Identificar e solucionar problemas de SNMP na estrutura da Cisco ACI

Introdução

Este documento descreve como configurar, verificar e solucionar problemas de SNMP na Cisco ACI para ACI versão 5.x e posterior. Ele aborda o modelo de política SNMP, os contratos de gerenciamento necessários, a configuração de interceptação, a verificação operacional usando consultas CLI e Objeto Gerenciado (MO) e fluxos de trabalho estruturados de solução de problemas para os cenários de falha mais comuns em switches leaf/spine e controladores APIC.

Informações de Apoio

O material neste documento foi elaborado a partir da nota técnica interna da equipe de entrega de soluções da Cisco ACI SNMP na ACI: Visão geral, configuração, solução de problemas e avisos/problemas de autoria de Tomás de Leon, complementados com o Guia de configuração de gerenciamento do sistema Cisco APIC (versão 5.x) e o Guia de referência rápida MIB da Cisco ACI.

Overview

Arquitetura SNMP na ACI

SNMP (Simple Network Management Protocol) é um protocolo baseado em UDP que governa o gerenciamento e o monitoramento de rede. Na ACI, o SNMP opera independentemente em cada entidade gerenciada. Cada switch leaf, switch spine e controlador APIC é seu próprio agente SNMP — cada um deve ser interrogado ou monitorado independentemente.

A ACI oferece suporte aos seguintes recursos SNMP:

- Operações de leitura (Get, GetNext, BulkGet, Walk) — suportadas em switches leaf/spine e controladores APIC.
- Notificações (Traps) — Interceptações SNMPv1, v2c e v3 suportadas em switches leaf/spine e controladores APIC.
- SNMPv3 — compatível com switches leaf/spine e controladores APIC.

- Write operations (Set) — SEM suporte em qualquer dispositivo ACI.
- IPv6 — O SNMP é suportado somente no IPv4.

Note: Em um cluster APIC, cada APIC fornece objetos MIB locais para si mesmo. Você deve pesquisar cada APIC de forma independente; não há agregação de SNMP em todo o cluster. Da mesma forma, cada switch leaf e spine deve ser consultado independentemente.

Arquitetura do SNMPD no APIC

O APIC executa o processo snmpd, que tem dois componentes internos:

- Agent — Um agente net-snmp de código aberto (versão 5.7.6 ou posterior) que trata do processamento do protocolo SNMP e do gerenciamento de sessão.
- DME (Data Model Engine) — Faz interface com a MIT (Management Information Tree, árvore de informações de gerenciamento) do APIC para ler MOs (Managed Objects, objetos gerenciados) e converter atributos MO no formato de objeto SNMP. As interceptações SNMP são geradas a partir de eventos e falhas levantadas em MOs.

Modelo de política SNMP e cadeia de implantação

A ACI usa um modelo orientado por políticas para o SNMP. A configuração de SNMP é abstraída como um objeto gerenciado snmpPol e deve ser associada ao grupo de política Pod da estrutura antes de ser implantada em qualquer nó. A cadeia de implantação completa é:

1. SNMP Policy (`snmpPol`) — define o estado do administrador, as strings de comunidade, as políticas de grupo de clientes (ACLs) e os usuários do SNMPv3.
2. Pod Policy Group — faz referência à política de SNMP junto com outras políticas de nível de pod (BGP, ISIS, NTP, etc.).
3. Seletor de perfis do Pod — aplica o Grupo de políticas do Pod aos pods da estrutura.

Além disso, a configuração de interceptação (trapping) SNMP requer:

1. SNMP Monitoring Destination Group (`snmpGroup`) — define hosts de destino de interceptação, porta, versão de SNMP e comunidade.
2. Monitoring Sources (`snmpSrc`) — vincula o grupo de destino a três escopos distintos de políticas de monitoramento: Padrão da estrutura, Política comum da estrutura e Padrão da política de acesso.

Contratos de gerenciamento que permitem a porta UDP 161 (solicitações SNMP) e a porta UDP 162 (interceptações SNMP) são necessários para nós APIC. Os nós leaf e spine também exigem

regras iptables corretas, que são programadas automaticamente quando as Políticas de Grupo de Clientes são configuradas.

MIBs suportados

As MIBs suportadas no APIC incluem:

- MIB de entidade — PhysicalTable
- MIB Cisco Entity Ext — PhysicalProcessorTable, LEDTable
- MIB de controle de FRU de entidade Cisco — PowerSupplyGroupTable, PowerStatusTable, FanTrayStatusTable, PhysicalTable
- Cisco Entity Sensor MIB — SensorValueTable, SensorThresholdTable
- Cisco Process MIB — CPUTotalTable, ProcessTable, ProcessExtRevTable, ThreadTable

Os switches leaf e spine expõem MIBs NX-OS padrão, incluindo IF-MIB, IP-MIB, CISCO-CDP-MIB, CISCO-ENTITY-QFP-MIB e o conjunto completo CISCO-ENTITY-FRU-CONTROL-MIB.

As interceptações SNMP geradas no APIC incluem: `cefcFRUInserted, cefcFRURemoved, cefcFanTrayStatusChange, cefcModuleStatusChange, entSensorThresholdNotification, cefcPowerStatusChange, cpmCPURisingThreshold, cpmCPUFallingThreshold.`

Configurar o SNMP na ACI

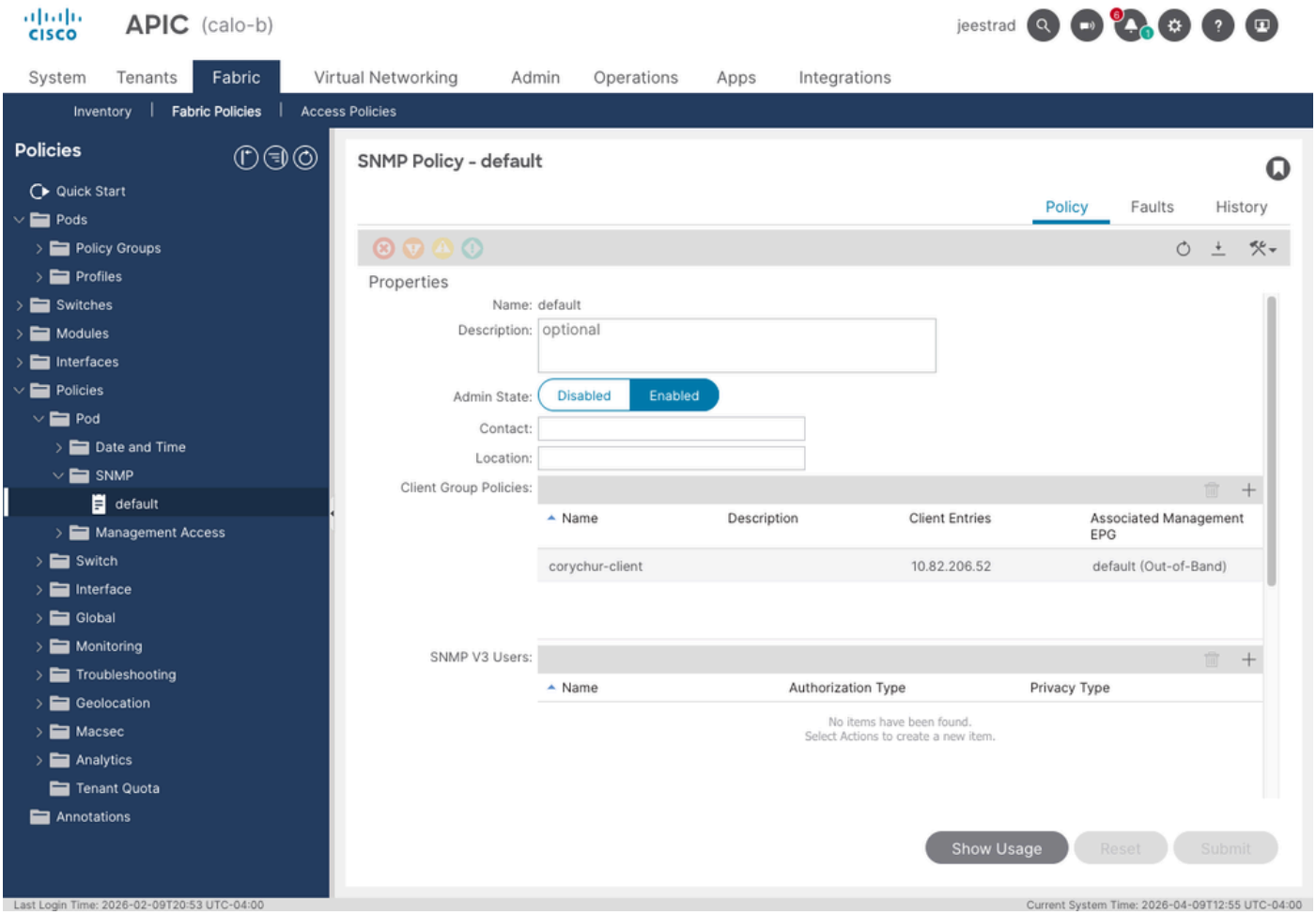
Note: Esta seção fornece um resumo do fluxo de trabalho de configuração como contexto para as seções de verificação e solução de problemas a seguir. Consulte o Guia de configuração de gerenciamento do sistema do Cisco APIC para obter procedimentos de configuração abrangentes.

Passo 1: Configurar a política SNMP

Navegue até Fabric > Fabric Policies > Policies > Pod > SNMP. Selecione (ou crie) a política SNMP, normalmente chamada de default. Configurar:

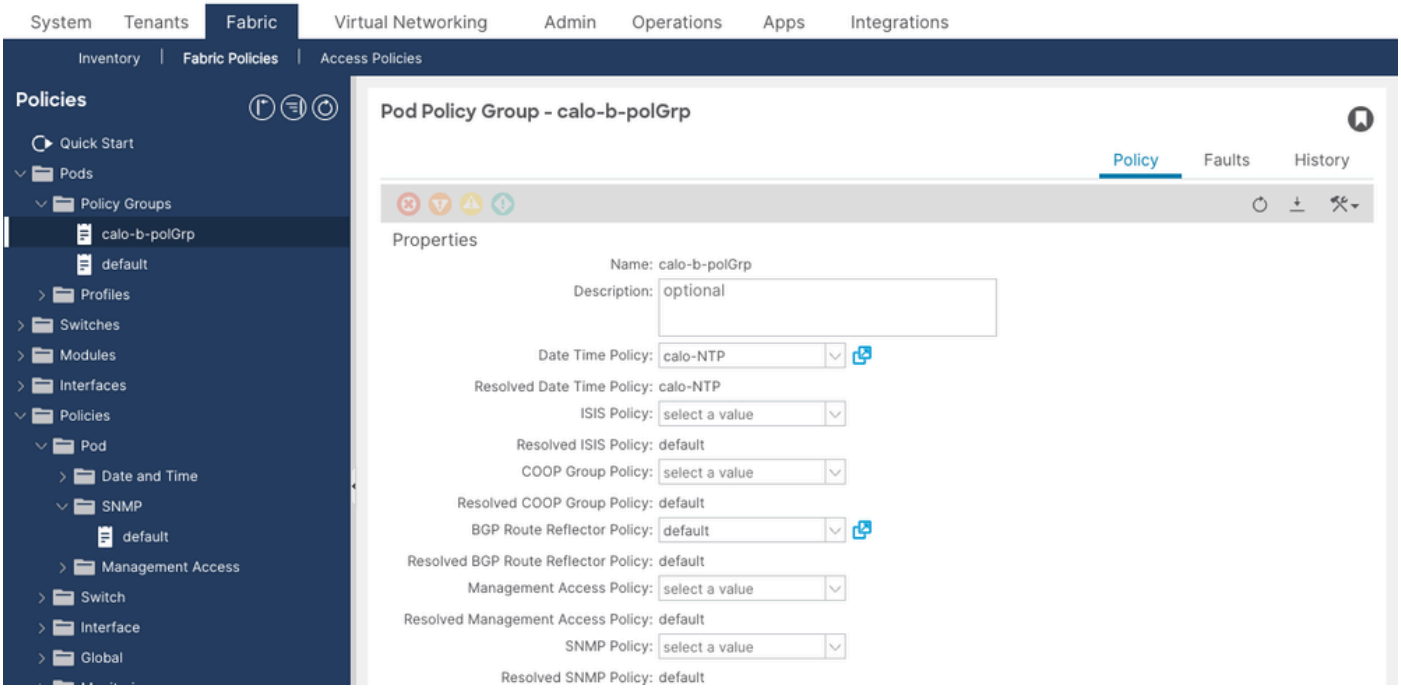
- Estado do administrador — definido como Habilitado.
- Políticas de comunidade — adicione a string de comunidade usada pelo NMS.
- Client Group Policies — define um ou mais perfis de grupo de clientes, cada um especificando os IPs de clientes SNMP permitidos e o EPG de gerenciamento associado (Fora da banda ou Dentro da banda).
- Usuários do SNMPv3 — se estiverem usando o SNMPv3, adicione usuários aqui com

parâmetros de autenticação e privacidade.



Passo 2: Associar a Política SNMP ao Grupo de Políticas do Pod

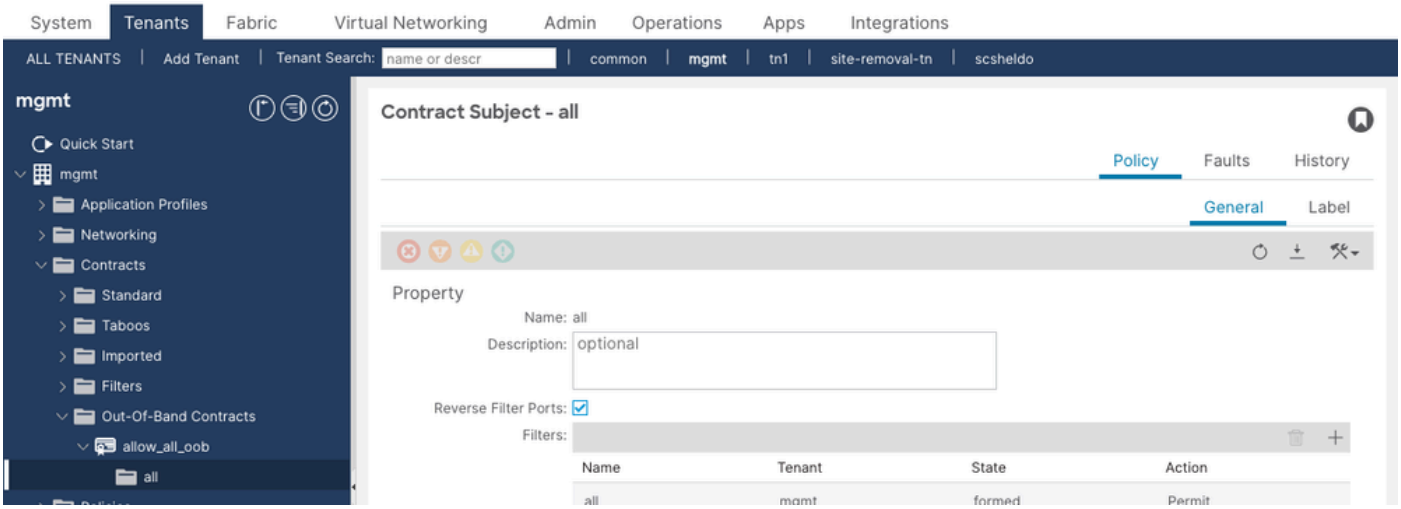
Navegue até Fabric > Fabric Policies > Pods > Policy Groups. Selecione o Grupo de Políticas do Pod ativo (normalmente chamado de padrão). Defina o campo SNMP Policy para apontar para a política SNMP criada na Etapa 1. Verifique se o campo Resolved SNMP Policy mostra o nome correto da política.



Em seguida, navegue para Fabric > Fabric Policies > Pods > Profiles, expanda o Perfil do Pod padrão e confirme se o seletor ativo faz referência ao Grupo de Políticas do Pod correto.

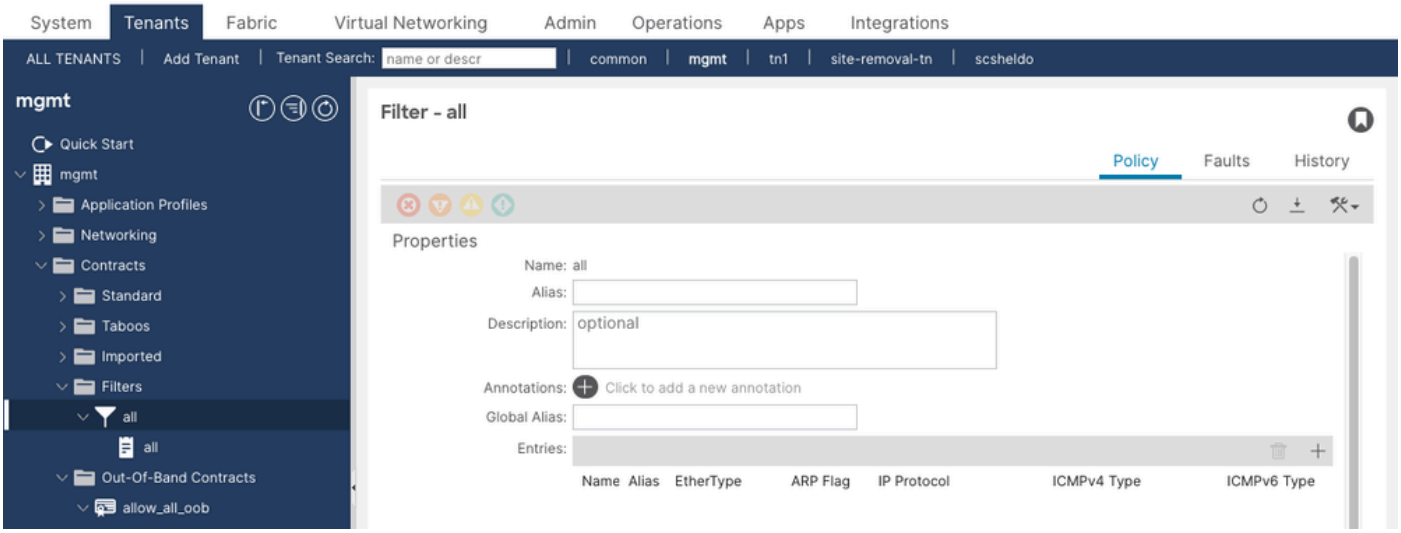
Passo 3: Configurar contratos de gerenciamento para a porta UDP 161

Navegue até Locatários > Gerenciamento > Contratos > Contratos fora da banda. Verifique se o assunto do contrato OOB ativo faz referência a uma entrada de filtro que permite a porta UDP 161 (solicitações SNMP). Sem esse contrato no APIC, todos os pacotes SNMP GET/WALK serão descartados silenciosamente.



As entradas de filtro anexadas ao assunto do contrato devem incluir uma entrada com EtherType IP, Protocol UDP e Destination Port 161. O exemplo acima mostra um filtro permitir tudo (protocolo não especificado) — isso permite o SNMP, mas é mais amplo do que o recomendado

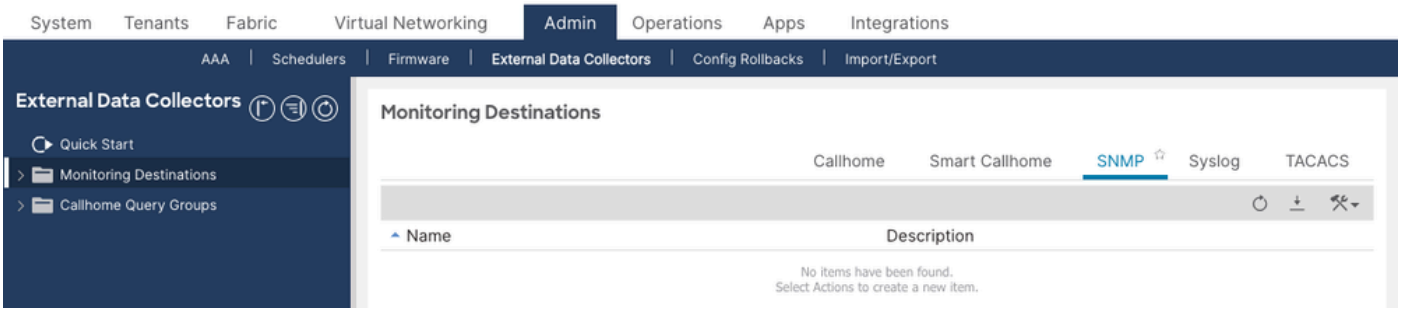
para produção. É preferível uma entrada de filtro SNMP dedicada com entradas UDP/161 e UDP/162 específicas.



Note: Em versões anteriores do firmware da ACI, certas portas sempre eram abertas nos nós leaf e spine, e um contrato de gerenciamento não era necessário para o SNMP. No ACI 5.x, o contrato é necessário para os nós APIC. Os nós leaf e spine usam regras iptables derivadas das Políticas de Grupo de Clientes, em vez de contratos de gerenciamento.

Passo 4: Configurar destinos de interceptações SNMP

Navegue até Admin > External Data Collectors > Monitoring Destinations > SNMP. Clique com o botão direito do mouse e selecione Create SNMP Monitoring Destination Group. A guia SNMP mostra todos os grupos de destinos configurados. Uma tabela vazia significa que nenhum destino de interceptação foi configurado ainda.



Definir:

- Nome do grupo
- Destinos de interceptação: nome de host/IP, porta UDP (padrão 162), versão SNMP, sequência de caracteres de comunidade e EPG de gerenciamento

Passo 5: Configurar Fontes de Monitoramento

As origens de monitoramento vinculam o grupo de destinos SNMP às políticas de monitoramento que controlam quais eventos e falhas geram interceptações. Você deve configurar uma origem de monitoramento em todos os três locais a seguir, ou interceptações de alguns tipos de nó não serão enviadas:

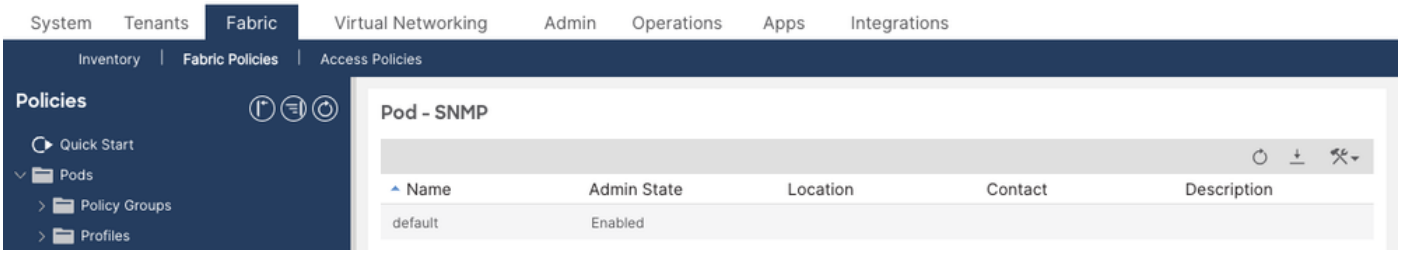
- Fabric > Fabric Policies > Policies > Monitoring > default > Callhome/Smart Callhome/SNMP/Syslog/TACACS (cobre eventos de infraestrutura de malha)
- Fabric > Fabric Policies > Policies > Monitoring > Common Policy > Callhome/Smart Callhome/SNMP/Syslog/TACACS (abrange eventos comuns em toda a malha)
- Fabric > Access Policies > Policies > Monitoring > default > Callhome/Smart Callhome/SNMP/Syslog (cobre eventos de acesso/infraestrutura)

Em cada local, selecione SNMP como o tipo de origem e crie uma nova origem SNMP referenciando o grupo de destinos criado na Etapa 4.

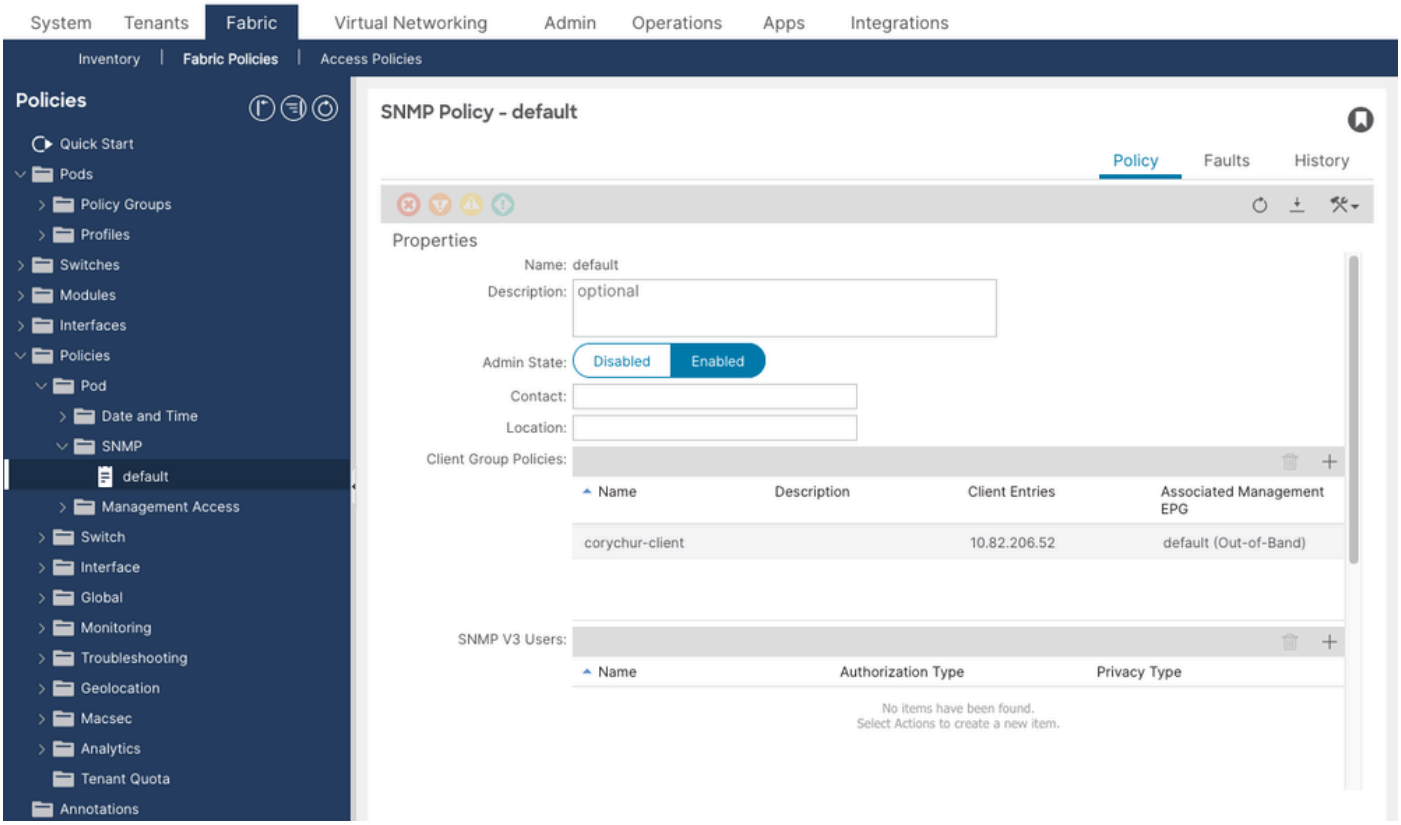
Verifique a configuração

Verificar a implantação da política SNMP

Navegue para Fabric > Fabric Policies > Policies > Pod > SNMP e confirme se a política SNMP padrão existe e se seu Admin State está definido como Enabled. A lista Grupos de política mostra todas as políticas SNMP configuradas com seu estado admin em um piscar de olhos.



Para verificação detalhada, clique no nome da política para abri-la. Confirme se a opção Admin State está definida como Enabled e se Client Group Policies lista todos os hosts NMS permitidos com seu EPG de gerenciamento associado.



Execute a seguinte consulta MO em qualquer APIC para confirmar se a política SNMP está presente e habilitada na estrutura:

<#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 `adminSt` estiver `desabilitado`, o SNMP não funcionará em nenhum nó. Ative-o na GUI do APIC em Fabric > Fabric Policies > Policies > Pod > SNMP > default.

Verificar a configuração da sequência de caracteres de comunidade

<#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 nenhuma comunidade for retornada, ou se o nome não corresponder ao que o NMS está usando, adicione ou corrija a sequência de comunidade na política SNMP.

Verificar as políticas de grupo do cliente (controle de acesso SNMP)

As Políticas de grupo de clientes funcionam como uma ACL para acesso SNMP GET/WALK. Cada política especifica quais endereços IP do cliente têm permissão para pesquisar nós leaf/spine sobre quais VRF de gerenciamento. Nos nós leaf/spine, essas políticas são convertidas em regras iptables.

<#root>

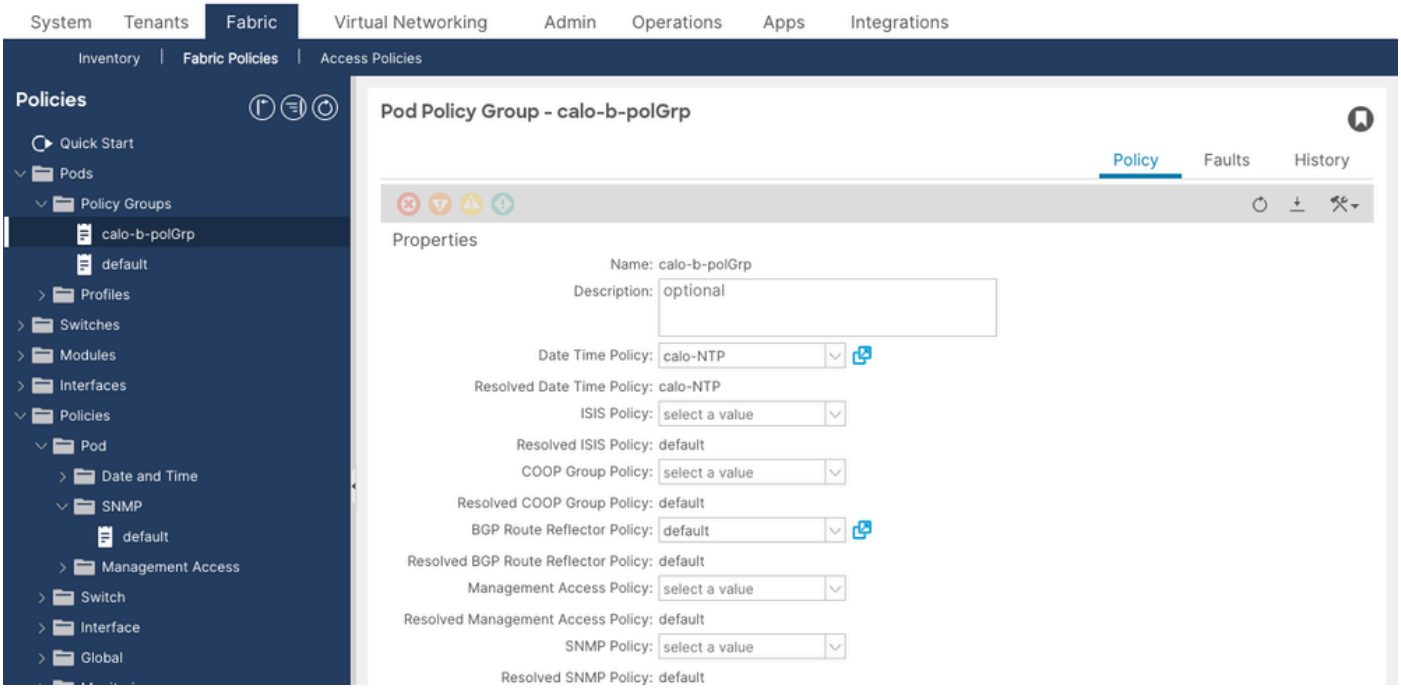
```
apic1#

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
```

Confirme se o IP do servidor NMS está presente nas entradas do cliente. Se um IP de cliente estiver ausente, as solicitações SNMP GET/WALK desse host serão descartadas por iptables em nós leaf/spine.

Note: Aviso de SNMPv3 — as políticas de grupo de clientes não são aplicadas ao APIC quando o SNMPv3 é usado. Qualquer SNMPv3 GET/WALK para um APIC é permitido independentemente da configuração do grupo de clientes. A imposição do grupo de clientes para SNMPv3 no APIC é uma limitação conhecida. Nos switches leaf e spine, a aplicação do grupo de clientes se comporta da mesma forma para SNMPv2c e SNMPv3.

Verificar as referências do grupo de políticas do Pod Política SNMP

Navegue para Fabric > Fabric Policies > Pods > Policy Groups e abra o Pod Policy Group ativo. Confirme se o campo suspenso SNMP Policy está definido como a política SNMP desejada e se o campo Resolved SNMP Policy mostra o mesmo nome. Uma política ausente ou não resolvida significa que a configuração SNMP nunca é enviada aos switches.



Na captura de tela acima, o campo SNMP Policy (Política de SNMP) mostra "select a value" (empty), enquanto a Resolved SNMP Policy (Política de SNMP resolvida) mostra "default" (padrão) — isso significa que a política é herdada do padrão de estrutura, mas não definida explicitamente. É recomendável definir explicitamente o campo SNMP Policy (Política de SNMP) para evitar ambiguidade.

Verificar via API REST:

<#root>

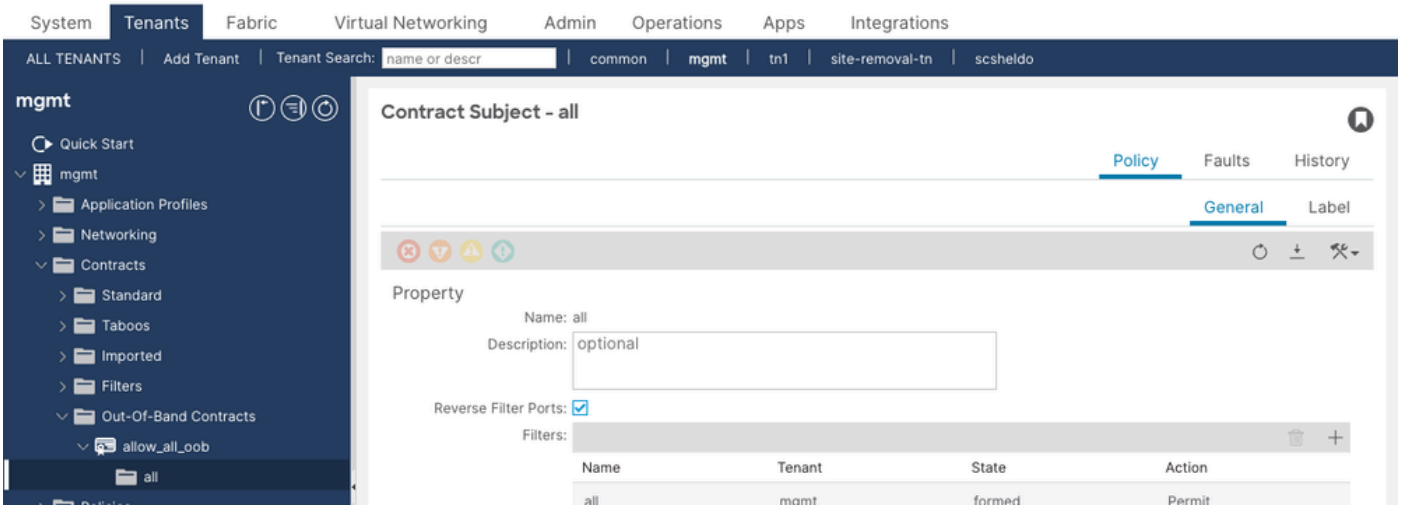
```
apic1#

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"
```

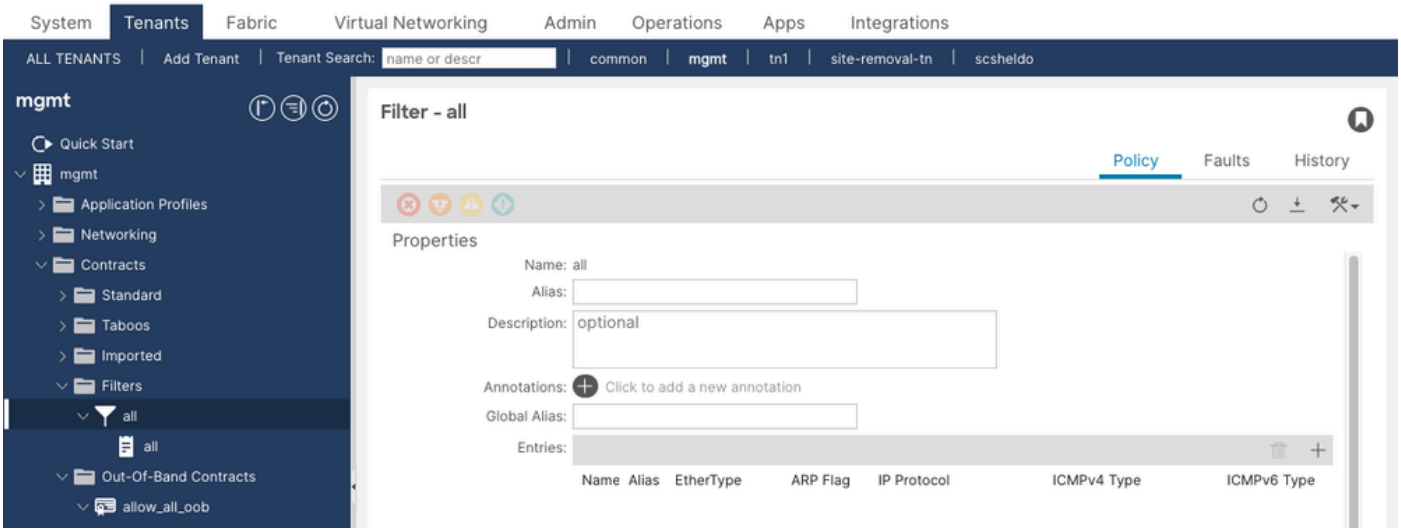
Se o `estado` não for `formado`, a relação da política SNMP será quebrada. Selecione novamente a política de SNMP no Grupo de Políticas de Pod e envie.

Verificar o contrato de gerenciamento para UDP 161 (nós APIC)

Navegue até Locatários > Gerenciamento > Contratos > Contratos fora da banda (e Contratos dentro da banda se estiver usando o gerenciamento INB). Abra o contrato OOB ativo e clique na guia Política. Verifique se o assunto faz referência a um filtro que permita a porta UDP 161.



Expanda o filtro referenciado pelo assunto e confirme se suas entradas incluem uma entrada com EtherType IP, Protocol UDP, Destination Port 161. As entradas de filtro determinam qual tráfego é permitido através do contrato de gerenciamento OOB para o APIC.



O filtro deve mostrar:

- EtherType: IP
- Protocolo IP: UDP
- Porta de Destino De: 161
- Porta de Destino: 161

Verifique também se a porta UDP 162 é permitida se você deseja que o APIC envie interceptações SNMP de saída através da interface OOB.

Verificar via consulta MO:

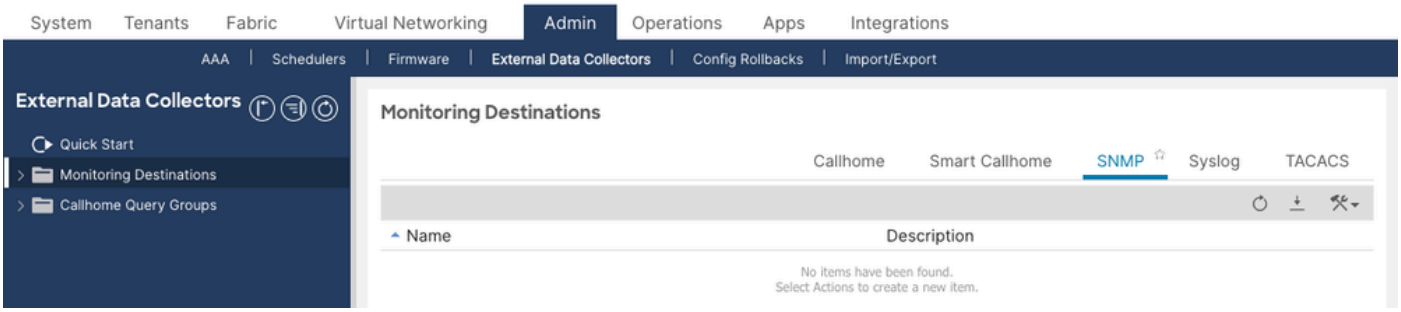
<#root>

```
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 nenhum resultado for retornado, não existe filtro para UDP 161. Adicione um ao contrato de gerenciamento.

Verificar a configuração do destino de interceptação SNMP

Navegue até Admin > External Data Collectors > Monitoring Destinations > SNMP para ver todos os grupos de destinos SNMP configurados. Uma lista vazia significa que nenhum destino de interceptação está configurado e nenhuma interceptação será enviada de qualquer nó.



<#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
```

Confirme se o IP de destino de interceptação, a porta, a versão, a string de comunidade e o VRF de gerenciamento (`mgmt:inb` ou `gerenciamento` para OOB) correspondem ao seu ambiente. O VRF deve corresponder ao EPG de gerenciamento atribuído ao destino.

Verifique se as fontes de monitoramento estão configuradas nos três escopos

As origens SNMP devem existir nos três escopos de política de monitoramento. A ausência de uma origem em qualquer escopo significa que as interceptações de eventos relacionados não serão encaminhadas.

<#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 algum dos três estiver ausente, crie a origem SNMP ausente na política de monitoramento correspondente usando a GUI.

Verificação operacional

Verificar o estado do SNMP usando show snmp summary (APIC)

Execute este comando diretamente em cada APIC para confirmar se o agente SNMP está em execução e se a configuração foi aplicada:

<#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
```

O que verificar na saída:

- O estado Admin deve ser `habilitado`.
- A comunidade deve corresponder ao que o NMS está configurado para usar.
- Client-Group deve listar todos os IPs NMS permitidos com EPG de gerenciamento correto.
- O host (destino de interceptação) deve listar o receptor de interceptação NMS com a porta e a versão corretas.

Verificar o estado do SNMP usando 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
```

O que verificar na saída:

- O estado Admin deve ser `habilitado, sendo executado` com um pid. Se ele mostrar `disabled`, a política SNMP não é aplicada ou a cadeia de políticas do pod é quebrada.
- O status da comunidade deve ser `ok`. Um status de `erro` indica um problema de implantação de política.
- O VRF do cliente para cada host NMS deve corresponder ao VRF do EPG de gerenciamento (`mgmt:inb` para In-Band, `gerenciamento` para OOB).
- O host de interceptação deve listar o destino com o contexto VRF correto.

Verifique se o processo snmpd está em execução

Numa folha ou coluna:

<#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
```

No 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 nenhum processo snmpd for encontrado em um leaf ou spine, o SNMP não estará sendo executado nesse nó. Verifique se a política de SNMP Admin State está habilitada e se a cadeia de política do pod está configurada corretamente.

Spoiler (Realce para ler)

Verifique se a porta SNMP está escutando

<#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 a porta 161 não estiver listada no estado LISTEN, o processo snmpd não está em execução ou falhou ao se vincular à porta.

Verificar as regras iptables em Leaf/Spine

As Políticas de Grupo de Clientes são convertidas em regras iptables em cada folha e coluna. Use o seguinte para inspecionar as regras:

<#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)
```

Para identificar os IDs de VRF corretos para sua estrutura, execute:

<#root>

```
leaf101#
```

show vrf

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

Os IDs de VRF nas regras iptables devem corresponder ao que `show vrf` relata. Se um IP cliente estiver ausente das regras iptables, as solicitações SNMP desse host serão silenciosamente descartadas, mesmo que o processo snmpd esteja em execução.

Use contadores para verificar se algum pacote SNMP foi correspondido ou descartado:

<#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
```

Note: Se o SNMP estiver em execução, mas o iptables não mostrar cadeias snmp_rules, ou se as cadeias estiverem vazias, você poderá reiniciar o processo snmpd para forçar a reprogramação da regra iptables. O envio de SIGKILL para o snmpd PID é seguro — o gerenciador de processos da ACI (`policiado`) o reiniciará automaticamente. Execute `pidof snmpd` para obter o PID e, em seguida, `kill -9 [snmpd_pid]`. Confirme o novo PID com `pidof snmpd` após 10-15 segundos.

Verifique se a porta SNMP está ouvindo leaf101# netstat -lutn | grep 161 Conexões ativas com a Internet (somente servidores) Proto Recv-Q Send-Q Endereço local Endereço externo Estado tcp 0 0 0 0.0.0.0:161 0.0.0.0:* LISTEN <— O agente SNMP está aceitando solicitações udp 0 0 0.0.0.0:161 0.0.0.0:* udp6 0 :::161 ::* Se a porta 161 não estiver listada no estado LISTEN, o processo snmpd não está em execução ou falhou ao se vincular porta. Verifique se as regras iptables nas políticas de grupo do cliente Leaf/Spine são convertidas em regras iptables em cada leaf e spine. Use o seguinte para inspecionar as regras: 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 <— porta SNMP 161 redireciona para cadeia snmp_rules -A snmp_rules -m vrf —vrf 2 -j vrf_2_snmp_rules <— VRF 2 = gerenciamento do OOB -A snmp_rules -m vrf —vrf 9 -j vrf_9_snmp_rules <— VRF 9 = In-Band management -A snmp_rules -j DROP <— default drop; somente clientes permitidos passam -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) Para identificar os IDs de VRF corretos para sua malha, execute: leaf101# show vrf VRF-Name VRF-ID State Reason management 2 Up — mgmt:inb 9 Up — Os IDs de VRF nas regras do iptables devem corresponder ao que o show vrf relata. Se um IP cliente estiver ausente das regras iptables, as solicitações SNMP desse host serão silenciosamente descartadas, mesmo que o processo snmpd esteja em execução. Use contadores para verificar se algum pacote SNMP foi correspondido ou descartado: leaf101# iptables -nvL | grep -A 20 "Chain snmp_rules" Chain snmp_rules (1 referências) 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 <— se pkts>0 aqui, os IPs do cliente estão ausentes Nota: Se o SNMP estiver em execução, mas o iptables não mostrar cadeias snmp_rules, ou se as cadeias estiverem vazias, você poderá reiniciar o processo snmpd para forçar a reprogramação da regra iptables. O envio de SIGKILL

para o snmpd PID é seguro — o gerenciador de processos da ACI (policiado) o reiniciará automaticamente. Execute pidof snmpd para obter o PID e elimine -9 [snmpd_pid]. Confirme o novo PID com pidof snmpd após 10-15 segundos.

Verificar a conectividade de rede para as portas 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
```

Confirme se as interfaces de gerenciamento estão ativas (sem incrementos RX-ERR) e transmitindo tráfego. `eth0` é a interface de gerenciamento OOB; `kpm_inb` é a interface de gerenciamento In-Band no switch.

Verificar o envio de interceptação SNMP com tcpdump

Para confirmar que as armadilhas estão sendo geradas e enviadas de um nó de folha ou coluna, capture o tráfego na interface apropriada. Acesse o nó como admin e use:

<#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
```

Para OOB:

<#root>

leaf101#

tcpdump -i eth0 -f port 162 -vv

Spoiler (Realce para ler)

Para armadilhas 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

Note: No APIC, bond0.1100 é a subinterface VLAN da interface de gerenciamento In-Band. Substitua 1100 pelo encapsulamento de VLAN configurado para o EPG de gerenciamento In-Band. Use oobmgmt como o nome da interface para capturas OOB no APIC.

Para armadilhas APIC (INB): apic1# tcpdump -i bond0.1100 -f porta 162 20:01:08.453473 IP apic1-inb.cisco.com.59417 > 10.1.1.50.snmptrap: C=público 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 Observação: No APIC, bond0.1100 é a subinterface VLAN da interface de gerenciamento In-Band. Substitua 1100 pelo compartimento de VLAN configurado para o EPG de gerenciamento In-Band. Use oobmgmt como o nome da interface para capturas OB no APIC.

Verificar solicitações SNMP GET/WALK com 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 você vir o GetRequest, mas não o GetResponse, a solicitação será recebida, mas não

respondida. Verifique o processo snmpd e a série de comunidade. Se você não vir solicitação nem resposta, a solicitação será bloqueada antes de chegar ao nó (verifique roteamento e iptables).

Troubleshooting de Fluxo de Trabalho

Árvore decisória de triagem

Use esta árvore decisória quando os engenheiros relatarem que o SNMP não está funcionando. Comece do sintoma observado e siga os ramos até o isolamento.

Sintoma: Nenhuma resposta às solicitações SNMP GET/WALK

1. Verifique o estado do administrador SNMP no APIC. Execute `moquery -c snmpPol`. Se `adminSt` estiver `desabilitado`, habilite-o e continue com a Etapa 7.
2. Verifique o processo snmpd. No nó afetado, execute `ps aux | grep snmp` ou `pidof snmpd`. Se nenhum processo estiver em execução, a política SNMP não será implantada. Verifique a cadeia de políticas do pod (Política SNMP → Grupo de Políticas do Pod → Perfil do Pod).
3. Verifique se a porta 161 está escutando. Execute `netstat -lutn | grep 161`. Se a porta 161 não estiver no estado LISTEN, o processo snmpd falhou; colete logs de `/var/log/dme/log/svc_ifc_dbgrelem.log*` e reinicie o processo.
4. Verifique o roteamento. Execute `show ip route vrf management` e `show ip route vrf mgmt:inb`. Confirme se existe uma rota para o host NMS no VRF correto.
5. Verifique o contrato de gerenciamento no APIC. Se o destino for um APIC (não uma folha/coluna), verifique se o UDP 161 é permitido no contrato de gerenciamento OOB ou INB.
6. Execute tcpdump no nó. Execute `tcpdump -i kpm_inb -f porta 161 -vv` (ou `eth0` para OOB). Se GetRequest for exibido, mas nenhuma GetResponse for exibida, a solicitação atingirá o nó, mas snmpd não estará respondendo — verifique a sequência de caracteres da comunidade. Se nenhuma solicitação aparecer, o problema é upstream (roteamento ou contrato).
7. Teste a partir de um cliente permitido. Execute `snmpget -v2c -c [community] [node-ip] SNMPv2-MIB::sysDescr.0` a partir de um host NMS listado no grupo de clientes. Uma resposta bem-sucedida confirma que o SNMP está totalmente operacional.

Sintoma: Nenhuma interceptação SNMP recebida no NMS

1. Verifique a configuração do destino de interceptação (trapping). Execute `moquery -c snmpTrapDest`. Confirme se o IP, a porta, a versão e a comunidade do NMS correspondem aos valores esperados do NMS.

2. Verifique se as fontes de monitoramento existem nos três escopos. Execute `moquery -c snmpSrc | egrep "snmp.Src|name|dn"`. Confirme se existem entradas com os valores `monPolDn` para `uni/fabric/monfab-default`, `uni/fabric/moncommon` e `uni/infra/moninfra-default`. Se algum estiver ausente, adicione a origem SNMP na política de monitoramento correspondente.
3. Verifique o processo snmpd. Verifique se o snmpd está em execução no nó que deveria estar enviando a interceptação (trap).
4. Gere um evento de teste e capture com tcpdump. Altere uma interface ou um estado para gerar um evento. No nó, execute `tcpdump -i kpm_inb -f porta 162 -vv`. Se nenhum tráfego de interceptação (trapping) aparecer no fio, o evento não está gerando uma interceptação — verifique novamente a fonte de monitoramento `incluindo` o atributo (deve incluir `falhas` ou `eventos`).
5. Verifique a conectividade com o receptor de interceptação. Confirme se o receptor de interceptação (trapping) pode ser alcançado no VRF de gerenciamento: `show ip route vrf mgmt:inb` deve mostrar um caminho para o host NMS.
6. Se as interceptações aparecerem no tcpdump, mas não no NMS, o problema será na rede: firewall, roteamento ou a configuração NMS. Verifique se o NMS está escutando no UDP 162 do IP de origem de gerenciamento do nó ACI.

Cenários comuns

Cenário 1: Política SNMP habilitada, mas nenhum dado foi retornado da folha/coluna

Problema: A Política SNMP no APIC mostra Estado Admin habilitado. O NMS pode acessar o IP de gerenciamento do leaf. `snmpget` expira sem resposta.

Verificação de configuração: Verifique se o Grupo de políticas do Pod faz referência à política de SNMP e se a Política de SNMP resolvida mostra o nome correto. Se o campo Política SNMP do Grupo de Políticas de Pod estiver vazio ou a relação não for formada, o processo snmpd pode não iniciar nos switches.

Verificação operacional: SSH para a folha afetada e execute `show snmp summary`. Se a saída mostrar `Admin State: desativada` mesmo que o APIC mostre ativado, a política não foi implantada. Verifique a cadeia de política do pod para um Grupo de Política do Pod ausente ou referenciado incorretamente.

Causa raiz: A política SNMP não está vinculada ao Grupo de Políticas do Pod ou o seletor de Perfil do Pod não está aplicando o Grupo de Políticas do Pod correto a este pod.

Solução:

1. Navegue até Fabric > Fabric Policies > Pods > Policy Groups > default.
2. Confirme se o campo SNMP Policy aponta para a política SNMP ativada.
3. Navegue para Fabric > Fabric Policies > Pods > Profiles e confirme as referências do seletor ativo neste Pod Policy Group.
4. Depois de salvar, verifique novamente `show snmp summary` no leaf em 2 minutos.

Cenário 2: O SNMP GET/WALK funciona para alguns hosts NMS, mas não para outros

Problema: Um servidor NMS pode pesquisar nós ACI com êxito. Um segundo servidor NMS em uma sub-rede diferente não recebe resposta.

Verificação de configuração: Execute `moquery -c snmpClientGrpP -x query-target=children` no APIC. Confirme se o IP do segundo servidor NMS está listado como uma entrada de cliente. Se estiver faltando, esse IP será bloqueado pela regra iptables DROP na parte inferior da cadeia snmp_rules.

Verificação operacional: na folha afetada, confirme se o UDP 161 é permitido no contrato de gerenciamento OOB ou INB. Se nenhum contrato ou filtro tiver portas SNMP, a solicitação será descartada.

Causa raiz: O segundo IP do servidor NMS não está na Política de Grupo do Cliente.

Solução: Adicione o NMS IP ausente como uma entrada de cliente na Política de grupo do cliente SNMP em Estrutura > Políticas de estrutura > Políticas > Pod > SNMP > padrão > Políticas de grupo do cliente. As regras iptables em todos os nós serão atualizadas minutos após o salvamento da política.

Cenário 3: Armadilhas SNMP Não Recebidas — As Armadilhas São Geradas Mas Não Entregues

Problema: As falhas são visíveis na tabela de falhas do APIC. `moquery -c snmpTrapDest` mostra o IP NMS correto. O NMS não recebe interceptações.

Verificação de configuração: Execute `moquery -c snmpSrc | egrep "snmp.Src|name|dn"`. Verifique se as fontes de monitoramento existem em todos os três escopos (`monfab-default`, `moncommon`, `moninfra-default`). Uma supervisão comum é configurar a origem somente na política Padrão de estrutura, que perde eventos de política de acesso.

Verificação operacional: Dispare um evento de teste (por exemplo, alterne uma interface para o

estado admin-down). No nó relevante, execute `tcpdump -i kpm_inb -f porta 162`. Se pacotes de interceptação (trapping) aparecerem na interface do nó, o lado da ACI está funcionando e o problema está no caminho de rede para o NMS (firewall, roteamento). Se nenhuma interceptação (trapping) aparecer na conexão, a fonte de monitoramento da ACI está ausente ou o tipo de evento não está incluído no atributo `incl` da fonte.

Causa raiz 1: Uma ou mais fontes de monitoramento estão ausentes nos escopos necessários.

Causa básica 2: O atributo `incl` de origem de monitoramento exclui o tipo de evento que está sendo gerado (por exemplo, `incl: eventos` sem `falhas` significa que armadilhas baseadas em falhas não serão enviadas).

Solução:

1. Adicione fontes de monitoramento ausentes na GUI para cada um dos três escopos (Fabric Default, Fabric Common, Access Default). Defina o grupo de destino para o seu grupo de destino SNMP configurado.
2. Verifique se o atributo `incl` inclui `auditorias,eventos,falhas` para uma cobertura de interceptação abrangente.
3. Após as alterações, acione novamente o evento de teste e verifique novamente tcpdump.

Spoiler (Realce para ler)

Note: No APIC, o `comando tcpdump/code> está disponível apenas para o usuário root. Para APIC e Switches, o comando iptables está disponível apenas para o usuário raiz.`

Cenário 4 : Aplicação de grupo de clientes SNMPv3 não funciona no APIC

Problema: Um cliente SNMP que NÃO está na Política de grupo do cliente pode consultar com êxito o APIC usando SNMPv3, mesmo que a mesma consulta falhe nos nós leaf/spine.

Causa raiz: Esta é uma **advertência conhecida**. As políticas de grupo de clientes (aplicação de IP de origem baseada em iptables) não são aplicadas para GETs/Walks de SNMPv3 para controladores APIC. Qualquer host pode consultar o APIC via SNMPv3 independentemente da configuração do grupo de clientes. Em switches leaf e spine, a aplicação do grupo de clientes funciona de forma idêntica para SNMPv2c e SNMPv3.

Atenuação: Use filtros de contrato de gerenciamento no APIC para restringir o acesso SNMP por sub-rede de origem. Os grupos de clientes são eficazes para nós leaf/spine. Para o APIC com SNMPv3, confie na filtragem baseada na origem do contrato de gerenciamento como o mecanismo de controle de acesso.

Cenário 5 : Consultas SNMP bem-sucedidas, mas os dados MIB estão incompletos ou obsoletos

Problema: O SNMP GET/WALK retorna dados, mas determinados OIDs MIB retornam valores vazios ou obsoletos. Em particular, as estatísticas da interface ou os dados do estado operacional não refletem o estado atual da malha.

Verificação operacional: Confirme qual APIC está sendo consultado. Cada APIC retorna somente objetos MIB para os dados locais a ele. Execute show snmp summary no APIC sendo consultado e compare o resultado com o esperado. Para dados em nível de switch (IF-MIB, entityMIB), consulte

o switch diretamente, não o APIC.

Causa raiz: Consultar um APIC para dados MIB de nível de folha. Cada APIC fornece objetos MIB somente para seus próprios objetos gerenciados. Os dados no nível do switch (estatísticas de interface, CPU, memória, sensores ambientais) devem ser recuperados fazendo polling em cada folha e coluna diretamente.

Solução: Configure seu NMS para pesquisar IPs de gerenciamento de leaf e spine diretamente para dados MIB de interface e hardware. Use IPs de gerenciamento do APIC somente para MIBs nativos do APIC (entidade, FRU, processo, sensor relacionado ao hardware do servidor APIC).

Cenário 6 : O SNMP funciona para leaf/spine, mas não para o APIC

Problema: O SNMPv2c GET do NMS para os nós de folha e coluna foi bem-sucedido. O mesmo NMS não pode sondar o APIC.

Verificação de configuração: O SNMP do APIC requer um contrato de gerenciamento explícito que permita o UDP 161. Navegue até **Locatários > gerenciamento** e verifique o contrato OOB/INB e seu filtro para UDP 161.

Verificação operacional: No APIC, execute iptables -S | grep 161. Se nenhuma regra ACCEPT para UDP 161 aparecer sob a cadeia fp-137 (ou contrato OOB equivalente), o filtro de contrato para UDP 161 está faltando ou não foi implantado.

```
<#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 essas regras estiverem ausentes, adicione uma entrada de filtro para UDP 161 ao assunto do contrato de gerenciamento e verifique novamente.

Causa raiz: Contrato de gerenciamento ausente ou configurado incorretamente. No ACI 5.x, os nós APIC aplicam estritamente o contrato de gerenciamento — os pacotes SNMP são descartados, a menos que exista uma permissão explícita.

Solução:

1. Navegue até **Locatários > Gerenciamento > Políticas de segurança > Contratos fora da banda**.
2. Expanda o contrato OOB, selecione o Assunto e verifique/adicione um filtro para a **porta UDP 161**.
3. Repita para o contrato In-Band se o NMS estiver alcançando o APIC no gerenciamento INB.
4. Verifique com iptables -S | grep 161 no APIC após a economia.

Cenário 7 : As regras de SNMP iptables estão ausentes ou incorretas

Problema: show snmp summary mostra a política SNMP aplicada, mas iptables -S | grep snmp não retorna nenhuma regra ou o IP do cliente NMS está ausente das regras.

Verificação operacional: Confirme se snmpd está sendo executado com pidof snmpd. Se o snmpd estiver em execução, mas o iptables não tiver regras de SNMP, o processo foi iniciado antes da Política de Grupo do Cliente ter sido implantada. Reinicie o snmpd para forçar a reprogramação da regra se o número de reinicializações for menor que 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

O gerenciador de processos da ACI reiniciará automaticamente o snmpd. Após a reinicialização, verifique:

```
<#root>

leaf101#
```

iptables -S | grep -i snmp

As cadeias snmp_rules e as regras ACCEPT por cliente VRF devem ser exibidas agora.

Causa raiz: o processo snmpd foi reiniciado ou iniciado antes que a Política de Grupo do Cliente fosse totalmente implantada no nó, deixando o iptables sem as regras de acesso SNMP.

Note: No APIC, o comando tcpdump/code> está disponível somente para o usuário raiz. Para APIC e Switches, o comando iptables só está disponível para o usuário raiz. Cenário 4 : A aplicação do grupo de clientes SNMPv3 não está funcionando no problema APIC: Um cliente SNMP que NÃO está na Política de grupo do cliente pode consultar com êxito o APIC usando SNMPv3, mesmo que a mesma consulta falhe nos nós leaf/spine. Causa raiz: Esta é uma advertência conhecida. As políticas de grupo de clientes (aplicação de IP de origem baseada em iptables) não são aplicadas para GETs/Walks de SNMPv3 para controladores APIC. Qualquer host pode consultar o APIC via SNMPv3 independentemente da configuração do grupo de clientes. Em switches leaf e spine, a aplicação do Grupo de clientes funciona de forma idêntica para SNMPv2c e SNMPv3. Mitigação: Use filtros de contrato de gerenciamento no APIC para restringir o acesso SNMP por sub-rede de origem. Os grupos de clientes são eficazes para nós leaf/spine. Para o APIC com SNMPv3, confie na filtragem baseada na origem do contrato de gerenciamento como o mecanismo de controle de acesso. Cenário 5 : Consultas SNMP bem-sucedidas, mas os dados MIB estão incompletos ou com problema obsoleto: O SNMP GET/WALK retorna dados, mas determinados OIDs MIB retornam valores vazios ou obsoletos. Em particular, as estatísticas da interface ou os dados do estado operacional não refletem o estado atual da malha. Verificação operacional: Confirme qual APIC está sendo consultado. Cada APIC retorna somente objetos MIB para os dados locais a ele. Execute show snmp summary no APIC sendo consultado e compare o resultado com o esperado. Para dados em nível de switch (IF-MIB, entityMIB), consulte o switch diretamente, não o APIC. Causa raiz: Consultar um APIC para dados MIB de nível de folha. Cada APIC fornece objetos MIB somente para seus próprios objetos gerenciados. Os dados no nível do switch (estatísticas de interface, CPU, memória, sensores ambientais) devem ser recuperados fazendo polling em cada folha e coluna diretamente. Solução: Configure seu NMS para pesquisar IPs de gerenciamento de leaf e spine diretamente para dados MIB

de interface e hardware. Use IPs de gerenciamento do APIC somente para MIBs nativos do APIC (entidade, FRU, processo, sensor relacionado ao hardware do servidor APIC). Cenário 6 : O SNMP funciona para leaf/spine, mas não para o problema do APIC: O SNMPv2c GET do NMS para os nós de folha e coluna foi bem-sucedido. O mesmo NMS não pode sondar o APIC. Verificação de configuração: O APIC SNMP requer um contrato de gerenciamento explícito que permita o UDP 161. Navegue até Locatários > Gerenciamento e verifique o contrato OOB/INB e seu filtro para UDP 161. Verificação operacional: No APIC, execute iptables -S | grep 161. Se nenhuma regra ACCEPT para UDP 161 aparecer sob a cadeia fp-137 (ou contrato OOB equivalente), o filtro de contrato para UDP 161 está ausente ou não foi implantado. apic1#iptables -S | grep 161 -A fp-137 -s 10.0.0.0/8 -p udp -m udp —dport 161 -j ACCEPT <— permit SNMP da sub-rede de gerenciamento -A fp-137 -s 172.18.0.0/16 -p udp -m udp —dport 161 -j ACCEPT <— permit SNMP da sub-rede de gerenciamento INB Se essas regras não existirem, adicione uma entrada de filtro para UDP 161 ao assunto do contrato de gerenciamento e verifique novamente. Causa raiz: Contrato de gerenciamento ausente ou configurado incorretamente. No ACI 5.x, os nós APIC aplicam estritamente o contrato de gerenciamento — os pacotes SNMP são descartados, a menos que exista uma permissão explícita. Solução: Navegue até Locatários > Gerenciamento > Políticas de segurança > Contratos fora da banda. Expanda o contrato OOB, selecione o Assunto e verifique/adicione um filtro para a porta UDP 161. Repita para o contrato In-Band se o NMS estiver alcançando o APIC no gerenciamento INB. Verifique com iptables -S | grep 161 no APIC após a poupança. Cenário 7 : As regras de SNMP iptables estão ausentes ou apresentam problema incorreto: show snmp summary mostra que a política SNMP é aplicada, mas iptables -S | grep snmp não retorna nenhuma regra ou o IP do cliente NMS está ausente das regras. Verificação operacional: Confirme se snmpd está sendo executado com pidof snmpd. Se o snmpd estiver em execução, mas o iptables não tiver regras de SNMP, o processo foi iniciado antes da Política de Grupo do Cliente ter sido implantada. Reinicie o snmpd para forçar a reprogramação da regra se o número de reinicializações for menor que 250: leaf101# pidof snmpd 5881leaf101# show system internal sysmgr service name snmpdService "snmpd" ("snmpd", 127):UUID = 0x1A, PID = 5881, SAP = 1545State: SRV_STATE_HANDSHAKED (inserido no horário Seg 25 19:23:50 2025).Contagem de reinicialização: 3Hora da última reinicialização: Seg, 25 de agosto de 2025, 19:23:48. PID anterior: 32080Motivo do último encerramento: SYSMGR_DEATH_REASON_FAILURE_SIGNALTag = N/ID do plugin: 0 leaf101# kill -9 5881 O gerenciador de processos da ACI reiniciará automaticamente o snmpd. Após a reinicialização, verifique: leaf101# iptables -S | grep -i snmp As cadeias snmp_rules e as regras de ACEITAÇÃO por cliente VRF devem aparecer agora. Causa raiz: o processo snmpd foi reiniciado ou iniciado antes que a Política de Grupo do Cliente fosse totalmente implantada no nó, deixando o iptables sem as regras de acesso SNMP.

Arquivos de log para solução de problemas estendida

Quando as etapas de verificação acima não resolvem o problema, os seguintes arquivos de log nos nós leaf, spine e APIC contêm informações de diagnóstico relacionadas ao 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/*

Esses logs contêm eventos de reinicialização snmpd, eventos de implantação de política e erros

de configuração de comunidade/cliente que não são visíveis por meio de show snmp summary.

Referências

- Guia de configuração de gerenciamento do sistema do Cisco APIC, versão 5.x — Gerenciamento de SNMP
- Guia de referência rápida MIB da Cisco ACI

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.