# Resolución de problemas de SNMP en Cisco ACI Fabric

## Introducción

Este documento describe cómo configurar, verificar y resolver problemas de SNMP en Cisco ACI para ACI versión 5.x y posteriores. Abarca el modelo de políticas SNMP, los contratos de gestión necesarios, la configuración de trampas, la verificación operativa mediante consultas de CLI y objetos administrados (MO) y los flujos de trabajo de solución de problemas estructurados para los escenarios de fallos más comunes en los switches de hoja/columna y los controladores APIC.

## Antecedentes

El material de este documento se ha extraído de la nota técnica interna SNMP del Equipo de entrega de soluciones de Cisco ACI en ACI: Descripción general, configuración, resolución de problemas y advertencias/problemas de la autoría de Tomás de León, complementados con la Guía de configuración de administración del sistema Cisco APIC (versión 5.x) y la Guía de referencia rápida de MIB de Cisco ACI.

## Overview

### Arquitectura SNMP en ACI

SNMP (protocolo simple de administración de red) es un protocolo basado en UDP que controla la administración y supervisión de la red. En ACI, SNMP funciona independientemente en cada entidad administrada. Cada switch de hoja, switch de columna y controlador APIC es su propio agente SNMP; cada uno debe sondearse o supervisarse de forma independiente.

ACI admite las siguientes capacidades SNMP:

- Operaciones de lectura (Get, GetNext, BulkGet, Walk): compatibles con switches de hoja/columna y controladores APIC.
- Notificaciones (trampas): trampas SNMPv1, v2c y v3 admitidas en switches de hoja/columna y controladores APIC.
- SNMPv3: compatible con switches de columna/hoja y controladores APIC.

- Operaciones de escritura (conjunto): NO se admiten en ningún dispositivo ACI.
- IPv6: SNMP sólo es compatible con IPv4.

---

Nota: En un clúster APIC, cada APIC proporciona objetos MIB locales para sí mismo. Debe sondear cada APIC por separado; no hay agregación SNMP en todo el clúster. Del mismo modo, cada switch de columna y hoja debe consultarse de forma independiente.

---

## Arquitectura SNMP en el APIC

El APIC ejecuta el proceso snmpd, que tiene dos componentes internos:

- Agente: agente net-snmp de código abierto (versión 5.7.6 o posterior) que administra el procesamiento del protocolo SNMP y la administración de sesiones.
- DME (motor de modelo de datos): interactúa con el árbol de información de gestión (MIT) de APIC para leer objetos gestionados (MO) y traducir los atributos MO al formato de objeto SNMP. Las trampas SNMP se generan a partir de eventos y fallas generados en los MO.

## Modelo de política SNMP y cadena de implementación

ACI utiliza un modelo dirigido por políticas para SNMP. La configuración SNMP se abstrae como un objeto administrado snmpPol y se debe asociar al grupo de políticas de grupo de dispositivos del fabric antes de que se implemente en cualquier nodo. La cadena de implementación completa es:

1. Política SNMP (`snmpPol`): define el estado de administración, las cadenas de comunidad, las políticas de grupo de clientes (ACL) y los usuarios SNMPv3.
2. Grupo de políticas de grupo: hace referencia a la política SNMP junto con otras políticas de nivel de grupo (BGP, ISIS, NTP, etc.).
3. Selector de perfiles de grupo: aplica el grupo de políticas de grupo a los grupos de dispositivos de fabric.

Además, la configuración de trampas SNMP requiere:

1. SNMP Monitoring Destination Group (`snmpGroup`): define los hosts de destino de trampa, el puerto, la versión de SNMP y la comunidad.
2. Orígenes de supervisión (`snmpSrc`): vincula el grupo de destino a tres ámbitos de directivas de supervisión distintos: Fabric Default, Fabric Common Policy y Access Policy Default.

Se requieren contratos de administración que permitan el puerto UDP 161 (solicitudes SNMP) y el puerto UDP 162 (capturas SNMP) para los nodos APIC. Los nodos de columna y de hojas

también requieren reglas iptables correctas, que se programan automáticamente cuando se configuran las directivas de grupo de clientes.

### MIB compatibles

Los MIB admitidos en el APIC incluyen:

- MIB de entidad: tabla física
- Cisco Entity Ext MIB: PhysicalProcessorTable, LEDTable
- MIB de control de FRU de entidad de Cisco: PowerSupplyGroupTable, PowerStatusTable, FanTrayStatusTable, PhysicalTable
- MIB de Cisco Entity Sensor: SensorValueTable, SensorThresholdTable
- Cisco Process MIB: CPUTotalTable, ProcessTable, ProcessExtRevTable, ThreadTable

Los switches de columna y de hoja exponen MIB de NX-OS estándar, incluidos IF-MIB, IP-MIB, CISCO-CDP-MIB, CISCO-ENTITY-QFP-MIB y el conjunto completo CISCO-ENTITY-FRU-CONTROL-MIB.

Las trampas SNMP generadas en el APIC incluyen: `cefcFRUInserted, cefcFRURemoved, cefcFanTrayStatusChange, cefcModuleStatusChange, entSensorThresholdNotification, cefcPowerStatusChange, cpmCPURisingThreshold, cpmCPUFallingThreshold.`

## Configuración de SNMP en ACI

---

Nota: Esta sección proporciona un resumen del flujo de trabajo de configuración como contexto para las siguientes secciones de verificación y solución de problemas. Consulte la Guía de configuración de la gestión del sistema Cisco APIC para obtener información detallada sobre los procedimientos de configuración.

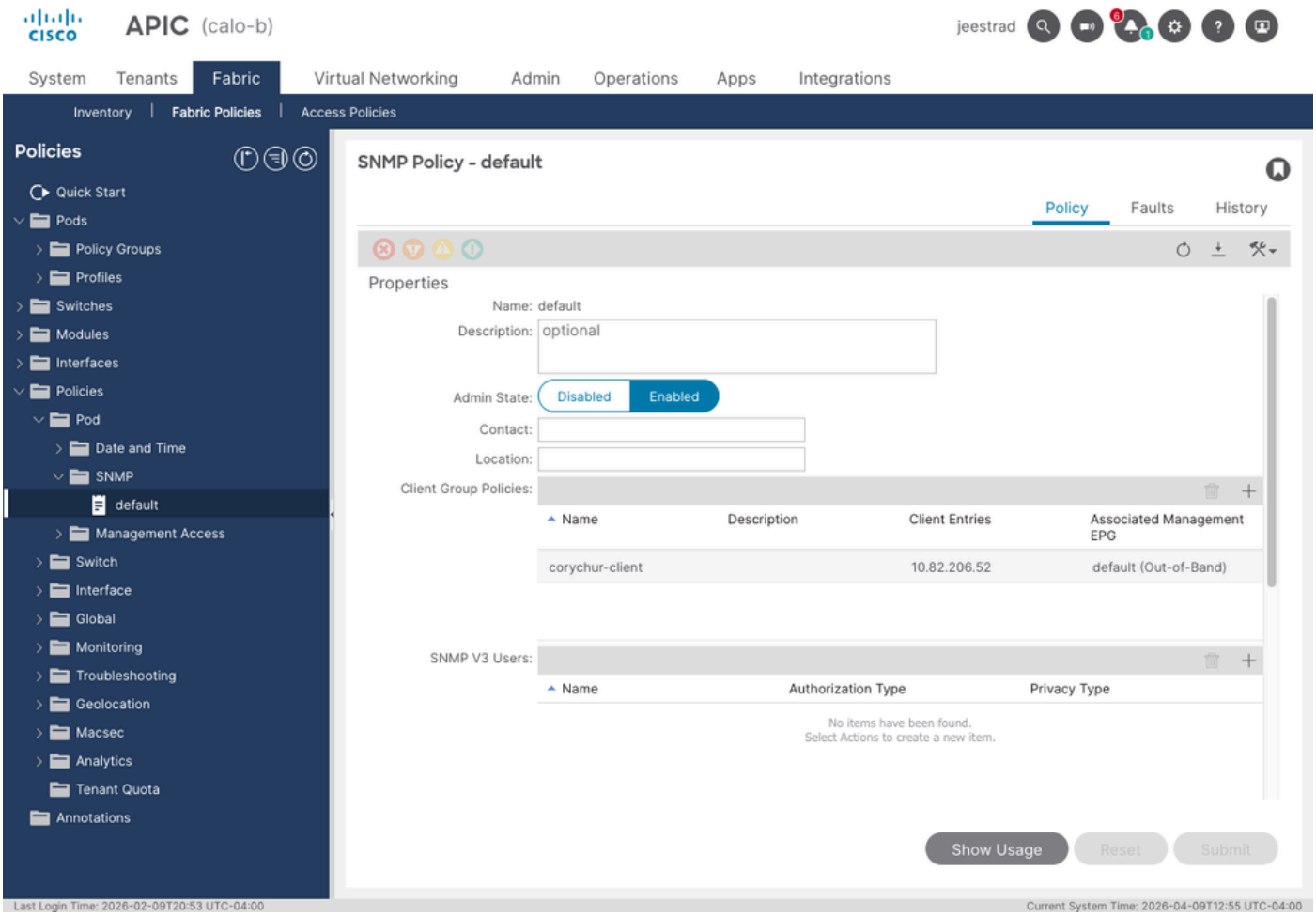
---

### Paso 1: Configuración de la política SNMP

Vaya a Fabric > Fabric Policies > Policies > Pod > SNMP. Seleccione (o cree) la política SNMP, normalmente denominada default. Configure

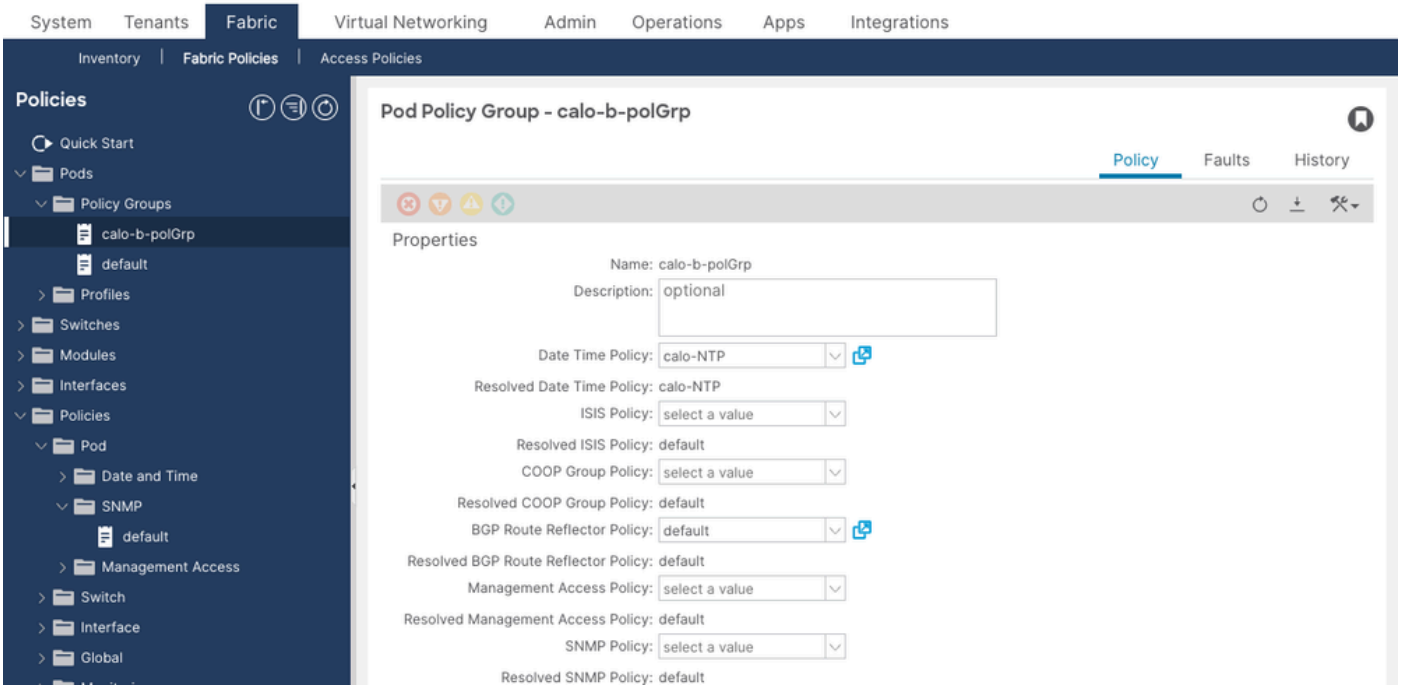
- Estado de administración: establecido en Activado.
- Directivas de comunidad: agregue la cadena de comunidad utilizada por el NMS.
- Políticas de grupo de clientes: defina uno o más perfiles de grupo de clientes, cada uno especificando las IP de cliente SNMP permitidas y el EPG de administración asociado (fuera de banda o en banda).

- Usuarios de SNMPv3: si utiliza SNMPv3, agregue aquí los usuarios con parámetros de autenticación y privacidad.




## Paso 2: Asociar la política SNMP al grupo de políticas de grupo

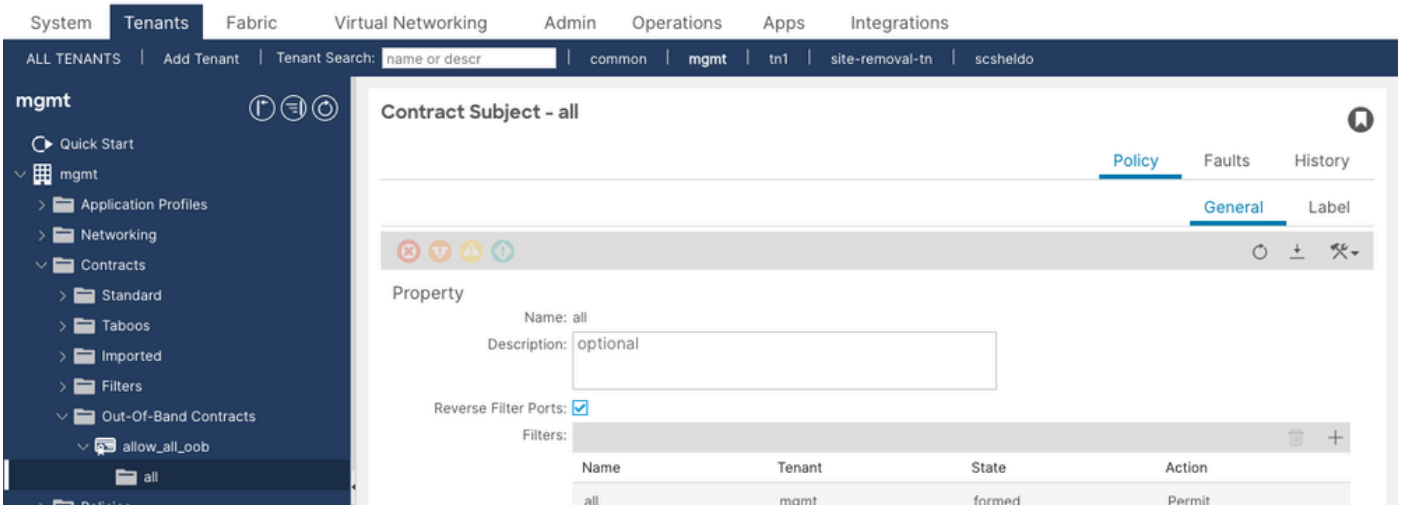
Vaya a Fabric > Fabric Policies > Pods > Policy Groups. Seleccione el grupo de políticas de grupo de dispositivos activo (normalmente denominado predeterminado). Establezca el campo SNMP Policy para que apunte a la política SNMP creada en el Paso 1. Verifique que el campo Resolved SNMP Policy muestra el nombre de política correcto.




A continuación, navegue hasta Fabric > Fabric Policies > Pods > Profiles, expanda el Pod Profile predeterminado y confirme que el selector activo hace referencia al Pod Policy Group correcto.

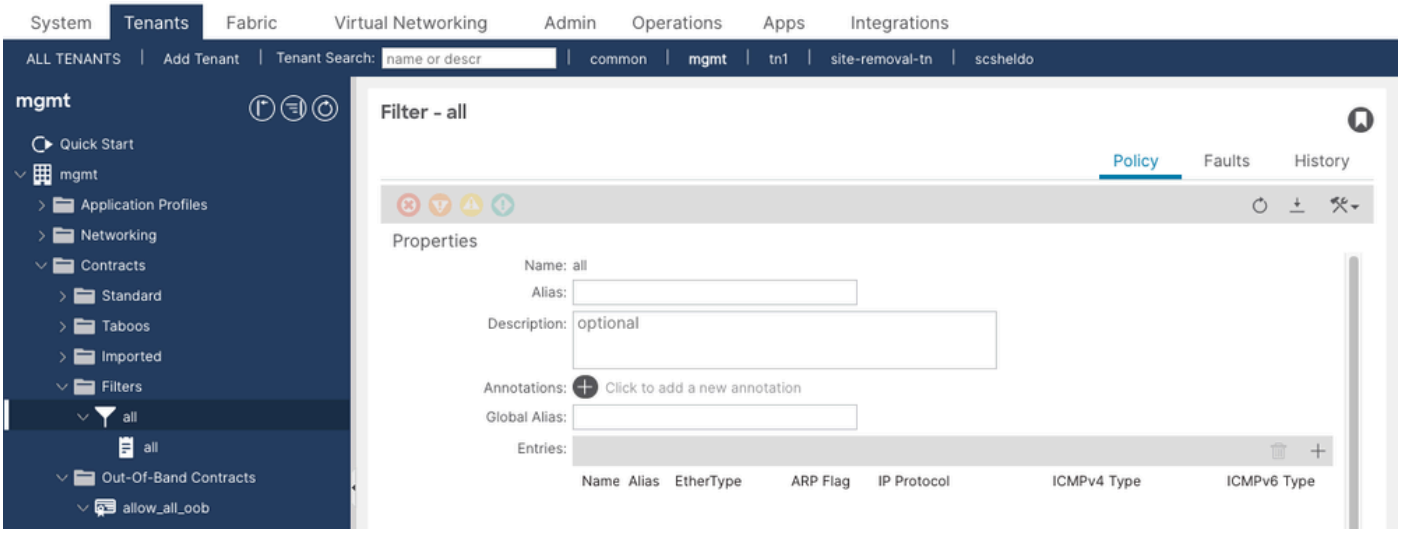
## Paso 3: Configuración de contratos de gestión para el puerto UDP 161

Navegue hasta Arrendatarios > Administración > Contratos > Contratos fuera de banda. Verifique que el Asunto del contrato OOB activo haga referencia a una entrada de filtro que permita el puerto UDP 161 (solicitudes SNMP). Sin este contrato en el APIC, todos los paquetes GET/WALK de SNMP se descartarán silenciosamente.




Las entradas de filtro asociadas al asunto del contrato deben incluir una entrada con EtherType IP, Protocol UDP y Destination Port 161. El ejemplo anterior muestra un filtro de permitir todo (protocolo no especificado): esto permite SNMP pero es más amplio de lo recomendado para

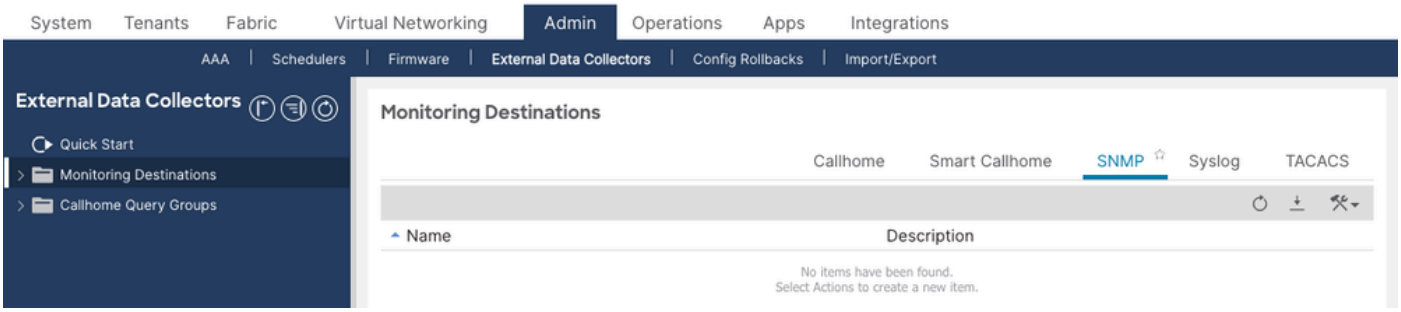
producción. Se prefiere una entrada de filtro SNMP dedicada con entradas UDP/161 y UDP/162 específicas.




Nota: En las versiones de firmware de ACI anteriores, determinados puertos estaban siempre abiertos en los nodos de columna y de hojas y no se requería un contrato de administración para SNMP. En ACI 5.x, el contrato es obligatorio para los nodos APIC. Los nodos de columna y de hojas utilizan reglas iptables derivadas de las directivas de grupo de clientes en lugar de contratos de administración.

## Paso 4: Configuración de Destinos de Trampas SNMP

Vaya a Admin > External Data Collectors > Monitoring Destinations > SNMP. Haga clic con el botón derecho y seleccione Crear grupo de destino de monitoreo SNMP. La ficha SNMP muestra todos los grupos de destino configurados. Una tabla vacía significa que aún no se han configurado destinos de trampa.




Definir:

- Nombre de grupo
- Destinos de trampa: nombre de host/IP, puerto UDP (predeterminado 162), versión SNMP,

cadena de comunidad y EPG de administración

### Paso 5: Configurar orígenes de supervisión

Los orígenes de supervisión vinculan el grupo de destino SNMP a las directivas de supervisión que controlan qué eventos y errores generan las capturas. Debe configurar un origen de monitoreo en las tres ubicaciones siguientes, o no se enviarán trampas de algunos tipos de nodo:

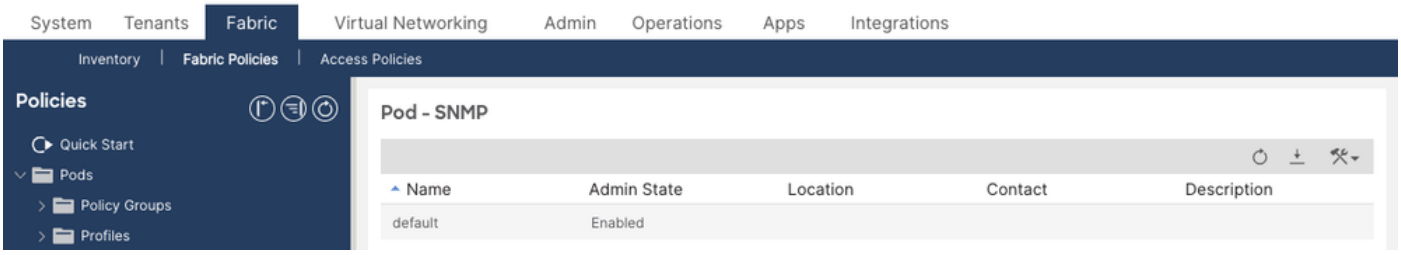
- Fabric > Fabric Policies > Policies > Monitoring > default > Callhome/Smart Callhome/SNMP/Syslog/TACACS (cubre eventos de infraestructura de fabric)
- Fabric > Fabric Policies > Policies > Monitoring > Common Policy > Callhome/Smart Callhome/SNMP/Syslog/TACACS (cubre los eventos comunes de todo el fabric)
- Fabric > Access Policies > Policies > Monitoring > default > Callhome/Smart Callhome/SNMP/Syslog (cubre eventos de acceso/infraestructura)

En cada ubicación, seleccione SNMP como tipo de origen y cree un nuevo origen SNMP que haga referencia al grupo de destino creado en el paso 4.

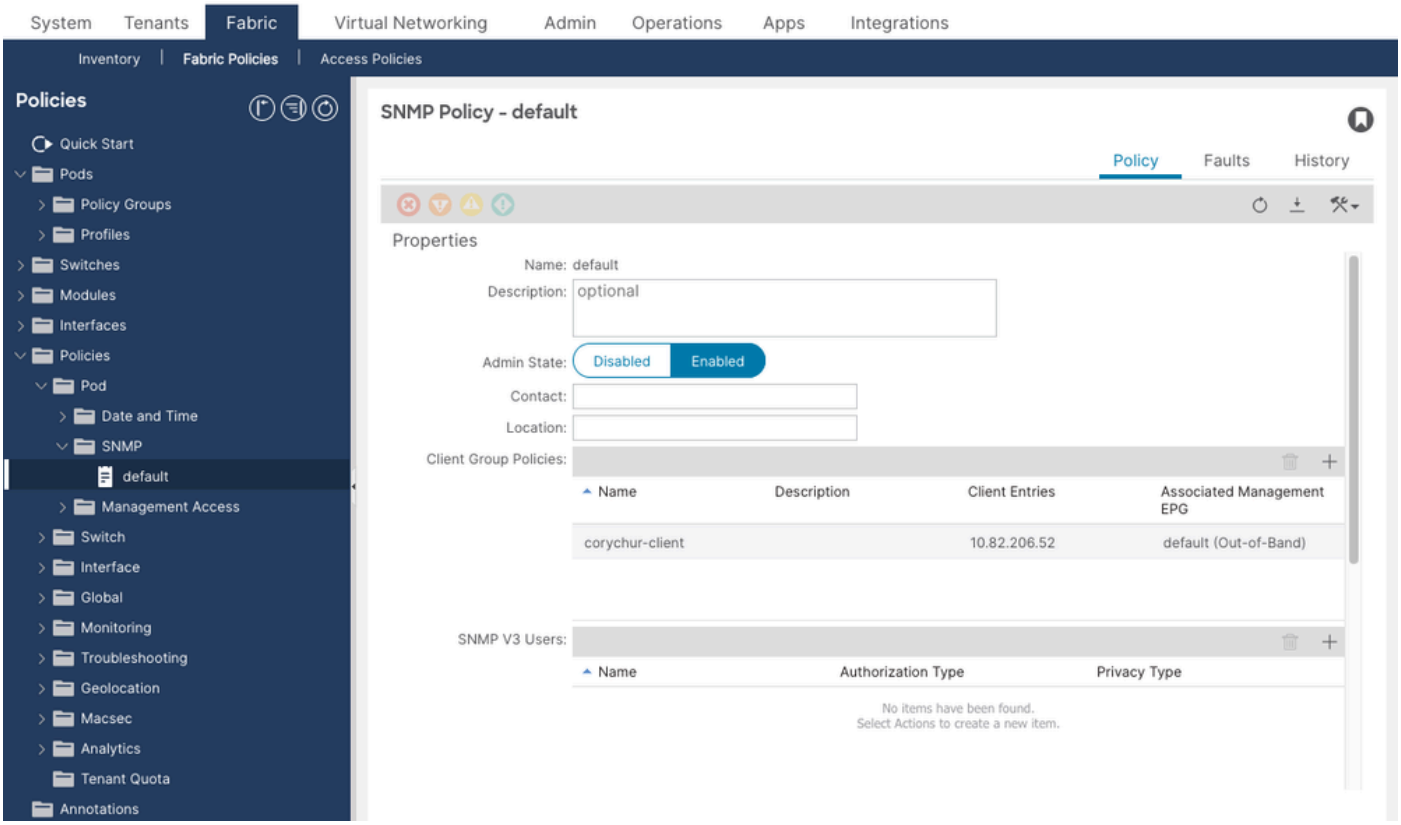
## Verifique la configuración

### Verificar la implementación de políticas SNMP

Navegue hasta Fabric > Fabric Policies > Policies > Pod > SNMP y confirme que la política predeterminada SNMP existe y que su estado de administración está configurado en Enabled. La lista Grupos de políticas muestra todas las políticas SNMP configuradas con su estado de administración de un vistazo.




Para una verificación detallada, haga clic en el nombre de la directiva para abrirla. Confirme que la alternancia de estado de administración esté configurada como Habilitada, y que las Políticas de grupo de clientes enumeren todos los hosts NMS permitidos con su EPG de administración asociado.




Ejecute la siguiente consulta MO en cualquier APIC para confirmar que la política SNMP está presente y habilitada en el fabric:

<#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
```

Si `adminSet` está `inhabilitado`, SNMP no funcionará en ningún nodo. Actívela en la GUI de APIC en Fabric > Fabric Policies > Pod > SNMP > default.

## Verificar configuración de cadena de comunidad

<#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
```

Si no se devuelve ninguna comunidad, o el nombre no coincide con lo que el NMS está utilizando, agregue o corrija la cadena de comunidad bajo la política SNMP.

## Comprobar las directivas de grupo de clientes (control de acceso SNMP)

Las políticas de grupo de clientes funcionan como una ACL para el acceso SNMP GET/WALK. Cada política especifica qué direcciones IP de cliente están autorizadas para sondear los nodos de columna/hoja sobre qué VRF de administración. En los nodos de columna/hoja, estas políticas se traducen en reglas iptables.

<#root>

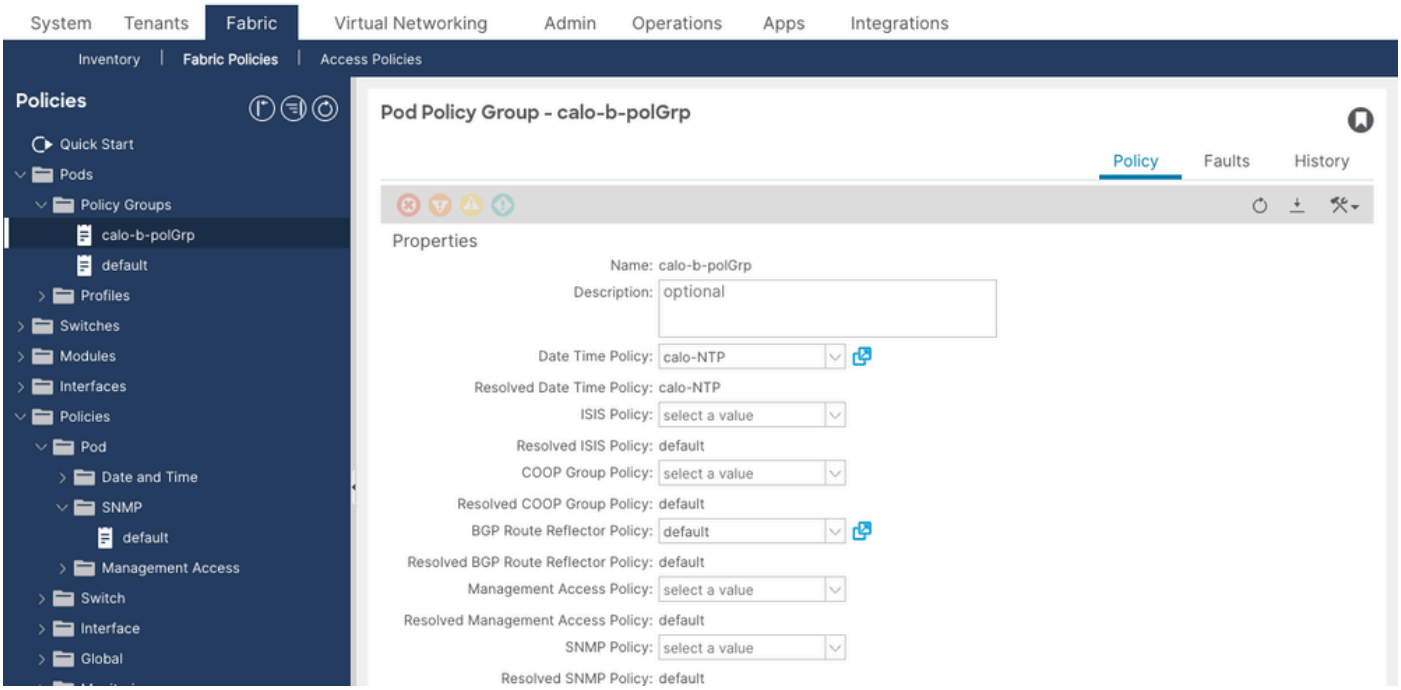
```
apic1#

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 que la IP del servidor NMS está presente en las entradas del cliente. Si falta una IP de cliente, las solicitudes GET/WALK SNMP de ese host serán descartadas por iptables en los nodos de columna/hoja.

Nota: Advertencia de SNMPv3: las políticas de grupo de clientes no se aplican en el APIC cuando se utiliza SNMPv3. Se permite cualquier GET/WALK SNMPv3 a un APIC independientemente de la configuración del grupo de clientes. La aplicación de grupos de clientes para SNMPv3 en el APIC es una limitación conocida. En los switches de columna y de hoja, la aplicación de grupos de clientes se comporta de la misma manera para SNMPv2c y SNMPv3.

## Verificar que el Grupo de Políticas de Pod Hace Referencia a la Política SNMP

Navegue hasta Fabric > Fabric Policies > Pods > Policy Groups y abra el grupo de políticas de POD activo. Confirme que el campo desplegable SNMP Policy esté configurado en la política SNMP deseada y que el campo Resolved SNMP Policy muestre el mismo nombre. Una política que falta o no se resuelve significa que la configuración SNMP nunca se envía a los switches.




En la captura de pantalla anterior, el campo Política SNMP muestra "select a value" (seleccionar un valor) (vacío) mientras que la Política SNMP resuelta muestra "default" (predeterminado), esto significa que la política se hereda del fabric predeterminado pero no se establece explícitamente. Se recomienda establecer explícitamente el campo Política SNMP para evitar ambigüedades.

Verificar a través de la API REST:

<#root>

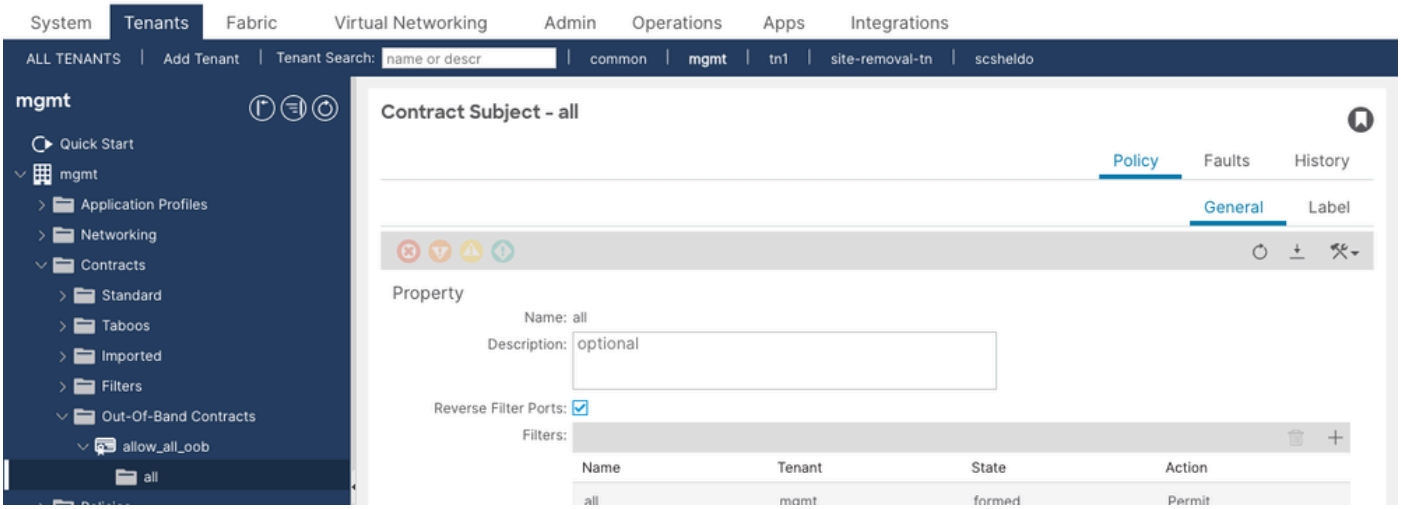
```
apic1#

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"
```

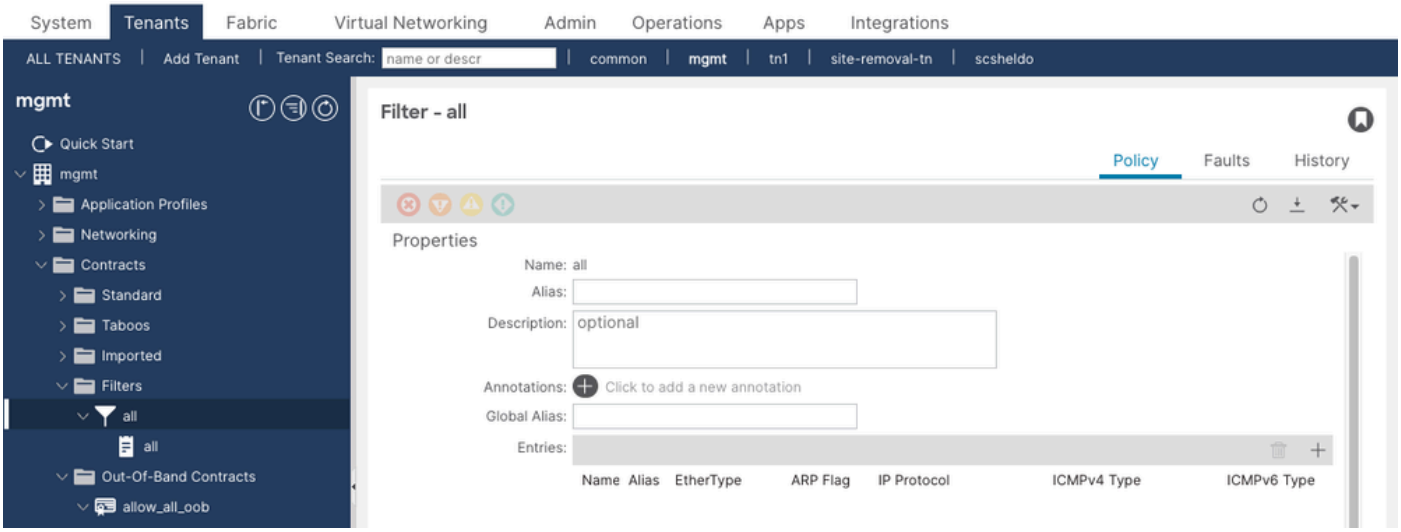
Si `state` no se `forma`, la relación de política SNMP se rompe. Vuelva a seleccionar la política SNMP en el grupo de políticas de grupo y realice el envío.

## Verificar contrato de gestión para UDP 161 (nodos APIC)

Vaya a Arrendatarios > Gestión > Contratos > Contratos fuera de banda (y Contratos en banda si utiliza la gestión INB). Abra el contrato OOB activo y haga clic en la pestaña Política. Verifique que el Asunto haga referencia a un filtro que permite el puerto UDP 161.




Expanda el filtro al que hace referencia el asunto y confirme que sus entradas incluyen una entrada con EtherType IP, Protocol UDP, Destination Port 161. Las entradas del filtro determinan qué tráfico se permite a través del contrato de administración OOB al APIC.




El filtro debe mostrar:

- EtherType: IP
- Protocolo IP: UDP
- Puerto de destino desde: 161
- Puerto de destino para: 161

También verifique que el puerto UDP 162 esté permitido si desea que el APIC envíe trampas SNMP salientes a través de la interfaz OOB.

Comprobación mediante consulta MO:

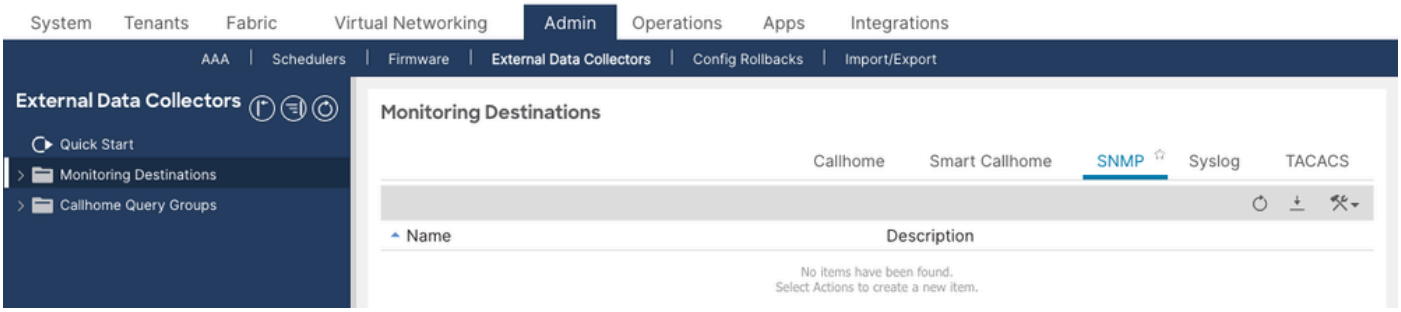
<#root>

```
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
```

Si no se devuelven resultados, no existe ningún filtro para UDP 161. Añada uno al contrato de gestión.

## Verificar la Configuración de Destino de Trampa SNMP

Navegue hasta Admin > External Data Collectors > Monitoring Destinations > SNMP para ver todos los grupos de destino SNMP configurados. Una lista vacía significa que no se configuran destinos de trampa y que no se enviarán trampas desde ningún 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
```

Confirme que la IP de destino de trampa, el puerto, la versión, la cadena de comunidad y la administración VRF (ya sea `mgmt:inb` o `management` para OOB) coincidan con su entorno. El VRF debe coincidir con el EPG de gestión asignado al destino.

## Comprobar que los orígenes de supervisión están configurados en los tres ámbitos

Los orígenes SNMP deben existir en los tres ámbitos de la directiva de supervisión. Si falta un origen en cualquier ámbito, las capturas de eventos relacionados no se reenviarán.

<#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
```

Si falta alguno de los tres, cree el origen SNMP que falta en la política de monitoreo correspondiente usando la GUI.

# Verificación operativa

## Verifique el estado de SNMP mediante show snmp summary (APIC)

Ejecute este comando directamente en cada APIC para confirmar que el agente SNMP se está ejecutando y que se ha aplicado la configuración:

**<#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
```

Qué comprobar en el resultado:

- El estado de administración debe estar `habilitado`.
- La comunidad debe coincidir con lo que el NMS está configurado para utilizar.
- Client-Group debe enumerar todas las IP de NMS permitidas con el EPG de administración correcto.
- El host (destino de trampa) debe enumerar el receptor de trampa NMS con el puerto y la versión correctos.

## Verifique el estado de SNMP mediante 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
```

Qué comprobar en el resultado:

- El estado de administración debe estar `habilitado y ejecutarse` con un pid. Si muestra `disabled`, la política SNMP no se aplica o la cadena de políticas de grupo se rompe.
- El estado de la comunidad debe ser `correcto`. Un estado de `error` indica un problema de implementación de políticas.
- El cliente VRF para cada host NMS debe coincidir con el VRF del EPG de administración (`mgmt:inb` para la banda interna, `management` para OOB).
- El Host de Trampa debe enumerar el destino con el contexto VRF correcto.

## Verifique que el proceso snmpd se esté ejecutando

En una hoja o columna:

```
<#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
```

En el 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
```

Si no se encuentra ningún proceso snmpd en una hoja o columna, SNMP no se está ejecutando en ese nodo. Verifique que el estado de administración de la política SNMP esté habilitado y que la cadena de políticas del grupo de dispositivos esté configurada correctamente.

Deflector (Destaque para leer)

## Verifique que el puerto SNMP esté escuchando

<#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           :::*
```

Si el puerto 161 no aparece en el estado LISTEN, el proceso snmpd no se está ejecutando o no se ha podido enlazar al puerto.

## Verificar reglas iptables en hoja/columna

Las políticas de grupo de clientes se traducen en reglas iptables en cada hoja y columna. Utilice lo siguiente para inspeccionar las reglas:

<#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 los ID de VRF correctos para el fabric, ejecute:

<#root>

```
leaf101#
```

**show vrf**

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

Los ID de VRF en las reglas iptables deben coincidir con lo que indica `show vrf`. Si una IP de cliente está ausente de las reglas iptables, las solicitudes SNMP de ese host se descartarán silenciosamente incluso si el proceso snmpd se está ejecutando.

Utilice los contadores para verificar si algún paquete SNMP ha sido encontrado o 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
```

---

Nota: Si SNMP se está ejecutando pero iptables no muestra cadenas snmp_rules, o las cadenas están vacías, puede reiniciar el proceso snmpd para forzar la reprogramación de reglas iptables. El envío de SIGKILL al PID de snmpd es seguro: el administrador de procesos de ACI (`controlado`) lo reiniciará automáticamente. Ejecute `pidof snmpd` para obtener el PID, luego `kill -9 [snmpd_pid]`. Confirme el nuevo PID con `pidof snmpd` después de 10-15 segundos.

---

Verify SNMP Port Is Listening 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 <— El agente SNMP está aceptando solicitudes udp 0 0 0.0.0.0:161 0.0.0.0:* udp6 0 0 :::161 ::* Si el puerto 161 no aparece en el estado LISTEN, el proceso snmpd no se está ejecutando o no se ha podido enlazar al puerto. Verificar que las Reglas iptables en las Políticas de Grupo de Clientes de Hoja/Columna se traduzcan en reglas iptables en cada hoja y columna. Utilice lo siguiente para inspeccionar las reglas: 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 <— El puerto SNMP 161 redirige a la cadena snmp_rules -A snmp_rules -m vrf —vrf 2 -j vrf_2_snmp_rules <— VRF 2 = administración OOB -A snmp_rules -m vrf —vrf 9 -j vrf_9_snmp_rules <— VRF 9 = Administración en banda -A snmp_rules -j DROP <— default drop; sólo los clientes permitidos pasan -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 los ID de VRF correctos para su fabric, ejecute: leaf101# show vrf VRF-Name VRF-ID State Reason management 2 Up — mgmt:inb 9 Up — Los ID de VRF en las reglas iptables deben coincidir con lo que muestra los informes vrf. Si una IP de cliente está ausente de las reglas iptables, las solicitudes SNMP de ese host se descartarán silenciosamente incluso si el proceso snmpd se está ejecutando. Utilice los contadores para verificar si algún paquete SNMP ha sido encontrado o descartado: leaf101# iptables -nvL | grep -A 20 "Chain snmp_rules" Chain snmp_rules (1 references) pkts bytes target port opt in out source destination 1 73 vrf_9_snmp_rules all — * 0.0.0.0/0 0.0.0.0/0 vrf 9 0 0 DROP all — * 0.0.0.0/0 0.0.0.0/0 <— if pkts>0 here, client IP are missing Nota: Si SNMP se está ejecutando pero iptables no muestra cadenas snmp_rules, o las cadenas están vacías, puede reiniciar el proceso snmpd para forzar la reprogramación de reglas iptables. El envío de SIGKILL a la PID de snmpd es seguro: el

administrador de procesos de ACI (controlado) lo reiniciará automáticamente. Ejecute pidof snmpd para obtener el PID y, a continuación, kill -9 [snmpd_pid]. Confirme el nuevo PID con pidof snmpd después de 10-15 segundos.

## Verifique la conectividad de red a los puertos 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 que las interfaces de administración estén activas (sin incrementos de RX-ERR) y que pasen tráfico. `eth0` es la interfaz de administración OOB; `kpm_inb` es la interfaz de administración en banda del switch.

## Verifique el envío de trampas SNMP con tcpdump

Para confirmar que se están generando y enviando capturas desde un nodo de columna o de hoja, capture el tráfico en la interfaz apropiada. Acceda al nodo como admin y utilice:

<#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**

Deflector (Destaque para leer)

Para trampas 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: En el APIC, `bond0.1100` es la subinterfaz VLAN de la interfaz de administración en banda. Reemplace `1100` con la encapsulación VLAN configurada para su EPG de administración en banda. Utilice `oobmgmt` como nombre de interfaz para las capturas OOB en el APIC.

---

Para trampas 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=pública 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: En el APIC, bond0.1100 es la subinterfaz VLAN de la interfaz de administración en banda. Reemplace 1100 con la encapsulación VLAN configurada para su EPG de administración en banda. Utilice oobmgmt como nombre de interfaz para las capturas OOB en el APIC.

## Verificar solicitudes 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
```

Si ve GetRequest pero no GetResponse, la solicitud se recibe pero no se contesta. Verifique el proceso snmpd y la cadena de comunidad. Si no ve ni solicitud ni respuesta, la solicitud se está bloqueando antes de llegar al nodo (verifique ruteo e iptables).

# Troubleshooting de Flujo

## Árbol de decisión de selección

Utilice este árbol de decisiones cuando los ingenieros informen de que SNMP no funciona. Partir del síntoma observado y seguir las ramas hasta el aislamiento.

Síntoma: No hay respuesta a las solicitudes GET/WALK de SNMP

1. Verifique el estado de administración de SNMP en APIC. Ejecute `moquery -c snmpPol`. Si `adminSet` está `inhabilitado`, actívelo y vaya al paso 7.
2. Verifique el proceso snmpd. En el nodo afectado, ejecute `ps aux | grep snmp` o `pidof snmpd`. Si no se está ejecutando ningún proceso, la política SNMP no se implementa. Verifique la cadena de políticas de grupo de dispositivos (Política SNMP → Grupo de políticas de grupo → Perfil de grupo de dispositivos).
3. Verifique que el puerto 161 esté escuchando. Ejecute `netstat -lutn | grep 161`. Si el puerto 161 no está en estado LISTEN, el proceso snmpd ha fallado; recopile los registros de `/var/log/dme/log/svc_ifc_dbgrelem.log*` y reinicie el proceso.
4. Verifique el ruteo. Ejecute `show ip route vrf management` y `show ip route vrf mgmt:inb`. Confirme que existe una ruta al host NMS en el VRF correcto.
5. Compruebe el contrato de gestión en APIC. Si el destino es un APIC (no una hoja/columna), verifique que UDP 161 esté permitido en el contrato de administración OOB o INB.
6. Realice tcpdump en el nodo. Ejecute `tcpdump -i kpm_inb -f port 161 -vv` (o `eth0` para OOB). Si aparece GetRequest pero no aparece GetResponse a continuación, la solicitud llega al nodo pero snmpd no responde; compruebe la cadena de comunidad. Si no aparece ninguna solicitud, el problema es ascendente (routing o contrato).
7. Pruebe desde un cliente permitido. Ejecute `snmpget -v2c -c [community] [node-ip] SNMPv2-MIB::sysDescr.0` desde un host NMS enumerado en el grupo de clientes. Una respuesta satisfactoria confirma que SNMP está completamente operativo.

Síntoma: No se recibieron trampas SNMP en el NMS

1. Verifique la configuración de destino de trampa. Ejecute `moquery -c snmpTrapDest`. Confirme que la IP, el puerto, la versión y la comunidad de NMS coincidan con los valores esperados de NMS.
2. Comprobar que los orígenes de supervisión existen en los tres ámbitos. Ejecute `moquery -c snmpSrc | egrep`

"snmp.Src|name|dn". Confirme que existen entradas con los valores monPolDn para uni/fabric/monfab-default, uni/fabric/moncommon y uni/infra/moninfra-default. Si falta alguno, agregue el origen SNMP en la directiva de supervisión correspondiente.
3. Verifique el proceso snmpd. Verifique que snmpd se esté ejecutando en el nodo que debe enviar la trampa.
4. Genere un evento de prueba y capture con tcpdump. Inmovilizar una interfaz o cambiar un estado para generar un evento. En el nodo, ejecute tcpdump -i kpm_inb -f port 162 -vv. Si no aparece tráfico de trampa en el cable, el evento no está generando una trampa — vuelva a verificar el origen de monitoreo incl atributo (debe incluir fallas o eventos).
5. Verifique la conectividad con el receptor de trampas. Confirme que el receptor de trampas es alcanzable desde el VRF de administración: show ip route vrf mgmt:inb debe mostrar una trayectoria al host NMS.
6. Si las trampas aparecen en tcpdump pero no en NMS, el problema es del lado de la red: firewall, routing o la configuración de NMS. Verifique que el NMS esté escuchando en UDP 162 desde la IP de origen de administración del nodo ACI.

# Escenarios de ejemplo

## Escenario 1: Política SNMP habilitada pero no se han devuelto datos desde la hoja/columna

Problema: La política SNMP del APIC muestra el estado de administración habilitado. El NMS puede alcanzar la IP de administración de la hoja. snmpget agota el tiempo de espera sin respuesta.

Comprobación de configuración: Verifique que el grupo de políticas de grupo de dispositivos hace referencia a la política SNMP y que la política SNMP resuelta muestra el nombre correcto. Si el campo de política SNMP del grupo de políticas de grupo de políticas de grupo de políticas de grupo está vacío o la relación no se ha formado, es posible que el proceso snmpd no se inicie en los switches.

Comprobación operativa: SSH a la hoja afectada y ejecute show snmp summary. Si el resultado muestra Admin State: inhabilitada aunque el APIC muestre enabled, la política no se ha implementado. Compruebe la cadena de políticas de grupo de dispositivos para ver si falta un grupo de políticas de grupo de dispositivos o si se hace referencia incorrectamente.

Causa raíz: La política SNMP no está vinculada al grupo de políticas de grupo o el selector de perfil de grupo no aplica el grupo de políticas de grupo correcto a este grupo.

Solución:

1. Vaya a Fabric > Fabric Policies > Pods > Policy Groups > default.
2. Confirme que el campo SNMP Policy apunte a la política SNMP habilitada.
3. Navegue hasta Fabric > Fabric Policies > Pods > Profiles y confirme que el selector activo hace referencia a este grupo de políticas de POD.
4. Después de guardar, vuelva a verificar `show snmp summary` en la hoja en 2 minutos.

## Escenario 2: SNMP GET/WALK funciona para algunos hosts NMS pero no para otros

Problema: Un servidor NMS puede sondear los nodos ACI correctamente. Un segundo servidor NMS en una subred diferente no obtiene respuesta.

Comprobación de configuración: Ejecute `moquery -c snmpClientGrpP -x query-target=children` en el APIC. Confirme que la IP del segundo servidor NMS aparece como una entrada de cliente. Si falta, esa IP será bloqueada por la regla DROP iptables en la parte inferior de la cadena snmp_rules.

Comprobación operativa: en la hoja afectada, confirme que UDP 161 está permitido en el contrato de administración OOB o INB. Si ningún contrato o filtro tiene puertos SNMP, la solicitud se descarta.

Causa raíz: La segunda dirección IP del servidor NMS no está en la directiva de grupo de clientes.

Solución: Agregue la IP de NMS que falta como una entrada de cliente en la política de grupo de clientes SNMP en Fabric > Fabric Policies > Policies > Pod > SNMP > default > Client Group Policies. Las reglas iptables en todos los nodos se actualizarán en minutos después de guardar la directiva.

## Escenario 3: Trampas SNMP no recibidas: las trampas se generan pero no se entregan

Problema: Los fallos son visibles en la tabla de fallos de APIC. `moquery -c snmpTrapDest` muestra la IP de NMS correcta. El NMS no recibe trampas.

Comprobación de configuración: Ejecute `moquery -c snmpSrc | egrep "snmp.Src|name|dn"`. Verifique que las fuentes de monitoreo existan en los tres ámbitos (`monfab-default`, `moncommon`, `moninfra-default`). Una omisión común es configurar el origen solo en la política Fabric Default, que omite los eventos de política de acceso.

Comprobación operativa: Desencadenar un evento de prueba (p. ej., cambiar una interfaz al estado de inactividad administrativa). En el nodo relevante, ejecute `tcpdump -i kpm_inb -f port 162`. Si aparecen paquetes de trampa en la interfaz del nodo, el lado de ACI está funcionando y el problema está en la trayectoria de red al NMS (firewall, ruteo). Si no aparece ninguna trampa en el cable, falta el origen de supervisión de ACI o el tipo de evento no se incluye en el atributo `incl` del origen.

Causa raíz 1: Faltan uno o más orígenes de supervisión en los ámbitos requeridos.

Causa raíz 2: El atributo `incl` de origen de supervisión excluye el tipo de evento que se genera (p. ej., `incl: eventos` sin `fallos` significa que no se enviarán trampas basadas en fallos).

Solución:

1. Agregue los orígenes de supervisión que faltan en la GUI para cada uno de los tres ámbitos (Fabric Default, Fabric Common y Access Default). Establezca el grupo de destino en el grupo de destino SNMP configurado.
2. Verifique que el atributo `incl` incluya `auditorías,eventos,fallas` para obtener una cobertura de trampa completa.
3. Después de los cambios, vuelva a activar el evento de prueba y vuelva a comprobar tcpdump.

Deflector (Destaque para leer)

---

Nota: En el APIC, el `comando tcpdump/code> sólo está disponible para el usuario root. Para APIC y switches, el comando iptables sólo está disponible para el usuario raíz.`

---

**Escenario 4: La aplicación del grupo de clientes SNMPv3 no funciona en APIC**

**Problema:** Un cliente SNMP que NO está en la directiva de grupo de clientes puede consultar correctamente el APIC mediante SNMPv3, aunque la misma consulta falle desde los nodos de columna/hoja.

**Causa raíz:** Esta es una **advertencia conocida**. Las políticas de grupo de clientes (aplicación de IP de origen basada en iptables) no se aplican para los GET/Walks to APIC de SNMPv3. Cualquier host puede consultar el APIC a través de SNMPv3 independientemente de la configuración del grupo de clientes. En los switches de columna y de hoja, la aplicación del grupo de clientes funciona de manera idéntica para SNMPv2c y SNMPv3.

**Mitigación:** Utilice filtros de contratos de administración en el APIC para restringir el acceso SNMP por subred de origen. Los grupos de clientes son efectivos para los nodos de columna/hoja. Para el APIC con SNMPv3, confíe en el filtrado basado en el origen del contrato de administración como mecanismo de control de acceso.

**Escenario 5: Consultas SNMP correctas pero los datos MIB están incompletos o obsoletos**

**Problema:** SNMP GET/WALK devuelve datos, pero ciertos MIB OID devuelven valores vacíos o obsoletos. En particular, las estadísticas de interfaz o los datos de estado operativo no reflejan el estado de fabric actual.

**Comprobación operativa:** Confirme qué APIC se está consultando. Cada APIC sólo devuelve objetos MIB para los datos locales. Ejecute show snmp summary en el APIC consultado y compare el resultado con lo que espera. Para los datos de nivel de switch (IF-MIB, entityMIB), consulte el switch directamente, no el APIC.

**Causa raíz:** Consulta de un APIC para obtener datos MIB de nivel de hoja. Cada APIC proporciona objetos MIB sólo para sus propios objetos administrados. Los datos de nivel de switch (estadísticas de interfaz, CPU, memoria, sensores de entorno) se deben recuperar consultando directamente cada hoja y columna.

**Solución:** Configure el NMS para sondear las IP de administración de columna y hojas directamente para los datos MIB de interfaz y hardware. Utilice IP de gestión de APIC solo para MIB nativas de APIC (entidad, FRU, proceso, sensor relacionado con el hardware del servidor de APIC).

### Escenario 6: SNMP funciona en la columna/hoja pero no en el APIC

**Problema:** SNMPv2c GET de NMS a los nodos de columna y hoja se realiza correctamente. El mismo NMS no puede sondear el APIC.

**Comprobación de configuración:** APIC SNMP requiere un contrato de administración explícito que permita UDP 161. Navegue hasta **Arrendatarios > admin** y verifique el contrato OOB/INB y su filtro para UDP 161.

**Comprobación operativa:** En el APIC, ejecute iptables -S | grep 161. Si no aparecen reglas ACCEPT para UDP 161 en la cadena fp-137 (o contrato OOB equivalente), falta el filtro de contrato para UDP 161 o no está implementado.

<#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

Si estas reglas están ausentes, agregue una entrada de filtro para UDP 161 al asunto del contrato de administración y vuelva a verificar.

**Causa raíz:** Falta el contrato de gestión o está mal configurado. En ACI 5.x, los nodos APIC aplican estrictamente el contrato de administración: los paquetes SNMP se descartan a menos que exista un permiso explícito.

**Solución:**

1. Navegue hasta **Arrendatarios > Administración > Políticas de seguridad > Contratos fuera de banda**.
2. Expanda el contrato OOB, seleccione el Asunto y verifique/agregue un filtro para el **puerto UDP 161**.
3. Repita este procedimiento para el contrato en banda si el NMS está llegando al APIC a través de la administración INB.
4. Verificar con iptables -S | grep 161 en el APIC después de guardar.

### Escenario 7: Las reglas iptables de SNMP están ausentes o son incorrectas

**Problema:** show snmp summary muestra que la política SNMP se aplica pero iptables -S | grep snmp devuelve no rules, o la IP del cliente NMS está ausente de las reglas.

**Comprobación operativa:** Confirme que snmpd se está ejecutando con pidof snmpd. Si snmpd se está ejecutando pero iptables no tiene reglas SNMP, el proceso se inició antes de que se implementara la directiva de grupo de clientes. Reinicie snmpd para forzar la reprogramación de reglas si el

número de reinicios es inferior 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**

El administrador de procesos de ACI reiniciará snmpd automáticamente. Después del reinicio, verifique:

<#root>

leaf101#

**iptables -S | grep -i snmp**

Ahora deben aparecer las cadenas snmp_rules y las reglas ACCEPT de cliente por VRF.

**Causa raíz**: el proceso snmpd se reinició o inició antes de que la directiva de grupo de clientes se implementara completamente en el nodo, dejando iptables sin las reglas de acceso SNMP.

Nota: En el APIC, el comando tcpdump/code> sólo está disponible para el usuario root. Para APIC y switches, el comando iptables sólo está disponible para el usuario raíz. Escenario 4: Problema de aplicación de grupo de clientes SNMPv3 que no funciona en APIC: Un cliente SNMP que NO está en la directiva de grupo de clientes puede consultar correctamente el APIC mediante SNMPv3, aunque la misma consulta falle desde los nodos de columna/hoja. Causa raíz: Esta es una advertencia conocida. Las políticas de grupo de clientes (aplicación de IP de origen basada en iptables) no se aplican para los GET/Walks to APIC de SNMPv3. Cualquier host puede consultar el APIC a través de SNMPv3 independientemente de la configuración del grupo de clientes. En los switches de columna y de hoja, la aplicación del grupo de clientes funciona de manera idéntica para SNMPv2c y SNMPv3. Mitigación: Utilice filtros de contratos de administración en el APIC para restringir el acceso SNMP por subred de origen. Los grupos de clientes son efectivos para los nodos de columna/hoja. Para el APIC con SNMPv3, confíe en el filtrado basado en el origen del contrato de administración como mecanismo de control de acceso. Escenario 5: Consultas SNMP correctas pero los datos MIB están incompletos o el problema es obsoleto: SNMP GET/WALK devuelve datos, pero ciertos MIB OID devuelven valores vacíos o obsoletos. En particular, las estadísticas de interfaz o los datos de estado operativo no reflejan el estado de fabric actual. Comprobación operativa: Confirme qué APIC se está consultando. Cada APIC sólo devuelve objetos MIB para los datos locales. Ejecute show snmp summary en el APIC consultado y compare el

resultado con lo que espera. Para los datos de nivel de switch (IF-MIB, entityMIB), consulte el switch directamente, no el APIC. Causa raíz: Consulta de un APIC para obtener datos MIB de nivel de hoja. Cada APIC proporciona objetos MIB sólo para sus propios objetos administrados. Los datos de nivel de switch (estadísticas de interfaz, CPU, memoria, sensores de entorno) se deben recuperar consultando directamente cada hoja y columna. Solución: Configure el NMS para sondear las IP de administración de columna y hojas directamente para los datos MIB de interfaz y hardware. Utilice IP de gestión de APIC solo para MIB nativas de APIC (entidad, FRU, proceso, sensor relacionado con el hardware del servidor de APIC).  Escenario 6: SNMP funciona en la columna/hoja pero no en el problema APIC: SNMPv2c GET de NMS a los nodos de columna y hoja se realiza correctamente. El mismo NMS no puede sondear el APIC. Comprobación de configuración: APIC SNMP requiere un contrato de administración explícito que permita UDP 161. Navegue hasta Arrendatarios > Gestión y verifique el contrato OOB/INB y su filtro para UDP 161. Comprobación operativa: En el APIC, ejecute iptables -S | grep 161. Si no aparecen reglas ACCEPT para UDP 161 en la cadena fp-137 (o contrato OOB equivalente), falta el filtro de contrato para UDP 161 o no está implementado. 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 subnet -A fp-137 -s 172.18.0.0/16 -p udp -m udp —dport 161 -j ACCEPT <— permit SNMP from INB management subnet Si estas reglas están ausentes, añada una entrada de filtro para UDP 161 al asunto del contrato de administración y vuelva a verificar. Causa raíz: Falta el contrato de gestión o está mal configurado. En ACI 5.x, los nodos APIC aplican estrictamente el contrato de administración: los paquetes SNMP se descartan a menos que exista un permiso explícito. Solución: Vaya a Arrendatarios > Gestión > Políticas de seguridad > Contratos fuera de banda. Expanda el contrato OOB, seleccione el Asunto y verifique/agregue un filtro para el puerto UDP 161. Repita este procedimiento para el contrato en banda si el NMS está alcanzando el APIC a través de la administración INB. Verificar con iptables -S | grep 161 en el APIC después de guardar.  Escenario 7: Las reglas iptables de SNMP están ausentes o tienen un problema incorrecto: show snmp summary muestra que la política SNMP se aplica pero iptables -S | grep snmp devuelve no rules, o la IP del cliente NMS está ausente de las reglas. Comprobación operativa: Confirme que snmpd se está ejecutando con pidof snmpd. Si snmpd se está ejecutando pero iptables no tiene reglas SNMP, el proceso se inició antes de que se implementara la directiva de grupo de clientes. Reinicie snmpd para forzar la reprogramación de reglas si el número de reinicios es inferior a 250: leaf101# pidof snmpd 5881leaf101# show system internal sysmgr service name snmpdService "snmpd" ("snmpd", 127):UUID = 0x1A, PID = 5881, SAP = 1545Estado: SRV_STATE_HANDSHAKED (introducido el lunes 25 de agosto a las 19:23:50 de 2025).Recuento de reinicio: 3Hora del último reinicio: Lun 25 de agosto 19:23:48 2025.PID anterior: 32080Motivo de la última rescisión: SYSMGR_DEATH_REASON_FAILURE_SIGNALTag = N/ID de complemento: 0 leaf101# kill -9 5881 El administrador de procesos de ACI reiniciará automáticamente snmpd. Después del reinicio, verifique: leaf101# iptables -S | grep -i snmp Ahora deben aparecer las cadenas snmp_rules y las reglas ACCEPT de cliente por VRF. Causa raíz: el proceso snmpd se reinició o inició antes de que la directiva de grupo de clientes se implementara completamente en el nodo, dejando iptables sin las reglas de acceso SNMP.

## Archivos de registro para solución de problemas ampliada

Cuando los pasos de verificación anteriores no resuelven el problema, los siguientes archivos de registro en los nodos de hoja, columna y APIC contienen información de diagnóstico relacionada con 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/*
```

Estos registros contienen eventos de reinicio snmpd, eventos de implementación de políticas y errores de configuración de comunidad/cliente que no son visibles a través de show snmp summary.

## Referencias

- Guía de configuración de administración del sistema Cisco APIC, versión 5.x – Administración de SNMP
- Guía de referencia rápida de Cisco ACI MIB

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).