Problemen met SNMP oplossen in Cisco ACI Fabric

Inleiding

In dit document wordt beschreven hoe u SNMP configureert, verifieert en oplost in Cisco ACI for ACI release 5.x en hoger. Het omvat het SNMP-beleidsmodel, vereiste beheercontracten, trapconfiguratie, bedrijfsverificatie met behulp van CLI- en Managed Object (MO)-query's en gestructureerde werkstromen voor probleemoplossing voor de meest voorkomende storingsscenario's voor switches van bladeren/wervelkolom en APIC-controllers.

Achtergrondinformatie

Het materiaal in dit document is afkomstig van de interne technologie SNMP van het Cisco ACI Solutions Delivery Team in ACI: Overview, Configuration, Troubleshooting, and Caveats/Issues geschreven door Tomas de Leon, aangevuld met de Cisco APIC System Management Configuration Guide (Release 5.x) en de Cisco ACI MIB Quick Reference Guide.

Overzicht

SNMP-architectuur in ACI

SNMP (Simple Network Management Protocol) is een op UDP gebaseerd protocol dat netwerkbeheer en -bewaking regelt. In ACI werkt SNMP onafhankelijk op elke beheerde entiteit. Elke switch, switch van de wervelkolom en APIC-controller is zijn eigen SNMP-agent - elk moet onafhankelijk worden gepolst of bewaakt.

ACI ondersteunt de volgende SNMP-mogelijkheden:

- Leesbewerkingen (Get, GetNext, BulkGet, Walk) — ondersteund op switches van bladeren/ruggengraat en APIC-controllers.
- Meldingen (Traps) — SNMPv1-, v2c- en v3-traps worden ondersteund op switches van bladeren/ruggengraat en APIC-controllers.
- SNMPv3 — ondersteund op switches van bladeren/ruggengraat en APIC-controllers.
- Schrijfbewerkingen (instellen) — NIET ondersteund op een ACI-apparaat.

- IPv6 — SNMP wordt alleen ondersteund via IPv4.

Opmerking: in een APIC-cluster biedt elk APIC MIB-objecten die lokaal op zichzelf staan. U moet elke APIC onafhankelijk peilen; er is geen clusterbrede SNMP-aggregatie. Op dezelfde manier moet elke blad- en wervelkolom-switch onafhankelijk worden onderzocht.

SNMPD-architectuur op de APIC

De APIC voert het snmpd-proces uit, dat twee interne componenten heeft:

- Agent — Een open-source net-snmp-agent (versie 5.7.6 of hoger) die SNMP-protocolverwerking en sessiebeheer afhandelt.
- DME (Data Model Engine) — Interfaces met de APIC Management Information Tree (MIT) om beheerde objecten (MO's) te lezen en MO-kenmerken te vertalen naar de SNMP Object-indeling. SNMP-traps worden gegenereerd op basis van gebeurtenissen en fouten die op MO's zijn gemaakt.

SNMP-beleidsmodel en implementatieketen

ACI gebruikt een beleidsgestuurd model voor SNMP. De SNMP-configuratie wordt geabstraheerd als een snmpPol Managed Object en moet worden gekoppeld aan de Pod Policy Group van de verbinding voordat deze wordt geïmplementeerd in een node. De volledige implementatieketen is:

1. SNMP-beleid (`snmpPol`) — definieert beheerdersstatus, communitystrings, clientgroepsbeleid (ACL's) en SNMPv3-gebruikers.
2. Pod Policy Group — verwijst naar het SNMP-beleid samen met ander beleid op pod-niveau (BGP, ISIS, NTP, enz.).
3. Pod Profile Selector — past de Pod Policy Group toe op de fabric pods.

Bovendien vereist de SNMP-trapconfiguratie het volgende:

1. SNMP Monitoring Destination Group (`snmpGroup`) — definieert trapbestemmingshosts, poort, SNMP-versie en community.
2. Bronnen voor bewaking (`snmpSrc`) — koppel de bestemmingsgroep aan drie verschillende beleidsgebieden voor bewaking: Fabric Default, Fabric Common Policy en Access Policy Default.

Voor APIC-knooppunten zijn beheercontracten vereist die UDP-poort 161 (SNMP-verzoeken) en UDP-poort 162 (SNMP-traps) toestaan. Blad- en wervelkolomknooppunten vereisen ook de juiste regels voor kieptabellen, die automatisch worden geprogrammeerd wanneer het beleid voor de

clientgroep wordt geconfigureerd.

Ondersteunde MIB's

De MIB's die op de APIC worden ondersteund, zijn onder meer:

- Entiteit MIB — Fysieke tabel
- Cisco Entity Ext MIB — PhysicalProcessorTable, LEDTable
- Cisco Entity FRU Control MIB — PowerSupplyGroupTable, PowerStatusTable, FanTrayStatusTable, PhysicalTable
- Cisco Entity Sensor MIB — SensorValueTable, SensorThresholdTable
- Cisco Process MIB — CPUTotalTable, ProcessTable, ProcessExtRevTable, ThreadTable

Leaf- en spine-switches stellen standaard NX-OS MIB's bloot, waaronder IF-MIB, IP-MIB, CISCO-CDP-MIB, CISCO-ENTITY-QFP-MIB en de volledige CISCO-ENTITY-FRU-CONTROL-MIB-suite.

SNMP-traps gegenereerd op de APIC zijn onder andere: cefcFRUInserted, cefcFRURemoved, cefcFanTrayStatusChange, cefcModuleStatusChange, entSensorThresholdNotification, cefcPowerStatusChange, cpmCPURisingThreshold, `cpmCPUFallingThreshold`.

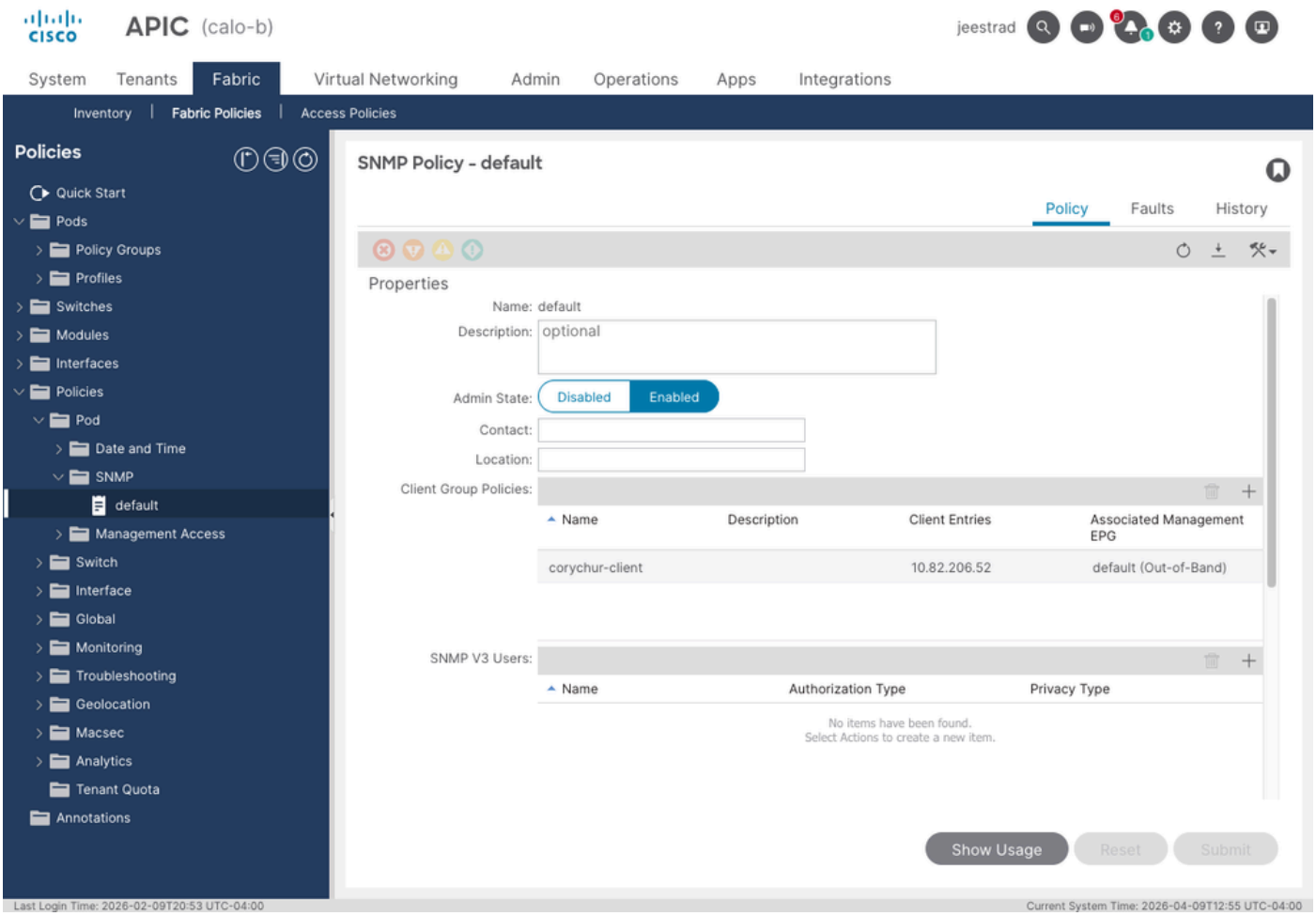
SNMP configureren in ACI

✎ Opmerking: deze sectie bevat een samenvatting van de configuratieworkflow als context voor de volgende secties voor verificatie en probleemoplossing. Raadpleeg de Cisco APIC System Management Configuration Guide voor uitgebreide configuratieprocedures.

Stap 1: Het SNMP-beleid configureren

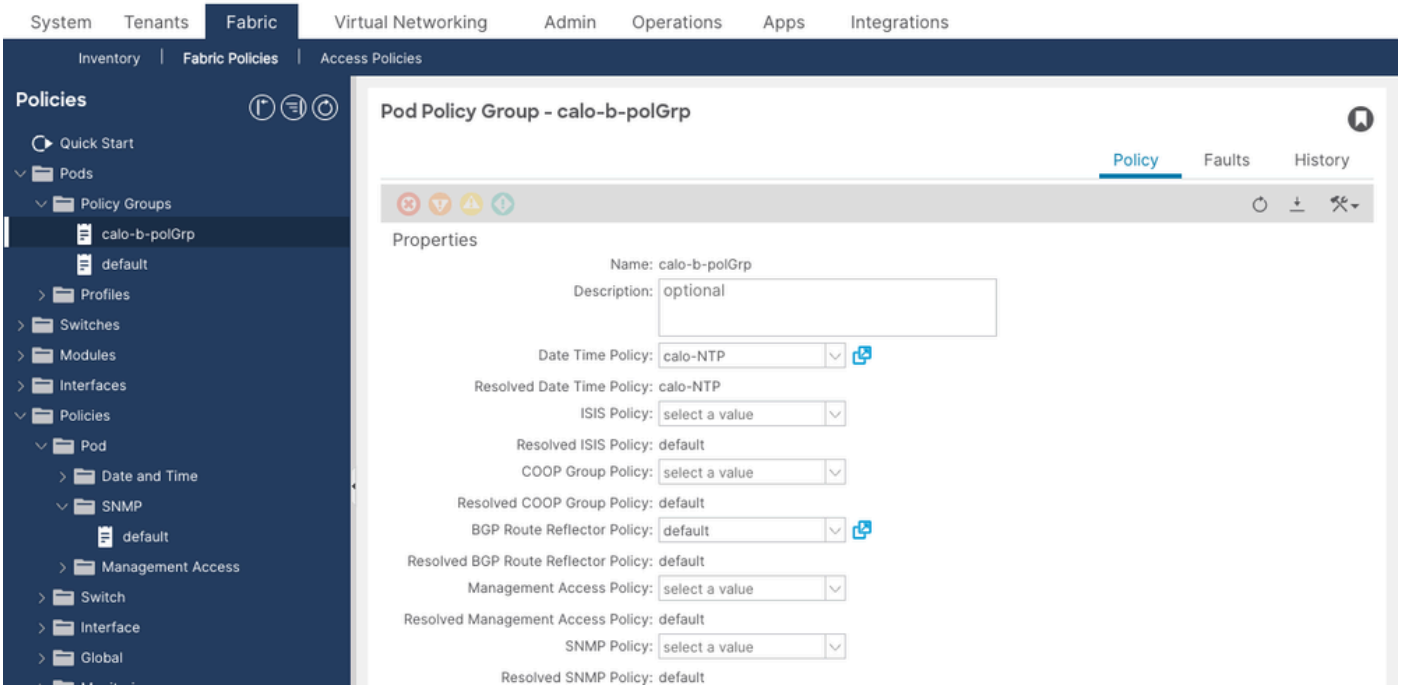
Navigeer naar Fabric > Fabric Policies > Policies > Pod > SNMP. Selecteer (of maak) het SNMP-beleid, meestal standaard genoemd. Configureren:

- Beheerstatus — ingesteld op Ingeschakeld.
- Communitybeleid — voeg de communitystring toe die wordt gebruikt door uw NMS.
- Beleid voor clientgroepen — definieer een of meer clientgroepsprofielen, waarbij elk de toegestane SNMP-client-IP's en de bijbehorende beheer-EPG (Out-of-Band of In-Band) specificeert.
- SNMPv3-gebruikers — als u SNMPv3 gebruikt, voegt u hier gebruikers toe met verificatie- en privacyparameters.



Stap 2: Koppel het SNMP-beleid aan de POD-beleidsgroep

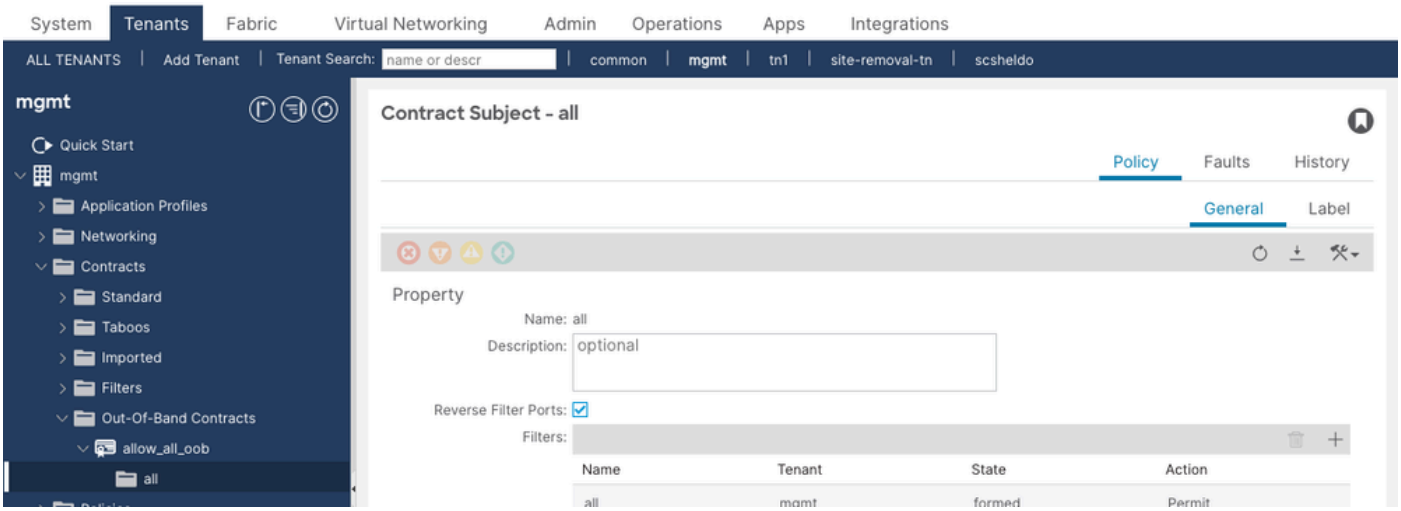
Navigeer naar Fabric > Fabric Policies > Pods > Policy Groups. Selecteer de actieve pod-beleidsgroep (meestal standaard genoemd). Stel het veld SNMP-beleid in om te verwijzen naar het SNMP-beleid dat is gemaakt in stap 1. Controleer of in het veld Opgelost SNMP-beleid de juiste naam voor het beleid wordt weergegeven.



Navigeer vervolgens naar Verbinding > Verbindingsbeleid > Pods > Profielen, vouw het standaardprofiel van de pod uit en bevestig dat de actieve selector verwijst naar de juiste groep van het pod-beleid.

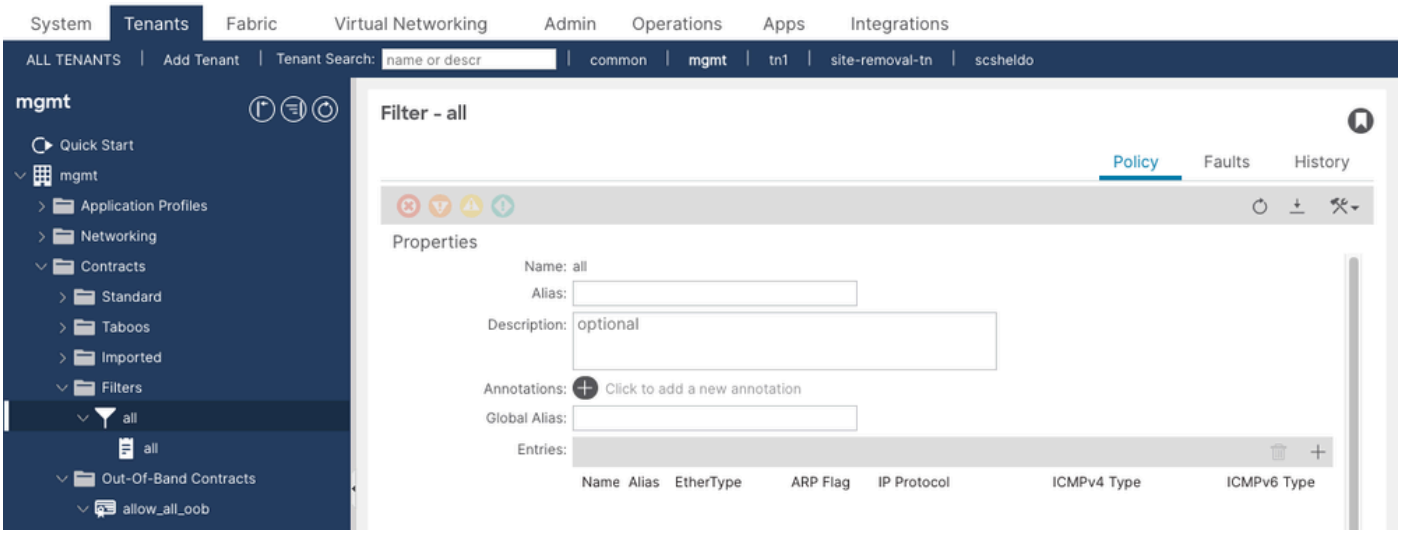
Stap 3: Beheercontracten configureren voor UDP-poort 161

Navigeer naar Huurders > beheer > Contracten > Out-Of-Band Contracten. Controleer of de onderwerpregel van het actieve OOB-contract verwijst naar een filtervermelding die UDP-poort 161 (SNMP-verzoeken) toestaat. Zonder dit contract op de APIC worden alle SNMP GET/WALK-pakketten stilletjes weggelaten.



De filteritems die aan het contractonderwerp zijn gekoppeld, moeten een vermelding bevatten met EtherType IP, Protocol UDP en bestemmingspoort 161. Het bovenstaande voorbeeld toont een

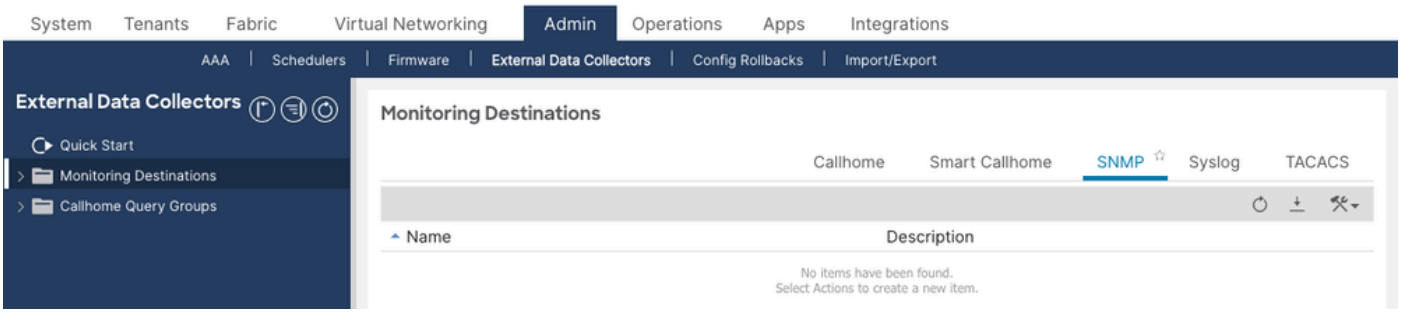
allow-all (niet-gespecificeerd protocol) filter - dit maakt SNMP mogelijk, maar is breder dan aanbevolen voor productie. Een speciale SNMP-filtervermelding met specifieke UDP/161- en UDP/162-vermeldingen heeft de voorkeur.



Opmerking: in eerdere ACI-firmwareversies waren bepaalde poorten altijd open op blad- en wervelkolomknooppunten en was er geen beheercontract vereist voor SNMP. In ACI 5.x is het contract vereist voor APIC-knooppunten. Blad- en wervelkolomknooppunten gebruiken iptables-regels die zijn afgeleid van het beleid van de clientgroep in plaats van beheercontracten.

Stap 4: SNMP-trapbestemmingen configureren

Navigeer naar Beheer > Externe gegevensverzamelaars > Bewaking van bestemmingen > SNMP. Klik met de rechtermuisknop en selecteer SNMP Monitoring Destination Group maken. Het tabblad SNMP toont alle geconfigureerde doelgroepen. Een lege tabel betekent dat er nog geen trapbestemmingen zijn geconfigureerd.



Definiëren:

- Groepsnaam

- Trap-bestemmingen: hostnaam/IP, UDP-poort (standaard 162), SNMP-versie, community-tekenreeks en beheer-EPG

Stap 5: Controlebronnen configureren

Monitoringbronnen koppelen de SNMP-bestemmingsgroep aan het monitoringbeleid dat bepaalt welke gebeurtenissen en fouten vallen genereren. U moet een controlebron configureren op alle drie van de volgende locaties, anders worden traps van sommige knooppunttypen niet verzonden:

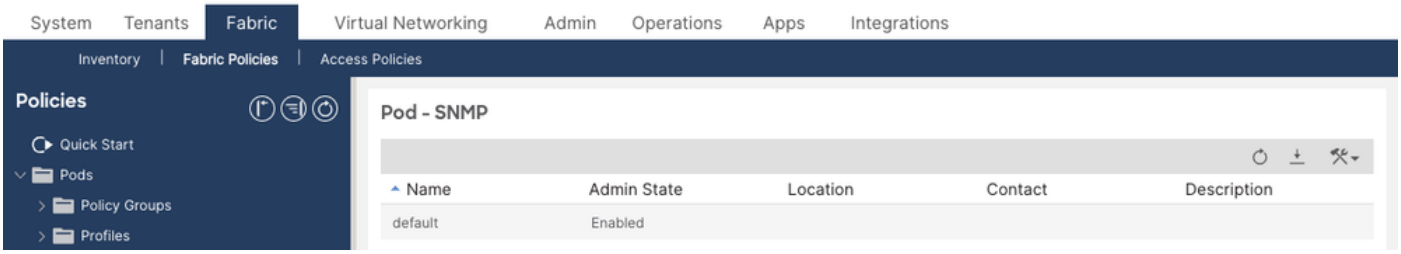
- Stof > Verbindingsbeleid > Beleid > Controle > Standaard > Callhome/Smart Callhome/SNMP/Syslog/TACACS (dekt gebeurtenissen in de infrastructuur van de fabric)
- Stof > Verbindingsbeleid > Beleid > Controle > Gemeenschappelijk beleid > Callhome/Smart Callhome/SNMP/Syslog/TACACS (dekt algemene gebeurtenissen voor de hele fabric)
- Fabric > Toegangsbeleid > Beleid > Controle > Standaard > Callhome/Smart Callhome/SNMP/Syslog (dekt toegangs-/infrastructuurgebeurtenissen)

Selecteer op elke locatie SNMP als brontype en maak een nieuwe SNMP-bron die verwijst naar de bestemmingsgroep die in stap 4 is gemaakt.

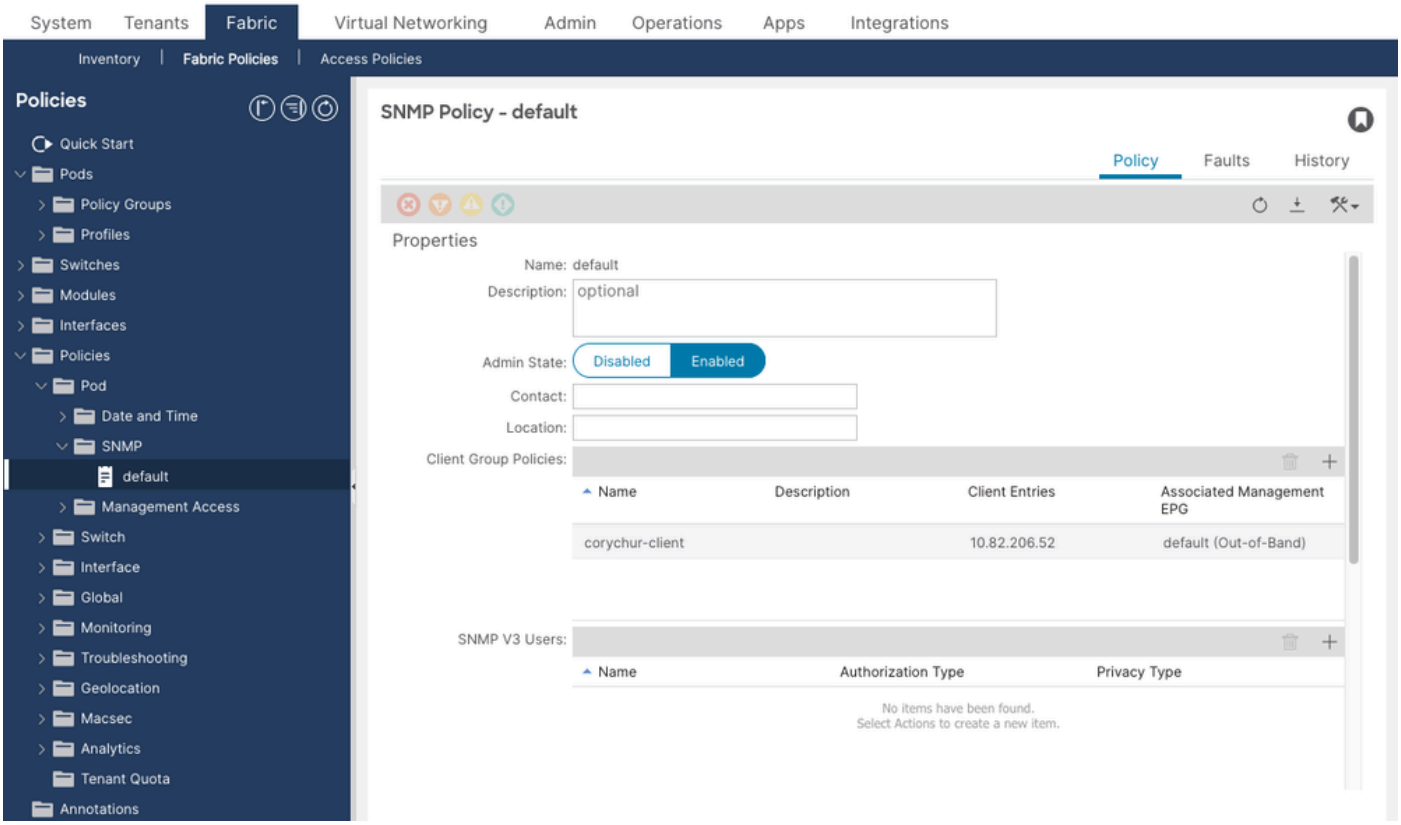
De configuratie verifiëren

SNMP-beleidsimplementatie controleren

Navigeer naar Fabric > Fabric Policies > Policies > Pod > SNMP en bevestig dat het standaard SNMP-beleid bestaat en dat de beheerdersstatus is ingesteld op Enabled. De lijst Beleidsgroepen toont alle geconfigureerde SNMP-beleidsregels met hun beheerdersstatus in één oogopslag.



Klik voor gedetailleerde verificatie op de naam van het beleid om deze te openen. Bevestig dat de schakeloptie Beheerstatus is ingesteld op Ingeschakeld, en dat in het Beleid voor clientgroepen alle toegestane NMS-hosts worden vermeld met de bijbehorende beheer-EPG.



Voer de volgende MO-query uit op een APIC om te bevestigen dat het SNMP-beleid aanwezig en ingeschakeld is in de structuur:

<#root>

```
apic1#

moquery -c snmpPol

Total Objects shown: 1

# snmp.Pol
name          : default
adminSt       : enabled                    <--- must be "enabled"
contact       : NOC Team
descr         : ACI Fabric SNMP Policy
dn            : uni/fabric/snmppol-default
loc           : DC1 ACI Fabric
monPolDn      : uni/fabric/monfab-default
```

Als `adminSt` is `uitgeschakeld`, werkt SNMP niet op een node. Schakel deze optie in de APIC GUI in onder Verbinding > Verbindingsbeleid > Beleid > Pod > SNMP > Standaard.

Communitytekenreeksconfiguratie controleren

<#root>

```
apic1#

moquery -c snmpCommunityP

Total Objects shown: 1

# snmp.CommunityP
name         : public                      <--- confirm this matches your NMS community string
dn           : uni/fabric/snmppol-default/community-public
descr        : SNMP Community String
```

Als er geen community wordt geretourneerd of als de naam niet overeenkomt met wat de NMS gebruikt, voegt u de community-tekenreeks toe of corrigeert u deze onder het SNMP-beleid.

Verifieer het clientgroepsbeleid (SNMP-toegangsbeheer)

Clientgroepsbeleid fungeert als een ACL voor SNMP GET/WALK-toegang. Elk beleid specificeert welke client-IP-adressen mogen worden gebruikt om leaf/spine-knooppunten te pollen over welk beheer VRF. Op blad/ruggengraat knooppunten, worden deze beleidslijnen vertaald in iptables regels.

<#root>

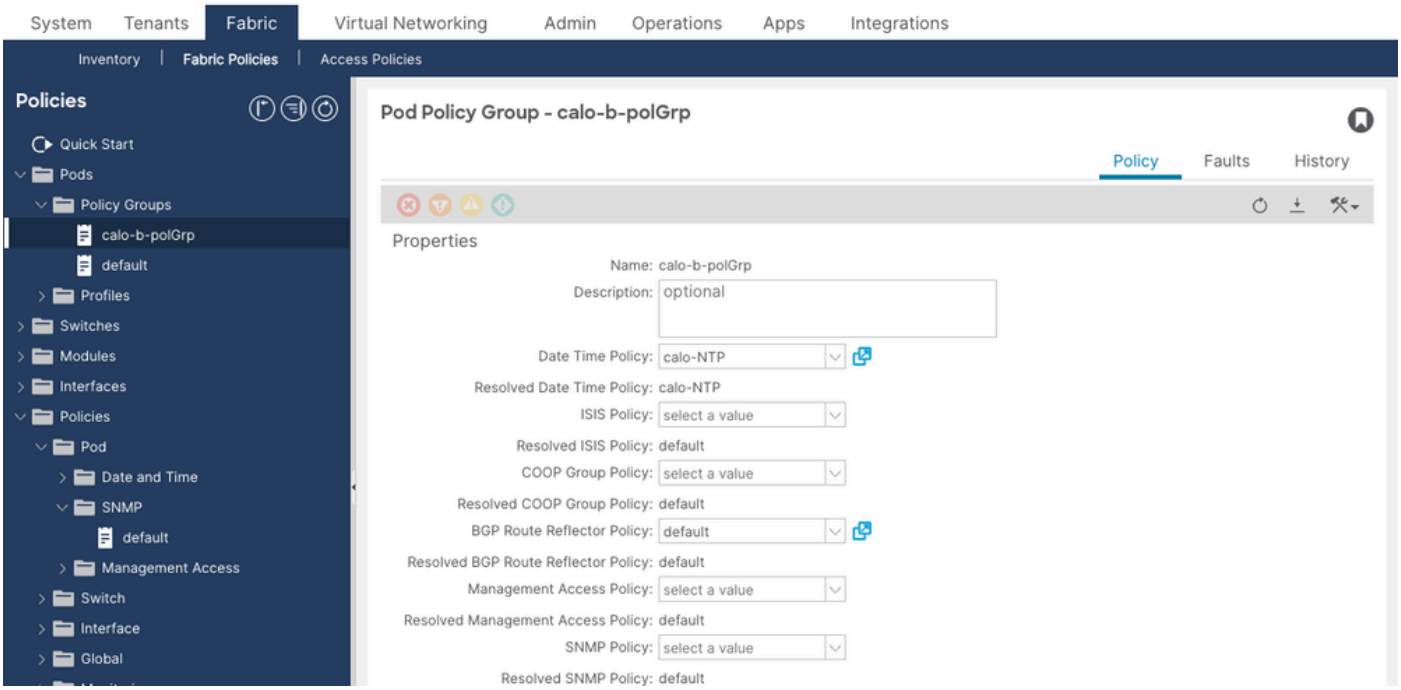
```
apic1#

moquery -c snmpClientGrpP -x query-target=children

Total Objects shown: 3

# snmp.ClientP
addr         : 10.1.1.50                   <--- NMS server IP
dn           : uni/fabric/snmppol-default/clgrp-NMS-Clients/client-[10.1.1.50]
name         : nms-server1

# snmp.ClientP
addr         : 10.1.1.51
dn           : uni/fabric/snmppol-default/clgrp-NMS-Clients/client-[10.1.1.51]
name         : nms-server2

# snmp.ClientGrpP
name         : NMS-Clients
dn           : uni/fabric/snmppol-default/clgrp-NMS-Clients
```

Bevestig dat de IP van de NMS-server aanwezig is in de clientvermeldingen. Als een client-IP ontbreekt, worden SNMP GET/WALK-verzoeken van die host door iptables op bladruimteknooppunten/ruggengraatknooppunten verwijderd.

Opmerking: SNMPv3-voorbehoud — Beleid voor clientgroepen wordt niet afgedwongen op de APIC bij gebruik van SNMPv3. Elke SNMPv3 GET/WALK naar een APIC is toegestaan, ongeacht de configuratie van de clientgroep. De handhaving van de clientgroep voor SNMPv3 op de APIC is een bekende beperking. Op blad- en ruggengraat switches, client group enforcement gedraagt zich hetzelfde voor zowel SNMPv2c en SNMPv3.

Verwijzingen POD-beleidsgroep controleren SNMP-beleid

Navigeer naar Verbinding > Verbindingsbeleid > Pods > Beleidsgroepen en open de actieve groep Pod-beleid. Bevestig dat het dropdownveld SNMP-beleid is ingesteld op het gewenste SNMP-beleid en dat dezelfde naam wordt weergegeven in het veld Opgelost SNMP-beleid. Een ontbrekend of onopgelost beleid betekent dat de SNMP-configuratie nooit naar switches wordt gepusht.



In de bovenstaande schermafbeelding toont het veld SNMP-beleid "selecteer een waarde" (leeg), terwijl het opgeloste SNMP-beleid "standaard" weergeeft. Dit betekent dat het beleid is overgeërfd van de standaardstructuur, maar niet expliciet is ingesteld. Om dubbelzinnigheid te voorkomen, is het raadzaam het veld SNMP-beleid expliciet in te stellen.

Verifiëren via REST API:

<#root>

```
apic1#
```

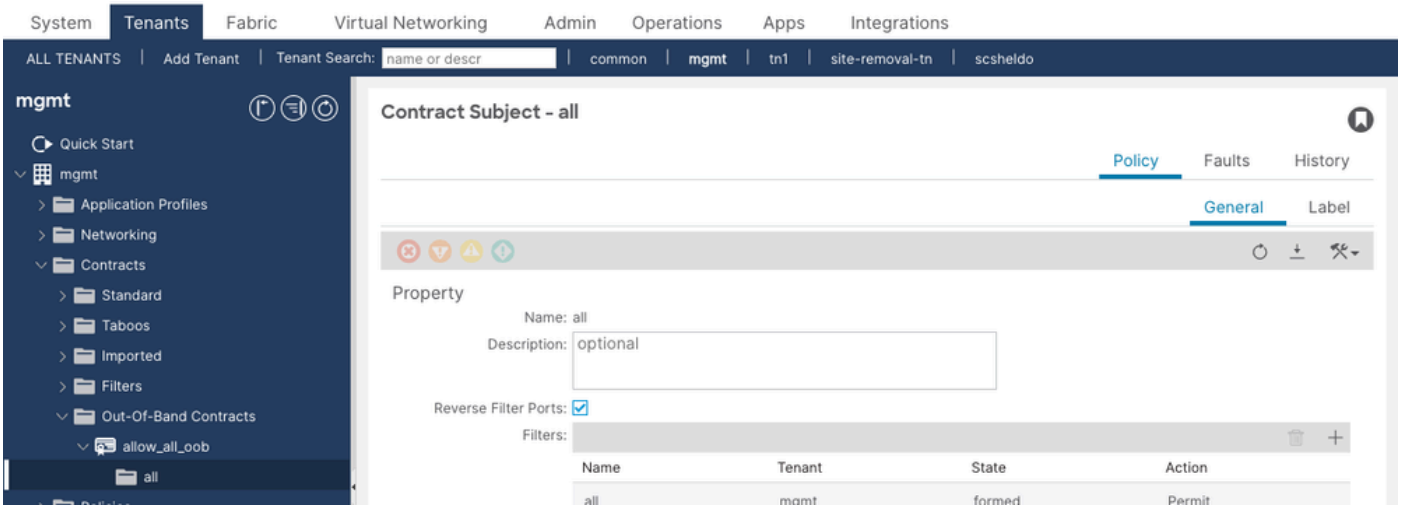
```
moquery -c fabricPodPGrp -x rsp-subtree=full
```

```
# fabric.PodPGrp
name          : default
dn            : uni/fabric/funcprof/podpgrp-default

  # fabric.RsSnmpPol
  tnSnmpPolName : default                  <--- must reference the SNMP policy
  state         : formed                   <--- must be "formed"
```

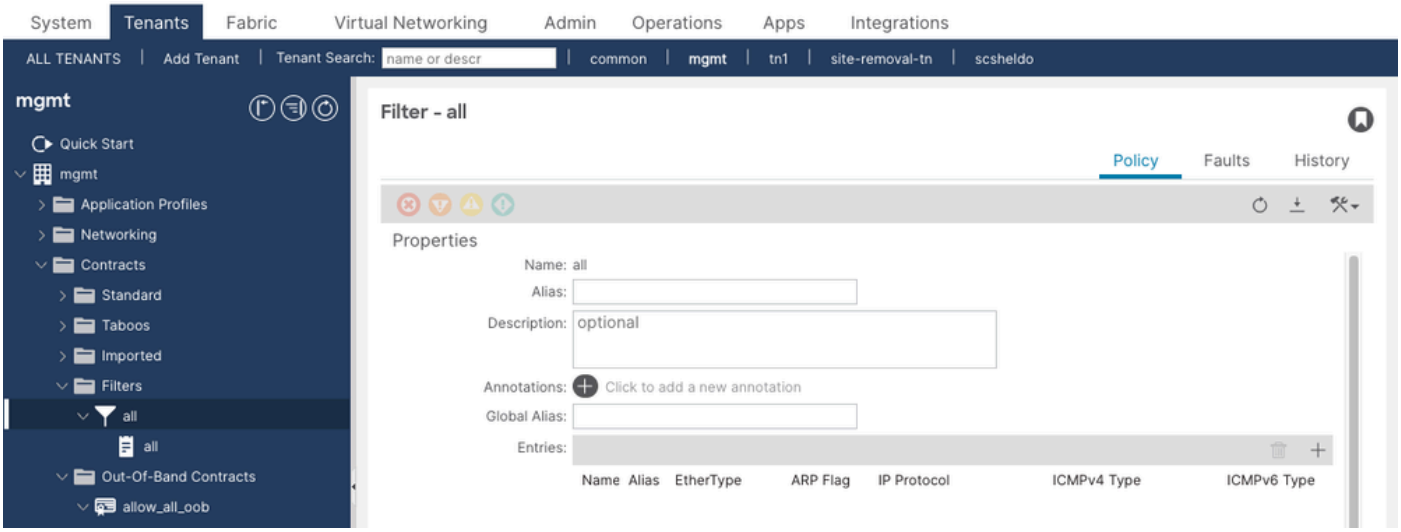
Als de `status` niet is `gevormd`, wordt de SNMP-beleidsrelatie verbroken. Selecteer het SNMP-beleid opnieuw in de Pod Policy Group en dien het beleid in.

Controleren van het beheercontract voor UDP 161 (APIC-knooppunten)

Navigeer naar Huurders > beheer > Contracten > Out-Of-Band Contracten (en In-Band Contracten bij gebruik van INB-beheer). Open het actieve OOB-contract en klik op het tabblad Beleid. Controleer of het onderwerp verwijst naar een filter dat UDP-poort 161 toestaat.



Vouw het filter waarnaar het onderwerp verwijst uit en bevestig dat de items een vermelding bevatten met EtherType IP, Protocol UDP, Bestemmingspoort 161. De filtervermeldingen bepalen welk verkeer is toegestaan via het OOB-beheercontract voor de APIC.



Het filter moet het volgende weergeven:

- EtherType: IP
- IP-protocol: UDP
- Bestemmingshaven vanaf: 161
- Bestemmingshaven naar: 161

Controleer ook of UDP-poort 162 is toegestaan als u wilt dat de APIC SNMP-traps uitstuurt via de OOB-interface.

Controleren via MO-query:

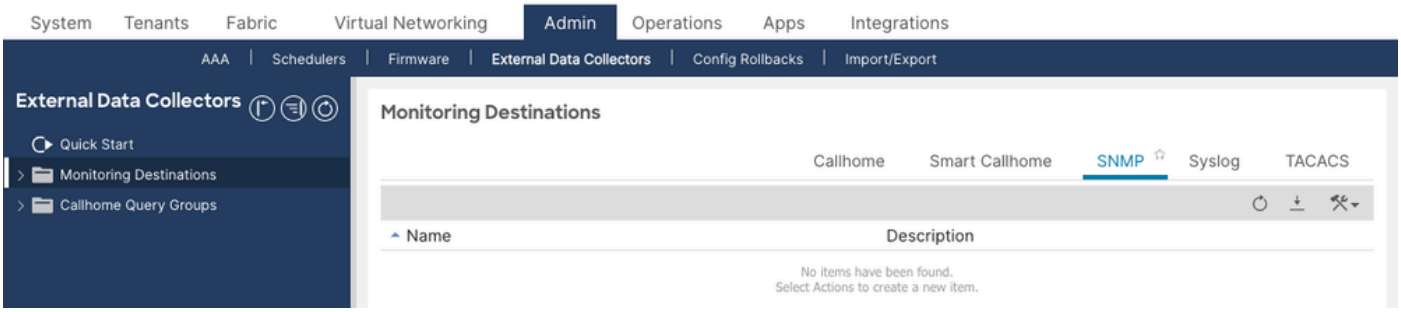
<#root>

```
apic1#

moquery -c vzEntry -x query-target-filter='and(eq(vzEntry.dFromPort,"161"),eq(vzEntry.prot,"17"))'

Total Objects shown: 2

# vz.Entry
name         : snmp-get
dn           : uni/tn-mgmt/flt-snmp-filter/e-snmp-get
dFromPort    : 161                        <--- destination port 161
dToPort      : 161
prot         : 17                         <--- UDP
stateful     : no
```

Als er geen resultaten worden geretourneerd, bestaat er geen filter voor UDP 161. Voeg er een toe aan het beheercontract.

Configuratie SNMP-trapbestemming controleren

Navigeer naar Beheer > Externe gegevensverzamelaars > Bewaking van bestemmingen > SNMP om alle geconfigureerde SNMP-doelgroepen te zien. Een lege lijst betekent dat er geen traps-bestemmingen zijn geconfigureerd en dat er geen traps worden verzonden vanaf een node.



<#root>

```
apic1#

moquery -c snmpTrapDest

Total Objects shown: 1

# snmp.TrapDest
host         : 10.1.1.50                  <--- NMS trap receiver IP
port         : 162                         <--- trap UDP port
ver          : v2c                         <--- SNMP version
secName      : public                      <--- community string (v2c) or username (v3)
v3SecLvl     : noauth
notifT       : traps
vrfName      : mgmt:inb                    <--- VRF used to reach the trap receiver
epgDn        : uni/tn-mgmt/mgmtp-default/inb-default
dn           : uni/fabric/snmpgroup-NMS-DestGrp/trapdest-10.1.1.50-port-162
```

Bevestig dat de IP-poort, versie, communitytekenreeks en beheer-VRF (`beheer:inb` of `beheer` voor OOB) overeenkomen met uw omgeving. De VRF moet overeenkomen met de EPG voor beheer die aan de bestemming is toegewezen.

Controleren of monitoringbronnen in alle drie de scènes zijn geconfigureerd

SNMP-bronnen moeten aanwezig zijn in alle drie de beleidsgebieden voor monitoring. Het ontbreken van een bron in welk bereik dan ook betekent dat vallen van gerelateerde gebeurtenissen niet worden doorgestuurd.

<#root>

```
apic1#

moquery -c snmpSrc | egrep "snmp.Src|name|dn|incl|minSev|monPolDn"


# snmp.Src
name          : NMS-snmpSrc
dn            : uni/fabric/monfab-default/snmpsrc-NMS-snmpSrc        <--- Fabric Default
incl          : audits,events,faults
minSev        : info
monPolDn      : uni/fabric/monfab-default

# snmp.Src
name          : NMS-snmpSrc
dn            : uni/fabric/moncommon/snmpsrc-NMS-snmpSrc              <--- Fabric Common
incl          : audits,events,faults
minSev        : info
monPolDn      : uni/fabric/moncommon

# snmp.Src
name          : NMS-snmpSrc
dn            : uni/infra/moninfra-default/snmpsrc-NMS-snmpSrc        <--- Access Default
incl          : audits,events,faults
minSev        : info
monPolDn      : uni/infra/moninfra-default
```

Als een van de drie ontbreekt, maakt u de ontbrekende SNMP-bron in het bijbehorende controlebeleid met behulp van de GUI.

operationele verificatie

SNMP-status controleren met behulp van snmp-overzicht weergeven (APIC)

Voer deze opdracht rechtstreeks uit op elke APIC om te bevestigen dat de SNMP-agent wordt uitgevoerd en dat de configuratie is toegepast:

<#root>

```
apic1#

show snmp summary


Active Policy:
default, Admin State: enabled             <--- admin state must be "enabled"

Local SNMP engineID: [Hex] 0x8000000980e2b692088976c75600000000

----------------------------------------
Community           Description
----------------------------------------
public              SNMP Community String  <--- community must be present
```

```
-------------------------------------------------------------
User                Authentication   Privacy
-------------------------------------------------------------
                                          <--- empty if using v2c only

-------------------------------------------------------------
Client-Group        Mgmt-Epg              Clients
-------------------------------------------------------------
NMS-Clients         default (In-Band)     10.1.1.50,10.1.1.51  <--- verify client IPs

-------------------------------------------------------------
Host                Port    Version   Level       SecName
-------------------------------------------------------------
10.1.1.50           162     v2c       noauth      public        <--- trap destination
```

Wat te controleren in de output:

- De beheerdersstatus moet zijn `ingeschakeld`.
- Community moet overeenkomen met wat de NMS is geconfigureerd om te gebruiken.
- Client-Group moet alle toegestane NMS-IP's met correct EPG-beheer vermelden.
- De host (trapbestemming) moet de NMS-trapontvanger vermelden met de juiste poort en versie.

SNMP-status controleren met behulp van snmp-overzicht tonen (blad/rug)

<#root>

```
leaf101#

show snmp summary

Admin State : enabled, running (pid:8192)  <--- must show "enabled, running" with a PID

Local SNMP engineID: [Hex] 80000009037C69F6105BF9

-----------------------------------------------------------------------
Community       Context         Status
-----------------------------------------------------------------------
public                          ok                                    <--- community status must be "o

-----------------------------------------------------------------------
Client          VRF             Status
-----------------------------------------------------------------------
10.1.1.50       mgmt:inb        ok                                    <--- client entry must be "ok"
10.1.1.51       mgmt:inb        ok

-------------------------------------------------------------------------------
Host            Port    Ver     Level   SecName         VRF
-------------------------------------------------------------------------------
10.1.1.50       162     v2c     noauth  public          mgmt:inb      <--- trap destination
```

Wat te controleren in de output:

- De beheerdersstatus moet zijn `ingeschakeld en worden uitgevoerd` met een PID. Als het `uitgeschakeld` wordt weergegeven, wordt het SNMP-beleid niet toegepast of wordt de keten van het pod-beleid verbroken.
- De communautaire status moet in `orde` zijn. Een `foutstatus` duidt op een probleem met beleidsimplementatie.
- Client VRF voor elke NMS-host moet overeenkomen met de VRF van het beheer van EPG (`beheer:` inb voor In-Band, `beheer` voor OOB).
- Trap Host moet de bestemming vermelden met de juiste VRF-context.

Controleren of het snmpd-proces wordt uitgevoerd

Op een blad of ruggengraat:

<#root>

```
leaf101#

ps aux | grep snmp

root      5881  2.5 1907404  411444 ?    Ssl  Apr05   /isan/bin/snmpd -f -s -d udp:161 udp6:161 tcp:161

leaf101#

pidof snmpd

5881
```

Op de APIC:

<#root>

```
apic1#

ps aux | grep snmp

ifc   32182  1.4   0.1  641196  239716  ?   Ssl  Apr10   /mgmt//bin/snmpd.bin \
  -f -p /tmp/snmpd2.pid -a -A -LE 0-2 -c /data//snmp/snmpd.conf
```

Als er geen snmpd-proces wordt gevonden op een blad of ruggengraat, wordt SNMP niet uitgevoerd op dat knooppunt. Controleer of de beheerdersstatus van het SNMP-beleid is ingeschakeld en of de keten van het pod-beleid correct is geconfigureerd.

spoiler (Markeren om te lezen)

Controleer of SNMP-poort luistert

<#root>

```
leaf101#
```

netstat -lutn | grep 161

```
Active Internet connections (only servers)
Proto  Recv-Q  Send-Q  Local Address    Foreign Address  State
tcp         0       0  0.0.0.0:161      0.0.0.0:*        LISTEN   <--- SNMP agent is accepting requests
udp         0       0  0.0.0.0:161      0.0.0.0:*
udp6        0       0  :::161           :::*
```

Als poort 161 niet wordt vermeld in de status LUISTEREN, wordt het snmpd-proces niet uitgevoerd of is er geen binding met de poort.

Verifieer de regels voor bladstelen/ruggegraat

Het beleid van de clientgroep wordt vertaald in iptables-regels voor elk blad en elke ruggengraat. Gebruik het volgende om de regels te bekijken:

<#root>

```
leaf101#
```

iptables -S | grep -i snmp

```
-N snmp_rules
-N vrf_2_snmp_rules
-N vrf_9_snmp_rules
-A INPUT -p udp -m udp --dport 161 -j snmp_rules    <--- SNMP port 161 redirects to snmp_rules chain
-A snmp_rules -m vrf --vrf 2 -j vrf_2_snmp_rules    <--- VRF 2 = OOB management
-A snmp_rules -m vrf --vrf 9 -j vrf_9_snmp_rules    <--- VRF 9 = In-Band management
-A snmp_rules -j DROP                                <--- default drop; only permitted clients pass
-A vrf_2_snmp_rules -s 10.1.1.50/32 -j ACCEPT       <--- permitted NMS client (OOB VRF)
-A vrf_9_snmp_rules -s 10.1.1.50/32 -j ACCEPT       <--- permitted NMS client (INB VRF)
```

Voer het volgende uit om de juiste VRF-ID's voor uw fabric te identificeren:

<#root>

```
leaf101#
```

show vrf

```
VRF-Name                VRF-ID  State   Reason
management              2       Up      --
mgmt:inb                9       Up      --
```

De VRF-ID's in de iptables-regels moeten overeenkomen met wat `vrf-`rapporten `weergeven`. Als een client-IP niet aanwezig is in de iptables-regels, worden SNMP-verzoeken van die host stilletjes verwijderd, zelfs als het snmpd-proces wordt uitgevoerd.

Gebruik tellers om te controleren of een SNMP-pakket is gekoppeld of gevallen:

<#root>

```
leaf101#

iptables -nvL | grep -A 20 "Chain snmp_rules"

Chain snmp_rules (1 references)
 pkts bytes target         prot opt in     out    source       destination
    1    73 vrf_9_snmp_rules all -- *      *      0.0.0.0/0    0.0.0.0/0    vrf 9
    0     0 DROP             all -- *      *      0.0.0.0/0    0.0.0.0/0    <--- if pkts>0 here, client
```

Opmerking: Als SNMP actief is maar iptables geen snmp_rules-ketens toont, of als de ketens leeg zijn, kunt u het snmpd-proces opnieuw starten om iptables-regelherprogrammering te forceren. Het verzenden van SIGKILL naar de snmpd PID is veilig - de ACI-procesmanager (`bewaakt`) start deze automatisch opnieuw op. Voer `pidof snmpd uit` om de PID te verkrijgen en `dood -9 [snmpd_pid]`. Bevestig de nieuwe PID met `pidof snmpd` na 10-15 seconden.

Controleer of SNMP-poort luisterblad101# netstat -lutn | grep 161 Actieve internetverbindingen (alleen servers) Proto Recv-Q Send-Q Local Address Foreign Address State tcp 0 0.0.0.0:161 0.0.0.0:* LUISTEREN <--- SNMP-agent accepteert verzoeken udp 0 0.0.0.0:161 0.0.0:* udp6 0:::161 :::* Als poort 161 niet in de status LUISTEREN wordt vermeld, wordt het snmpd-proces niet uitgevoerd of niet uitgevoerd Kan niet aan de poort binden. Verifieer dat de regels voor het beleid voor de clientgroep van bladeren/ruggengraat worden vertaald in regels voor bladzijden en ruggengraat. Gebruik het volgende om de regels te inspecteren: leaf101# iptables -S | grep -i snmp -N snmp_rules -N vrf_2_snmp_rules -N vrf_9_snmp_rules -A INPUT -p udp -m udp --dport 161 -j snmp_rules <----- SNMP port 161 leidt door naar snmp_rules chain -A snmp_rules -m vrf --vrf 2 -j vrf_2_snmp_rules <---- VRF 2 = OOB management -A snmp_rules -m vrf -vrf-vrf 9 vrf_9_snmp_rules <--- VRF 9 = In-Band-beheer -A snmp_rules -j DROP <--- default drop; alleen toegestane clients passeren -A vrf_2_snmp_rules -s 10.1.1.50/32 -j ACCEPTEREN <--- toegestane NMS-client (OOB VRF) -A vrf_9_snmp_rules -s 10.1.1.50/32 -j ACCEPTEREN <---- toegestane NMS-client (INB VRF) Om de juiste VRF-ID's voor uw fabric te identificeren, voert u: leaf101# show vrf VRF-Name VRF-ID - State Reason management Up 2 mgmt: inb 9 Up -- De VRF-ID's in de iptables-regels moeten overeenkomen met de waarden die in vrf-rapporten worden weergegeven. Als een client-IP niet aanwezig is in de iptables-regels, worden SNMP-verzoeken van die host stilletjes verwijderd, zelfs als het snmpd-proces wordt uitgevoerd. Gebruik tellers om te controleren of een SNMP-pakket is gematcht of verwijderd: leaf101# iptables -nvL | grep -A 20 "Chain snmp_rules" Chain snmp_rules (1 referenties) pkts bytes target prot opt in out source destination 1 73 vrf_9_snmp_rules all -- * * 0.0.0.0/0 0.0.0.0/0 vrf 9 0 0 DROP all -- * 0.0.0.0/0 0.0.0.0/0 <----- als hier client-IP's ontbreken Opmerking: Als SNMP actief is maar iptables geen snmp_rules-ketens toont, of de ketens leeg zijn, kunt u opnieuw starten snmpd-proces om iptables regel herprogrammering forceren. Het verzenden van SIGKILL naar de snmpd PID is veilig - de

ACI-procesmanager (onder toezicht) start deze automatisch opnieuw op. Voer pidof snmpd uit om de PID te verkrijgen en dood vervolgens -9 [snmpd_pid]. Bevestig de nieuwe PID met pidof snmpd na 10-15 seconden.

Netwerkconnectiviteit met SNMP-poorten controleren

```
<#root>

leaf101#

netstat -ai | grep eth0

Iface  MTU  Met  RX-OK  RX-ERR  RX-DRP  RX-OVR  TX-OK  TX-ERR  TX-DRP  TX-OVR  Flg
eth0   1500   0  501277      0       0       0  633546      0       0       0  BMRU

leaf101#

netstat -ai | grep kpm_inb

Iface     MTU  Met    RX-OK  RX-ERR  RX-DRP  RX-OVR    TX-OK  TX-ERR  TX-DRP  TX-OVR  Flg
kpm_inb  9300   0  10361421     0       0       0   8958506      0     126       0  BMRU
```

Bevestig dat de beheerinterfaces actief zijn (geen RX-ERR-stappen) en verkeer doorgeven. `eth0` is de OOB-beheerinterface; `kpm_inb` is de In-Band-beheerinterface op de switch.

SNMP-trap verzenden verifiëren met tcpdump

Om te bevestigen dat traps worden gegenereerd en verzonden vanaf een blad- of wervelkolomknooppunt, legt u verkeer vast op de juiste interface. Toegang tot de node als beheerder en gebruik:

```
<#root>

leaf101#

tcpdump -i kpm_inb -f port 162 -vv

tcpdump: listening on kpm_inb, link-type EN10MB (Ethernet), capture size 65535 bytes
17:21:49.810052 IP (tos 0x0, ttl 64, id 63116, proto UDP, length 218)
    172.18.242.14.35582 > 10.1.1.50.snmp-trap: { SNMPv2c C=public
    { V2Trap(171) R=253 system.sysUpTime.0=5888267
      S:1.1.4.1.0=E:cisco.9.276.0.1
      interfaces.ifTable.ifEntry.ifIndex.436224000=436224000
      interfaces.ifTable.ifEntry.ifOperStatus.436224000=2 }}        <--- verify trap is being sent to N
```

Voor OOB:

<#root>

```
leaf101#
```

tcpdump -i eth0 -f port 162 -vv

spoiler (Markeren om te lezen)

Voor APIC-vallen (INB):

<#root>

```
apic1#
```

tcpdump -i bond0.1100 -f port 162

```
20:01:08.453473 IP apic1-inb.cisco.com.59417 > 10.1.1.50.snmptrap: C=public V2Trap(85) S:
1.1.4.1.0=E:cisco.9.117.2.0.2 E:cisco.9.117.1.1.2.1.1.10548=1 E:cisco.9.117.1.1.2.1.2.10548=2
```

Opmerking: Op de APIC is `bond0.1100` de In-Band-beheerinterface VLAN-subinterface. Vervang `1100` door de VLAN-encap die is geconfigureerd voor uw In-Band EPG-beheer. Gebruik `obmgmt` als interfacenaam voor OOB-opnamen op de APIC.

Voor APIC-traps (INB): apic1# tcpdump -i bond0.1100 -f poort 162 20:01:08.453473 IP apic1-inb.cisco.com.59417 > 10.1.1.50.snmptrap: C=public V2Trap(85) S: 1.1.4.1.0=E:cisco.9.117.2.0.2 E:cisco.9.117.1.1.2.1.1.10548=1 E:cisco.9.117.1.1.2.1.2.10548=2 Opmerking: Op de APIC is bond0.1100 de in-band beheerinterface VLAN-subinterface. Vervang 1100 door de VLAN-encap die is geconfigureerd voor uw In-Band-beheer-EPG. Gebruik obmgmt als de interfacenaam voor OOB-opnamen op de APIC.

SNMP GET/WALK-aanvragen verifiëren met tcpdump

<#root>

```
leaf101#
```

tcpdump -i kpm_inb -f port 161 -vv

```
17:26:08.548149 IP 10.1.1.50.64245 > leaf101.cisco.com.snmp: { SNMPv2c C=public
  { GetRequest(28) R=949769396 system.sysDescr.0 }}              <--- GET request received
17:26:08.552290 IP leaf101.cisco.com.snmp > 10.1.1.50.64245: { SNMPv2c C=public
  { GetResponse(191) R=949769396
    system.sysDescr.0="Cisco NX-OS(tm) aci, Software (aci-n9000-system), \
Version 15.0(1k), RELEASE SOFTWARE" }}                          <--- response returned; SNMP working
```

Als u de GetRequest maar geen GetResponse ziet, wordt de aanvraag ontvangen maar niet

beantwoord. Controleer het snmpd-proces en de community-tekenreeks. Als u geen verzoek of reactie ziet, wordt het verzoek geblokkeerd voordat het de node bereikt (controleer routering en iptables).

Werkstroom voor probleemoplossing

triage-beslisboom

Gebruik deze beslisboom wanneer technici melden dat SNMP niet werkt. Begin bij het waargenomen symptoom en volg de takken tot isolatie.

Symptoom: geen reactie op SNMP GET/WALK-verzoeken

1. Controleer de SNMP-beheerstatus op APIC. Voer `moquery -c snmpPol uit`. Als `adminSt` is `uitgeschakeld`, schakelt u het in en gaat u verder met stap 7.
2. Controleer het snmpd-proces. Voer op de betreffende node `ps aux | grep snmp` of `pidof snmpd uit`. Als er geen proces wordt uitgevoerd, wordt het SNMP-beleid niet geïmplementeerd. Controleer de pod-beleidsketen (SNMP Policy → Pod Policy Group → Pod Profile).
3. Controleer of poort 161 luistert. Voer `netstat -lutn uit | grep 161`. Als poort 161 niet in de status LISTEN staat, is het snmpd-proces mislukt; verzamel logs van `/var/log/dme/log/svc_ifc_dbgrelem.log*` en start het proces opnieuw op.
4. Controleer de routering. Voer `ip-routebeheer uit` en `toon ip-route vrf mgmt:inb`. Bevestig dat er een route naar de NMS-host bestaat in de juiste VRF.
5. Controleer het beheercontract op APIC. Als het doel een APIC is (geen blad/ruggengraat), controleer dan of UDP 161 is toegestaan in het OOB- of INB-beheercontract.
6. Voer tcpdump uit op de node. Voer `tcpdump -i kpm_inb -f poort 161 -vv uit` (of `eth0` voor OOB). Als de GetRequest wordt weergegeven, maar er geen GetResponse volgt, bereikt het verzoek de node, maar snmpd reageert niet - controleer de community-tekenreeks. Als er helemaal geen verzoek verschijnt, is het probleem upstream (routering of contract).
7. Test bij een toegestane klant. Voer `snmpget -v2c -c [community] [node-ip] SNMPv2-MIB::sysDescr.0 uit` vanaf een NMS-host die in de clientgroep wordt vermeld. Een succesvolle respons bevestigt dat SNMP volledig operationeel is.

Symptoom: Geen SNMP-vallen ontvangen bij de NMS

1. Controleer de bestemmingsconfiguratie van de overvulling. Voer `moquery -c snmpTrapDest uit`. Bevestig dat de IP, poort, versie en community van het NMS overeenkomen met de verwachte waarden van het NMS.
2. Controle monitoring bronnen bestaan in alle drie de scopes. Voer `moquery -c snmpSrc | egrep "snmp.Src|name|dn"` uit. Bevestig dat items bestaan met `monPolDn` waarden voor `uni/fabric/monfab-`

`default`, `uni/fabric/moncommon`, en `uni/infra/moninfra-default`. Als er een ontbreekt, voegt u de SNMP-bron toe aan het bijbehorende controlebeleid.
3. Controleer het snmpd-proces. Controleer of snmpd wordt uitgevoerd op de node die de trap moet verzenden.
4. Genereer een testgebeurtenis en leg vast met tcpdump. Flap een interface of wijzig een status om een gebeurtenis te genereren. Voer op de node `tcpdump -i kpm_inb -f poort 162 -vv uit`. Als er geen overvulverkeer op de kabel verschijnt, genereert de gebeurtenis geen overvulling — controleer opnieuw de bron `incl`. attribuut (moet `fouten` of `gebeurtenissen` bevatten).
5. Controleer de connectiviteit met de trapontvanger. Bevestig dat de trapontvanger bereikbaar is vanaf de VRF-beheerserver: `toon ip-route vrf mgmt:inb` moet een pad naar de NMS-host tonen.
6. Als traps op tcpdump verschijnen maar niet op de NMS, is het probleem netwerkzijde: firewall, routing of de NMS-configuratie. Controleer of de NMS luistert op UDP 162 vanaf de beheerbron IP van de ACI-node.

Gemeenschappelijke scenario's

Scenario 1: SNMP-beleid ingeschakeld, maar geen gegevens geretourneerd van blad/rug

Probleem: in het SNMP-beleid op de APIC wordt aangegeven dat de beheerdersstatus is ingeschakeld. De NMS kan het IP-beheer van het blad bereiken. `snmpget` time-out zonder reactie.

Configuratiecontrole: Controleer of de referenties van de pod-beleidsgroep naar het SNMP-beleid verwijzen en het opgeloste SNMP-beleid de juiste naam weergeeft. Als het veld SNMP-beleid van de Pod Policy Group leeg is of als de relatie niet is gevormd, wordt het snmpd-proces mogelijk niet gestart op de switches.

Operationele controle: SSH naar het betreffende blad en uitvoeren `tonen snmp samenvatting`. Als de uitvoer de `beheerdersstatus` toont: `uitgeschakeld` hoewel de APIC ingeschakeld is, is het beleid niet geïmplementeerd. Controleer de pod-beleidsketen op een ontbrekende of onjuist gerefereerde pod-beleidsgroep.

Hoofdoorzaak: het SNMP-beleid is niet gekoppeld aan de beleidsgroep Pod of de selector voor het profiel Pod past de juiste beleidsgroep Pod niet toe op deze pod.

Oplossing:

1. Navigeer naar Fabric > Fabric Policies > Pods > Policy Groups > default.
2. Bevestig dat het veld SNMP-beleid verwijst naar het ingeschakeld SNMP-beleid.

3. Navigeer naar Verbinding > Verbindingsbeleid > Pods > Profielen en bevestig de actieve selectorverwijzingen naar deze Pod-beleidsgroep.
4. Controleer na het opslaan de `snmp-samenvatting` op het blad binnen 2 minuten `weergeven`.

Scenario 2: SNMP GET / WALK werkt voor sommige NMS-hosts, maar niet voor anderen

Probleem: één NMS-server kan met succes ACI-knooppunten pollen. Een tweede NMS-server op een ander subnet krijgt geen antwoord.

Configuratiecontrole: Voer `moquery -c snmpClientGrpP -x query-target=kinderen uit` op de APIC. Bevestig dat het IP-adres van de tweede NMS-server wordt vermeld als clientinvoer. Als het ontbreekt, wordt dat IP geblokkeerd door de drop-regel iptables onderaan de snmp_rules-keten.

Operationele controle: Bevestig op het betreffende blad dat UDP 161 is toegestaan in het OOB- of INB-beheercontract. Als geen enkel contract of filter SNMP-poorten heeft, wordt het verzoek ingetrokken.

Hoofdoorzaak: De tweede IP-adres van de NMS-server staat niet in het clientgroepsbeleid.

Oplossing: voeg de ontbrekende NMS IP toe als clientvermelding in het SNMP-clientgroepsbeleid onder Fabric > Fabric Policies > Policies > Pod > SNMP > default > Client Group Policies. De iptables-regels voor alle nodes worden binnen enkele minuten na het opslaan van het beleid bijgewerkt.

Scenario 3: SNMP-traps niet ontvangen — traps worden gegenereerd maar niet geleverd

Probleem: Fouten zijn zichtbaar in de APIC-fouttabel. `moquery -c snmpTrapDest` toont de juiste NMS IP. De NMS ontvangt geen valstrikken.

Configuratiecontrole: Voer `moquery -c snmpSrc | egrep "snmp.Src|name|dn"` uit. Controleer of er in alle drie de scopes monitoringbronnen bestaan (`monfab-default`, `moncommon`, `moninfra-default`). Een algemeen overzicht is het configureren van de bron alleen in het beleid Fabric Default, dat gebeurtenissen in het toegangsbeleid mist.

Operationele controle: een testevent activeren (bijvoorbeeld een interface naar de beheerdersstatus schakelen). Voer op de relevante node `tcpdump -i kpm_inb -f-poort 162 uit`. Als overvulpakketten worden weergegeven op de interface van de node, werkt de ACI-zijde en bevindt het probleem zich in het netwerkpad naar de NMS (firewall, routering). Als er geen

overvulling op de draad verschijnt, ontbreekt de ACI-monitoringbron of is het gebeurtenistype niet opgenomen in het `incl`-kenmerk van de bron.

Root Cause 1: Een of meer monitoringbronnen ontbreken in de vereiste scopes.

Hoofdoorzaak 2: bron bewaken `incl.` attribuut sluit het gebeurtenistype uit dat wordt gegenereerd (`incl. gebeurtenissen` zonder `fouten` betekent dat op fouten gebaseerde traps niet worden verzonden).

Oplossing:

1. Voeg ontbrekende bewakingsbronnen toe aan de GUI voor elk van de drie scopes (Fabric Default, Fabric Common, Access Default). Stel de bestemmingsgroep in op de geconfigureerde SNMP-bestemmingsgroep.
2. Controleer of het `incl`-kenmerk `audits, gebeurtenissen en fouten` bevat voor een uitgebreide trapdekking.
3. Na wijzigingen, opnieuw activeren van de test gebeurtenis en opnieuw controleren tcpdump.

spoiler (Markeren om te lezen)

Opmerking: op de APIC `is` de `opdracht tcpdump/code> alleen beschikbaar voor rootgebruikers. Voor APIC en Switches is iptables alleen beschikbaar voor root-gebruikers.`

Scenario 4: SNMPv3 Client Group Enforcement werkt niet aan APIC

Probleem: een SNMP-client die NIET in het clientgroepsbeleid staat, kan met SNMPv3 de APIC-query uitvoeren, ook al mislukt dezelfde query van de bladeren/ruggengraatknooppunten.

Root Cause: Dit is een **bekend voorbehoud**. Clientgroepbeleid (op iptables gebaseerde bron-IP-handhaving) wordt niet toegepast voor SNMPv3 GET's/Walks op APIC-controllers. Elke host kan de APIC via SNMPv3 opvragen, ongeacht de configuratie van de clientgroep. Op blad- en ruggengraat switches, Client Group handhaving werkt identiek voor SNMPv2c en SNMPv3.

Mitigatie: gebruik contractbeheerfilters op de APIC om SNMP-toegang per bronsubnet te beperken. Clientgroepen zijn effectief voor blad-/wervelkolomknooppunten. Vertrouw voor de APIC met SNMPv3 op brongebaseerde beheerbrongebaseerde filtering als toegangscontrolemechanisme.

Scenario 5: SNMP-query's slagen, maar MIB-gegevens zijn onvolledig of verouderd

Probleem: SNMP GET/WALK retourneert gegevens, maar bepaalde MIB OID's retourneren lege of stabiele waarden. Interfacestatistieken of gegevens over de operationele status geven met name de huidige fabric-status niet weer.

Operationele controle: Bevestig welke APIC wordt opgevraagd. Elke APIC retourneert alleen MIB-objecten voor de lokale gegevens. Voer een snmp-overzicht uit op de APIC die wordt gevraagd en vergelijk het resultaat met wat u verwacht. Voor gegevens op switch-niveau (IF-MIB, entityMIB) moet u de switch rechtstreeks bevragen, niet de APIC.

Hoofdoorzaak: een APIC opvragen voor MIB-gegevens op bladniveau. Elke APIC biedt MIB-objecten alleen voor de eigen beheerde objecten. Gegevens op switch-niveau (interfacestatus, processor, geheugen, omgevingssensoren) moeten worden opgehaald door elk blad en elke ruggengraat rechtstreeks te peilen.

Oplossing: Configureer uw NMS om blad- en ruggengraatbeheer-IP's rechtstreeks te pollen voor interface- en hardware-MIB-gegevens. Gebruik APIC-beheer-IP's alleen voor APIC-native MIB's (entiteit, FRU, proces, sensor met betrekking tot de APIC-serverhardware).

Scenario 6: SNMP werkt naar blad / ruggengraat, maar niet naar de APIC

Probleem: SNMPv2c GET van NMS naar blad- en wervelkolomknooppunten slaagt. Dezelfde NMS kan de APIC niet peilen.

Configuratiecontrole: APIC SNMP vereist een expliciet beheercontract dat UDP 161 toestaat. Navigeer naar **Huurders > beheer** en controleer het OOB / INB-contract en het filter voor UDP 161.

Operationele controle: Op de APIC, run iptables -S | grep 161. Als er geen Accept-regels voor UDP 161 worden weergegeven onder de fp-137-keten (of een gelijkwaardig OOB-contract), ontbreekt het contractfilter voor UDP 161 of wordt het niet ingezet.

```
<#root>

apic1#

iptables -S | grep 161

-A fp-137 -s 10.0.0.0/8 -p udp -m udp --dport 161 -j ACCEPT     <--- permit SNMP from the management su
-A fp-137 -s 172.18.0.0/16 -p udp -m udp --dport 161 -j ACCEPT  <--- permit SNMP from INB management su
```

Als deze regels ontbreken, voegt u een filtervermelding voor UDP 161 toe aan het onderwerp van het beheercontract en controleert u deze opnieuw.

Hoofdoorzaak: ontbrekend of verkeerd geconfigureerd beheercontract. In ACI 5.x handhaven APIC-knooppunten het beheercontract strikt - SNMP-pakketten worden verwijderd tenzij er een expliciete toestemming is.

Oplossing:

1. Navigeer naar **Huurders > Beheer > Beveiligingsbeleid > Out-of-band contracten**.
2. Vouw het OOB-contract uit, selecteer het onderwerp en controleer/voeg een filter toe voor **UDP-poort 161**.
3. Herhaal voor het In-Band contract als de NMS de APIC bereikt over het INB-beheer.
4. Controleer met iptables -S | grep 161 op de APIC na het opslaan.

Scenario 7: SNMP-regels ontbreken of zijn onjuist

Probleem: snmp-overzicht tonen toont dat het SNMP-beleid wordt toegepast, maar iptables -S | grep snmp geeft geen regels terug, of de IP van de NMS-client is afwezig in de regels.

Operationele controle: Bevestig dat snmpd wordt uitgevoerd met pidof snmpd. Als snmpd wordt uitgevoerd maar iptables geen SNMP-regels heeft, is het proces gestart voordat het clientgroepsbeleid werd geïmplementeerd. Start snmpd opnieuw om de herprogrammering van de regel af te dwingen als het aantal herstarts minder dan 250 is:

```
<#root>

leaf101#

pidof snmpd

5881

leaf101# show system internal sysmgr service name snmpd
Service "snmpd" ("snmpd", 127):
```

UUID = 0x1A, PID = 5881, SAP = 1545
State: SRV_STATE_HANDSHAKED (entered at time Mon Aug 25 19:23:50 2025).

Restart count: 3

Time of last restart: Mon Aug 25 19:23:48 2025.
Previous PID: 32080
Reason of last termination: SYSMGR_DEATH_REASON_FAILURE_SIGNAL
Tag = N/A
Plugin ID: 0
leaf101#

kill -9 5881

De ACI-procesmanager start snmpd automatisch opnieuw op. Controleer na het opnieuw starten:

<#root>

leaf101#

iptables -S | grep -i snmp

De regels snmp_rules chains en per-VRF client ACCEPT moeten nu verschijnen.

Hoofdoorzaak: het snmpd-proces is opnieuw gestart of gestart voordat het clientgroepsbeleid volledig was geïmplementeerd in de node, waardoor iptables zonder de SNMP-toegangsregels bleven.

Opmerking: op de APIC is de opdracht tcpdump/code> alleen beschikbaar voor rootgebruikers. Voor APIC en Switches iptables is de opdracht alleen beschikbaar voor rootgebruikers. Scenario 4: SNMPv3 Client Group Enforcement werkt niet aan APIC-probleem: een SNMP-client die NIET in het clientgroepsbeleid staat, kan de APIC met SNMPv3 doorzoeken, ook al mislukt dezelfde query van de bladeren/ruggengraatknooppunten. Oorzaak: Dit is een bekend voorbehoud. Clientgroepbeleid (op iptables gebaseerde bron-IP-handhaving) wordt niet toegepast voor SNMPv3 GET's/Walks op APIC-controllers. Elke host kan de APIC via SNMPv3 opvragen, ongeacht de configuratie van de clientgroep. Op blad- en ruggengraat switches, Client Group handhaving werkt identiek voor SNMPv2c en SNMPv3. Mitigatie: gebruik contractbeheerfilters op de APIC om SNMP-toegang per bronsubnet te beperken. Clientgroepen zijn effectief voor blad-/wervelkolomknooppunten. Vertrouw voor de APIC met SNMPv3 op brongebaseerde beheerbrongebaseerde filtering als toegangscontrolemechanisme. Scenario 5: SNMP-query's slagen, maar MIB-gegevens zijn onvolledig of verouderd Probleem: SNMP GET/WALK retourneert gegevens, maar bepaalde MIB OID's retourneren lege of stabiele waarden. Interfacestatistieken of gegevens over de operationele status geven met name de huidige fabric-status niet weer. Operationele controle: Bevestig welke APIC wordt opgevraagd. Elke APIC retourneert alleen MIB-objecten voor de lokale gegevens. Voer een samenvatting van de show snmp uit op de APIC die wordt gevraagd en vergelijk het resultaat met wat u verwacht. Voor gegevens op switch-niveau (IF-MIB, entityMIB) moet u de switch rechtstreeks bevragen, niet de APIC. Hoofdoorzaak: een APIC opvragen voor MIB-gegevens op bladniveau. Elke APIC biedt MIB-objecten alleen voor de eigen beheerde objecten. Gegevens op switch-niveau (interfacestatus, processor, geheugen, omgevingssensoren) moeten worden opgehaald door elk blad en elke ruggengraat rechtstreeks te peilen. Oplossing: Configureer uw NMS om blad- en ruggengraatbeheer-IP's rechtstreeks te pollen voor interface- en hardware-MIB-gegevens. Gebruik APIC-beheer-IP's alleen voor APIC-native MIB's (entiteit, FRU, proces, sensor met betrekking tot de APIC-serverhardware). Scenario 6: SNMP werkt naar blad / ruggengraat maar niet naar het APIC-probleem: SNMPv2c GET van NMS naar blad- en wervelkolomknooppunten slaagt. Dezelfde NMS kan de APIC niet peilen. Configuratiecontrole: APIC SNMP vereist een expliciet beheercontract dat UDP 161 toestaat. Navigeer naar Huurders > beheer en controleer het OOB / INB-contract en het filter voor UDP 161. Operationele controle: Op de APIC, run iptables -S | grep 161. Als er geen Accept-regels voor UDP 161 worden weergegeven onder de keten van het fp-137-contract (of een equivalent van het OOB-contract), ontbreekt het contractfilter voor UDP 161 of wordt het niet gebruikt. apic1# iptables -S | grep 161 -A fp-137 -s 10.0.0.0/8 -p udp -m udp --dport 161 -j

ACCEPTEREN <--- vergunning SNMP van het beheersubnet -A fp-137 -s 172.18.0.0/16 -p udp -m udp --dport 161 -j ACCEPTEREN <---- vergunning SNMP van INB-beheersubnet Als deze regels ontbreken, voegt u een filtervermelding voor UDP 161 toe aan het onderwerp van het beheercontract en controleert u opnieuw. Hoofdoorzaak: ontbrekend of verkeerd geconfigureerd beheercontract. In ACI 5.x handhaven APIC-knooppunten het beheercontract strikt - SNMP-pakketten worden verwijderd tenzij er een expliciete toestemming is. Oplossing: Navigeer naar huurders > beheer > Beveiligingsbeleid > Out-of-band contracten. Vouw het OOB-contract uit, selecteer het onderwerp en controleer/voeg een filter toe voor UDP-poort 161. Herhaal voor het In-Band contract als de NMS de APIC bereikt over het INB-beheer. Verifieer met iptables -S | grep 161 op de APIC na het opslaan. Scenario 7: SNMP-iptables Rules Are Absent or Incorrect Probleem: show snmp summary geeft aan dat het SNMP-beleid is toegepast, maar iptables -S | grep snmp geeft geen regels terug, of dat het NMS-client-IP ontbreekt in de regels. Operationele controle: Bevestig dat snmpd wordt uitgevoerd met pidof snmpd. Als snmpd wordt uitgevoerd maar iptables geen SNMP-regels heeft, is het proces gestart voordat het clientgroepsbeleid werd geïmplementeerd. Herstart snmpd om regel herprogrammering af te dwingen als het aantal herstarts minder is dan 250: leaf101# pidof snmpd 5881leaf101# toon systeem interne systeemservicenaam snmpdService "snmpd" ("snmpd", 127): UUID = 0x1A, PID = 5881, SAP = 1545Staat: SRV_STATE_HANDSHAKED (ingevoerd op tijdstip ma 25 augustus 19:23:50 2025).Herstart telling: 3Tijd van laatste herstart: ma aug 25 19:23:48 2025.Vorige PID: 32080Reden van laatste beëindiging: SYSMGR_DEATH_REASON_FAILURE_SIGNALTag = N/APlugin ID: 0 leaf101# kill -9 5881 De ACI-procesmanager start snmpd automatisch opnieuw op. Controleer na het opnieuw opstarten: leaf101# iptables -S | grep -i snmp De regels snmp_rules chains en per-VRF client ACCEPT moeten nu verschijnen. Hoofdoorzaak: het snmpd-proces werd opnieuw gestart of gestart voordat het clientgroepsbeleid volledig was geïmplementeerd in de node, waardoor iptables zonder de SNMP-toegangsregels bleven.

Logbestanden voor uitgebreide probleemoplossing

Als het probleem niet wordt opgelost met de bovenstaande verificatiestappen, bevatten de volgende logbestanden op de bladader-, ruggengraat- en APIC-knooppunten diagnostische informatie met betrekking tot SNMP:

<#root>

leaf101#

zgrep "snmp" /var/log/dme/log/svc_ifc_dbgrelem.log*

leaf101#

zgrep "snmpd" /var/log/dme/log/svc_ifc_dbgrelem.log*

leaf101#

zgrep "snmpd_log" /var/log/dme/log/*

Deze logs bevatten snmpd-herstartgebeurtenissen, beleidsimplementatiegebeurtenissen en configuratiefouten voor community/client die niet zichtbaar zijn via snmp-overzicht weergeven.

Referenties

- Configuratiegids voor Cisco APIC-systeembeheer, versie 5.x – SNMP beheren
- Cisco ACI MIB Naslaggids

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.