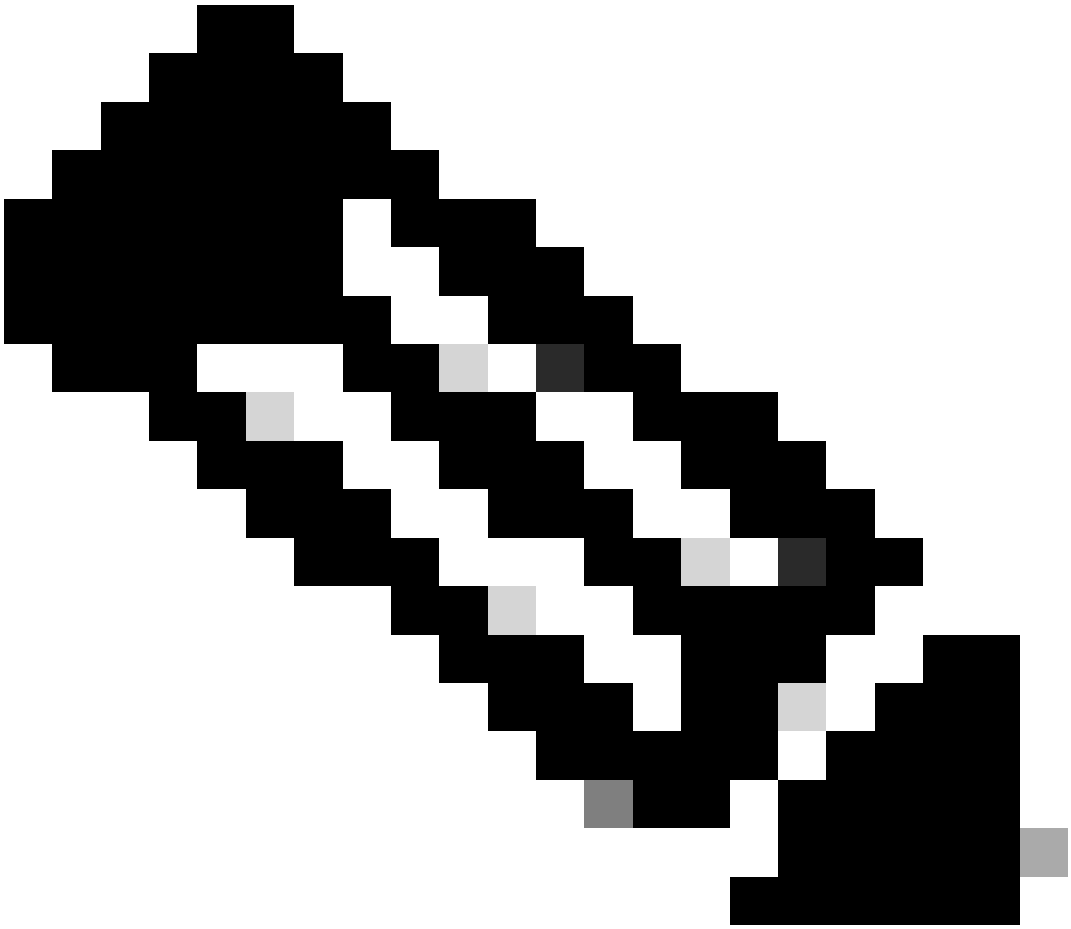


Opmerking: U kunt elke combinatie van deze kiezen om te configureren volgens uw behoeften.

Optie 1. SNMP-bron definiëren onder toegangsbeleid

Ga daarom naar het APIC web GUI-pad; Fabric > Access Polices > Polices > Monitoring > Default > Callhome/Smart Callhome/SNMP/Syslog/TACACS.

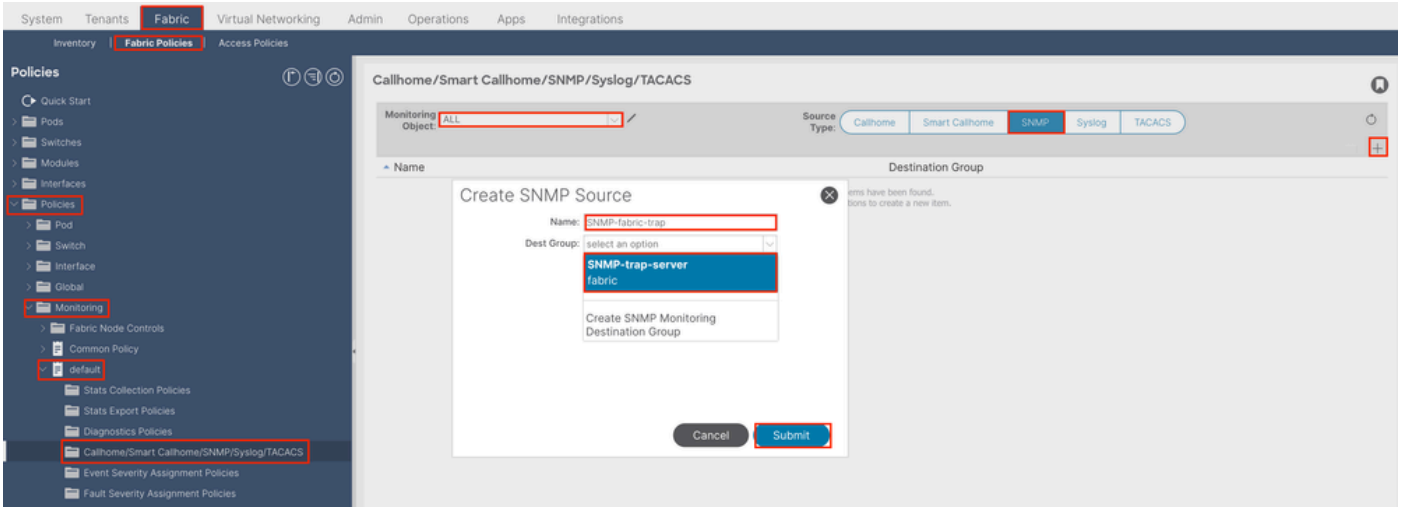

System
Tenants
Fabric
Virtual Networking
Admin
Operations
Apps
Integrations
Inventory
Fabric Policies
Access Policies
Policies
Quick Start
Interface Configuration
Switch Configuration
Switches
Modules
Interfaces
Policies
Switch
Interface
Global
Monitoring
default
Monitoring
Callhome/Smart Callhome/SNMP/Syslog
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



Opmerking: u kunt een op maat gemaakt bewakingsbeleid gebruiken (indien geconfigureerd) in plaats van het standaardbeleid. Gebruik hier het standaardbeleid. U kunt aangeven welk controleobject u moet bewaken. Alle zijn hier gebruikt.

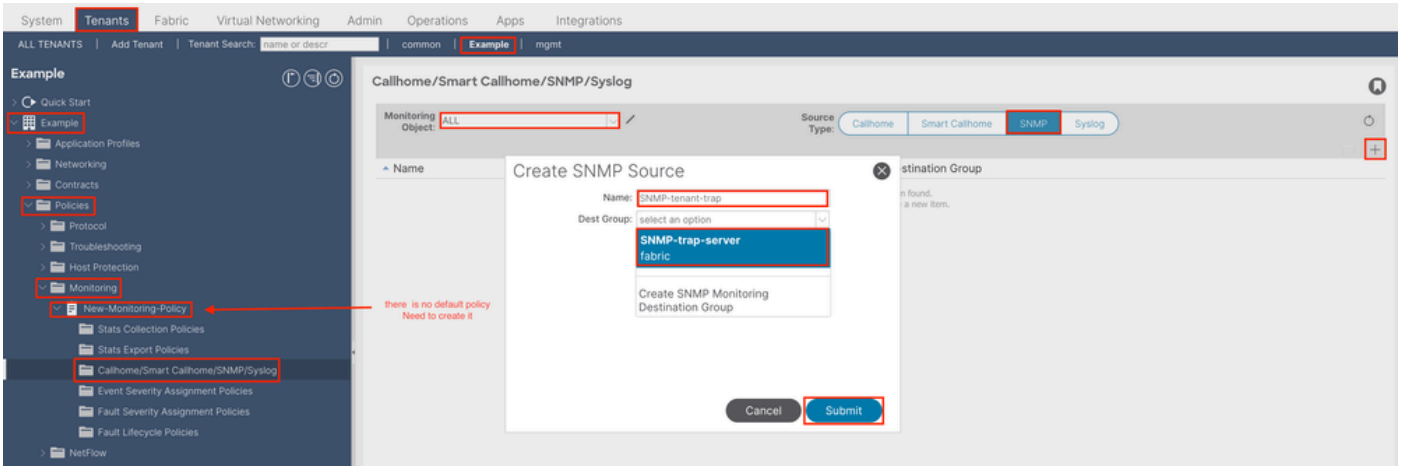
Optie 2. SNMP-bron definiëren onder fabric-beleid

Ga daarom naar het APIC web GUI-pad; Fabric > Fabric Polices > Polices > Monitoring > Default > Callhome/Smart Callhome/SNMP/Syslog/TACACS.



Optie 3. SNMP-bron definiëren onder huurbeleid

Ga daarom naar het APIC web GUI-pad; Tenant > (Tenant Name) > Polices > Monitoring > (Custom monitoring policy) > Callhome/Smart Callhome/SNMP/Syslog/TACACS.



Verifiëren

Opdracht Snelpad gebruiken om te controleren

Kijk eerst eens naar het halen van SNMP-gegevens uit de wereldwijde scope van een switch. Het gebruik van de snmpwalk commando kan

precies dat doen; snmpwalk -v 2c -c New-1 x.x.x.x.

Dit opgesplitste commando vertegenwoordigt:

snmpwalk = de snmpwalk uitvoerbaar geïnstalleerd op MacOS/Linux/Windows

-v = Specificeert de versie van SNMP die u wilt gebruiken

2c= Specificaties die SNMP versie 2c gebruiken

-c= Specificeert dat een bepaalde community-string

New-1= De community-string wordt gebruikt voor het ophalen van wereldwijde scope SNMP-gegevens

x.x.x.x= Het IP-adres voor out-of-band beheer van mijn switch

Opdrachtresultaat:

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

In de gegnipte opdrachtoutput kunt u zien dat de snmpwalk succesvol is en dat er hardware-specifieke informatie werd verzameld. Als u de snmpwalk verder laat gaan, ziet u de hardware-interfacenamen, beschrijvingen, enzovoort.

Ga nu verder met het ophalen van VRF-context SNMP-gegevens, eerder gemaakte SNMP-contexten, **New-VRF-SNMP** voor VRF's met behulp van de SNMP-community-string, **New-1**.

Aangezien dezelfde community-string wordt gebruikt, **New-1**, over twee verschillende SNMP-contexten, moet u specificeren van welke SNMP-context u de SNMP-gegevens wilt halen. Er is de snmpwalk syntaxis die u moet gebruiken om een bepaalde SNMP Context te specificeren; snmpwalk -v 2c -c New-1@New-VrF-SNMP 10.x.x.x.

U kunt zien dat om uit een specifieke SNMP Context te trekken, u het formaat gebruikt:
COMMUNITY_NAME_HERE@SNMP_CONTEXT_NAME_HERE .

Opdrachten op CLI-display gebruiken

Over APIC:

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

Aan de Switch:

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

CLI-moquery-opdrachten gebruiken

Op APIC/Switch:

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

CLI-kattenopdrachten gebruiken

Over APIC:

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

Problemen oplossen

Controleer het SNMP-proces

Aan de Switch:

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

Over APIC:

```
ps aux | grep snmp
```

Als het proces normaal is, neemt u contact op met Cisco TAC voor meer assistentie.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.