Risoluzione dei problemi relativi al protocollo SNMP in Cisco ACI Fabric

Introduzione

In questo documento viene descritto come configurare, verificare e risolvere i problemi di SNMP in Cisco ACI per ACI release 5.x e successive. Il documento descrive il modello di regole SNMP, i contratti di gestione richiesti, la configurazione trap, la verifica operativa tramite query CLI e MO (Managed Object) e i flussi di lavoro per la risoluzione strutturata dei problemi relativi agli scenari di errore più comuni tra switch foglia/spine e controller APIC.

Premesse

Il materiale illustrato in questo documento viene tratto dalla nota tecnica interna SNMP del Cisco ACI Solutions Delivery Team in ACI: Panoramica, configurazione, risoluzione dei problemi e avvertenze/problemi scritti da Tomas de Leon, integrati dalla Cisco APIC System Management Configuration Guide (versione 5.x) e dalla Cisco ACI MIB Quick Reference Guide.

Panoramica

Architettura SNMP in ACI

SNMP (Simple Network Management Protocol) è un protocollo basato su UDP che gestisce la gestione e il monitoraggio della rete. In ACI, il protocollo SNMP funziona in modo indipendente su ciascuna entità gestita. Ogni switch foglia, switch spine e controller APIC è il proprio agente SNMP; è necessario eseguire il polling o il monitoraggio di ciascuno in modo indipendente.

ACI supporta le seguenti funzionalità SNMP:

- Operazioni di lettura (Get, GetNext, BulkGet, Walk) — supportate su switch foglia/dorso e controller APIC.
- Notifiche (Trap): trap SNMPv1, v2c e v3 supportate su switch foglia/dorso e controller APIC.
- SNMPv3: supportato su switch foglia/dorso e controller APIC.
- Operazioni di scrittura (Set) - NON supportate su nessun dispositivo ACI.
- IPv6: SNMP è supportato solo su IPv4.

Nota: In un cluster APIC, ogni APIC fornisce oggetti MIB locali a se stesso. Il polling di ciascun APIC deve essere eseguito in modo indipendente; nessuna aggregazione SNMP a livello di cluster. Analogamente, ciascun interruttore a foglia e dorso deve essere interrogato in modo indipendente.

Architettura SNMPD sull'APIC

L'APIC esegue il processo snmpd, che ha due componenti interni:

- Agent: un agente net-snmp open-source (versione 5.7.6 o successive) che gestisce l'elaborazione del protocollo SNMP e la gestione delle sessioni.
- DME (Data Model Engine): si interfaccia con l'MIT (Management Information Tree) APIC per leggere oggetti gestiti e convertire gli attributi MO in formato oggetto SNMP. Le trap SNMP vengono generate da eventi e guasti generati sui dischi magneto-ottici.

Modello di policy SNMP e catena di distribuzione

ACI utilizza un modello basato su regole per SNMP. La configurazione SNMP viene astratta come un oggetto gestito snmpPol e deve essere associata al gruppo di criteri POD dell'infrastruttura prima di essere distribuita in qualsiasi nodo. La catena di distribuzione completa è:

1. SNMP Policy (`snmpPol`): definisce lo stato di amministrazione, le stringhe della community, i criteri di gruppo dei client (ACL) e gli utenti SNMPv3.
2. Pod Policy Group: fa riferimento alla policy SNMP insieme ad altre policy a livello di pod (BGP, ISIS, NTP, ecc.).
3. Pod Profile Selector — applica il Pod Policy Group ai pod fabric.

Inoltre, la configurazione delle trap SNMP richiede:

1. SNMP Monitoring Destination Group (`snmpGroup`): definisce gli host di destinazione delle trap, la porta, la versione SNMP e la community.
2. Origini di monitoraggio (`snmpSrc`): collegare il gruppo di destinazione a tre ambiti di criteri di monitoraggio distinti: Predefinito fabric, Criterio comune fabric e Predefinito criterio di accesso.

Per i nodi APIC sono richiesti contratti di gestione che consentano l'uso della porta UDP 161 (richieste SNMP) e della porta UDP 162 (trap SNMP). I nodi foglia e spine richiedono inoltre regole iptables corrette, che vengono programmate automaticamente quando vengono configurati Criteri di gruppo client.

MIB supportati

I MIB supportati su APIC includono:

- Entità MIB — PhysicalTable
- Cisco Entity Ext MIB - PhysicalProcessorTable, tabella LEDT
- MIB controllo FRU entità Cisco: PowerSupplyGroupTable, PowerStatusTable, FanTrayStatusTable, PhysicalTable
- MIB sensore entità Cisco: SensorValueTable, SensorThresholdTable
- MIB processo Cisco: CPUTotalTable, ProcessTable, ProcessExtRevTable, ThreadTable

Gli switch foglia e spine espongono i MIB NX-OS standard, tra cui IF-MIB, IP-MIB, CISCO-CDP-MIB, CISCO-ENTITY-QFP-MIB e la suite completa CISCO-ENTITY-FRU-CONTROL-MIB.

Le trap SNMP generate sull'APIC includono: `cefcFRUInserted`, `cefcFRURemoved`, `cefcFanTrayStatusChange`, `cefcModuleStatusChange`, `entSensorThresholdNotification`, `cefcPowerStatusChange`, `cpmCPURisingThreshold`, `cpmCPUFallingThreshold`.

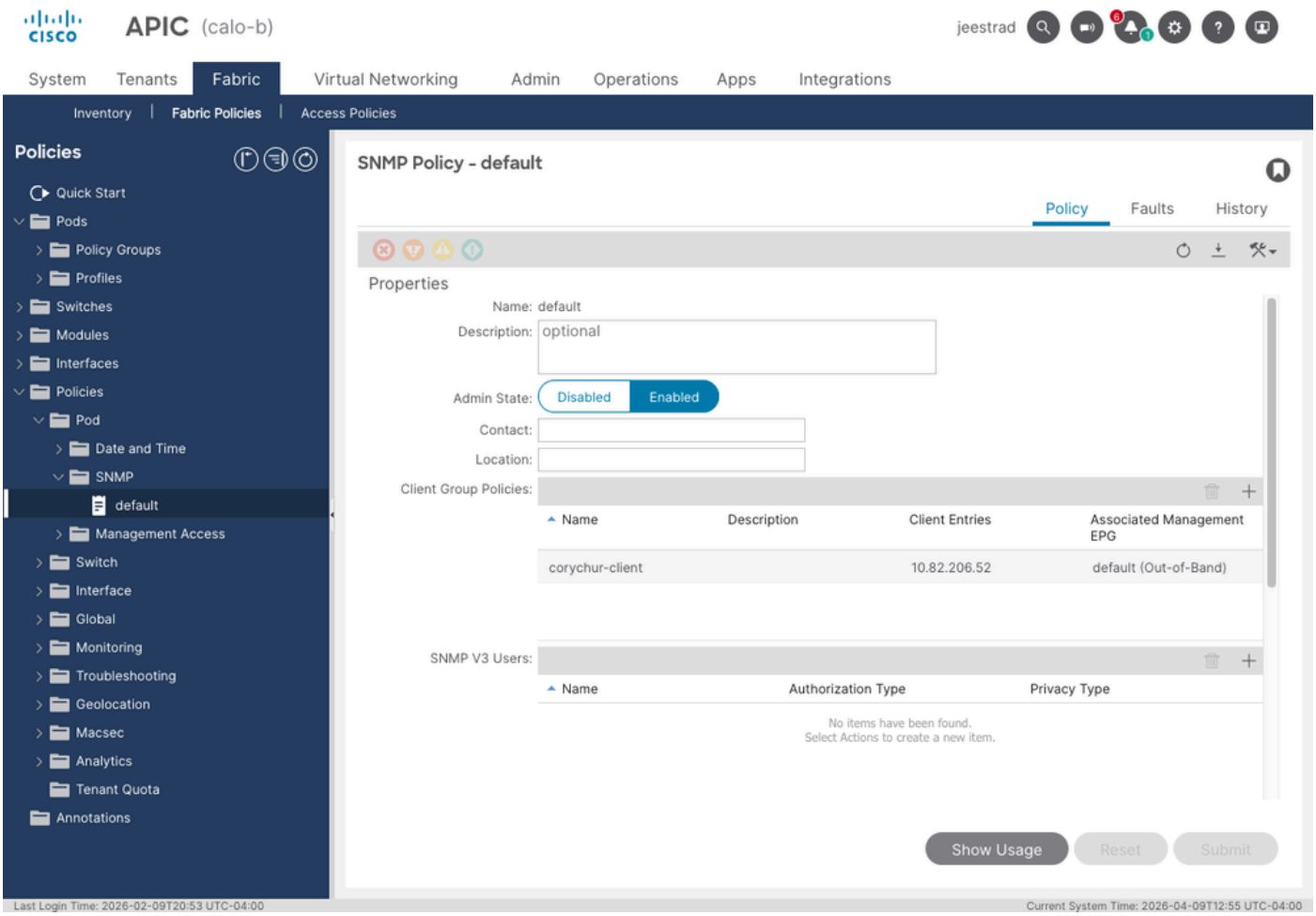
Configurazione di SNMP in ACI

Nota: In questa sezione viene fornito un riepilogo del flusso di lavoro di configurazione come contesto per le sezioni di verifica e risoluzione dei problemi riportate di seguito. Per procedure di configurazione complete, consultare la guida alla configurazione di Cisco APIC System Management.

Passaggio 1: Configurare il criterio SNMP

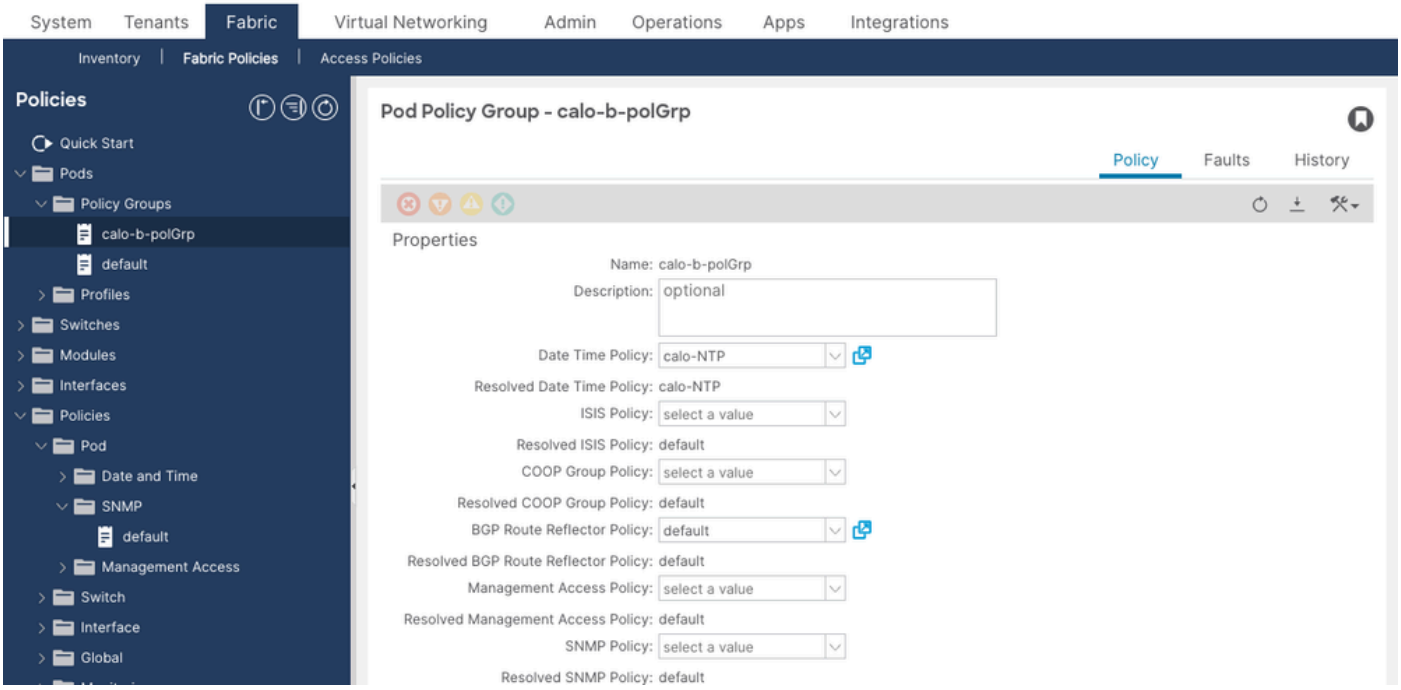
Selezionare Fabric > Fabric Policies > Policies > Pod > SNMP. Selezionare (o creare) il criterio SNMP, in genere denominato default. Configurazione:

- Stato amministrazione — impostato su Abilitato.
- Criteri di community — aggiungere la stringa della community utilizzata dal proprio NMS.
- Criteri gruppo client: definire uno o più profili di gruppo client, ciascuno dei quali specifica gli IP client SNMP consentiti e la gestione associata EPG (Out-of-Band o In-Band).
- Utenti SNMPv3: se si utilizza SNMPv3, aggiungere qui gli utenti con i parametri di autenticazione e privacy.



Passaggio 2: Associare i criteri SNMP al gruppo di criteri POD

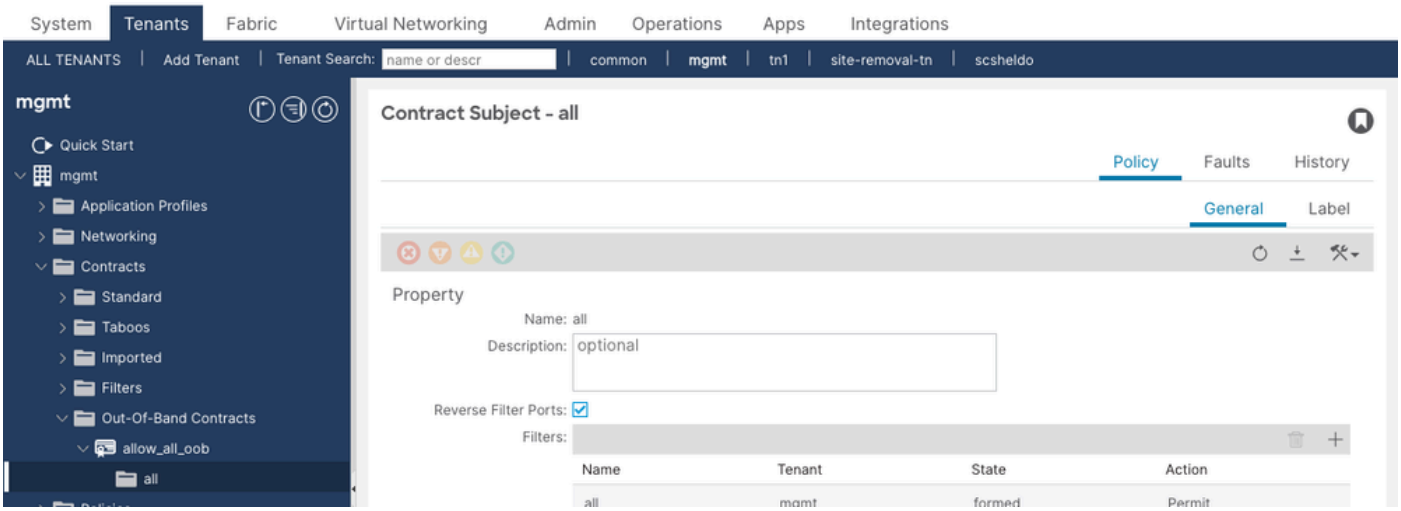
Passare a Fabric > Fabric Policies > Pods > Policy Groups (Infrastruttura > Criteri fabric > Pod > Gruppi di criteri). Selezionare il gruppo di criteri POD attivo (in genere denominato predefinito). Impostare il campo Criteri SNMP in modo che punti al criterio SNMP creato nel passaggio 1. Verificare che il campo Criteri SNMP risolti visualizzi il nome corretto del criterio.



Quindi, selezionare Fabric > Fabric Policies > Pods > Profiles (Infrastruttura > Criteri fabric > Profilati), espandere il profilo predefinito del pod e verificare che il selettore attivo faccia riferimento al gruppo di criteri del pod corretto.

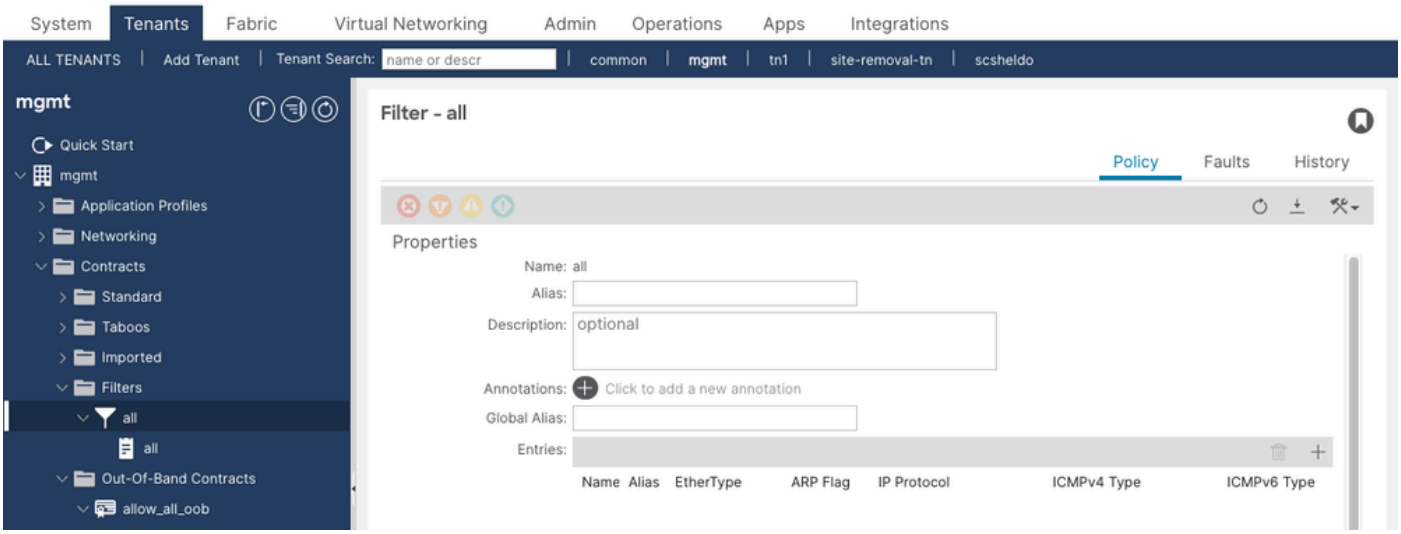
Passaggio 3: Configura contratti di gestione per la porta UDP 161

Passare a Tenant > Gestione > Contratti > Contratti fuori banda. Verificare che l'oggetto del contratto OOB attivo faccia riferimento a una voce di filtro che consente la porta UDP 161 (richieste SNMP). Senza questo contratto sull'APIC, tutti i pacchetti GET/WALK SNMP verranno eliminati automaticamente.



Le voci di filtro associate all'oggetto del contratto devono includere una voce con EtherType IP, Protocol UDP e Destination Port 161. L'esempio precedente mostra un filtro allow-all (unspecified

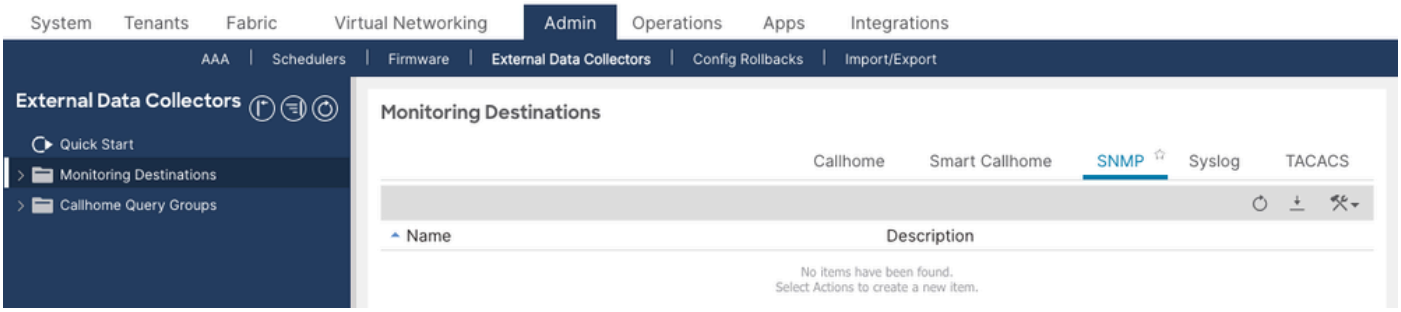
protocol): consente l'uso del protocollo SNMP ma è più ampio di quello consigliato per la produzione. È preferibile una voce di filtro SNMP dedicata con voci UDP/161 e UDP/162 specifiche.



Nota: Nelle versioni precedenti del firmware ACI, alcune porte erano sempre aperte su nodi foglia e dorso e non era necessario un contratto di gestione per SNMP. In ACI 5.x, il contratto è obbligatorio per i nodi APIC. I nodi foglia e colonna vertebrale utilizzano le regole iptable derivate dai Criteri di gruppo del client anziché i contratti di gestione.

Passaggio 4: Configurazione delle destinazioni delle trap SNMP

Selezionare Admin > External Data Collectors > Monitoring Destinations > SNMP (Amministratore > Raccoglitori di dati esterni > Destinazioni di controllo > SNMP). Fare clic con il pulsante destro del mouse e selezionare Crea gruppo di destinazione di monitoraggio SNMP. La scheda SNMP mostra tutti i gruppi di destinazione configurati. Una tabella vuota indica che non è stata ancora configurata alcuna destinazione di trap.



Definisci:

- Nome gruppo

- Destinazioni trap: hostname/IP, porta UDP (predefinito: 162), versione SNMP, stringa della community e gestione EPG

Passaggio 5: Configura origini di monitoraggio

Le origini di monitoraggio collegano il gruppo di destinazione SNMP ai criteri di monitoraggio che controllano quali eventi e errori generano le trap. È necessario configurare un'origine di monitoraggio in tutti e tre i percorsi seguenti, altrimenti le trap da alcuni tipi di nodi non verranno inviate:

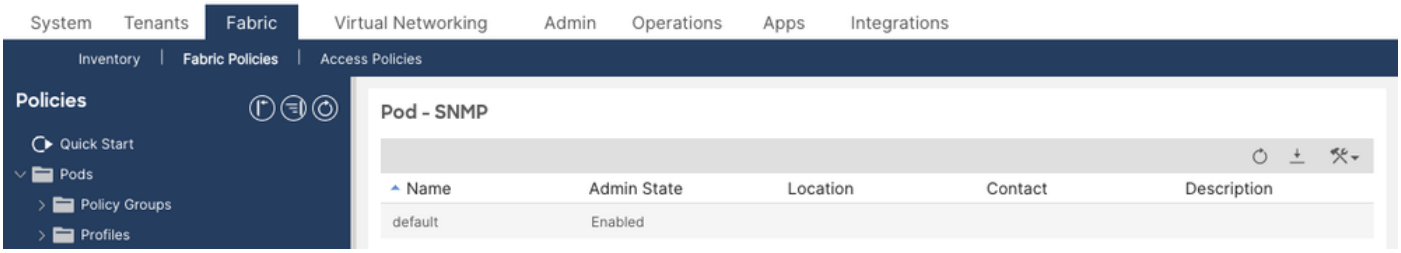
- Fabric > Fabric Policies > Policies > Monitoring > default > Callhome/Smart Callhome/SNMP/Syslog/TACACS (copre gli eventi dell'infrastruttura fabric)
- Fabric > Fabric Policies > Policies > Monitoring > Common Policy > Callhome/Smart Callhome/SNMP/Syslog/TACACS (copre gli eventi comuni a livello di fabric)
- Fabric > Criteri di accesso > Criteri > Monitoraggio > predefinito > Callhome/Smart Callhome/SNMP/Syslog (copre gli eventi di accesso/infrastruttura)

In ciascuna posizione, selezionare SNMP come tipo di origine e creare una nuova origine SNMP facendo riferimento al gruppo di destinazione creato nel passaggio 4.

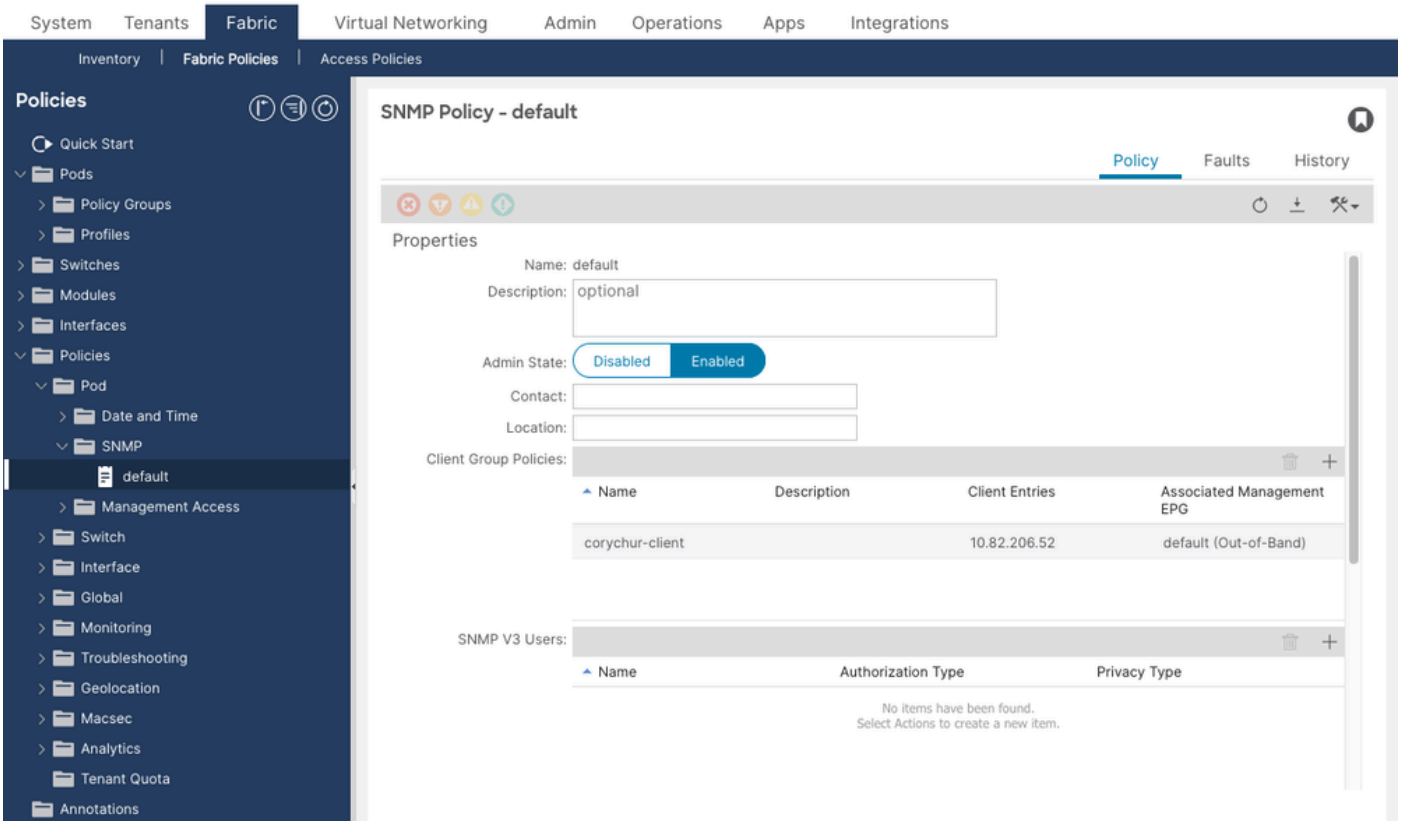
Verifica della configurazione

Verifica della distribuzione dei criteri SNMP

Passare a Fabric > Fabric Policies > Policies > Pod > SNMP e verificare che il criterio SNMP predefinito esista e che il relativo stato Admin sia impostato su Enabled. L'elenco Gruppi di criteri mostra a colpo d'occhio tutti i criteri SNMP configurati con il relativo stato di amministrazione.



Per una verifica dettagliata, fare clic sul nome del criterio per aprirlo. Confermare che l'opzione Admin State sia impostata su Enabled (Abilitata) e che in Client Group Policies (Criteri di gruppo client) siano elencati tutti gli host NMS autorizzati con il rispettivo EPG di gestione associato.



Eseguire la seguente query MO su qualsiasi APIC per verificare che il criterio SNMP sia presente e abilitato nell'infrastruttura:

<#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
```

Se `adminSet` è `disabilitato`, il protocollo SNMP non funzionerà su alcun nodo. Abilitarlo nella GUI APIC in Fabric > Fabric Policies > Policies > Pod > SNMP > default (Fabric > Criteri fabric > Criteri > Pod > SNMP > Predefinito).

Verifica della configurazione delle stringhe della community

<#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
```

Se non viene restituita alcuna community o il nome non corrisponde a quello utilizzato dal servizio NMS, aggiungere o correggere la stringa della community nel criterio SNMP.

Verifica dei criteri di gruppo del client (controllo di accesso SNMP)

I Criteri di gruppo client funzionano come ACL per l'accesso GET/WALK SNMP. Ogni criterio specifica gli indirizzi IP dei client autorizzati a eseguire il polling dei nodi foglia/spine su cui viene eseguito il VRF di gestione. Sui nodi foglia/dorso, questi criteri vengono convertiti in regole iptables.

<#root>

apic1#

moquery -c snmpClientGrpP -x query-target=children

Total Objects shown: 3

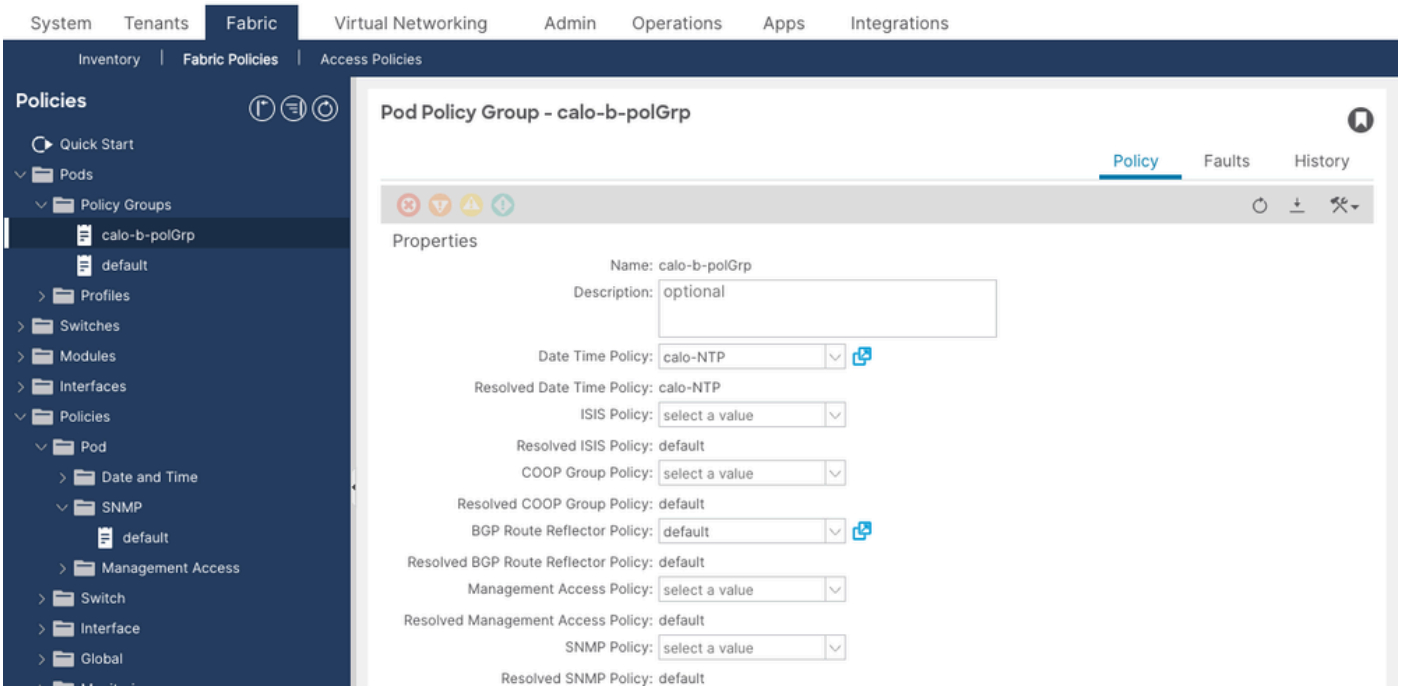
```
# snmp.ClientP
addr         : 10.1.1.50                   <--- NMS server IP
dn           : uni/fabric/snmppol-default/clgrp-NMS-Clients/client-[10.1.1.50]
name         : nms-server1

# 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
```

Verificare che l'indirizzo IP del server NMS sia presente nelle voci client. Se manca un IP client, le richieste GET/WALK SNMP da tale host verranno eliminate dalle iptable sui nodi foglia/spine.

Nota: Avvertenza SNMPv3: i criteri di gruppo client non vengono applicati all'APIC quando si utilizza SNMPv3. Qualsiasi GET/WALK SNMPv3 a un APIC è consentito indipendentemente dalla configurazione del gruppo client. L'imposizione del gruppo client per SNMPv3 sull'APIC è una limitazione nota. Sugli switch foglia e dorso, l'imposizione dei gruppi di client funziona allo stesso modo sia per SNMPv2c che per SNMPv3.

Verifica dei riferimenti al gruppo di criteri POD per i criteri SNMP

Passare a Fabric > Fabric Policies > Pods > Policy Groups (Infrastruttura > Criteri fabric > Pod > Gruppi di criteri) e aprire il gruppo di criteri per i pod attivo. Verificare che il campo a discesa Criterio SNMP sia impostato sul criterio SNMP desiderato e che il campo Criterio SNMP risolto abbia lo stesso nome. Un criterio mancante o non risolto indica che la configurazione SNMP non viene mai sottoposta a PUSH sugli switch.



Nello screenshot precedente, il campo Criterio SNMP mostra "select a value" (vuoto), mentre il criterio SNMP risolto mostra "default". Ciò significa che il criterio è ereditato dal valore predefinito della struttura, ma non è impostato in modo esplicito. Per evitare ambiguità, si consiglia di impostare in modo esplicito il campo Criteri SNMP.

Verifica tramite API REST:

<#root>

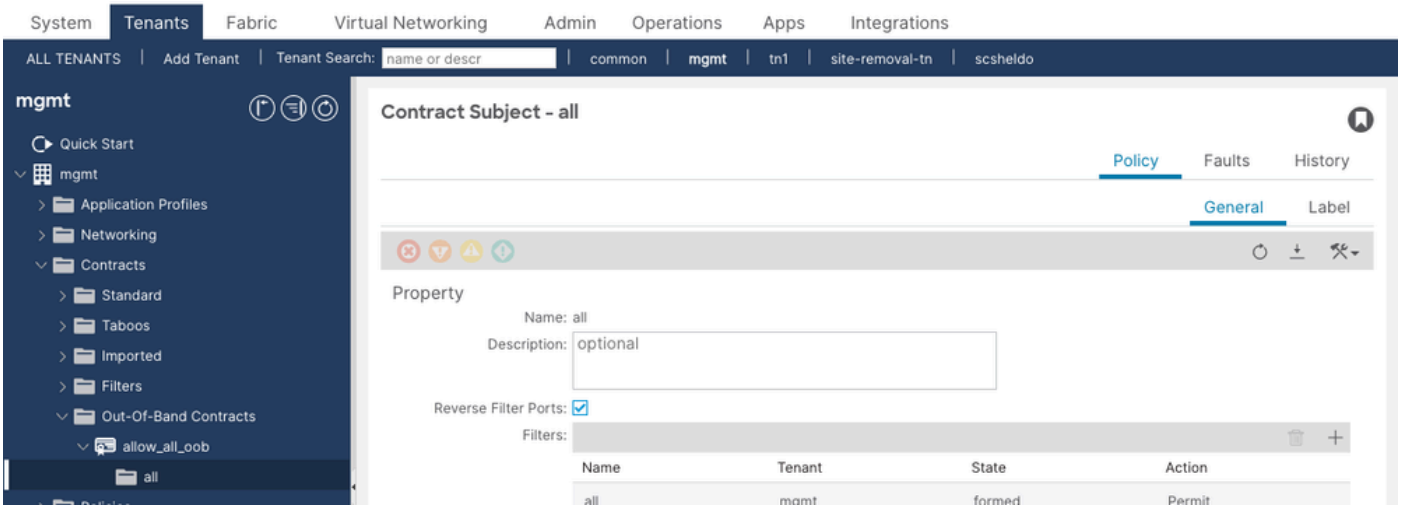
```
apic1#

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"
```

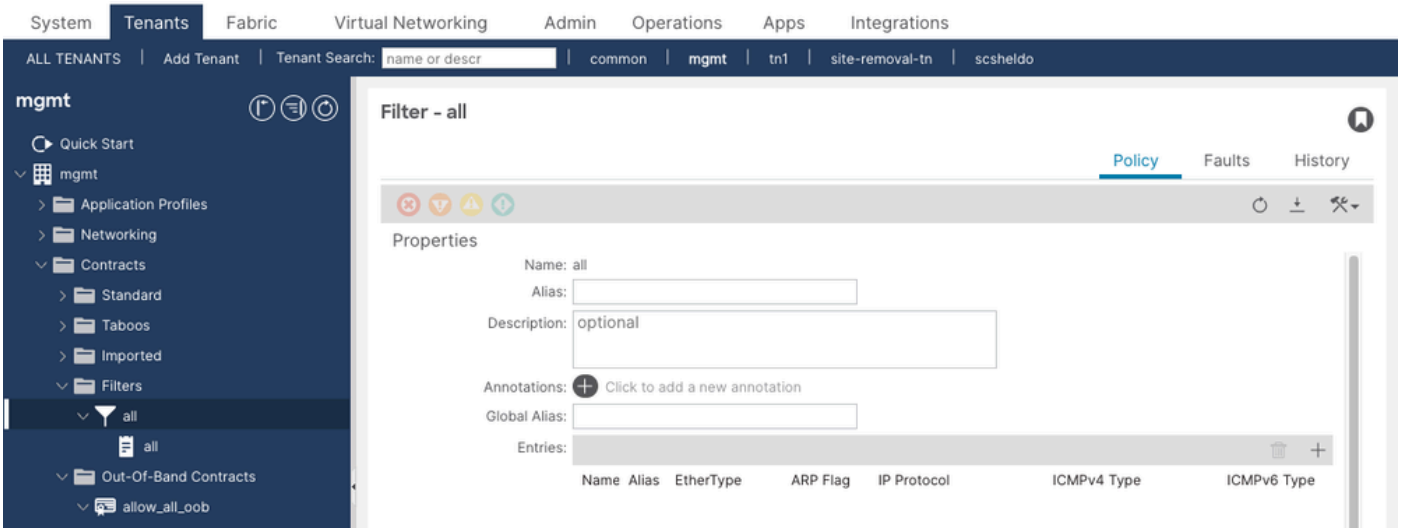
Se `lo stato` non è `formato`, la relazione tra i criteri SNMP viene interrotta. Selezionare nuovamente il criterio SNMP nel gruppo di criteri POD e inviarlo.

Verifica del contratto di gestione per UDP 161 (nodi APIC)

Passare a Tenant > Gestione > Contratti > Contratti fuori banda (e Contratti in banda se si utilizza la gestione INB). Aprire il contratto Fuori sede attivo e fare clic sulla scheda Criterio. Verificare che l'oggetto faccia riferimento a un filtro che consente la porta UDP 161.



Espandere il filtro al quale fa riferimento il soggetto e confermare le voci includendo una voce con EtherType IP, Protocol UDP, Destination Port 161. Le voci del filtro determinano il traffico autorizzato attraverso il contratto di gestione OOB verso l'APIC.



Il filtro dovrebbe mostrare:

- EtherType: IP
- Protocollo IP: UDP
- Porta di destinazione da: 161
- Porta di destinazione: 161

Verificare inoltre che la porta UDP 162 sia consentita se si desidera che l'APIC invii trap SNMP in uscita tramite l'interfaccia OOB.

Verifica tramite query MO:

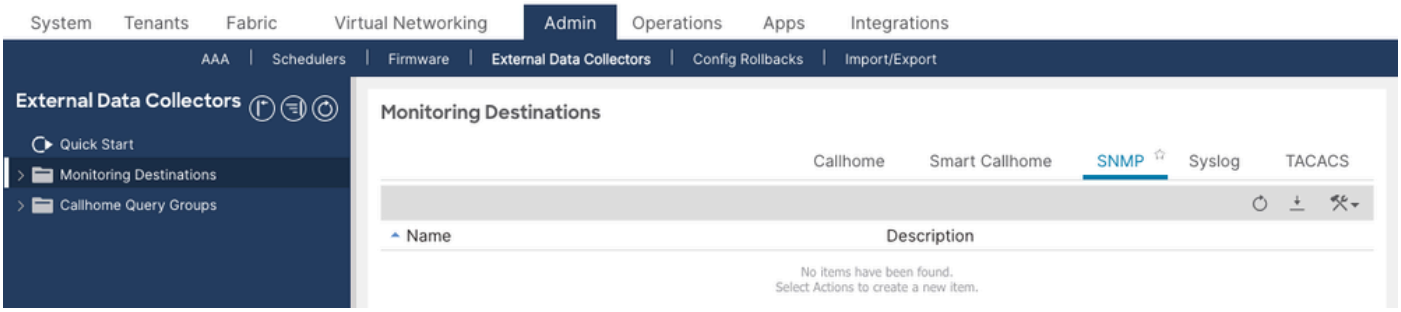
<#root>

```
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
```

Se non viene restituito alcun risultato, non esiste alcun filtro per UDP 161. Aggiungerne uno al contratto di gestione.

Verifica della configurazione della destinazione delle trap SNMP

Passare a Admin > External Data Collector > Monitoring Destinations > SNMP per visualizzare tutti i gruppi di destinazione SNMP configurati. Un elenco vuoto indica che non sono configurate destinazioni di trap e che non verranno inviate trap da alcun nodo.



<#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
```

Verificare che l'indirizzo IP, la porta, la versione, la stringa della community e il file VRF di gestione della destinazione della trap (`mgmt:inb` o `management` for OOB) corrispondano all'ambiente. Il VRF deve corrispondere all'EPG di gestione assegnato alla destinazione.

Verifica della configurazione delle origini di monitoraggio in tutti e tre gli ambiti

Le origini SNMP devono esistere in tutti e tre gli ambiti dei criteri di monitoraggio. Se in un ambito manca un'origine, le trap dagli eventi correlati non verranno inoltrate.

<#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
```

Se manca una delle tre, creare l'origine SNMP mancante nel criterio di monitoraggio corrispondente utilizzando la GUI.

Verifica operativa

Verifica dello stato SNMP tramite il comando show snmp summary (APIC)

Eseguire questo comando direttamente su ciascuna APIC per verificare che l'agente SNMP sia in esecuzione e che la configurazione sia stata applicata:

<#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
```

Cosa verificare nell'output:

- Lo stato dell'amministratore deve essere `abilitato`.
- La community deve corrispondere all'NMS configurato per l'utilizzo.
- Il gruppo client deve elencare tutti gli IP NMS consentiti con EPG di gestione corretto.
- L'host (destinazione trap) deve elencare il ricevitore trap NMS con la porta e la versione corrette.

Verifica dello stato SNMP tramite il riepilogo show snmp (foglia/dorso)

<#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
```

Cosa verificare nell'output:

- Lo stato dell'amministratore deve essere `abilitato, in esecuzione` con un PID. Se viene visualizzato `disabled` (disabilitato), il criterio SNMP non viene applicato o la catena di criteri del pod viene interrotta.
- Lo stato della community deve essere `corretto`. Lo stato di `errore` indica un problema di distribuzione dei criteri.
- Il VRF del client per ciascun host NMS deve corrispondere al VRF dell'EPG di gestione (`mgmt:inb` per In-Band, `gestione` per OOB).
- L'host trap deve elencare la destinazione con il contesto VRF corretto.

Verificare che il processo snmpd sia in esecuzione

Su una foglia o sul dorso:

<#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
```

Nell'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
```

Se non viene trovato alcun processo snmpd su una foglia o su un dorso, il protocollo SNMP non è in esecuzione su tale nodo. Verificare che lo stato di amministrazione del criterio SNMP sia abilitato e che la catena di criteri del pod sia configurata correttamente.

Spoiler (Evidenziato da leggere)

Verifica dell'ascolto della porta SNMP

<#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           :::*
```

Se la porta 161 non è elencata nello stato LISTEN, il processo snmpd non è in esecuzione o non è riuscito a eseguire il binding alla porta.

Verifica regole iptables su foglia/dorso

I Criteri di gruppo client vengono convertiti in regole iptables su ogni foglia e dorso. Utilizzare quanto segue per esaminare le regole:

<#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)
```

Per identificare gli ID VRF corretti per l'infrastruttura, eseguire:

<#root>

```
leaf101#

show vrf

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

Gli ID VRF nelle regole iptables devono corrispondere ai report `show vrf`. Se un IP client è assente dalle regole iptables, le richieste SNMP provenienti da quell'host verranno automaticamente eliminate anche se il processo snmpd è in esecuzione.

Utilizzare i contatori per verificare se un pacchetto SNMP è stato abbinato o scartato:

<#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
```

Nota: Se SNMP è in esecuzione ma iptables non mostra catene snmp_rules o le catene sono vuote, è possibile riavviare il processo snmpd per forzare la riprogrammazione delle regole iptables. L'invio di SIGKILL al PID snmpd è sicuro: ACI Process Manager (`sottoposto a policy`) lo riavvia automaticamente. Eseguire `pidof snmpd` per ottenere il PID, quindi `terminare -9 [snmpd_pid]`. Confermare il nuovo PID con `pidof snmpd` dopo 10-15 secondi.

Verificare che la porta SNMP sia in ascolto di leaf101# netstat -lutn | grep 161 Connessioni Internet attive (solo server) Proto Recv-Q Send-Q Indirizzo locale Indirizzo esterno Stato tcp 0 0 0.0.0.0:161 0.0.0.0:* LISTEN <— L'agente SNMP accetta richieste udp 0 0 0.0.0.0:161 0.0.0.0:* udp6 0 :::161 ::* Se la porta 161 non è elencata nello stato LISTEN, il processo snmpd non è in esecuzione o non è riuscito a collegarsi alla porta. Verificare che le regole iptables sui criteri di gruppo del client foglia/dorso siano convertite in regole iptables su ogni foglia e dorso. Utilizzare quanto segue per esaminare le regole: 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 <— la porta SNMP 161 reindirizza alla catena snmp_rules -A snmp_rules -m vrf —vrf 2 -j vrf_2_snmp_rules <— VRF 2 = Gestione OOB -A snmp_rules -m vrf —vrf 9 -j vrf_9_snmp_rules < VRF 9 = Gestione in banda -A snmp_rules -j DROP <— drop predefinito; Solo i client autorizzati superano -A vrf_2_snmp_rules -s 10.1.1.50/32 -j ACCEPT <— allowed NMS client (OOB VRF) -A vrf_9_snmp_rules -s 10.1.1.50/32 -j ACCEPT <— allowed NMS client (INB VRF) Per identificare gli ID VRF corretti per l'infrastruttura, eseguire: leaf101# show vrf VRF-Name VRF-ID State Reason management 2 Up — mgmt:inb 9 Up — Gli ID VRF nelle regole iptables devono corrispondere ai report show vrf. Se un IP client è assente dalle regole iptables, le richieste SNMP provenienti da quell'host verranno automaticamente eliminate anche se il processo snmpd è in esecuzione. Utilizzare i contatori per verificare se un pacchetto SNMP è stato abbinato o scartato: leaf101# iptables -nvL | grep -A 20 "Chain snmp_rules" Chain snmp_rules (1 riferimenti) pkts byte porta destinazione opt in out destinazione 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 <— se pkts>0 qui, gli IP client sono mancanti Nota: Se SNMP è in esecuzione ma iptables non mostra catene snmp_rules o le catene sono vuote, è possibile riavviare il processo snmpd per forzare la riprogrammazione delle regole iptables. L'invio di SIGKILL al PID snmpd è sicuro: ACI Process Manager (sottoposto a policy) lo riavvia automaticamente. Eseguire pidof snmpd per ottenere il PID, quindi terminare -9 [snmpd_pid].

Confermare il nuovo PID con pidof snmpd dopo 10-15 secondi.

Verifica della connettività di rete alle porte SNMP

<#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
```

Verificare che le interfacce di gestione siano attive (senza incrementi di RX-ERR) e che il traffico sia in transito. `eth0` è l'interfaccia di gestione OOB; `kpm_inb` è l'interfaccia di gestione in-band dello switch.

Verifica dell'invio di trap SNMP con tcpdump

Per verificare che le trap vengano generate e inviate da un nodo foglia o da una direttrice, acquisire il traffico sull'interfaccia appropriata. Accedere al nodo come admin e utilizzare:

<#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
```

Per OOB:

<#root>

```
leaf101#

tcpdump -i eth0 -f port 162 -vv
```

Spoiler (Evidenziato da leggere)

Per le trap APIC (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
```

Nota: Nell'APIC, `bond0.1100` è l'interfaccia VLAN dell'interfaccia di gestione in-band. Sostituire il modello `1100` con l'interfaccia VLAN configurata per l'EPG di gestione in-band. Utilizzare `oobmgmt` come nome di interfaccia per le acquisizioni OOB sull'interfaccia APIC.

Per le trap APIC (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 Nota: Sull'APIC, bond0.1100 è l'interfaccia VLAN dell'interfaccia di gestione In-Band. Sostituire il modello 1100 con l'encap VLAN configurata per la gestione in-band EPG. Utilizzare oobmgmt come nome di interfaccia per le acquisizioni OOB sull'APIC.

Verifica delle richieste GET/WALK SNMP con 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
```

Se viene visualizzato GetRequest ma non GetResponse, la richiesta verrà ricevuta ma non riceverà risposta. Controllare il processo snmpd e la stringa della community. Se non vengono visualizzate né la richiesta né la risposta, la richiesta viene bloccata prima di raggiungere il nodo

(verificare routing e iptables).

Flusso di lavoro di risoluzione dei problemi

Struttura decisionale Triage

Utilizzare questo albero decisionale quando i tecnici segnalano che il protocollo SNMP non funziona. Iniziare dal sintomo osservato e seguire i rami fino all'isolamento.

Sintomo: Nessuna risposta alle richieste GET/WALK SNMP

1. Controllare lo stato di amministrazione di SNMP su APIC. Eseguire `moquery -c snmpPol`. Se `adminSet` è `disabilitato`, abilitarlo e procedere al Passaggio 7.
2. Controllare il processo snmpd. Sul nodo interessato, eseguire `ps aux | grep snmp` o `pidof snmpd`. Se non è in esecuzione alcun processo, il criterio SNMP non viene distribuito. Verificare la catena di criteri pod (Criteri SNMP → Gruppo di criteri POD → Profilo POD).
3. Verificare che la porta 161 sia in ascolto. Esegui `netstat -lutn | grep 161`. Se la porta 161 non è in stato LISTEN, il processo snmpd non è riuscito; raccogliere i log da `/var/log/dme/log/svc_ifc_dbgrelem.log*` e riavviare il processo.
4. Controllare il routing. Eseguire `show ip route vrf management` e `show ip route vrf mgmt:inb`. Verificare che esista un percorso verso l'host NMS nel VRF corretto.
5. Controllare il contratto di gestione su APIC. Se la destinazione è un APIC (non una foglia o un dorso), verificare che nel contratto di gestione OOB o INB sia consentito l'UDP 161.
6. Eseguire tcpdump sul nodo. Eseguire `tcpdump -i kpm_inb -f port 161 -v` (o `eth0` per OOB). Se viene visualizzato GetRequest ma non GetResponse, la richiesta raggiunge il nodo ma snmpd non risponde — controllare la stringa della community. Se non viene visualizzata alcuna richiesta, il problema è a monte (routing o contratto).
7. Test da un client autorizzato. Eseguire `snmpget -v2c -c [community] [node-ip] SNMPv2-MIB::sysDescr.0` da un host NMS elencato nel gruppo client. Una risposta positiva conferma che il protocollo SNMP è pienamente operativo.

Sintomo: Nessun trap SNMP ricevuto sul sistema NMS

1. Controllare la configurazione della destinazione trap. Eseguire `moquery -c snmpTrapDest`. Confermare che l'indirizzo IP, la porta, la versione e la community del server dei nomi corrispondano ai valori previsti dal server dei nomi.
2. Verificare che le origini di monitoraggio siano presenti in tutti e tre gli ambiti. Esegui `moquery -c snmpSrc | egrep "snmp.Src|name|dn"`. Confermare l'esistenza di voci con valori `monPolDn` per `uni/fabric/monfab-default`, `uni/fabric/moncommon` e `uni/infra/moninfra-default`. Se mancano alcune, aggiungere l'origine SNMP nel criterio di monitoraggio corrispondente.

3. Controllare il processo snmpd. Verificare che snmpd sia in esecuzione nel nodo che deve inviare la trap.
4. Generare un evento di test e acquisirlo con tcpdump. Inversione di un'interfaccia o modifica di uno stato per generare un evento. Sul nodo, eseguire `tcpdump -i kpm_inb -f port 162 -v`. Se sul cavo non viene visualizzato traffico di trap, l'evento non genera una trap - ricontrolla origine di monitoraggio `con` attributo (deve includere `errori` o `eventi`).
5. Controllare la connettività al ricevitore trap. Verificare che il ricevitore trap sia raggiungibile dal VRF di gestione: `show ip route vrf mgmt:inb` deve visualizzare un percorso all'host NMS.
6. Se i trap vengono visualizzati su tcpdump ma non su NMS, il problema è relativo alla rete: firewall, routing o configurazione NMS. Verificare che il sistema NMS sia in ascolto su UDP 162 dall'indirizzo IP di origine della gestione del nodo ACI.

Scenari comuni

Scenario 1: Criterio SNMP abilitato ma nessun dato restituito da foglia/dorso

Problema: Nel criterio SNMP sull'APIC è indicato che lo stato dell'amministratore è abilitato. L'NMS può raggiungere l'IP di gestione della foglia. `snmpget` timeout senza risposta.

Controllo configurazione: Verificare che il gruppo di criteri POD faccia riferimento al criterio SNMP e che il criterio SNMP risolto visualizzi il nome corretto. Se il campo Criteri SNMP del gruppo di criteri POD è vuoto o la relazione non è formata, il processo snmpd potrebbe non avviarsi sugli switch.

Controllo operativo: SSH sulla foglia interessata ed eseguire `show snmp summary`. Se nell'output viene visualizzato `Admin State: disattivato` anche se l'APIC è attivato, il criterio non è stato distribuito. Verificare se nella catena di criteri del pod è presente un gruppo di criteri del pod mancante o a cui si fa riferimento in modo errato.

Causa principale: Il criterio SNMP non è collegato al gruppo di criteri per i pod oppure il selettore del profilo di pod non applica il gruppo di criteri per i pod corretto a questo pod.

Soluzione:

1. Passare a Fabric > Fabric Policies > Pods > Policy Groups > default (Fabric > Criteri fabric > Pod > Gruppi di criteri > predefiniti).
2. Verificare che il campo Criteri SNMP punti al criterio SNMP abilitato.
3. Passare a Fabric > Fabric Policies > Pods > Profiles e confermare il selettore attivo che fa riferimento a questo Pod Policy Group.
4. Dopo il salvataggio, ricontrollare `show snmp summary` sulla foglia entro 2 minuti.

Scenario 2: SNMP GET/WALK funziona per alcuni host NMS ma non per altri

Problema: Un server NMS può eseguire correttamente il polling dei nodi ACI. Un secondo server NMS in una subnet diversa non riceve alcuna risposta.

Controllo configurazione: Eseguire `moquery -c snmpClientGrpP -x query-target=children` su APIC. Verificare che l'indirizzo IP del secondo server NMS sia elencato come voce client. Se manca, l'IP verrà bloccato dalla regola iptables DROP nella parte inferiore della catena snmp_rules.

Controllo operativo: sull'elemento foglia interessato, confermare che l'UDP 161 è consentito nel contratto di gestione OOB o INB. Se nessun contratto o filtro dispone di porte SNMP, la richiesta viene eliminata.

Causa principale: Il secondo indirizzo IP del server NMS non è incluso nei Criteri di gruppo del client.

Soluzione: Aggiungere l'indirizzo IP NMS mancante come voce client in Criteri di gruppo client SNMP in Fabric > Criteri fabric > Criteri > Pod > SNMP > predefinito > Criteri di gruppo client. Le regole iptables su tutti i nodi verranno aggiornate entro pochi minuti dal salvataggio del criterio.

Scenario 3: Trap SNMP non ricevute — Le trap vengono generate ma non consegnate

Problema: Gli errori sono visibili nella tabella degli errori APIC. `moquery -c snmpTrapDest` mostra l'indirizzo IP NMS corretto. Il sistema NMS non riceve trap.

Controllo configurazione: Esegui `moquery -c snmpSrc | egrep "snmp.Src|name|dn"`. Verificare che le origini di monitoraggio siano presenti in tutti e tre gli ambiti (`monfab-default`, `moncommon`, `moninfra-default`). Una supervisione comune consiste nella configurazione dell'origine solo nei criteri predefiniti dell'infrastruttura, che non prevedono eventi dei criteri di accesso.

Controllo operativo: Attivazione di un evento di test (ad esempio, attivazione o disattivazione di un'interfaccia). Sul nodo corrispondente, eseguire `tcpdump -i kpm_inb -f porta 162`. Se i pacchetti trap vengono visualizzati sull'interfaccia del nodo, il lato ACI funziona e il problema si trova nel percorso di rete dell'NMS (firewall, routing). Se non viene visualizzata alcuna trap, l'origine di monitoraggio ACI risulta mancante o il tipo di evento non è incluso nell'attributo `incl` dell'origine.

Causa principale 1: Una o più origini di monitoraggio mancanti dagli ambiti richiesti.

Causa principale 2: L'attributo di origine di monitoraggio `incl` esclude il tipo di evento generato (ad

esempio, `incl: eventi` senza `errori` significa che le trap basate su errori non verranno inviate).

Soluzione:

1. Aggiungere le origini di monitoraggio mancanti nella GUI per ognuno dei tre ambiti (Fabric Default, Fabric Common, Access Default). Impostare il gruppo di destinazione sul gruppo di destinazione SNMP configurato.
2. Verificare che l'attributo `incl` includa `controlli, eventi e errori` per la copertura completa delle trap.
3. Dopo le modifiche, riattivare l'evento di test e controllare nuovamente tcpdump.

Spoiler (Evidenziato da leggere)

Nota: Nell'APIC, il `comando tcpdump/code> è disponibile solo per l'utente root. Per APIC e Switch, il comando iptables è disponibile solo per l'utente root.`

Scenario 4: Applicazione del gruppo di client SNMPv3 non funzionante su APIC

Problema: Un client SNMP che NON è incluso in Criteri di gruppo client può eseguire correttamente una query sull'APIC utilizzando SNMPv3, anche se la stessa query ha esito negativo sui nodi foglia/spine.

Causa principale: Si tratta di una **nota avvertenza**. I Criteri di gruppo client (imposizione IP di origine basata su iptable) non vengono applicati per le istruzioni GET/Walk di SNMPv3 ai controller APIC. Qualsiasi host può eseguire query sull'APIC tramite SNMPv3 indipendentemente dalla configurazione del gruppo client. Sugli switch foglia e dorso, l'imposizione del gruppo client funziona in modo identico per SNMPv2c e SNMPv3.

Attenuazione: Usare i filtri dei contratti di gestione sull'APIC per limitare l'accesso SNMP alla subnet di origine. I gruppi client sono validi per i nodi foglia/dorso. Per l'APIC con SNMPv3, il meccanismo di controllo degli accessi deve basarsi sul filtro basato sull'origine del contratto di gestione.

Scenario 5: Query SNMP riuscite ma dati MIB incompleti o non aggiornati

Problema: SNMP GET/WALK restituisce dati, ma alcuni OID MIB restituiscono valori vuoti o non aggiornati. In particolare, le statistiche dell'interfaccia o i dati sullo stato operativo non riflettono lo stato corrente del fabric.

Controllo operativo: Confermare l'APIC su cui si sta eseguendo la query. Ogni APIC restituisce solo oggetti MIB per i dati locali. Eseguire il comando show snmp summary sull'APIC su cui si sta eseguendo la query e confrontare il risultato con quello previsto. Per i dati a livello di switch (IF-MIB, entityMIB), eseguire una query direttamente sullo switch, non sull'APIC.

Causa principale: Query su un APIC per i dati MIB di livello foglia. Ogni APIC fornisce oggetti MIB solo per i propri oggetti gestiti. I dati a livello di switch (stato dell'interfaccia, CPU, memoria, sensori ambientali) devono essere recuperati eseguendo il polling diretto di ogni foglia e dorso.

Soluzione: Configurare il sistema NMS in modo che esegua il polling degli IP di gestione delle interfacce e delle spine direttamente per i dati MIB di interfaccia e hardware. Usare gli IP di gestione APIC solo per i MIB nativi APIC (entità, FRU, processo, sensore correlato all'hardware del server APIC).

Scenario 6: Il protocollo SNMP funziona su Leaf/Spine ma non su APIC

Problema: SNMPv2c GET da NMS ai nodi foglia e di colonna vertebrale riuscito. Lo stesso NMS non

è in grado di eseguire il polling dell'APIC.

Controllo configurazione: Il protocollo SNMP APIC richiede un contratto di gestione esplicito che consenta l'uso di UDP 161. Passare a **Tenant > gestione** e controllare il contratto OOB/INB e il relativo filtro per UDP 161.

Controllo operativo: Nell'APIC eseguire iptables -S | grep 161. Se sotto la catena fp-137 (o contratto OOB equivalente) non vengono visualizzate le regole ACCEPT per UDP 161, il filtro del contratto per UDP 161 risulta mancante o non è implementato.

```
<#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
```

Se queste regole non sono presenti, aggiungere una voce di filtro per UDP 161 all'oggetto del contratto di gestione e ripetere la verifica.

Causa principale: Contratto di gestione mancante o non configurato correttamente. In ACI 5.x, i nodi APIC applicano il contratto di gestione in modo rigoroso: i pacchetti SNMP vengono eliminati a meno che non esista un'autorizzazione esplicita.

Soluzione:

1. Passare a **Tenant > Gestione > Criteri di sicurezza > Contratti fuori banda**.
2. Espandere il contratto OOB, selezionare il soggetto e verificare/aggiungere un filtro per la **porta UDP 161**.
3. Ripetere l'operazione per il contratto In-Band se l'NMS sta raggiungendo l'APIC sulla gestione INB.
4. Verifica con iptables -S | grep 161 sull'APIC dopo il risparmio.

Scenario 7: Le regole iptable SNMP sono assenti o non corrette

Problema: show snmp summary visualizza il criterio SNMP applicato ma iptables -S | grep snmp non restituisce regole o l'IP del client NMS è assente dalle regole.

Controllo operativo: Confermare che snmpd è in esecuzione con pidof snmpd. Se snmpd è in esecuzione ma iptables non dispone di regole SNMP, il processo è stato avviato prima della distribuzione di Criteri di gruppo client. Riavviare snmpd per forzare la riprogrammazione delle regole se il numero di riavvii è inferiore a 250:

```
<#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

ACI Process Manager riavvia automaticamente snmpd. Dopo il riavvio, verificare:

```
<#root>

leaf101#
```

iptables -S | grep -i snmp

Verranno visualizzate le regole di accettazione snmp_rules e per-VRF client.

Causa principale: Il processo snmpd è stato riavviato prima che i Criteri di gruppo del client fossero completamente distribuiti nel nodo, lasciando iptables senza le regole di accesso SNMP.

Nota: Nell'APIC, il comando tcpdump/code> è disponibile solo per l'utente root. Il comando iptables di APIC e Switch è disponibile solo per l'utente root. Scenario 4: Applicazione del gruppo di client SNMPv3 non funzionante sul problema APIC: Un client SNMP che NON è incluso in Criteri di gruppo client può eseguire correttamente una query sull'APIC utilizzando SNMPv3, anche se la stessa query ha esito negativo sui nodi foglia/spine. Causa principale: Si tratta di un avvertimento noto. I Criteri di gruppo client (imposizione IP di origine basata su iptable) non vengono applicati per le istruzioni GET/Walk di SNMPv3 ai controller APIC. Qualsiasi host può eseguire query sull'APIC tramite SNMPv3 indipendentemente dalla configurazione del gruppo client. Sugli switch foglia e dorso, l'imposizione del gruppo client funziona in modo identico per SNMPv2c e SNMPv3. Riduzione: Usare i filtri dei contratti di gestione sull'APIC per limitare l'accesso SNMP alla subnet di origine. I gruppi client sono validi per i nodi foglia/dorso. Per l'APIC con SNMPv3, il meccanismo di controllo degli accessi deve basarsi sul filtro basato sull'origine del contratto di gestione. Scenario 5: Le query SNMP sono state completate, ma i dati MIB sono incompleti o hanno problemi obsoleti: SNMP GET/WALK restituisce dati, ma alcuni OID MIB restituiscono valori vuoti o non aggiornati. In particolare, le statistiche dell'interfaccia o i dati sullo stato operativo non riflettono lo stato corrente del fabric. Controllo operativo: Confermare l'APIC su cui si sta eseguendo la query. Ogni APIC restituisce solo oggetti MIB per i dati locali. Eseguire il comando show snmp summary sull'APIC su cui viene eseguita la query e confrontare il risultato con quello previsto. Per i dati a livello di switch (IF-MIB, entityMIB), eseguire una query direttamente sullo switch, non sull'APIC. Causa principale: Query su un APIC per i dati MIB di livello foglia. Ogni APIC fornisce oggetti MIB solo per i propri oggetti gestiti. I dati a livello di switch (stato dell'interfaccia, CPU, memoria, sensori ambientali) devono essere recuperati eseguendo il polling diretto di ogni foglia e dorso. Soluzione: Configurare il sistema NMS in modo che esegua il polling degli IP di gestione delle interfacce e delle spine direttamente per i dati MIB di interfaccia e hardware. Usare gli IP di gestione APIC solo per i MIB nativi APIC (entità, FRU, processo, sensore correlato all'hardware del server APIC). Scenario 6: Il protocollo SNMP funziona su Leaf/Spine ma non su APIC Problem: SNMPv2c GET da NMS ai nodi foglia e di colonna vertebrale riuscito. Lo stesso NMS non è in grado di eseguire il polling dell'APIC. Controllo configurazione: L'SNMP APIC richiede un contratto di gestione esplicito che consenta l'uso di UDP 161. Passare a Tenant > gestione e controllare il contratto OOB/INB e il relativo filtro per UDP 161. Controllo operativo: Su APIC, eseguire iptables -S | grep 161. Se sotto la catena fp-137 (o contratto OOB equivalente) non vengono visualizzate regole ACCEPT per UDP 161, il filtro del contratto per UDP 161 risulta mancante o non è implementato. apic1# iptables -S | grep 161 -A fp-137 -s 10.0.0.0/8 -p udp -m udp —dport 161 -j ACCEPT <— allow SNMP from the management subnet -A fp-137 -s 172.18.0.0/16 -p udp -m udp —dport 161 -j ACCEPT <— allow SNMP from INB management subnet Se queste regole non sono presenti, aggiungere una voce di filtro per UDP 161 al soggetto del

contratto di gestione e verificare nuovamente. Causa principale: Contratto di gestione mancante o non configurato correttamente. In ACI 5.x, i nodi APIC applicano il contratto di gestione in modo rigoroso: i pacchetti SNMP vengono eliminati a meno che non esista un'autorizzazione esplicita. Soluzione: Passare a Tenant > Gestione > Criteri di sicurezza > Contratti fuori banda. Espandere il contratto OOB, selezionare l'oggetto e verificare/aggiungere un filtro per la porta UDP 161. Ripetere per il contratto In-Band se il NMS raggiunge l'APIC tramite la gestione INB. Verifica con iptables -S | grep 161 sull'APIC dopo il risparmio. Scenario 7: Le regole iptable SNMP sono assenti o presentano un problema errato: show snmp summary visualizza il criterio SNMP applicato ma iptables -S | grep snmp non restituisce alcuna regola oppure l'IP del client NMS è assente dalle regole. Controllo operativo: Conferma esecuzione di snmpd con pidof snmpd. Se snmpd è in esecuzione ma iptables non dispone di regole SNMP, il processo è stato avviato prima della distribuzione di Criteri di gruppo client. Riavviare snmpd per forzare la riprogrammazione delle regole se il numero di riavvii è inferiore a 250: leaf101# pidof snmpd 5881leaf101# show system internal sysmgr service name snmpdService "snmpd" ("snmpd", 127):UUID = 0x1A, PID = 5881, SAP = 1545State: SRV_STATE_HANDSHAKED (immesso al tempo Mon Ago 25 19:23:50 2025).Numero di riavvii: 3Ora ultimo riavvio: lun 25 ago 19:23:48 2025.PID precedente: 32080Motivo dell'ultima interruzione: SYSMGR_DEATH_REASON_FAILURE_SIGNALTag = N/ID APlugin: 0 leaf101# kill -9 5881 ACI process manager riavvierà automaticamente snmpd. Dopo il riavvio, verificare: leaf101# iptables -S | grep -i snmp Le catene snmp_rules e le regole ACCEPT client per-VRF dovrebbero essere visualizzate. Causa principale: Il processo snmpd è stato riavviato prima che i Criteri di gruppo del client fossero completamente distribuiti nel nodo, lasciando iptables senza le regole di accesso SNMP.

File di log per la risoluzione dei problemi estesa

Quando le operazioni di verifica descritte in precedenza non risolvono il problema, i seguenti file di log su nodi foglia, direttrice e APIC contengono informazioni di diagnostica relative a 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/*

Questi registri contengono eventi di riavvio snmpd, eventi di distribuzione dei criteri ed errori di configurazione della community/client non visibili tramite mostra riepilogo snmp.

Riferimenti

- Guida alla configurazione di Cisco APIC System Management, versione 5.x – Gestione di SNMP
- Guida di riferimento rapida di Cisco ACI MIB

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).