Fehlerbehebung für SNMP in der Cisco ACI Fabric

Einleitung

In diesem Dokument wird beschrieben, wie SNMP in der Cisco ACI für die ACI Version 5.x und höher konfiguriert, überprüft und Fehler behoben werden. Es umfasst das SNMP-Richtlinienmodell, erforderliche Managementverträge, Trap-Konfiguration, betriebliche Verifizierung mithilfe von CLI- und MO-Abfragen (Managed Object) und strukturierte Workflows zur Fehlerbehebung für die gängigsten Fehlerszenarien bei Leaf-/Spine-Switches und APIC-Controllern.

Hintergrundinformationen

Das Material in diesem Dokument basiert auf dem internen SNMP-Technote des Cisco ACI Solutions Delivery Team in der ACI: Übersicht, Konfiguration, Fehlerbehebung und Hinweise/Probleme von Tomas de Leon, ergänzt durch den Konfigurationsleitfaden für das Cisco APIC-Systemmanagement (Version 5.x) und die Kurzreferenz zur Cisco ACI MIB.

Überblick

SNMP-Architektur in der ACI

SNMP (Simple Network Management Protocol) ist ein UDP-basiertes Protokoll, das die Netzwerkverwaltung und -überwachung steuert. In der ACI arbeitet SNMP unabhängig auf jeder verwalteten Einheit. Jeder Leaf-Switch, Spine-Switch und APIC-Controller ist ein eigener SNMP-Agent - jeder muss einzeln abgefragt oder überwacht werden.

Die ACI unterstützt die folgenden SNMP-Funktionen:

- Lesevorgänge (Get, GetNext, BulkGet, Walk) - werden auf Leaf-/Spine-Switches und APIC-Controllern unterstützt.
- Benachrichtigungen (Traps) - SNMPv1-, v2c- und v3-Traps, die von Leaf-/Spine-Switches und APIC-Controllern unterstützt werden.
- SNMPv3 - wird von Leaf-/Spine-Switches und APIC-Controllern unterstützt.

- Schreibvorgänge (Festlegen) - werden auf keinem ACI-Gerät unterstützt.
- IPv6 - SNMP wird nur über IPv4 unterstützt.

Anmerkung: In einem APIC-Cluster stellt jeder APIC MIB-Objekte lokal für sich selbst bereit. Die einzelnen APICs müssen separat abgefragt werden. Es gibt keine clusterweite SNMP-Aggregation. Ebenso müssen alle Leaf- und Spine-Switches unabhängig voneinander abgefragt werden.

SNMPD-Architektur auf dem APIC

Der APIC führt den snmpd-Prozess aus, der aus zwei internen Komponenten besteht:

- Agent - Ein Open-Source-net-snmp-Agent (Version 5.7.6 oder höher), der die SNMP-Protokollverarbeitung und Sitzungsverwaltung übernimmt.
- DME (Data Model Engine) - Schnittstelle zum APIC Management Information Tree (MIT) zum Lesen von Managed Objects (MOs) und Übersetzen von MO-Attributen in das SNMP-Objektformat. SNMP-Traps werden aus Ereignissen und Fehlern generiert, die auf MOs ausgelöst werden.

SNMP-Richtlinienmodell und Bereitstellungskette

Die ACI verwendet ein richtliniengesteuertes Modell für SNMP. Die SNMP-Konfiguration wird als snmpPol-verwaltetes Objekt abstrahiert und muss mit der Pod Policy Group der Fabric verknüpft werden, bevor sie auf einem Knoten bereitgestellt wird. Die gesamte Bereitstellungskette umfasst:

1. SNMP-Richtlinie (`snmpPol`) - definiert den Admin-Status, Community-Strings, Client-Gruppenrichtlinien (ACLs) und SNMPv3-Benutzer.
2. Pod-Richtliniengruppe — verweist auf die SNMP-Richtlinie zusammen mit anderen Richtlinien auf Pod-Ebene (BGP, ISIS, NTP usw.).
3. Pod-Profilauswahl - Wendet die Pod-Richtliniengruppe auf die Fabric Pods an.

Darüber hinaus erfordert die SNMP-Trap-Konfiguration Folgendes:

1. SNMP Monitoring Destination Group (`snmpGroup`) - definiert Trap-Ziel-Hosts, Ports, SNMP-Version und Community.
2. Überwachungsquellen (`snmpSrc`) - Verknüpfen der Zielgruppe mit drei unterschiedlichen Überwachungsrichtlinienbereichen: Fabric-Standard, Fabric Common Policy und Access Policy-Standard

Für die APIC-Knoten sind Managementverträge erforderlich, die den UDP-Port 161 (SNMP-

Anforderungen) und den UDP-Port 162 (SNMP-Traps) zulassen. Leaf- und Spine-Knoten erfordern ebenfalls korrekte iptables-Regeln, die automatisch programmiert werden, wenn Client-Gruppenrichtlinien konfiguriert werden.

Unterstützte MIBs

Der APIC unterstützt unter anderem folgende MIBs:

- Einheit MIB — PhysicalTable
- 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- und Spine-Switches verwenden Standard-NX-OS-MIBs, einschließlich IF-MIB, IP-MIB, CISCO-CDP-MIB, CISCO-ENTITY-QFP-MIB und der vollständigen CISCO-ENTITY-FRU-CONTROL-MIB-Suite.

Folgende SNMP-Traps werden auf dem APIC generiert: `cefcFRUInserted, cefcFRURemoved, cefcFanTrayStatusChange, cefcModuleStatusChange, entSensorThresholdNotification, cefcPowerStatusChange, cpmCPURisingThreshold, cpmCPUFallingThreshold`.

Konfigurieren von SNMP in der ACI

Anmerkung: Dieser Abschnitt enthält eine Zusammenfassung des Konfigurations-Workflows als Kontext für die nachfolgenden Abschnitte zur Überprüfung und Fehlerbehebung. Ausführliche Konfigurationsanweisungen finden Sie im Konfigurationsleitfaden zur Systemverwaltung des Cisco APIC.

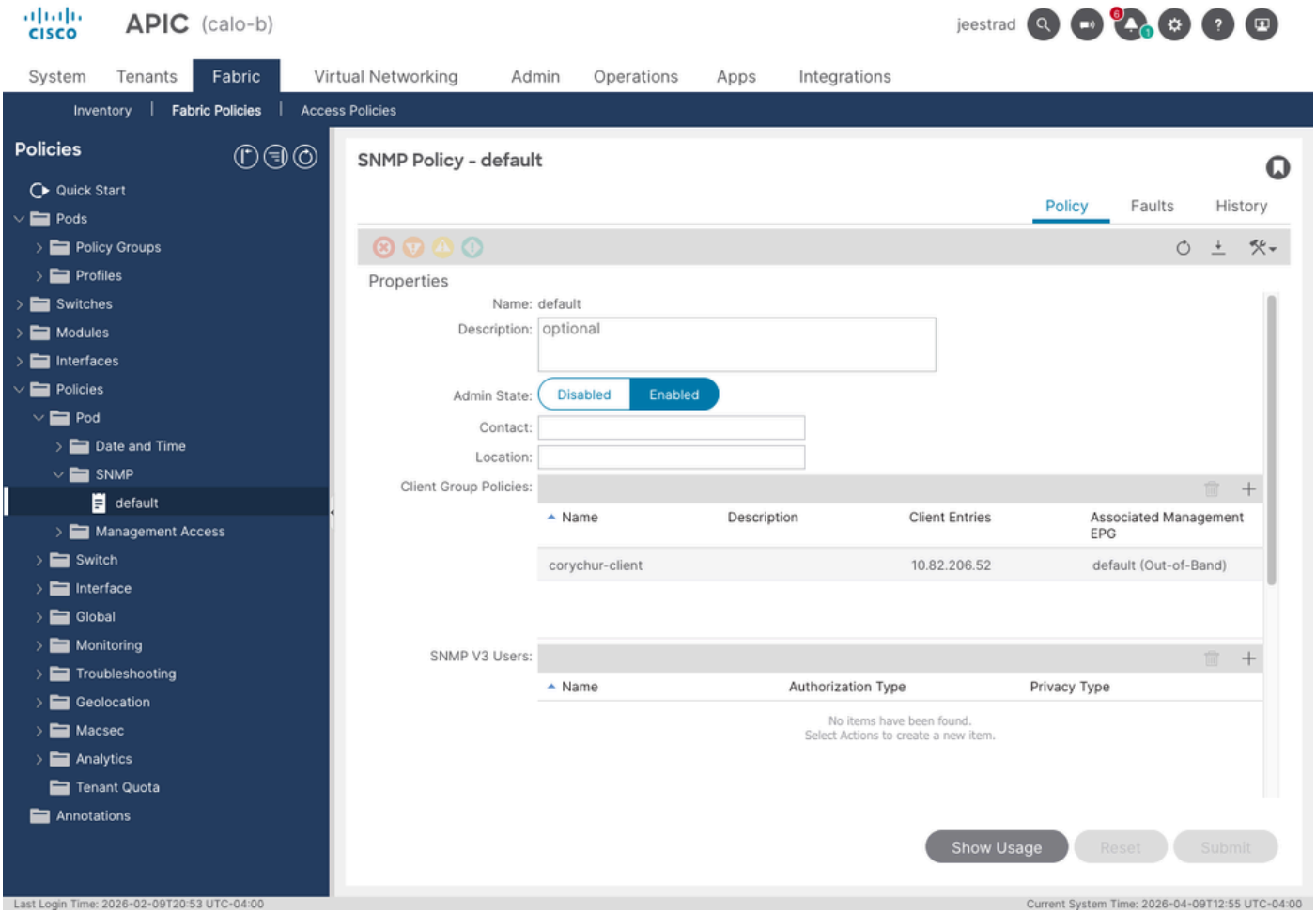
Schritt 1: Konfigurieren der SNMP-Richtlinie

Navigieren Sie zu Fabric > Fabric Policies > Policies > Pod > SNMP. Wählen (oder erstellen) Sie die SNMP-Richtlinie, die normalerweise default heißt. Konfiguration:

- Admin State (Admin-Status): auf "Enabled" (Aktiviert).
- Community Policies (Community-Richtlinien): Fügen Sie den vom NMS verwendeten Community String hinzu.
- Client-Gruppenrichtlinien - Definieren Sie ein oder mehrere Client-Gruppenprofile, von denen

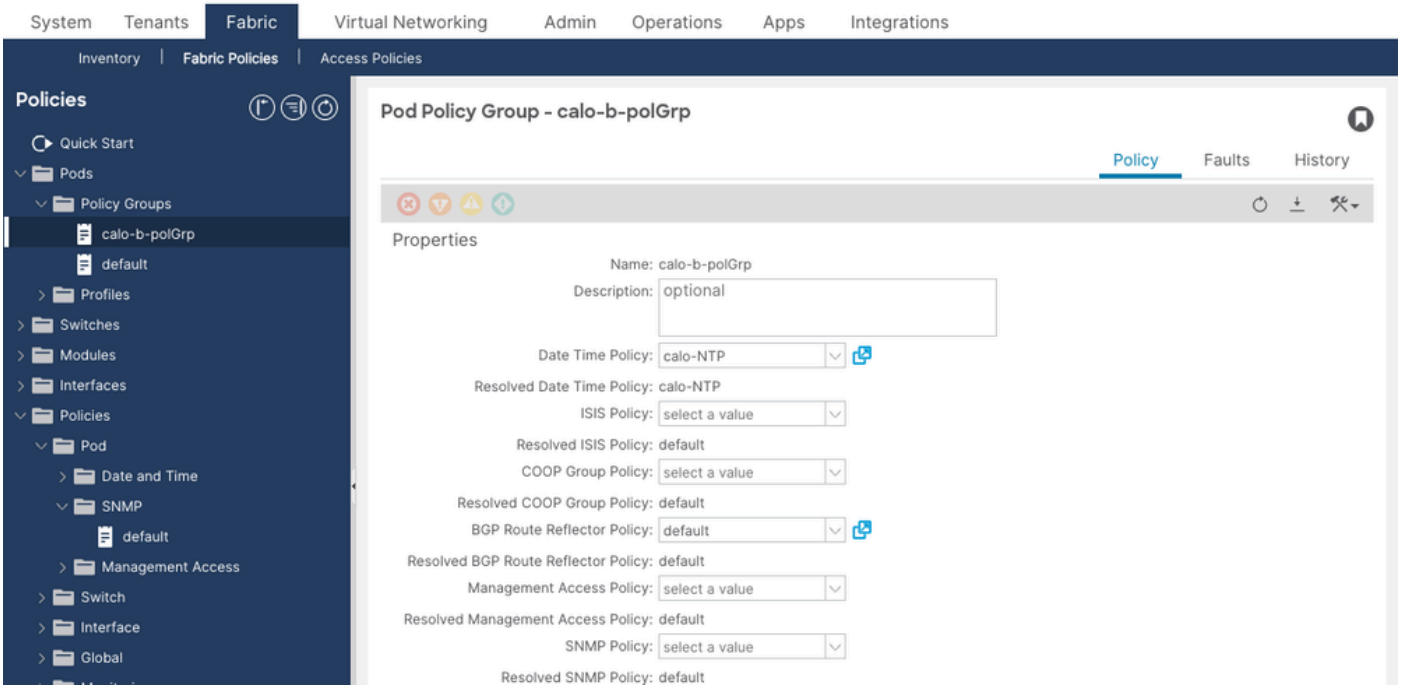
jedes die zulässigen SNMP-Client-IPs und die zugehörige Verwaltungs-EPG (Out-of-Band oder In-Band) angibt.

- SNMPv3-Benutzer - Wenn Sie SNMPv3 verwenden, fügen Sie hier Benutzer mit Authentifizierungs- und Datenschutzparametern hinzu.



Phase 2: Verknüpfen Sie die SNMP-Richtlinie mit der Pod Policy Group.

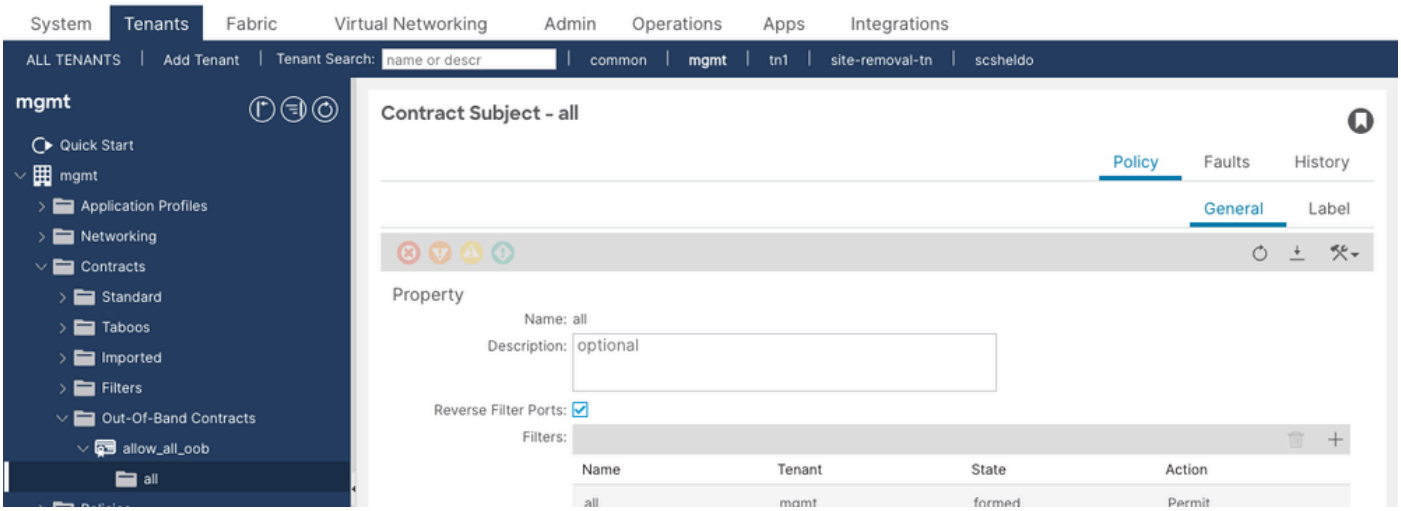
Navigieren Sie zu Fabric > Fabric Policies > Pods > Policy Groups. Wählen Sie die aktive Pod-Richtliniengruppe aus (wird in der Regel als Standard bezeichnet). Legen Sie fest, dass das Feld SNMP-Richtlinie auf die in Schritt 1 erstellte SNMP-Richtlinie zeigt. Stellen Sie sicher, dass im Feld Gelöste SNMP-Richtlinie der richtige Richtlinienname angezeigt wird.



Navigieren Sie anschließend zu Fabric > Fabric Policies > Pods > Profiles, erweitern Sie das Standard-Pod-Profil, und bestätigen Sie, dass der aktive Selektor auf die richtige Pod-Policy-Gruppe verweist.

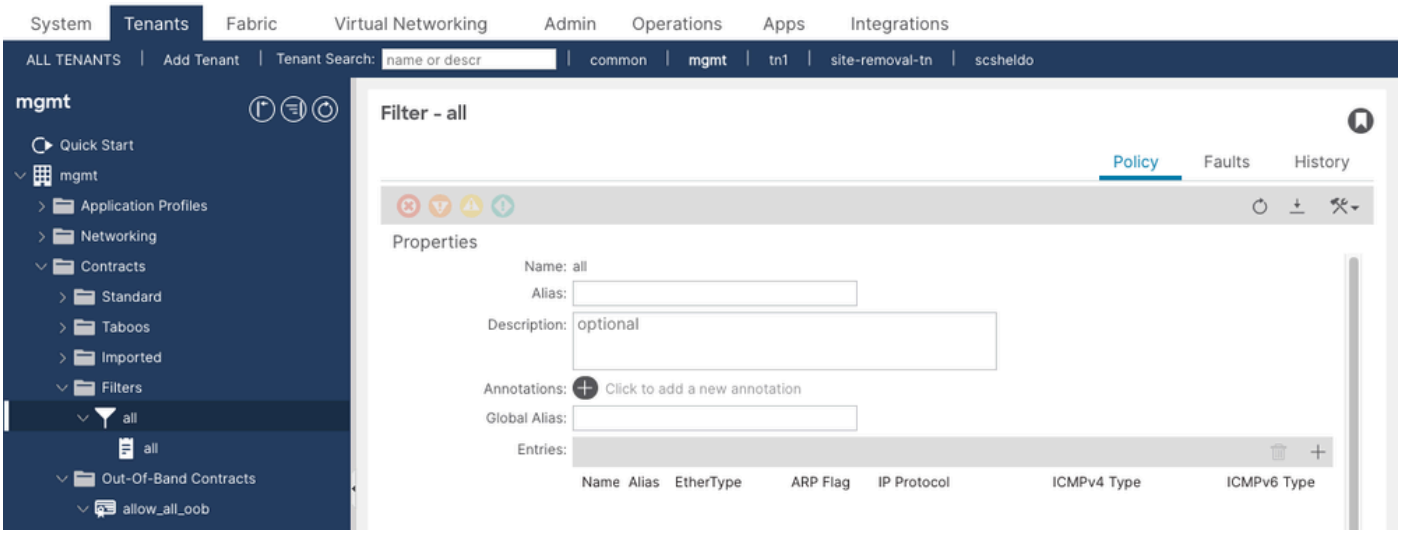
Schritt 3: Managementverträge für UDP-Port 161 konfigurieren

Navigieren Sie zu Tenants > mgmt > Contracts > Out-Of-Band Contracts. Überprüfen Sie, ob der Betreff des aktiven OOB-Vertrags auf einen Filtereintrag verweist, der den UDP-Port 161 (SNMP-Anforderungen) zulässt. Ohne diesen Vertrag für den APIC werden alle SNMP GET/WALK-Pakete ohne Unterbrechung verworfen.



Die Filtereinträge, die mit dem Vertragsgegenstand verknüpft sind, müssen einen Eintrag mit EtherType-IP, Protocol UDP und Zielport 161 enthalten. Das obige Beispiel zeigt einen allow-all-

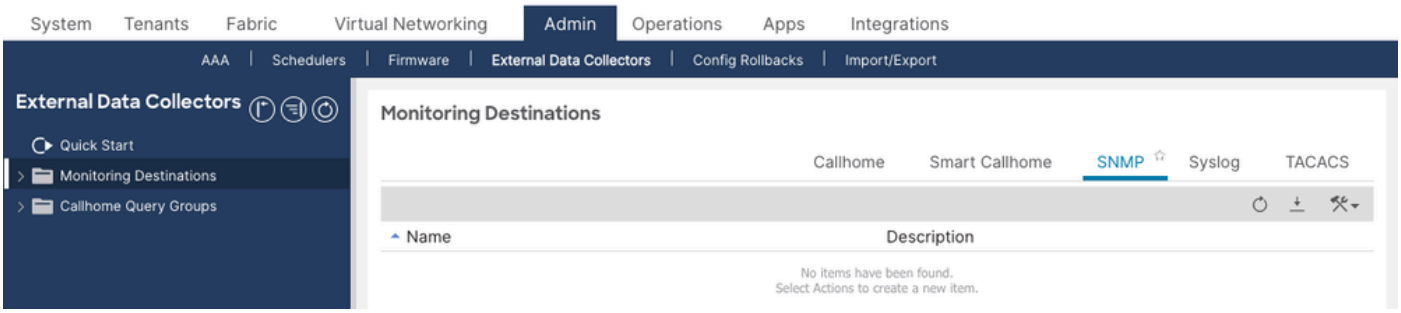
Filter (nicht angegebenes Protokoll), der SNMP zulässt, aber breiter ist als für die Produktion empfohlen. Ein dedizierter SNMP-Filtereintrag mit spezifischen UDP/161- und UDP/162-Einträgen wird bevorzugt.



Anmerkung: In früheren ACI-Firmware-Versionen waren bestimmte Ports auf Leaf- und Spine-Knoten immer offen, und ein Managementvertrag für SNMP war nicht erforderlich. In ACI 5.x ist der Vertrag für APIC-Knoten erforderlich. Leaf- und Spine-Knoten verwenden anstelle von Managementverträgen iptables-Regeln, die von den Client-Gruppenrichtlinien abgeleitet werden.

Schritt 4: SNMP-Trap-Ziele konfigurieren

Navigieren Sie zu Admin > External Data Collectors > Monitoring Destinations > SNMP. Klicken Sie mit der rechten Maustaste, und wählen Sie SNMP-Überwachungszielgruppe erstellen aus. Auf der Registerkarte SNMP werden alle konfigurierten Zielgruppen angezeigt. Eine leere Tabelle bedeutet, dass noch keine Trap-Ziele konfiguriert wurden.



Definieren:

- Gruppenname

- Trap-Ziele: Hostname/IP, UDP-Port (Standard 162), SNMP-Version, Community String und Verwaltungs-EPG

Schritt 5: Überwachungsquellen konfigurieren

Die Überwachungsquellen verknüpfen die SNMP-Zielgruppe mit den Überwachungsrichtlinien, die steuern, welche Ereignisse und Fehler Traps generieren. Sie müssen eine Überwachungsquelle an allen drei der folgenden Standorte konfigurieren, da Traps von einigen Knotentypen nicht gesendet werden:

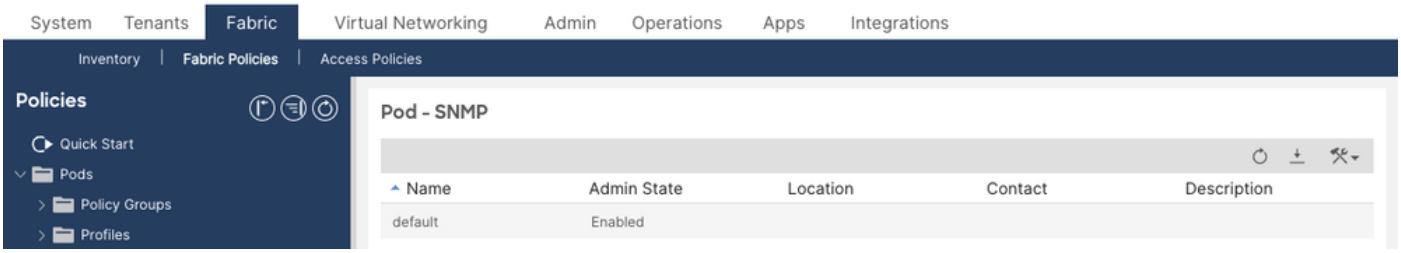
- Fabric > Fabric Policies > Policies > Monitoring > Default > Callhome/Smart Callhome/SNMP/Syslog/TACACS (deckt Fabric-Infrastrukturereignisse ab)
- Fabric > Fabric Policies > Policies > Monitoring > Common Policy > Callhome/Smart Callhome/SNMP/Syslog/TACACS (deckt Fabric-weite allgemeine Ereignisse ab)
- Fabric > Access Policies > Policies > Monitoring > Default > Callhome/Smart Callhome/SNMP/Syslog (deckt Zugriffs-/Infrastrukturereignisse ab)

Wählen Sie an jedem Standort SNMP als Quelltyp aus, und erstellen Sie eine neue SNMP-Quelle, die auf die in Schritt 4 erstellte Zielgruppe verweist.

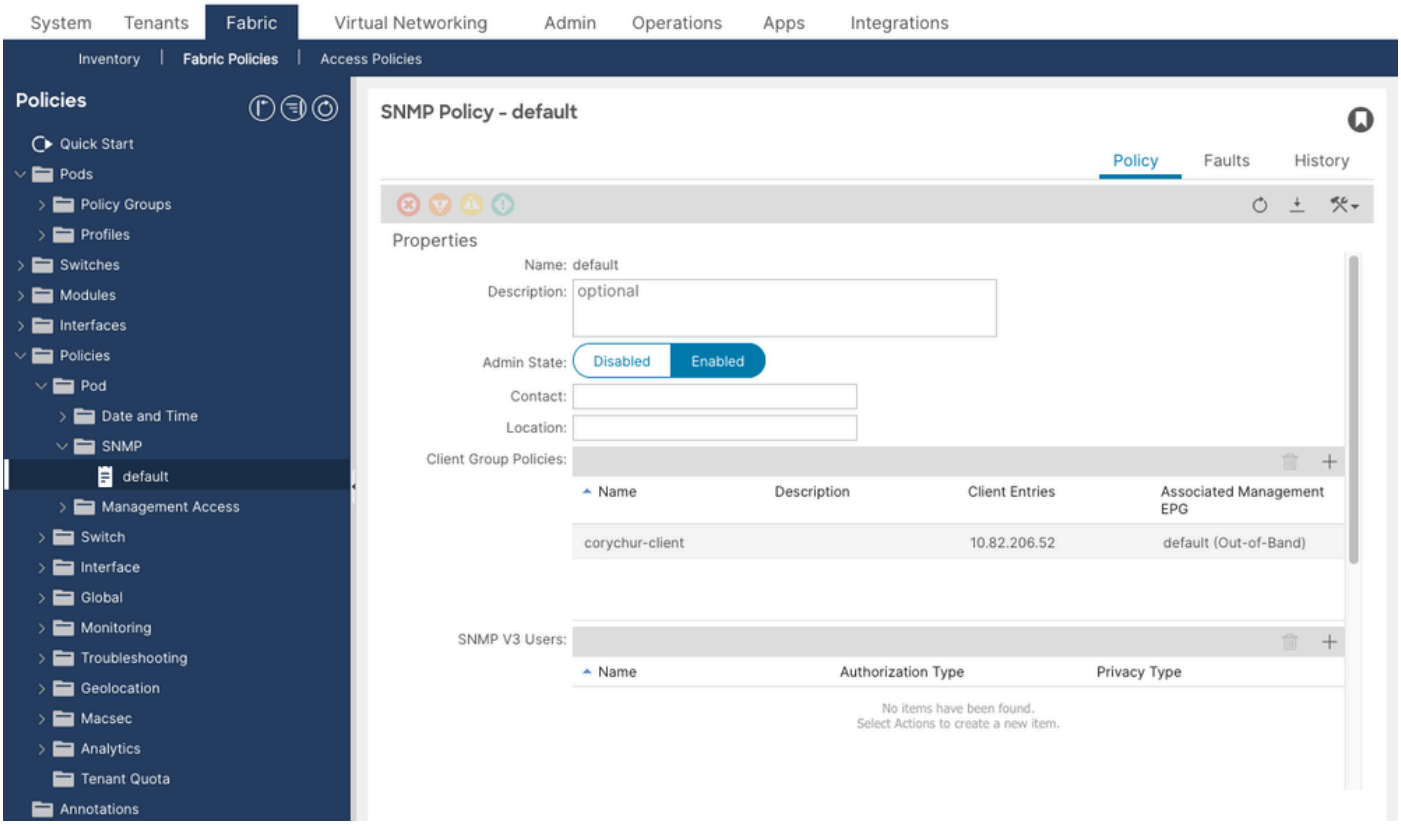
Konfiguration überprüfen

Überprüfung der SNMP-Richtlinienbereitstellung

Navigieren Sie zu Fabric > Fabric Policies > Policies > Pod > SNMP, und bestätigen Sie, dass die Standard-SNMP-Richtlinie vorhanden ist und der Admin-Status auf Enabled festgelegt ist. Die Liste der Richtliniengruppen zeigt alle konfigurierten SNMP-Richtlinien mit ihrem Admin-Status auf einen Blick.



Klicken Sie zur detaillierten Überprüfung auf den Richtliniennamen, um ihn zu öffnen. Vergewissern Sie sich, dass die Option "Admin State" (Admin-Status) auf "Enabled" (Aktiviert eingestellt ist, und dass die Client-Gruppenrichtlinien alle zulässigen NMS-Hosts mit der zugehörigen Management-EPG auflisten.



Führen Sie auf einem beliebigen APIC die folgende MO-Abfrage aus, um zu bestätigen, dass die SNMP-Richtlinie vorhanden und in der Fabric aktiviert ist:

<#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
```

Wenn `adminSt deaktiviert` ist, funktioniert SNMP auf keinem Knoten. Aktivieren Sie sie in der APIC-GUI unter Fabric > Fabric Policies > Policies > Pod > SNMP > default.

Community-String-Konfiguration überprüfen

<#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
```

Wenn keine Community zurückgegeben wird oder der Name nicht mit dem übereinstimmt, was das NMS verwendet, fügen Sie den Community String unter der SNMP-Richtlinie hinzu, oder korrigieren Sie ihn.

Überprüfen von Client-Gruppen-Richtlinien (SNMP-Zugriffskontrolle)

Client-Gruppenrichtlinien fungieren als ACL für SNMP GET/WALK-Zugriffe. Jede Richtlinie legt fest, welche Client-IP-Adressen Leaf-/Spine-Knoten abfragen dürfen, über welche Management-VRF-Instanz sie verfügen. Auf Leaf-/Spine-Knoten werden diese Richtlinien in iptables-Regeln übersetzt.

<#root>

apic1#

moquery -c snmpClientGrpP -x query-target=children

Total Objects shown: 3

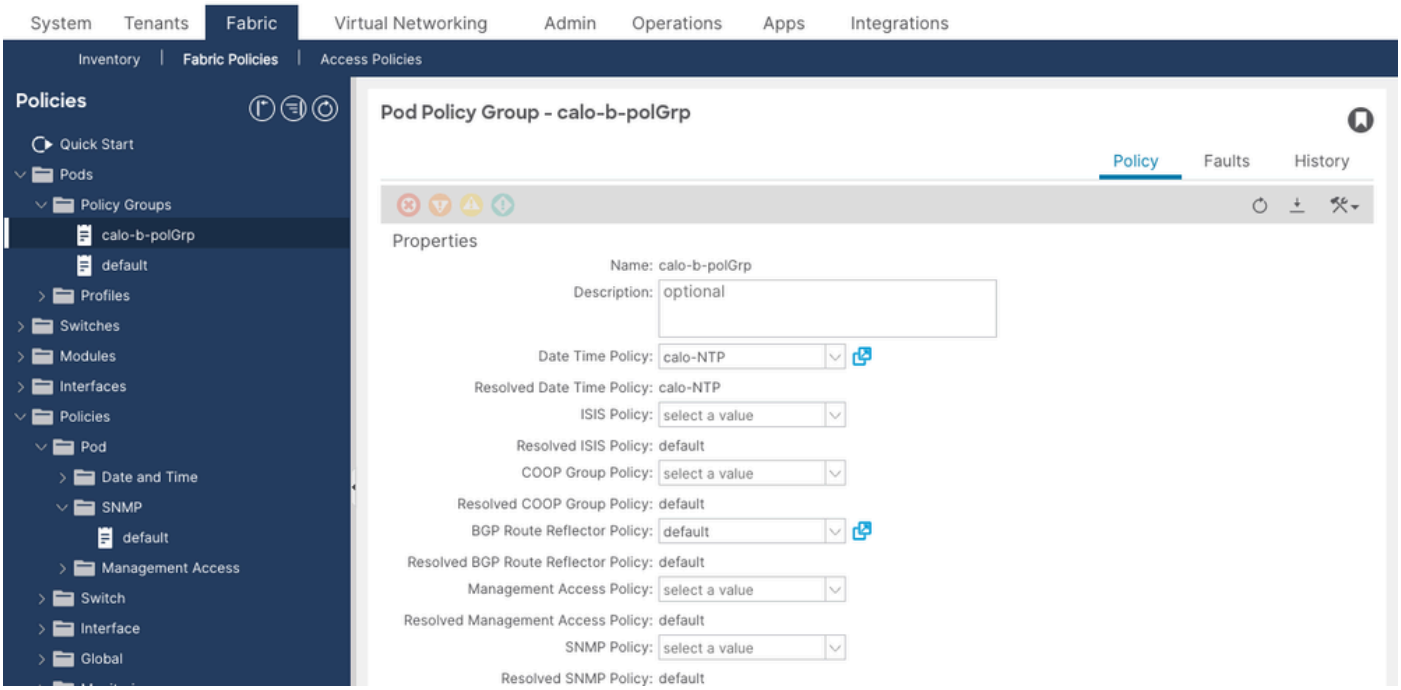
```
# snmp.ClientP
addr         : 10.1.1.50                   <--- NMS server IP
dn           : uni/fabric/snmppol-default/clgrp-NMS-Clients/client-[10.1.1.50]
name         : nms-server1

# 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
```

Bestätigen Sie, dass die IP-Adresse des NMS-Servers in den Clienteinträgen vorhanden ist. Wenn eine Client-IP fehlt, werden SNMP GET/WALK-Anforderungen von diesem Host durch iptables auf Leaf-/Spine-Knoten verworfen.

Anmerkung: SNMPv3 caveat - Client-Gruppenrichtlinien werden auf dem APIC nicht erzwungen, wenn SNMPv3 verwendet wird. Jegliche SNMPv3 GET/WALK zu einem APIC ist unabhängig von der Client-Gruppenkonfiguration zulässig. Die Durchsetzung von Client-Gruppen für SNMPv3 auf dem APIC ist eine bekannte Einschränkung. Auf Leaf- und Spine-Switches verhält sich die Client-Gruppendurchsetzung für SNMPv2c und SNMPv3 gleich.

Überprüfung der Pod-Richtliniengruppen-Referenzen SNMP-Richtlinie

Navigieren Sie zu Fabric > Fabric Policies > Pods > Policy Groups, und öffnen Sie die aktive Pod Policy Group. Vergewissern Sie sich, dass das Dropdown-Feld SNMP Policy (SNMP-Richtlinie) auf die gewünschte SNMP-Richtlinie eingestellt ist und das Feld Resolved SNMP Policy (Aufgelöste SNMP-Richtlinie) denselben Namen aufweist. Eine fehlende oder nicht aufgelöste Richtlinie bedeutet, dass die SNMP-Konfiguration niemals an Switches weitergeleitet wird.



Im obigen Screenshot wird im Feld "SNMP Policy" (SNMP-Richtlinie) "select a value" (einen Wert auswählen) (leer) angezeigt, während in der aufgelösten SNMP-Richtlinie "default" (Standard) angezeigt wird. Dies bedeutet, dass die Richtlinie vom Fabric-Standard übernommen, aber nicht explizit festgelegt wurde. Es wird empfohlen, das Feld "SNMP Policy" explizit festzulegen, um Mehrdeutigkeiten zu vermeiden.

Überprüfung über REST-API:

<#root>

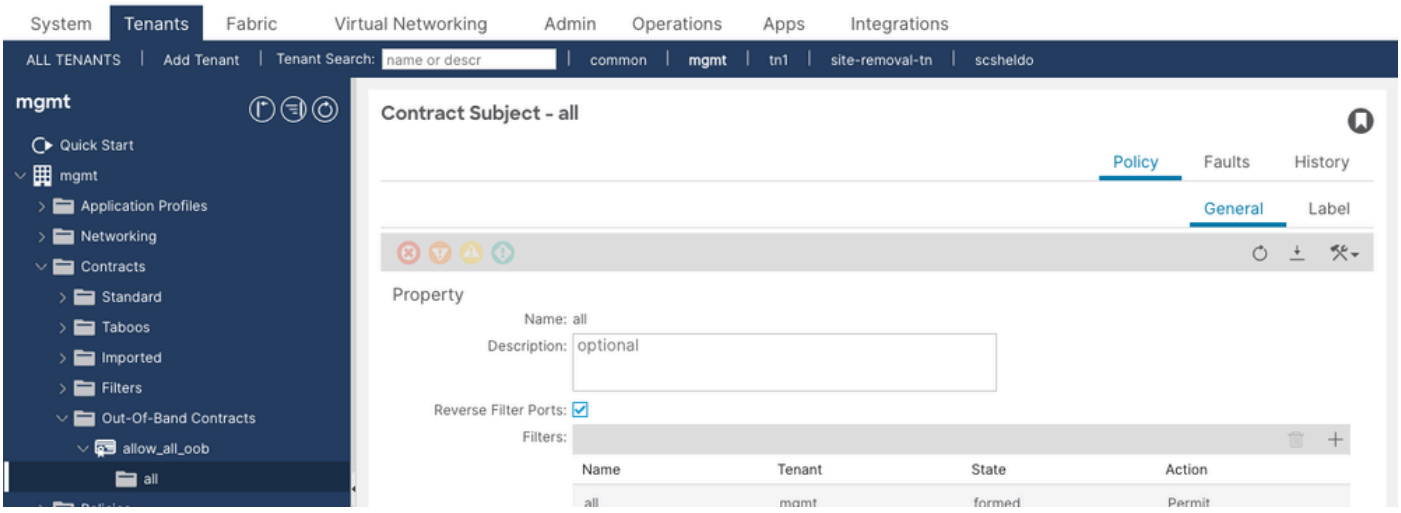
```
apic1#
```

```
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"
```

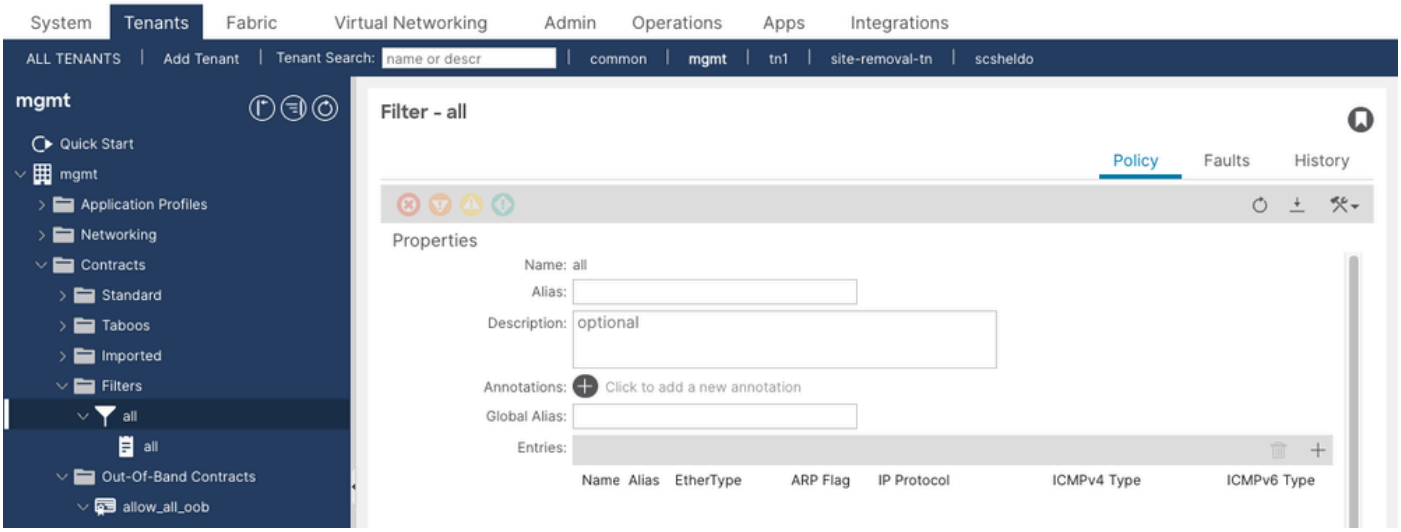
Wenn `der Status` nicht `gebildet` wird, ist die SNMP-Richtlinienbeziehung unterbrochen. Wählen Sie die SNMP-Richtlinie in der Pod Policy Group erneut aus, und senden Sie sie.

Überprüfen des Managementvertrags für UDP 161 (APIC-Knoten)

Navigieren Sie zu Tenants > mgmt > Contracts > Out-Of-Band Contracts (und In-Band Contracts bei Verwendung des INB-Managements). Öffnen Sie den aktiven OOB-Vertrag, und klicken Sie auf die Registerkarte Policy (Richtlinie). Überprüfen Sie, ob der Betreff auf einen Filter verweist, der den UDP-Port 161 zulässt.



Erweitern Sie den Filter, auf den der Betreff verweist, und bestätigen Sie, dass die Einträge einen Eintrag mit EtherType-IP, Protocol UDP, Destination Port 161 enthalten. Die Filtereinträge bestimmen, welcher Datenverkehr über den OOB-Managementvertrag zum APIC zulässig ist.



Der Filter sollte Folgendes anzeigen:

- Ethertyp: IP
- IP-Protokoll: UDP
- Zielport von: 161
- Zielport an: 161

Stellen Sie außerdem sicher, dass der UDP-Port 162 zulässig ist, wenn der APIC SNMP-Traps über die OOB-Schnittstelle senden soll.

Prüfung über MO-Abfrage:

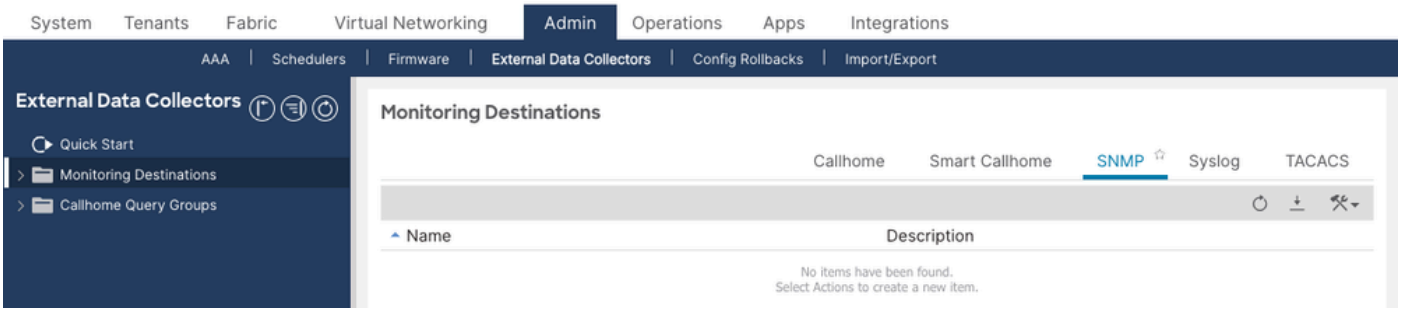
<#root>

```
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
```

Wenn keine Ergebnisse zurückgegeben werden, ist kein Filter für UDP 161 vorhanden. Fügen Sie eine zum Managementvertrag hinzu.

SNMP-Trap-Zielkonfiguration überprüfen

Navigieren Sie zu Admin > External Data Collectors > Monitoring Destinations > SNMP, um alle konfigurierten SNMP-Zielgruppen anzuzeigen. Eine leere Liste bedeutet, dass keine Trap-Ziele konfiguriert sind und keine Traps von einem Knoten gesendet werden.



<#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
```

Überprüfen Sie, ob die Trap-Ziel-IP, der Port, die Version, der Community-String und die Management-VRF (entweder `mgmt:inb` oder `management` for OOB) mit Ihrer Umgebung übereinstimmen. Die VRF-Instanz muss mit der dem Ziel zugewiesenen Management-EPG übereinstimmen.

Überprüfen der Konfiguration der Überwachungsquellen in allen drei Bereichen

SNMP-Quellen müssen in allen drei Überwachungsrichtlinienbereichen vorhanden sein. Wenn eine Quelle in einem Bereich fehlt, werden Traps von verwandten Ereignissen nicht weitergeleitet.

<#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
```

Wenn eine der drei Optionen fehlt, erstellen Sie die fehlende SNMP-Quelle mithilfe der GUI in der entsprechenden Überwachungsrichtlinie.

Betriebliche Überprüfung

Überprüfung des SNMP-Status mithilfe von show snmp summary (APIC)

Führen Sie diesen Befehl direkt auf jedem APIC aus, um zu überprüfen, ob der SNMP-Agent ausgeführt wird und die Konfiguration angewendet wurde:

<#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
```

Was in der Ausgabe zu überprüfen:

- Admin State muss `aktiviert` sein.
- Die Community muss mit den Geräten übereinstimmen, die das NMS verwenden soll.
- Die Client-Gruppe muss alle zulässigen NMS-IPs mit der richtigen Management-EPG auflisten.
- Der Host (Trap-Ziel) muss den NMS-Trap-Empfänger mit dem richtigen Port und der richtigen Version auflisten.

Überprüfung des SNMP-Status mithilfe von show snmp summary (Leaf/Spine)

<#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
```

Was in der Ausgabe zu überprüfen:

- Admin State muss `aktiviert` sein `und` mit einem PID `ausgeführt werden`. Wenn sie `deaktiviert` ist, wird die SNMP-Richtlinie nicht angewendet, oder die POD-Richtlinienkette ist unterbrochen.
- Der Community-Status muss `ok` sein. Ein `Fehlerstatus` weist auf ein Problem bei der Richtlinienbereitstellung hin.
- Client-VRF für jeden NMS-Host muss mit der VRF-Instanz der Management-EPG übereinstimmen (`mgmt:inb` für In-Band, `management` für OOB).
- Der Trap-Host muss das Ziel mit dem richtigen VRF-Kontext auflisten.

Überprüfen der Ausführung des snmpd-Prozesses

Auf einem Blatt oder Rückgrat:

<#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
```

Im 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
```

Wenn kein snmpd-Prozess auf einem Leaf oder Spine gefunden wird, wird SNMP auf diesem Knoten nicht ausgeführt. Überprüfen Sie, ob die SNMP-Richtlinie "Admin State" aktiviert und die

POD-Richtlinienkette richtig konfiguriert ist.

Spoiler (Zum Lesen markieren)

Überprüfung, ob der SNMP-Port abhört

<#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           :::*
```

Wenn Port 161 nicht im LISTEN-Status aufgeführt ist, wird der snmpd-Prozess nicht ausgeführt oder konnte keine Bindung zum Port herstellen.

Verifizieren von iptables-Regeln auf Leaf/Spine

Client-Gruppenrichtlinien werden auf jedem Leaf und Spine in iptables-Regeln übersetzt. Verwenden Sie folgende Punkte, um die Regeln zu überprüfen:

<#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)
```

Führen Sie folgende Schritte aus, um die richtigen VRF-IDs für Ihre Fabric zu ermitteln:

<#root>

```
leaf101#
```

show vrf

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

Die VRF-IDs in den IP-Tabellen müssen mit den `angezeigten VRF-`Berichten übereinstimmen. Wenn eine Client-IP nicht in den iptables-Regeln enthalten ist, werden SNMP-Anforderungen von diesem Host automatisch verworfen, selbst wenn der snmpd-Prozess ausgeführt wird.

Verwenden Sie Leistungsindikatoren, um zu überprüfen, ob ein SNMP-Paket zugeordnet oder verworfen wurde:

<#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
```

Anmerkung: Wenn SNMP ausgeführt wird, iptables jedoch keine snmp_rules-Ketten anzeigt oder die Ketten leer sind, können Sie den snmpd-Prozess neu starten, um eine Neuprogrammierung der iptables-Regel zu erzwingen. Das Senden von SIGKILL an die snmpd-PID ist sicher - der ACI-Prozess-Manager (`per Richtlinie`) startet das Programm automatisch neu. Führen Sie `pidof snmpd aus`, um die PID zu erhalten, und `beenden Sie -9 [snmpd_pid]`. Bestätigen Sie die neue PID mit `pidof snmpd` nach 10-15 Sekunden.

Überprüfen Sie, ob der SNMP-Port Endknoten abhört101# netstat -lutn | grep 161 Aktive Internetverbindungen (nur Server) Proto Recv-Q Send-Q Lokale Adresse Fremde Adresse Zustand tcp 0 0.0.0.0:161 0.0.0.0:* LISTEN <— SNMP-Agent akzeptiert Anfragen udp 0 0 0.0.0.0:161 0.0.0.0:* udp6 0 0 :::161 :::* Wenn Port 161 nicht im LISTEN-Status aufgeführt ist, wird der snmpd-Prozess nicht ausgeführt oder konnte keine Bindung mit dem Port herstellen. Überprüfen Sie, ob iptables-Regeln für Leaf/Spine-Client-Gruppenrichtlinien in iptables-Regeln für jedes Leaf und jeden Spine übersetzt werden. Verwenden Sie folgende Punkte, um die Regeln zu überprüfen: 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; Nur zugelassene Clients übergeben -A vrf_2_snmp_rules -s 10.1.1.50/32 -j ACCEPT <— zulässiger NMS-Client (OOB VRF) -A vrf_9_snmp_rules -s 10.1.1.50/32 -j ACCEPT <— zulässiger NMS-Client (INB VRF) Führen Sie Folgendes aus, um die richtigen VRF-IDs für Ihre Fabric zu ermitteln: leaf101# show vrf VRF-Name VRF-ID State Reason management 2 Up — mgmt:inb 9 Up — Die VRF-IDs in den iptables-Regeln müssen mit den angezeigten VRF-Berichten übereinstimmen. Wenn eine Client-IP nicht in den iptables-Regeln enthalten ist, werden SNMP-Anforderungen von diesem Host automatisch verworfen, selbst wenn

der snmpd-Prozess ausgeführt wird. Verwenden Sie Leistungsindikatoren, um zu überprüfen, ob ein SNMP-Paket zugeordnet oder verworfen wurde: leaf101# iptables -nvL | grep -A 20 "Chain snmp_rules" Chain snmp_rules (1 Referenzen) pkts bytes target port 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 IPs are missing Hinweis: Wenn SNMP ausgeführt wird, iptables jedoch keine snmp_rules-Ketten anzeigt oder die Ketten leer sind, können Sie den snmpd-Prozess neu starten, um eine Neuprogrammierung der iptables-Regel zu erzwingen. Das Senden von SIGKILL an die snmpd-PID ist sicher - der ACI-Prozess-Manager (per Richtlinie) startet das Programm automatisch neu. Führen Sie pidof snmpd aus, um die PID zu erhalten, und beenden Sie dann -9 [snmpd_pid]. Bestätigen Sie die neue PID mit pidof snmpd nach 10-15 Sekunden.

Überprüfung der Netzwerkverbindung mit SNMP-Ports

<#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
```

Vergewissern Sie sich, dass die Verwaltungsschnittstellen aktiv sind (keine RX-ERR-Inkremente) und Datenverkehr weiterleiten. `eth0` die OOB-Management-Schnittstelle ist; `kpm_inb` ist die In-Band-Managementschnittstelle des Switches.

Überprüfung des SNMP-Trap-Sendens mit tcpdump

Um zu bestätigen, dass Traps von einem Leaf- oder Spine-Knoten generiert und gesendet werden, erfassen Sie den Datenverkehr über die entsprechende Schnittstelle. Greifen Sie als Administrator auf den Knoten zu, und verwenden Sie:

<#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 NM
```

Für OOB:

<#root>

```
leaf101#
```

tcpdump -i eth0 -f port 162 -vv

Spoiler (Zum Lesen markieren)

Für APIC-Traps (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
```

Anmerkung: Auf dem APIC ist `bond0.1100` die In-Band-VLAN-Subschnittstelle der Management-Schnittstelle. Ersetzen Sie `1100` durch das für die In-Band-Management-EPG konfigurierte VLAN Encap. Verwenden Sie `oobmgmt` als Schnittstellennamen für OOB-Erfassungen auf dem APIC.

Für APIC-Traps (INB): 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 Hinweis: bond0.1100 ist die In-Band-VLAN-Subschnittstelle des APIC. Ersetzen Sie 1100 durch das für die In-Band-Verwaltungs-EPG konfigurierte VLAN-Encap. Verwenden Sie "obmgmt" als Schnittstellennamen für OOB-Erfassungen auf dem APIC.

Verifizieren von SNMP GET/WALK-Anforderungen mit 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
```

Wenn GetRequest angezeigt wird, aber keine GetResponse, wird die Anforderung empfangen, aber nicht beantwortet. Überprüfen Sie den snmpd-Prozess und den Community-String. Wenn weder Anfrage noch Antwort angezeigt wird, wird die Anfrage blockiert, bevor der Knoten erreicht wird (Routing und IP-Tabellen überprüfen).

Fehlerbehebung-Workflow

Entscheidungsablauf der Triage

Verwenden Sie diesen Entscheidungsbaum, wenn Techniker berichten, dass SNMP nicht funktioniert. Beginnen Sie mit dem beobachteten Symptom und folgen Sie den Zweigen bis zur Isolation.

Symptom: Keine Antwort auf SNMP GET/WALK-Anforderungen

1. Überprüfen Sie den SNMP-Verwaltungsstatus auf dem APIC. Führen Sie `moquery -c snmpPol aus`. Wenn `adminSt deaktiviert` ist, aktivieren Sie es, und fahren Sie mit Schritt 7 fort.
2. Überprüfen Sie den snmpd-Prozess. Führen Sie auf dem betroffenen Knoten `ps aux aus. | grep snmp` oder `pidof snmpd`. Wenn kein Prozess ausgeführt wird, wird die SNMP-Richtlinie nicht bereitgestellt. Überprüfen Sie die Pod-Richtlinienkette (SNMP-Richtlinie → Pod-Richtliniengruppe → Pod-Profil).
3. Überprüfen Sie, ob Port 161 abhört. `netstat -lutn` ausführen `| grep 161`. Wenn Port 161 sich nicht im LISTEN-Zustand befindet, ist der snmpd-Prozess fehlgeschlagen. Protokolle von `/var/log/dme/log/svc_ifc_dbgrelem.log*` sammeln und den Prozess neu starten.
4. Routing überprüfen. Führen Sie `show ip route vrf management` und `show ip route vrf mgmt:inb aus`. Bestätigen Sie, dass eine Route zum NMS-Host in der richtigen VRF-Instanz vorhanden ist.
5. Überprüfen Sie den Management-Vertrag für den APIC. Wenn das Ziel ein APIC (kein Leaf/Spine) ist, stellen Sie sicher, dass UDP 161 im OOB- oder INB-Managementvertrag zulässig ist.
6. Führen Sie tcpdump für den Knoten aus. Führen Sie `tcpdump -i kpm_inb -f Port 161 -vv aus` (oder `eth0` für OOB). Wenn GetRequest angezeigt wird, aber keine GetResponse folgt, erreicht die Anforderung den Knoten, snmpd reagiert jedoch nicht - überprüfen Sie die

Community-Zeichenfolge. Wenn überhaupt keine Anforderung angezeigt wird, liegt das Problem im Upstream (Routing oder Vertrag).
7. Test von einem zugelassenen Client aus. Führen Sie `snmpget -v2c -c [community] [node-ip] SNMPv2-MIB::sysDescr.0` von einem NMS-Host aus, der in der Client-Gruppe aufgeführt ist. Eine erfolgreiche Antwort bestätigt, dass SNMP voll betriebsbereit ist.

Symptom: Keine SNMP-Traps am NMS empfangen

1. Überprüfen Sie die Trap-Zielkonfiguration. Führen Sie `moquery -c snmpTrapDest aus`. Bestätigen Sie, dass die IP-Adresse, der Port, die Version und die Community des NMS den erwarteten Werten entsprechen.
2. Überprüfen Sie, ob in allen drei Bereichen Überwachungsquellen vorhanden sind. Ausführen von `moquery -c snmpSrc | egrep "snmp.src|name|dn"`. Bestätigen Sie, dass Einträge mit `monPolDn`-Werten für `uni/fabric/monfab-default`, `uni/fabric/moncommon` und `uni/infra/moninfra-default` vorhanden sind. Wenn SNMP-Quellen fehlen, fügen Sie sie der entsprechenden Überwachungsrichtlinie hinzu.
3. Überprüfen Sie den snmpd-Prozess. Stellen Sie sicher, dass snmpd auf dem Knoten ausgeführt wird, der das Trap senden soll.
4. Generieren Sie ein Testereignis, und erfassen Sie es mit tcpdump. Klappen einer Schnittstelle oder Ändern eines Status, um ein Ereignis zu generieren. Führen Sie auf dem Knoten `tcpdump -i kpm_inb -f Port 162 -vv aus`. Wenn kein Trap-Datenverkehr über die Leitung übertragen wird, generiert das Ereignis kein Trap. Überprüfen Sie die Überwachungsquelle `inkl`. Attribut (muss `Fehler` oder `Ereignisse` enthalten).
5. Überprüfen Sie die Verbindung zum Trap-Empfänger. Vergewissern Sie sich, dass der Trap-Empfänger von der Management-VRF-Instanz erreichbar ist: `show ip route vrf mgmt:inb` sollte einen Pfad zum NMS-Host anzeigen.
6. Wenn Traps auf tcpdump, aber nicht auf dem NMS angezeigt werden, liegt das Problem auf der Netzwerkseite: Firewall, Routing oder die NMS-Konfiguration. Überprüfen Sie, ob das NMS auf UDP 162 von der Management-Quell-IP-Adresse des ACI-Knotens abhört.

Gängige Szenarien

Szenario 1: SNMP-Richtlinie aktiviert, aber keine Daten von Leaf/Spine zurückgegeben

Problem: Die SNMP-Richtlinie auf dem APIC zeigt an, dass der Admin-Status aktiviert ist. Das NMS kann die Verwaltungs-IP des Leafs erreichen. `snmpget` wird ohne Antwort zu spät abgerufen.

Konfigurationsprüfung: Vergewissern Sie sich, dass die Pod Policy Group auf die SNMP-Richtlinie verweist und die Resolved SNMP Policy den richtigen Namen anzeigt. Wenn das Feld SNMP-Richtlinie der Pod-Richtliniengruppe leer ist oder die Beziehung nicht gebildet wurde, kann der

snmpd-Prozess auf den Switches nicht gestartet werden.

Betriebsprüfung: SSH auf das betroffene Leaf übertragen und `show snmp summary` ausführen. Wenn die Ausgabe den `Admin State` anzeigt: `deaktiviert`, obwohl der APIC aktiviert anzeigt, wurde die Richtlinie nicht bereitgestellt. Überprüfen Sie die POD-Richtlinienkette auf eine fehlende oder falsch referenzierte POD-Richtliniengruppe.

Ursache: Die SNMP-Richtlinie ist nicht mit der Pod Policy Group verknüpft, oder der Pod Profile-Selektor wendet nicht die richtige Pod Policy Group auf diesen Pod an.

Lösung:

1. Navigieren Sie zu Fabric > Fabric Policies > Pods > Policy Groups > default.
2. Bestätigen Sie, dass das Feld SNMP-Richtlinie auf die aktivierte SNMP-Richtlinie verweist.
3. Navigieren Sie zu Fabric > Fabric Policies > Pods > Profiles, und bestätigen Sie, dass der aktive Selektor auf diese Pod Policy Group verweist.
4. Nach dem Speichern überprüfen Sie `show snmp summary` auf dem Blatt innerhalb von 2 Minuten erneut.

Szenario 2: SNMP GET/WALK funktioniert für einige NMS-Hosts, aber nicht für andere

Problem: Ein NMS-Server kann ACI-Knoten erfolgreich abfragen. Ein zweiter NMS-Server in einem anderen Subnetz erhält keine Antwort.

Konfigurationsprüfung: Führen Sie `moquery -c snmpClientGrpP -x query-target=children` auf dem APIC aus. Bestätigen Sie, dass die IP-Adresse des zweiten NMS-Servers als Clienteintrag aufgeführt ist. Wenn sie fehlt, wird diese IP durch die iptables DROP-Regel am unteren Rand der snmp_rules-Kette blockiert.

Operational Check: Vergewissern Sie sich auf dem betroffenen Leaf, dass UDP 161 im OOB- oder INB-Managementvertrag erlaubt ist. Wenn kein Vertrag oder Filter über SNMP-Ports verfügt, wird die Anforderung verworfen.

Ursache: Die zweite NMS-Server-IP befindet sich nicht in der Client-Gruppenrichtlinie.

Lösung: Fügen Sie die fehlende NMS-IP als Client-Eintrag in der SNMP-Client-Gruppenrichtlinie unter Fabric > Fabric-Richtlinien > Richtlinien > Pod > SNMP > Standard > Client-Gruppenrichtlinien hinzu. Die iptables-Regeln auf allen Knoten werden innerhalb weniger Minuten nach dem Speichern der Richtlinie aktualisiert.

Szenario 3: SNMP-Traps nicht empfangen - Traps werden generiert, aber nicht bereitgestellt

Problem: Die Fehler sind in der Fehlertabelle des APIC sichtbar. `moquery -c snmpTrapDest` zeigt die richtige NMS-IP an. Das NMS empfängt keine Traps.

Konfigurationsprüfung: Ausführen von `moquery -c snmpSrc | egrep "snmp.src|name|dn"`. Überprüfen Sie, ob die Überwachungsquellen in allen drei Bereichen vorhanden sind (`monfab-default`, `moncommon`, `moninfra-default`). Eine häufige Überwachungsfunktion besteht darin, die Quelle nur in der Fabric-Standardrichtlinie zu konfigurieren, bei der Zugriffsrichtlinienereignisse nicht berücksichtigt werden.

Betriebsprüfung: Auslösen eines Testereignisses (z. B. Umschalten einer Schnittstelle in den deaktivierten Administratorzustand) Führen Sie auf dem relevanten Knoten `tcpdump -i kpm_inb -f Port 162 aus.` Wenn Trap-Pakete an der Schnittstelle des Knotens auftreten, funktioniert die ACI-Seite, und das Problem liegt im Netzwerkpfad zum NMS (Firewall, Routing). Wenn kein Trap auf dem Kabel erscheint, fehlt die ACI-Überwachungsquelle oder der Ereignistyp ist nicht im `incl-` Attribut der Quelle enthalten.

Ursache 1: Mindestens eine Überwachungsquelle fehlt in den erforderlichen Bereichen.

Ursache 2: Die Überwachungsquelle `inkl.` Attribut schließt den generierten Ereignistyp aus (z.B. `inkl.: Ereignisse` ohne `Fehler` bedeutet, dass keine fehlerbasierten Traps gesendet werden).

Lösung:

1. Fügen Sie fehlende Überwachungsquellen in der GUI für jeden der drei Bereiche hinzu (Fabric-Standard, Fabric Common, Access-Standard). Legen Sie die Zielgruppe auf die konfigurierte SNMP-Zielgruppe fest.
2. Vergewissern Sie sich, dass das `incl`-Attribut `Audits, Ereignisse und Fehler` für eine umfassende Trap-Abdeckung enthält.
3. Nach den Änderungen muss das Testereignis erneut ausgelöst werden, und tcpdump muss erneut überprüft werden.

Spoiler (Zum Lesen markieren)

Anmerkung: Auf dem APIC `ist der Befehl tcpdump/code> nur für Root-Benutzer verfügbar. Für APIC und Switches ist der Befehl iptables nur für Root-Benutzer verfügbar.`

Szenario 4: SNMPv3-Client-Gruppendurchsetzung für APIC funktioniert nicht

Problem: Ein SNMP-Client, der NICHT in der Client-Gruppenrichtlinie enthalten ist, kann den APIC erfolgreich über SNMPv3 abfragen, obwohl die gleiche Abfrage von Leaf-/Spine-Knoten fehlschlägt.

Ursache: Dies ist ein **bekannter Vorbehalt**. Client-Gruppenrichtlinien (IP-basierte IP-Quelldurchsetzung) werden für SNMPv3 GETs/Walks zu APIC-Controllern nicht angewendet. Jeder Host kann den APIC über SNMPv3 abfragen, unabhängig von der Konfiguration der Client-Gruppe. Auf Leaf- und Spine-Switches funktioniert die Durchsetzung von Client-Gruppen für SNMPv2c und SNMPv3 identisch.

Eindämmung: Verwenden Sie Managementvertragsfilter auf dem APIC, um den SNMP-Zugriff nach Quell-Subnetz zu beschränken. Client-Gruppen sind für Leaf-/Spine-Knoten effektiv. Verlassen Sie sich beim APIC mit SNMPv3 auf die quellenbasierte Filterung für Managementverträge als Zugriffskontrollmechanismus.

Szenario 5: SNMP-Abfragen erfolgreich, aber MIB-Daten sind unvollständig oder veraltet

Problem: SNMP GET/WALK gibt Daten zurück, aber bestimmte MIB OIDs geben leere oder veraltete Werte zurück. Insbesondere spiegeln Schnittstellenstatistiken oder Betriebsstatusdaten nicht den aktuellen Fabric-Status wider.

Betriebsprüfung: Bestätigen Sie, welcher APIC abgefragt wird. Jeder APIC gibt nur MIB-Objekte für die lokalen Daten zurück. Führen Sie show snmp summary für den abgefragten APIC aus, und vergleichen Sie das Ergebnis mit dem, was Sie erwarten. Abfragen von Switch-Daten (IF-MIB, entityMIB) direkt am Switch, nicht am APIC.

Ursache: Abfragen eines APIC auf Leaf-MIB-Daten. Jeder APIC stellt MIB-Objekte nur für seine eigenen verwalteten Objekte bereit. Daten auf Switch-Ebene (Schnittstellenstatus, CPU, Speicher, Umgebungssensoren) müssen durch direktes Polling aller Leaf- und Spine-Knoten abgerufen werden.

Lösung: Konfigurieren Sie das NMS so, dass es Leaf- und Spine-Management-IPs direkt nach den Schnittstellen- und Hardware-MIB-Daten abfragt. Verwenden Sie APIC-Management-IPs nur für APIC-native MIBs (Einheit, FRU, Prozess, Sensor in Bezug auf die APIC-Serverhardware).

Szenario 6: SNMP Kompatibel mit Leaf/Spine, jedoch nicht mit dem APIC

Problem: SNMPv2c GET vom NMS zu Leaf- und Spine-Knoten ist erfolgreich. Dasselbe NMS kann den APIC nicht abfragen.

Konfigurationsprüfung: Für das APIC-SNMP ist ein expliziter Managementvertrag erforderlich, der UDP 161 zulässt. Navigieren Sie zu **Tenants > mgmt**, und überprüfen Sie den OOB-/INB-Vertrag und dessen Filter auf UDP 161.

Betriebsprüfung: Führen Sie auf dem APIC iptables -S aus. | grep 161. Wenn keine ACCEPT-Regeln für UDP 161 in der fp-137-Kette (oder einem entsprechenden OOB-Vertrag) angezeigt werden, fehlt der Vertragsfilter für UDP 161 oder wurde nicht bereitgestellt.

```
<#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
```

Wenn diese Regeln fehlen, fügen Sie dem Betreff des Managementvertrags einen Filtereintrag für UDP 161 hinzu, und überprüfen Sie diesen erneut.

Ursache: Fehlender oder falsch konfigurierter Managementvertrag. In ACI 5.x setzen APIC-Knoten den Managementvertrag strikt durch - SNMP-Pakete werden verworfen, es sei denn, es besteht eine explizite Genehmigung.

Lösung:

1. Navigieren Sie zu **Tenants > mgmt > Security Policies > Out-Of-Band Contracts**.
2. Erweitern Sie den OOB-Vertrag, wählen Sie den Betreff aus, und überprüfen/fügen Sie einen Filter für den **UDP-Port 161 hinzu**.
3. Wiederholen Sie den In-Band-Vertrag, wenn das NMS den APIC über das INB-Management erreicht.
4. Verifizieren mit iptables -S | Grep 161 auf dem APIC nach dem Speichern.

Szenario 7: SNMP-iptables-Regeln fehlen oder sind falsch

Problem: show snmp summary zeigt, dass die SNMP-Richtlinie angewendet wurde, aber iptables -S | grep snmp gibt keine Regeln zurück, oder die NMS-Client-IP ist nicht in den Regeln enthalten.

Betriebsprüfung: Bestätigen Sie, dass snmpd mit pidof snmpd ausgeführt wird. Wenn snmpd ausgeführt wird, iptables jedoch keine SNMP-Regeln hat, wurde der Prozess vor der Bereitstellung der Client-Gruppenrichtlinie gestartet. Starten Sie snmpd neu, um eine Neuprogrammierung der Regel zu erzwingen, wenn die Anzahl der Neustarts kleiner als 250 ist:

<#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

Der ACI-Prozessmanager startet snmpd automatisch neu. Überprüfen Sie nach dem Neustart:

<#root>

leaf101#

iptables -S | grep -i snmp

Die snmp_rules-Ketten und ACCEPT-Regeln für VRF-Clients sollten jetzt angezeigt werden.

Ursache: Der snmpd-Prozess wurde neu gestartet oder gestartet, bevor die Client-Gruppenrichtlinie vollständig auf dem Knoten bereitgestellt wurde, sodass iptables nicht über die SNMP-Zugriffsregeln verfügen.

Anmerkung: Auf dem APIC ist der Befehl tcpdump/code> nur für Root-Benutzer verfügbar. Der Befehl iptables für den APIC und die Switches ist nur für Root-Benutzer verfügbar. Szenario 4: Die Durchsetzung der SNMPv3-Clientgruppe funktioniert nicht mit dem APIC-Problem: Ein SNMP-

Client, der NICHT in der Client-Gruppenrichtlinie enthalten ist, kann den APIC erfolgreich über SNMPv3 abfragen, obwohl die gleiche Abfrage von Leaf-/Spine-Knoten fehlschlägt. Ursache: Dies ist ein bekannter Vorbehalt. Client-Gruppenrichtlinien (IP-basierte IP-Quelldurchsetzung) werden für SNMPv3 GETs/Walks zu APIC-Controllern nicht angewendet. Jeder Host kann den APIC über SNMPv3 abfragen, unabhängig von der Konfiguration der Client-Gruppe. Auf Leaf- und Spine-Switches funktioniert die Durchsetzung von Client-Gruppen für SNMPv2c und SNMPv3 identisch. Abschwächung: Verwenden Sie Managementvertragsfilter auf dem APIC, um den SNMP-Zugriff nach Quell-Subnetz zu beschränken. Client-Gruppen sind für Leaf-/Spine-Knoten effektiv. Verlassen Sie sich beim APIC mit SNMPv3 auf die quellenbasierte Filterung für Managementverträge als Zugriffskontrollmechanismus. Szenario 5: SNMP-Abfragen erfolgreich, aber MIB-Daten sind unvollständig oder veraltet: SNMP GET/WALK gibt Daten zurück, aber bestimmte MIB OIDs geben leere oder veraltete Werte zurück. Insbesondere spiegeln Schnittstellenstatistiken oder Betriebsstatusdaten nicht den aktuellen Fabric-Status wider. Betriebsprüfung: Bestätigen Sie, welcher APIC abgefragt wird. Jeder APIC gibt nur MIB-Objekte für die lokalen Daten zurück. Führen Sie show snmp summary auf dem abgefragten APIC aus, und vergleichen Sie das Ergebnis mit Ihren Erwartungen. Abfragen von Switch-Daten (IF-MIB, entityMIB) direkt am Switch, nicht am APIC. Ursache: Abfragen eines APIC auf Leaf-MIB-Daten. Jeder APIC stellt MIB-Objekte nur für seine eigenen verwalteten Objekte bereit. Daten auf Switch-Ebene (Schnittstellenstatus, CPU, Speicher, Umgebungssensoren) müssen durch direktes Polling aller Leaf- und Spine-Knoten abgerufen werden. Lösung: Konfigurieren Sie das NMS so, dass es Leaf- und Spine-Management-IPs direkt nach den Schnittstellen- und Hardware-MIB-Daten abfragt. Verwenden Sie APIC-Management-IPs nur für APIC-native MIBs (Einheit, FRU, Prozess, Sensor in Bezug auf die APIC-Serverhardware). Szenario 6: SNMP Kompatibel mit Leaf/Spine, jedoch nicht mit dem APIC-Problem: SNMPv2c GET vom NMS zu Leaf- und Spine-Knoten ist erfolgreich. Dasselbe NMS kann den APIC nicht abfragen. Konfigurationsprüfung: Für das APIC-SNMP ist ein expliziter Managementvertrag erforderlich, der UDP 161 zulässt. Navigieren Sie zu Tenants > mgmt, und überprüfen Sie den OOB-/INB-Vertrag und dessen Filter auf UDP 161. Operational Check: Führen Sie auf dem APIC iptables -S aus. | grep 161. Wenn keine ACCEPT-Regeln für UDP 161 in der fp-137-Kette (oder einem entsprechenden OOB-Vertrag) angezeigt werden, fehlt der Vertragsfilter für UDP 161 oder wurde nicht bereitgestellt. apic1# iptables -S | grep 161 -A fp-137 -s 10.0.0.0/8 -p udp -m udp —dport 161 -j ACCEPT <— SNMP vom Management-Subnetz zulassen -A fp-137 -s 172.18.0.0/16 -p udp -m udp —dport 161 -j ACCEPT <— permit SNMP vom INB-Management-Subnetz Wenn diese Regeln nicht vorhanden sind, fügen Sie dem Betreff des Managementvertrags einen Filtereintrag für UDP 161 hinzu, und überprüfen Sie diesen erneut. Ursache: Fehlender oder falsch konfigurierter Managementvertrag. In ACI 5.x setzen APIC-Knoten den Managementvertrag strikt durch - SNMP-Pakete werden verworfen, es sei denn, es besteht eine explizite Genehmigung. Lösung: Navigieren Sie zu Tenants > mgmt > Security Policies > Out-Of-Band Contracts. Erweitern Sie den OOB-Vertrag, wählen Sie den Betreff aus, und überprüfen/fügen Sie einen Filter für den UDP-Port 161 hinzu. Wiederholen Sie den Vorgang für den In-Band-Vertrag, wenn das NMS den APIC über das INB-Management erreicht. Verifizieren mit iptables -S | grep 161 auf dem APIC nach dem Speichern. Szenario 7: SNMP-iptables-Regeln fehlen oder falsches Problem: show snmp summary zeigt, dass die SNMP-Richtlinie angewendet wurde, aber iptables -S | grep snmp gibt keine Regeln zurück, oder die NMS-Client-IP ist in den Regeln nicht enthalten. Betriebsprüfung: Bestätigen, dass snmpd mit pidof snmpd ausgeführt wird. Wenn snmpd ausgeführt wird, iptables jedoch keine SNMP-Regeln hat, wurde der Prozess vor der Bereitstellung der Client-Gruppenrichtlinie gestartet. Starten Sie snmpd neu, um eine Neuprogrammierung der Regel zu erzwingen, wenn die Anzahl der Neustarts kleiner als 250 ist: leaf101# pidof snmpd 5881leaf101# show system internal sysmgr service name snmpdService "snmpd" ("snmpd", 127):UUID = 0x1A, PID = 5881, SAP = 1545Status: SRV_STATE_HANDSHAKED (eingetragen am 25. August um 19:23:50 Uhr 2025).Anzahl der Neustarts: 3Zeitpunkt des letzten Neustarts: Montag, 25. August 2025, 19:23:48 Uhr.Vorherige PID: 32080Grund der letzten Kündigung: SYSMGR_DEATH_REASON_FAILURE_SIGNALTag = N/APlugin-ID: 0 leaf101# kill -9 5881 Der ACI-Prozessmanager startet snmpd automatisch neu. Überprüfen Sie nach dem Neustart: leaf101# iptables -S | grep -i snmp Die snmp_rules-Ketten und ACCEPT-Regeln für VRF-Clients sollten jetzt angezeigt werden. Ursache: Der snmpd-Prozess wurde neu gestartet oder gestartet, bevor die Client-Gruppenrichtlinie vollständig auf dem Knoten bereitgestellt wurde, sodass iptables nicht über die SNMP-Zugriffsregeln verfügen.

Protokolldateien für die erweiterte Fehlerbehebung

Wenn das Problem durch die obigen Verifizierungsschritte nicht behoben wird, enthalten die folgenden Protokolldateien auf Leaf-, Spine- und APIC-Knoten Diagnoseinformationen, die sich auf das SNMP beziehen:

<#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/*

Diese Protokolle enthalten snmpd-Neustartereignisse, Richtlinienbereitstellungsereignisse und Community-/Client-Konfigurationsfehler, die in show snmp summary nicht sichtbar sind.

Referenzen

- Konfigurationsleitfaden zur Cisco APIC-Systemverwaltung, Version 5.x - SNMP-Verwaltung
- Cisco ACI MIB - Kurzreferenz

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.