Solución de problemas de administración de ACI y servicios principales: políticas de POD

Contenido

Introducción

Este documento describe los pasos para comprender y resolver problemas de las políticas de POD de ACI.

Antecedentes

El material de este documento se ha extraído de la Solución de problemas de Cisco Application Centric Infrastructure, segunda edición , concretamente los servicios de gestión y principales, **Políticas de POD: BGP RR/ Date&Time / SNMP** capítulo.

Descripción general de políticas Pod

Los servicios de administración como RR BGP, Fecha y hora y SNMP se aplican en el sistema mediante un grupo de políticas de grupo de dispositivos. Un grupo de políticas de grupo controla un grupo de políticas de grupo relacionadas con las funciones esenciales de un fabric de ACI. Estas políticas de grupo de dispositivos están relacionadas con los siguientes componentes, muchos de los cuales se aprovisionan de forma predeterminada en un fabric de ACI.

Políticas Pod

Política Pod	Requiere configuración manual
Fecha y hora	Yes
Reflector de ruta BGP	Yes
SNMP (protocolo de administración de redes de servidores)	Yes
ISIS	No
COOP	No

Acceso de administración	No
MAC Sec	Yes

Incluso en un único fabric ACI, es necesario configurar el grupo de políticas y el perfil de grupo de dispositivos. Esto no es específico de un Multi-Pod o incluso de una implementación Multi-Site. Este requisito se aplica a **todos los** tipos de implementación de ACI.

Este capítulo se centra en estas políticas de POD esenciales y en cómo comprobar que se aplican correctamente.

Política de fecha y hora

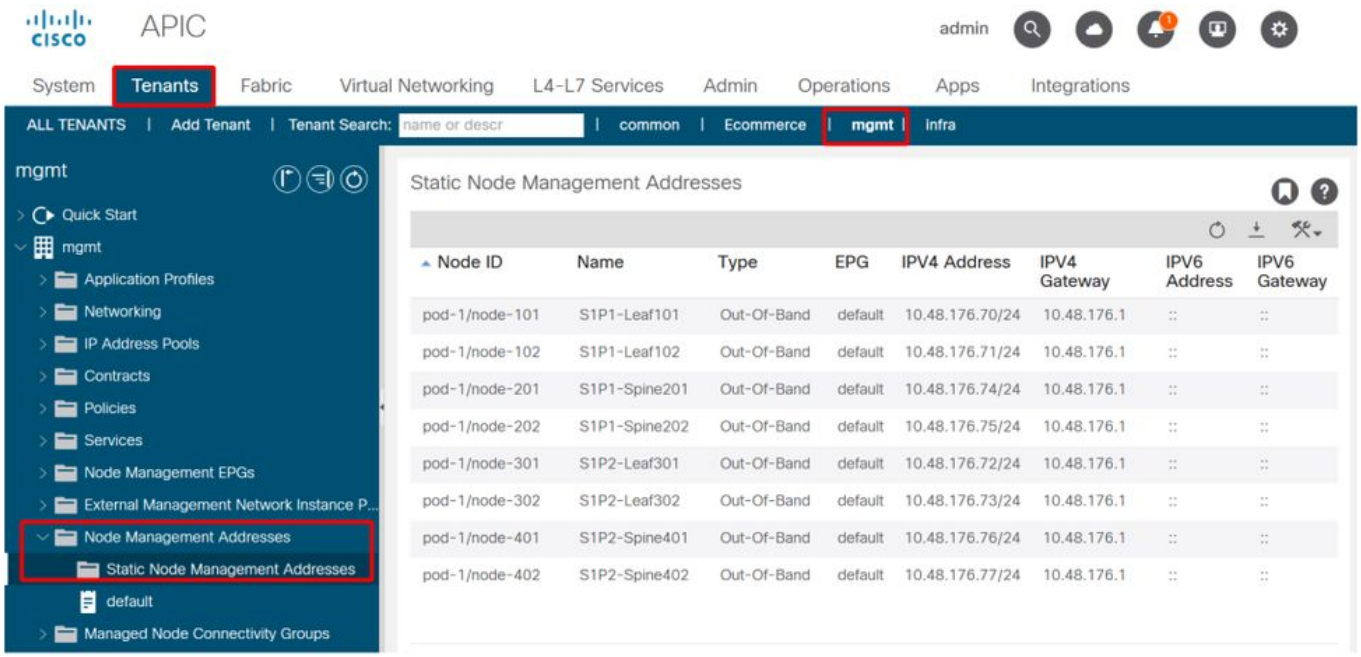
La sincronización horaria desempeña un papel fundamental en el fabric de ACI. Desde la validación de certificados hasta el mantenimiento uniforme de las marcas de tiempo de registro en APIC y switches, se recomienda sincronizar los nodos del fabric de ACI con una o varias fuentes de tiempo fiables mediante NTP.

Para que los nodos estén sincronizados correctamente con un proveedor de servidor NTP, existe una dependencia para asignar nodos con direcciones de administración. Esto se puede realizar en el arrendatario de administración mediante Direcciones de administración de nodos estáticos o Grupos de conectividad de nodos de administración.

Troubleshooting de Flujo

1. Compruebe si las direcciones de administración de nodos están asignadas a todos los nodos

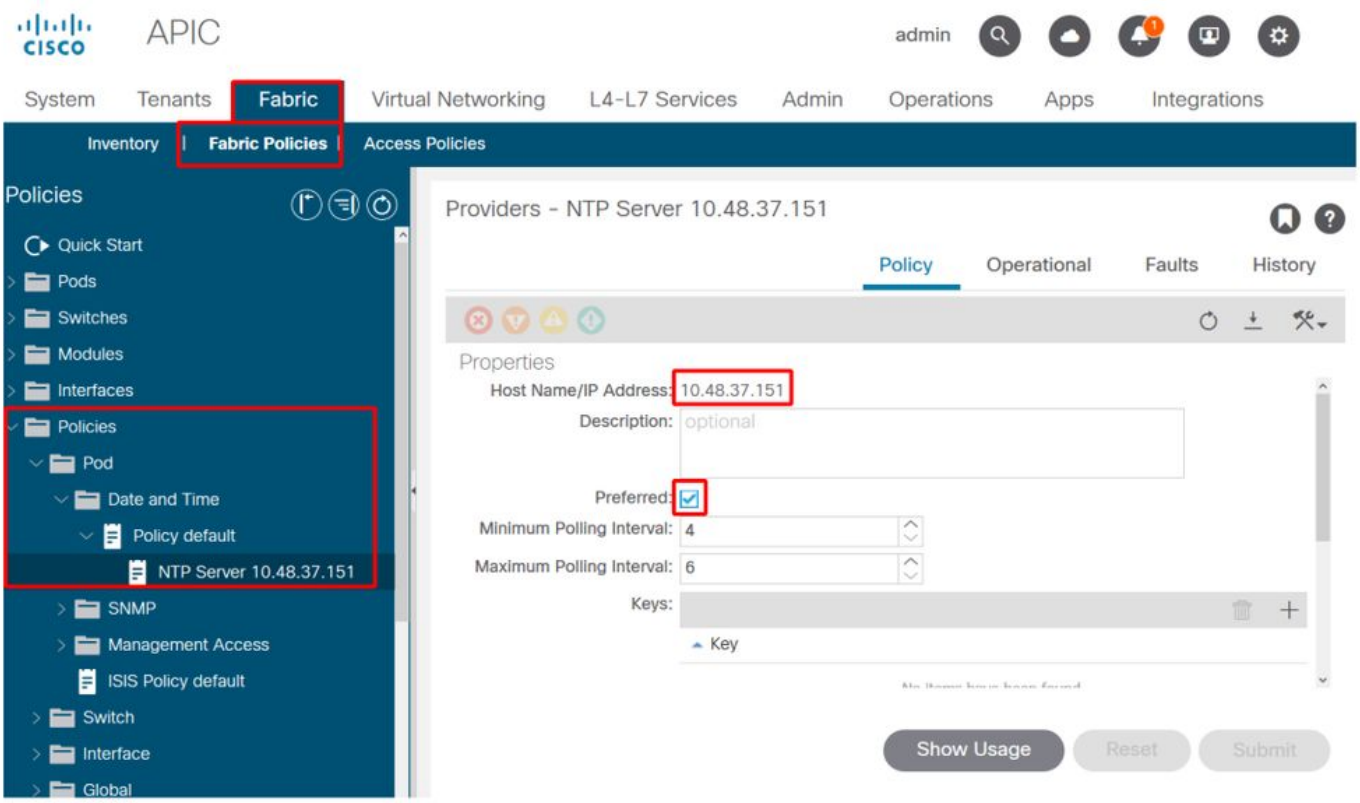
Arrendatario de administración: direcciones de administración de nodos



2. Compruebe si un servidor NTP se ha configurado como proveedor NTP

Si hay varios proveedores de NTP, marque al menos uno de ellos como la fuente de tiempo preferida usando la casilla de verificación 'Preferido' según la figura a continuación.

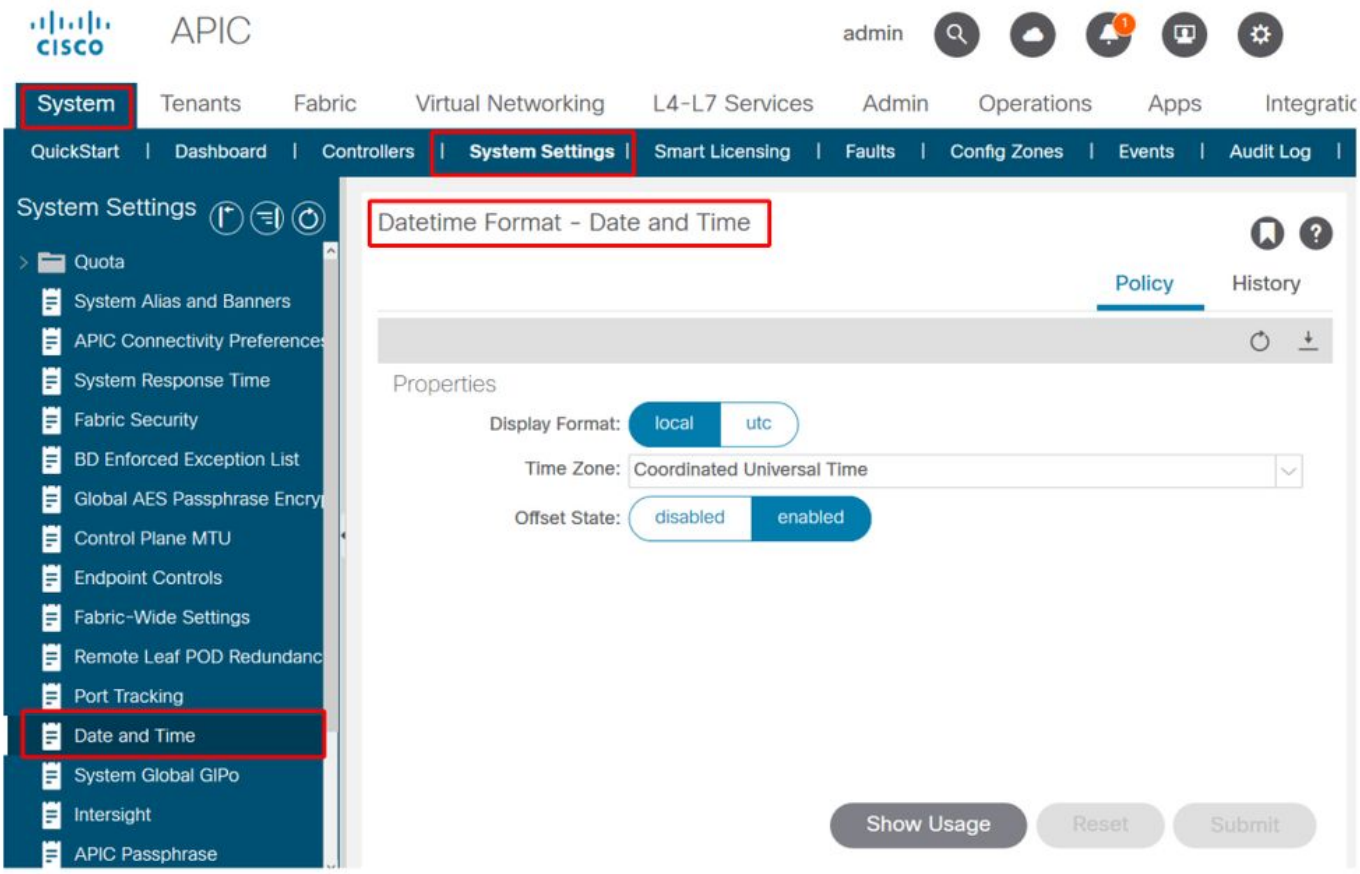
Proveedor/servidor NTP bajo Política de Pod de Fecha y Hora



3. Compruebe el formato de fecha y hora en Configuración del sistema

La siguiente figura muestra un ejemplo en el que el formato de fecha y hora se ha establecido en UTC.

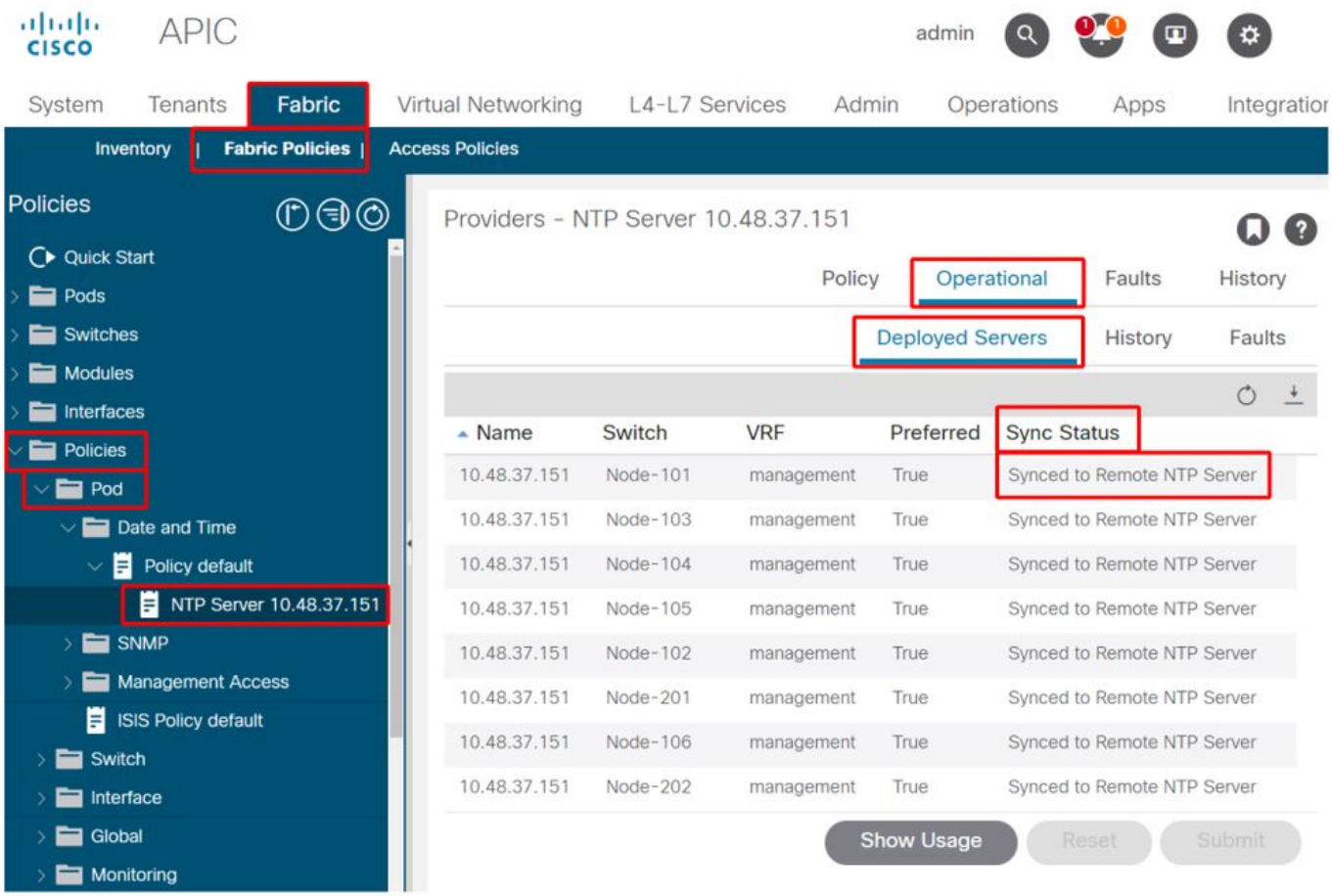
Configuración de fecha y hora en Configuración del sistema



4. Verifique el estado de sincronización operacional del proveedor NTP para todos los nodos

Como se muestra en la siguiente figura, la columna Estado de sincronización debe mostrar 'Sincronizado con servidor NTP remoto'. Tenga en cuenta que el estado de sincronización puede tardar varios minutos en converger correctamente con el servidor NTP .Synced remoto. estado.

Estado de sincronización del proveedor/servidor NTP



Alternativamente, los métodos CLI se pueden utilizar en los APIC y los switches para verificar la sincronización horaria correcta contra el servidor NTP.

APIC: NX-OS CLI

La columna 'refId' que aparece a continuación muestra el origen de la próxima vez de los servidores NTP en función del estrato.

```
apic1# show ntpq
nodeid     remote                          refid                      st        t   when
poll      reach     auth  delay     offset    jitter
------  -  ------------------------------  -------------------------  --------  --  --------  -
-------  --------  ----  --------  --------  --------
1       *  10.48.37.151                    192.168.1.115              2         u   25
64        377       none  0.214     -0.118    0.025
2       *  10.48.37.151                    192.168.1.115              2         u   62
64        377       none  0.207     -0.085    0.043
3       *  10.48.37.151                    192.168.1.115              2         u   43
64        377       none  0.109     -0.072    0.030
```

```
apic1# show clock
Time : 17:38:05.814 UTC Wed Oct 02 2019
```

APIC - Bash

```
apic1# bash
admin@apic1:~> date
Wed Oct  2 17:38:45 UTC 2019
```

Switch

Utilice el comando 'show ntp peers' para asegurarse de que la configuración del proveedor NTP se ha enviado correctamente al switch.

```
leaf1# show ntp peers
-------------------------------------------------------------------------------
   Peer IP Address                 Serv/Peer Prefer KeyId   Vrf
-------------------------------------------------------------------------------
   10.48.37.151                    Server    yes    None    management

leaf1# show ntp peer-status
Total peers : 1
* - selected for sync, + - peer mode(active),
- - peer mode(passive), = - polled in client mode
   remote                       local           st poll reach delay vrf
-------------------------------------------------------------------------------
*10.48.37.151                    0.0.0.0         2  64   377   0.000  management
```

El carácter '*' es esencial aquí, ya que controla si el servidor NTP se está utilizando realmente para la sincronización.

Verifique el número de paquetes enviados/recibidos en el siguiente comando para asegurarse de que los nodos ACI tengan disponibilidad para el servidor NTP.

```
leaf1# show ntp statistics peer ipaddr 10.48.37.151
...
packets sent:         256
packets received:     256
...
```

política BGP Route Reflector

Un fabric ACI utiliza BGP multiprotocolo (MP-BGP) y, más concretamente, VPNv4 iBGP entre nodos de columna y de hojas para intercambiar rutas de arrendatario recibidas de routers externos (conectados en L3Outs). Para evitar una topología de peer iBGP de malla completa, los nodos de columna reflejan los prefijos VPNv4 recibidos de una hoja a otros nodos de hoja del fabric.

Sin la política BGP Route Reflector (BGP RR), no se creará ninguna instancia de BGP en los switches y no se establecerán las sesiones BGP VPNv4. En una implementación de varios dispositivos, cada dispositivo requiere al menos un conmutador central configurado como RR BGP y, básicamente, más de uno para redundancia.

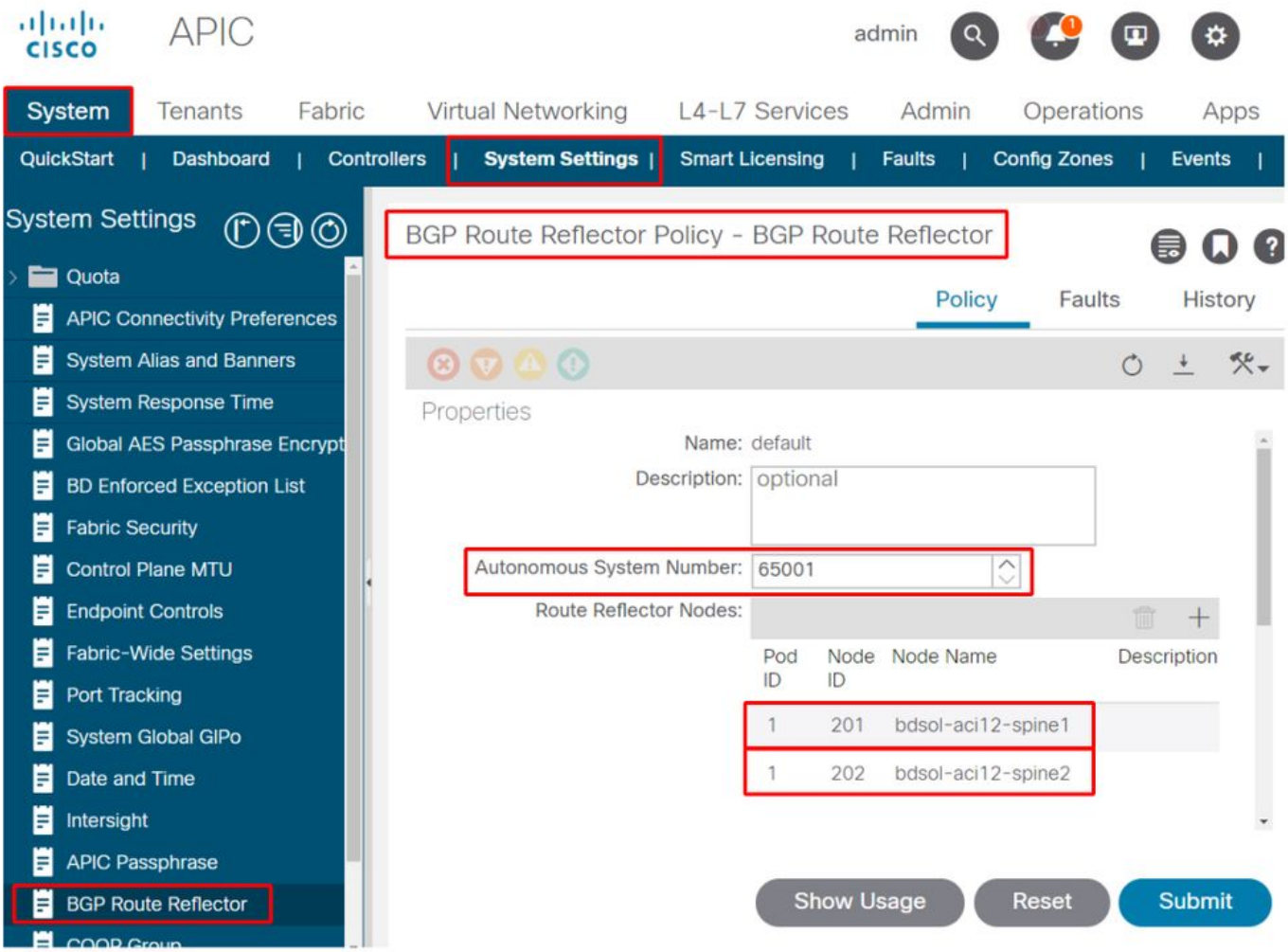
Como resultado, la política BGP RR es una pieza esencial de configuración en cada fabric ACI. La política BGP RR también contiene el ASN que el fabric ACI utiliza para el proceso BGP en cada switch.

Troubleshooting de Flujo

1. Verifique si la política BGP RR tiene un ASN y al menos una columna configurada

El siguiente ejemplo hace referencia a una implementación de POD única.

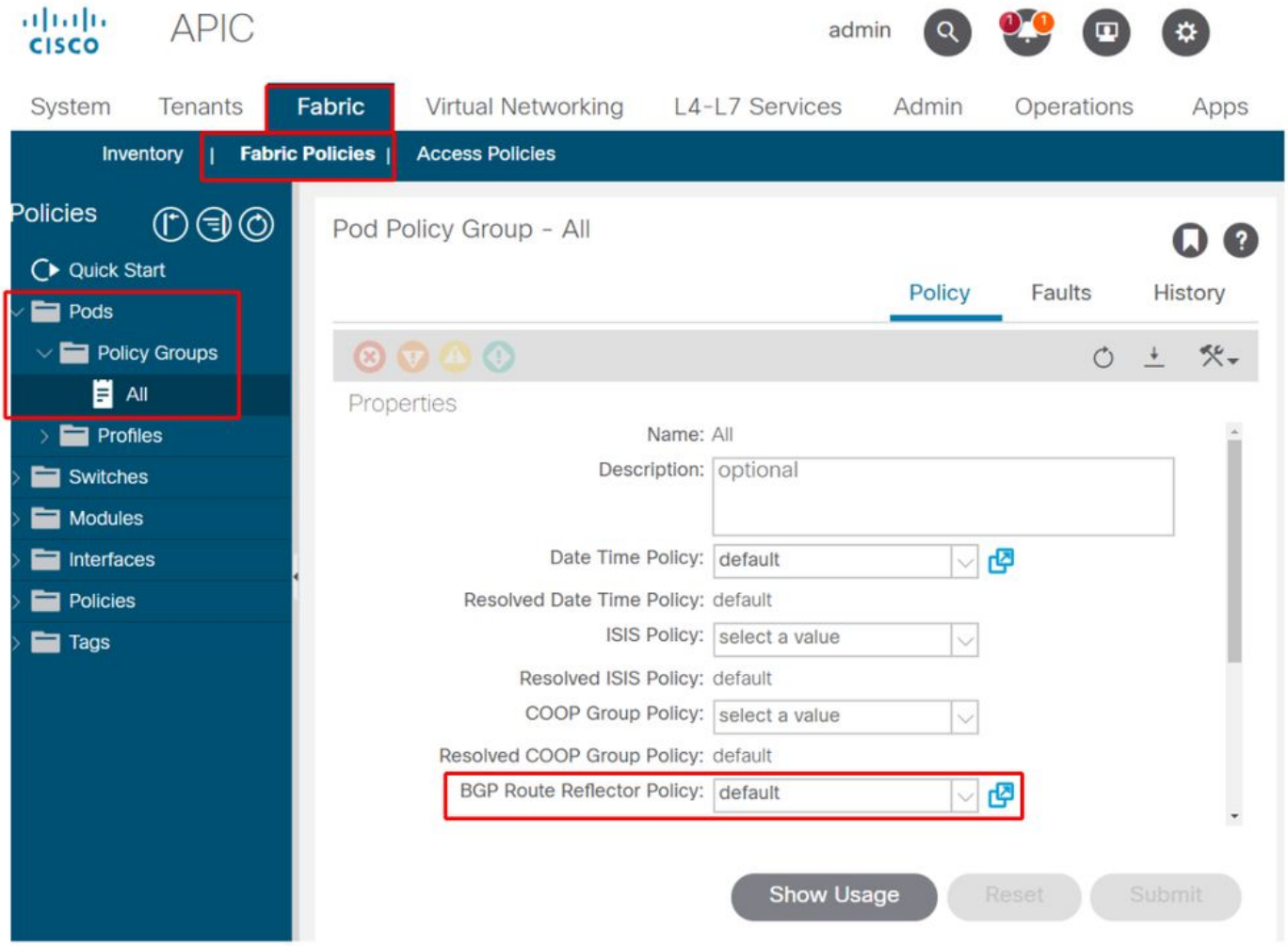
Política de Reflector de Rutas BGP en Configuración del Sistema



2. Verifique si la política BGP RR se aplica bajo el grupo de políticas Pod

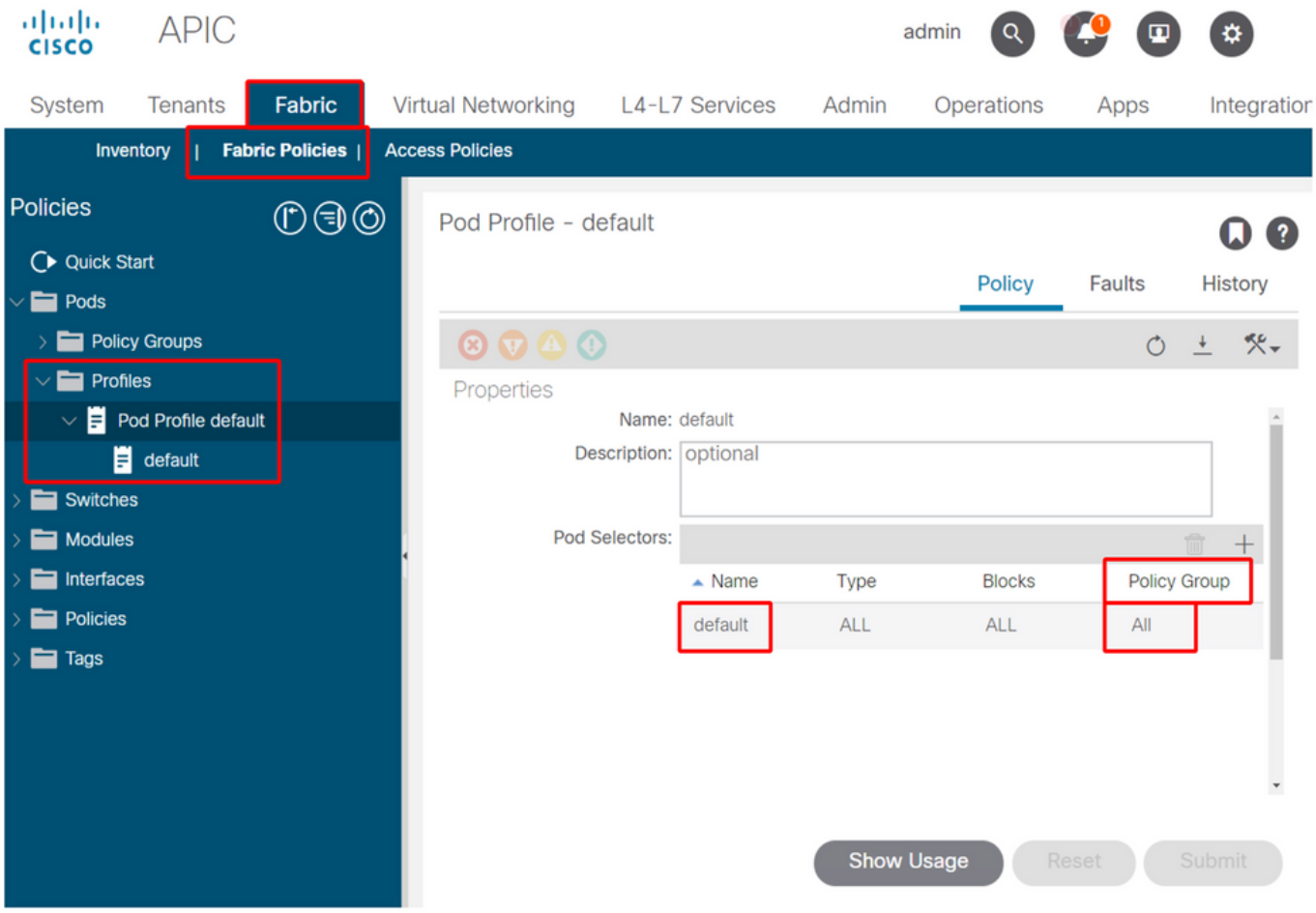
Aplique una política BGP RR predeterminada en el grupo de políticas Pod. Incluso si la entrada está en blanco, la política BGP RR predeterminada se aplicará como parte del grupo de políticas Pod.

Política de Reflector de Rutas BGP aplicada en el Grupo de Políticas de Pod



3. Compruebe si el grupo de políticas de grupo se aplica en el perfil de grupo

Grupo de políticas de grupo de dispositivos aplicado en el perfil de grupo de dispositivos



4. Inicie sesión en una columna y verifique si el proceso BGP se está ejecutando con sesiones de peer VPN4 establecidas

```
spine1# show bgp process vrf overlay-1

BGP Process Information
BGP Process ID                 : 26660
BGP Protocol Started, reason:  : configuration
BGP Protocol Tag               : 65001
BGP Protocol State             : Running
BGP Memory State               : OK
BGP asformat                   : asplain
Fabric SOO                     : SOO:65001:33554415
Multisite SOO                  : SOO:65001:16777199
Pod SOO                        : SOO:1:1
...
   Information for address family VPNv4 Unicast in VRF overlay-1
   Table Id                    : 4
   Table state                 : UP
   Table refcount              : 9
   Peers      Active-peers    Routes     Paths      Networks    Aggregates
     7          6               0          0          0           0

   Redistribution
       None

   Wait for IGP convergence is not configured
   Additional Paths Selection route-map interleak_rtmap_golf_rtmap_path_advertise_all
   Is a Route-reflector
```

```
   Nexthop trigger-delay
       critical 500 ms
       non-critical 5000 ms

   Information for address family VPNv6 Unicast in VRF overlay-1
   Table Id                  : 80000004
   Table state               : UP
   Table refcount            : 9
   Peers      Active-peers    Routes     Paths      Networks   Aggregates
   7          6               0          0          0          0

   Redistribution
       None

   Wait for IGP convergence is not configured
   Additional Paths Selection route-map interleak_rtmap_golf_rtmap_path_advertise_all
   Is a Route-reflector

   Nexthop trigger-delay
       critical 500 ms
       non-critical 5000 ms
...
   Wait for IGP convergence is not configured
   Is a Route-reflector

   Nexthop trigger-delay
       critical 500 ms
       non-critical 5000 ms
```

Como se muestra anteriormente, MP-BGP entre los nodos de columna y de hoja transporta únicamente familias de direcciones VPNv4 y VPNv6. La familia de direcciones IPv4 se utiliza en MP-BGP sólo en los nodos de hoja.

Las sesiones BGP VPNv4 y VPNv6 entre los nodos de columna y hoja también se pueden observar fácilmente mediante el siguiente comando.

```
spine1# show bgp vpnv4 unicast summary vrf overlay-1
BGP summary information for VRF overlay-1, address family VPNv4 Unicast
BGP router identifier 10.0.136.65, local AS number 65001
BGP table version is 15, VPNv4 Unicast config peers 7, capable peers 6
0 network entries and 0 paths using 0 bytes of memory
BGP attribute entries [0/0], BGP AS path entries [0/0]
BGP community entries [0/0], BGP clusterlist entries [0/0]

Neighbor        V      AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.0.136.64     4   65001     162     156       15    0    0 02:26:00 0
10.0.136.67     4   65001     154     154       15    0    0 02:26:01 0
10.0.136.68     4   65001     152     154       15    0    0 02:26:00 0
10.0.136.69     4   65001     154     154       15    0    0 02:26:01 0
10.0.136.70     4   65001     154     154       15    0    0 02:26:00 0
10.0.136.71     4   65001     154     154       15    0    0 02:26:01 0


spine1# show bgp vpnv6 unicast summary vrf overlay-1
BGP summary information for VRF overlay-1, address family VPNv6 Unicast
BGP router identifier 10.0.136.65, local AS number 65001
BGP table version is 15, VPNv6 Unicast config peers 7, capable peers 6
0 network entries and 0 paths using 0 bytes of memory
BGP attribute entries [0/0], BGP AS path entries [0/0]
BGP community entries [0/0], BGP clusterlist entries [0/0]

Neighbor        V      AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
```

```
10.0.136.64     4   65001     162     156       15    0    0 02:26:11 0
10.0.136.67     4   65001     155     155       15    0    0 02:26:12 0
10.0.136.68     4   65001     153     155       15    0    0 02:26:11 0
10.0.136.69     4   65001     155     155       15    0    0 02:26:12 0
10.0.136.70     4   65001     155     155       15    0    0 02:26:11 0
10.0.136.71     4   65001     155     155       15    0    0 02:26:12 0
```

Observe la columna 'Arriba/Abajo' de la salida anterior. Debería enumerar un tiempo de duración que denota el tiempo que se ha establecido la sesión BGP. Tenga en cuenta también que en el ejemplo la columna 'PfxRcd' muestra 0 para cada par VPNv4/VPNv6 BGP, ya que este fabric ACI aún no tiene L3Outs configurados y, por lo tanto, ninguna ruta/prefijo externo es un intercambio entre nodos de columna y de hoja.

5. Inicie sesión en una hoja y verifique si el proceso BGP se está ejecutando con sesiones de peer VPN4 establecidas

```
leaf1# show bgp process vrf overlay-1

BGP Process Information
BGP Process ID                 : 43242
BGP Protocol Started, reason:  : configuration
BGP Protocol Tag               : 65001
BGP Protocol State             : Running
...

leaf1#  show bgp vpnv4 unicast summary vrf overlay-1
BGP summary information for VRF overlay-1, address family VPNv4 Unicast
BGP router identifier 10.0.136.64, local AS number 65001
BGP table version is 7, VPNv4 Unicast config peers 2, capable peers 2
0 network entries and 0 paths using 0 bytes of memory
BGP attribute entries [0/0], BGP AS path entries [0/0]
BGP community entries [0/0], BGP clusterlist entries [0/0]

Neighbor        V      AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.0.136.65     4   65001     165     171        7    0    0 02:35:52 0
10.0.136.66     4   65001     167     171        7    0    0 02:35:53 0
```

Los resultados del comando anterior muestran una cantidad de sesiones VPNv4 BGP igual al número de nodos de columna presentes en el fabric ACI. Esto difiere de los nodos de columna porque establecen sesiones para cada hoja y los otros nodos de columna reflectores de ruta.

SNMP (Protocolo de administración de red simple)

Es importante aclarar desde el principio qué subconjunto específico de funciones SNMP cubre esta sección. Las funciones SNMP de un fabric ACI están relacionadas con la función SNMP Walk o la función SNMP Trap. La distinción importante aquí es que SNMP Walk controla los flujos de tráfico **ingress** SNMP en el puerto UDP 161 mientras que SNMP Trap controla los flujos de tráfico **outgoing** SNMP con un servidor SNMP Trap que escucha en el puerto UDP 162.

El tráfico de gestión de entrada en los nodos de ACI requiere que los EPG de gestión de nodos (en banda o fuera de banda) proporcionen los contratos necesarios para permitir el flujo del tráfico. Esto también se aplica a los flujos de tráfico SNMP de entrada.

En esta sección se tratan los flujos de tráfico SNMP de entrada (SNMP Walks) en los nodos ACI (APIC y switches). No cubrirá los flujos de tráfico SNMP de salida (trampas SNMP), ya que esto ampliaría el alcance de esta sección en Políticas de supervisión y dependencias de políticas de supervisión (es decir, alcance de la política de supervisión, paquetes de supervisión, etc.).

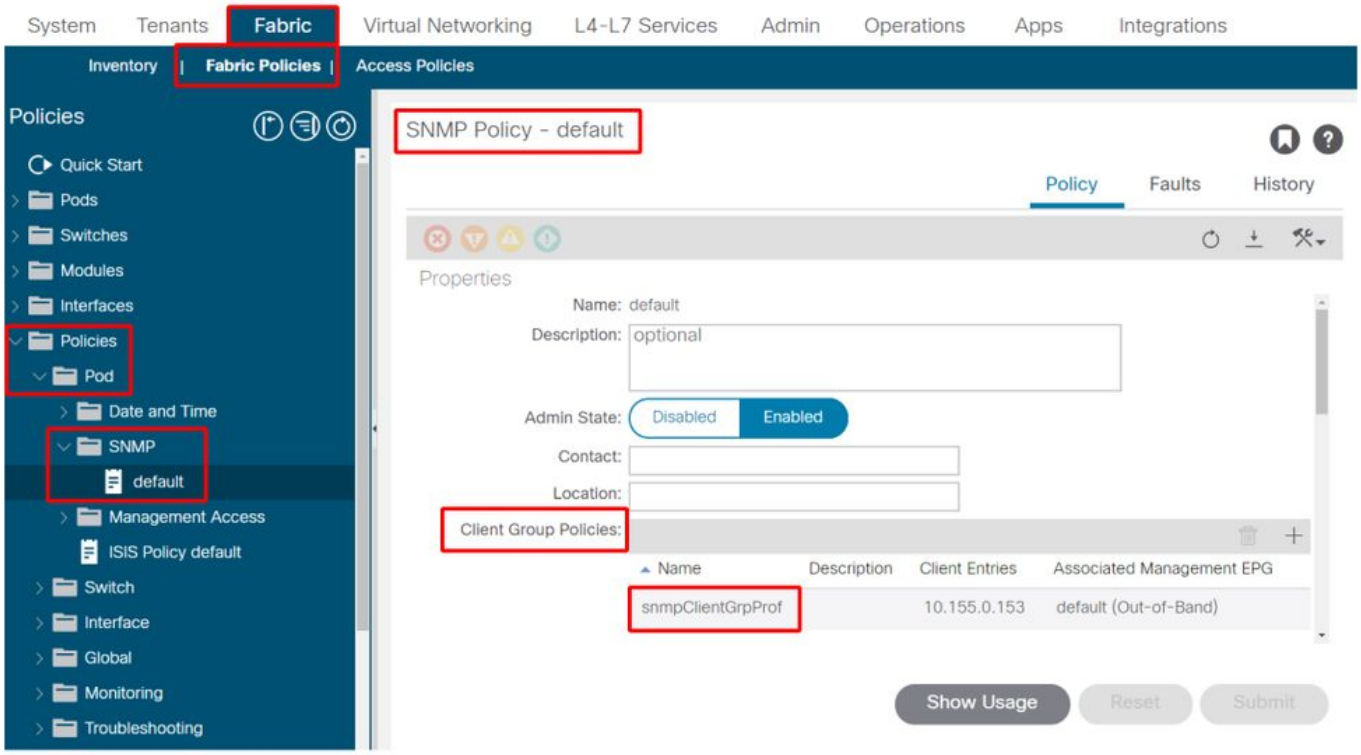
Esta sección tampoco cubre qué MIB de SNMP admite ACI. Esta información está disponible en el sitio web de Cisco CCO en el siguiente enlace: https://www.cisco.com/c/dam/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/mib/list/mib-support.html

Troubleshooting de Flujo

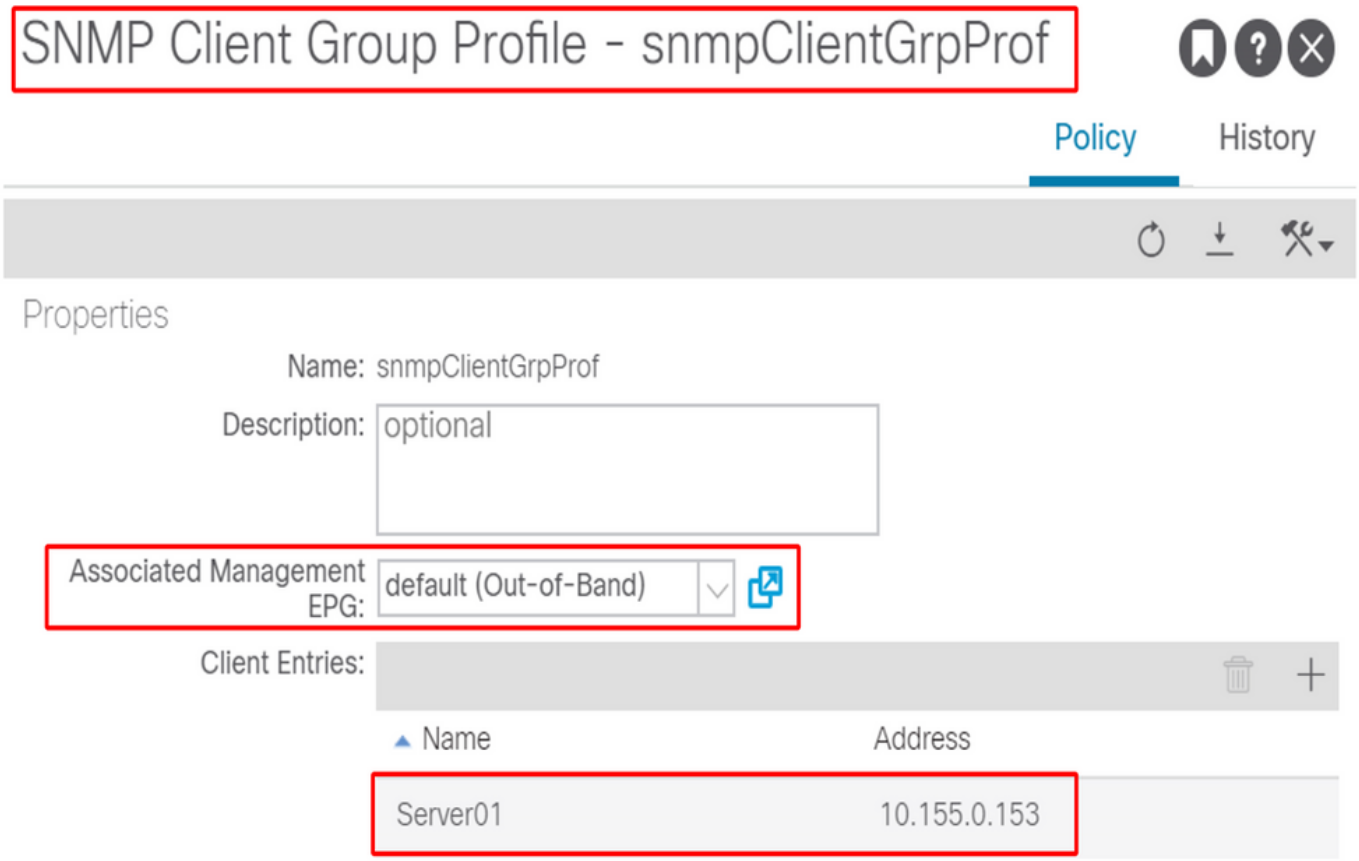
1. Directiva de grupo SNMP: verifique si se ha configurado una directiva de grupo de clientes

Asegúrese de que al menos un cliente SNMP esté configurado como parte de la política de grupo de clientes, como se muestra en las capturas de pantalla siguientes.

Políticas de grupo de clientes — Política SNMP — Políticas de grupo de clientes

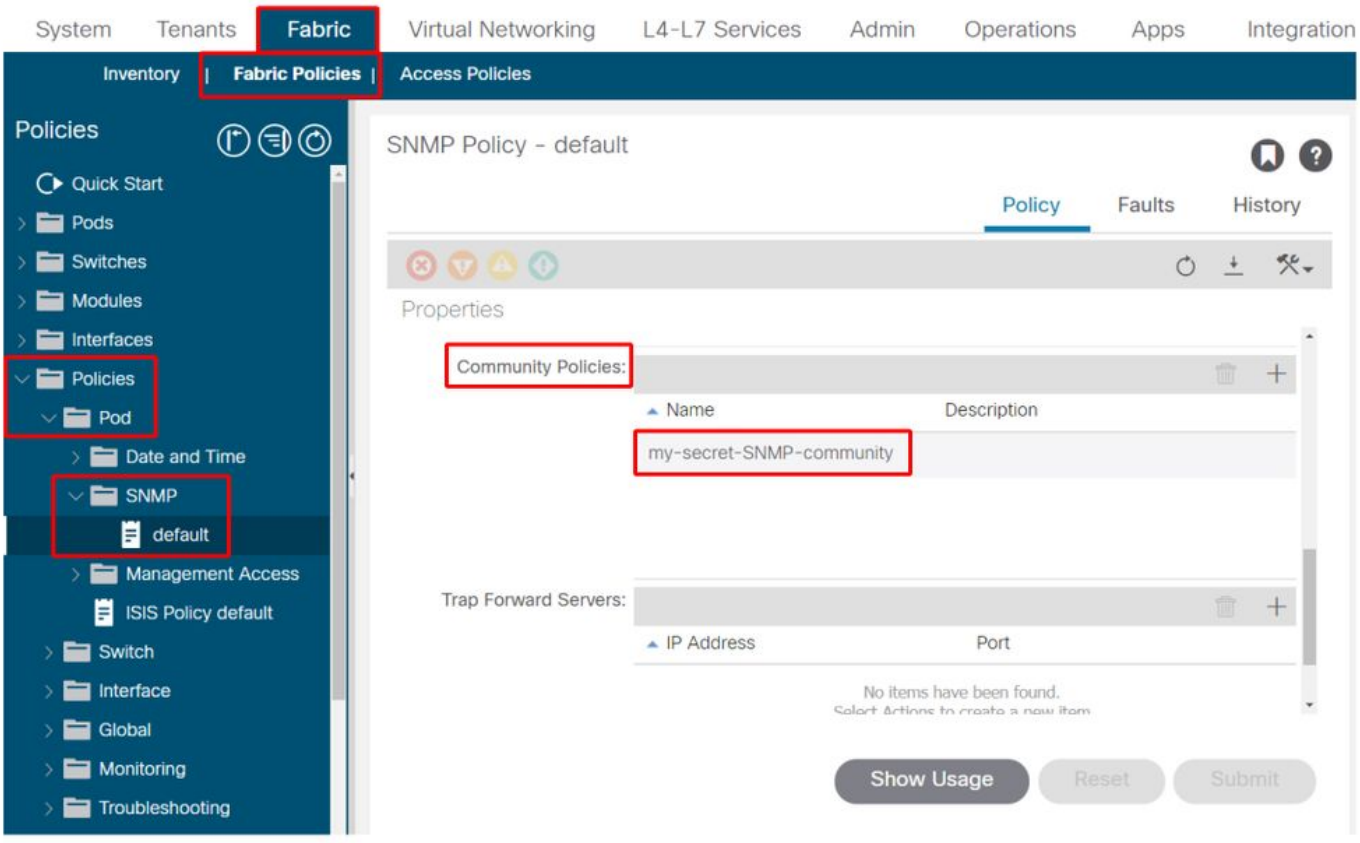


Políticas de grupo de clientes — Política SNMP — Políticas de grupo de clientes

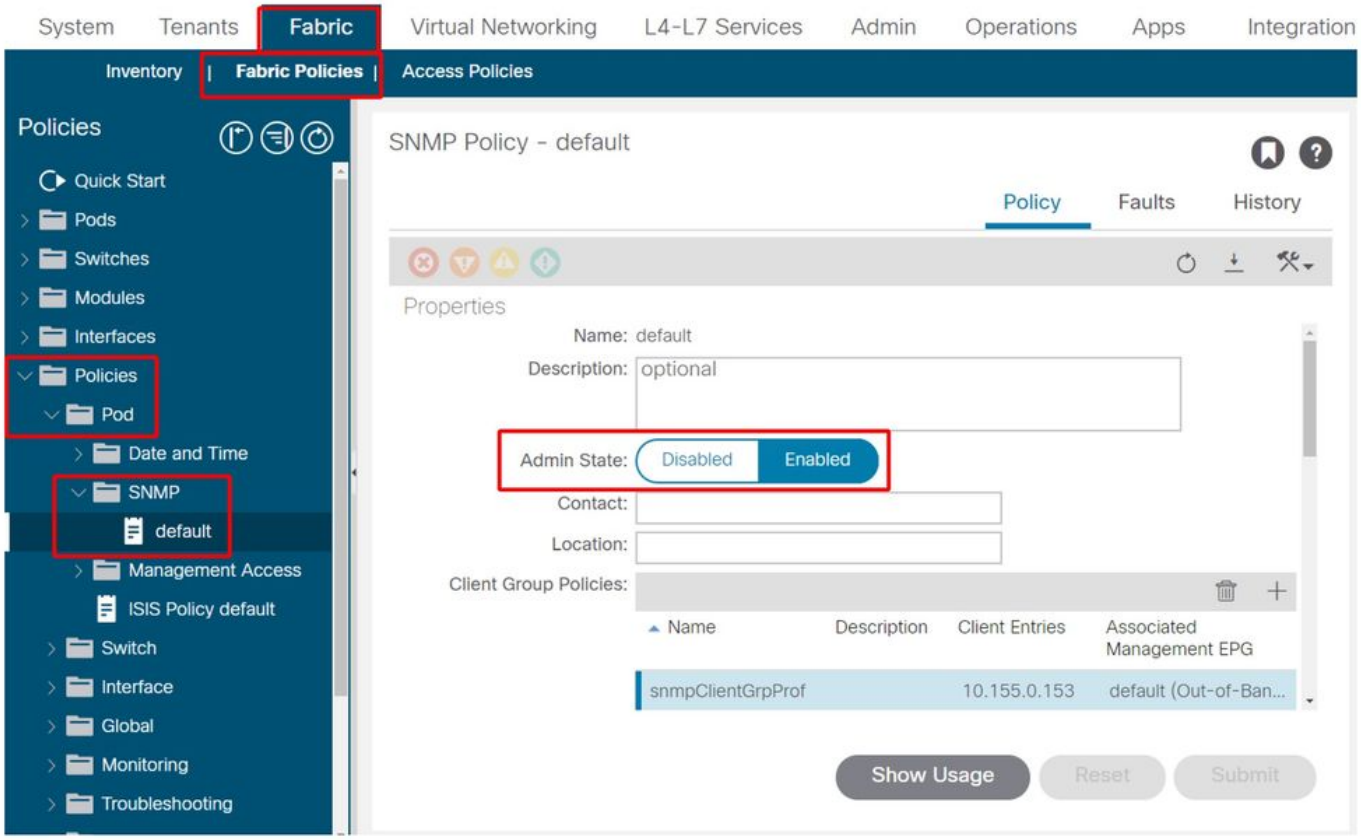


2. Política de Pod SNMP: verifique si al menos una política de comunidad está configurada

Políticas de grupo de dispositivos — Política SNMP — Políticas comunitarias



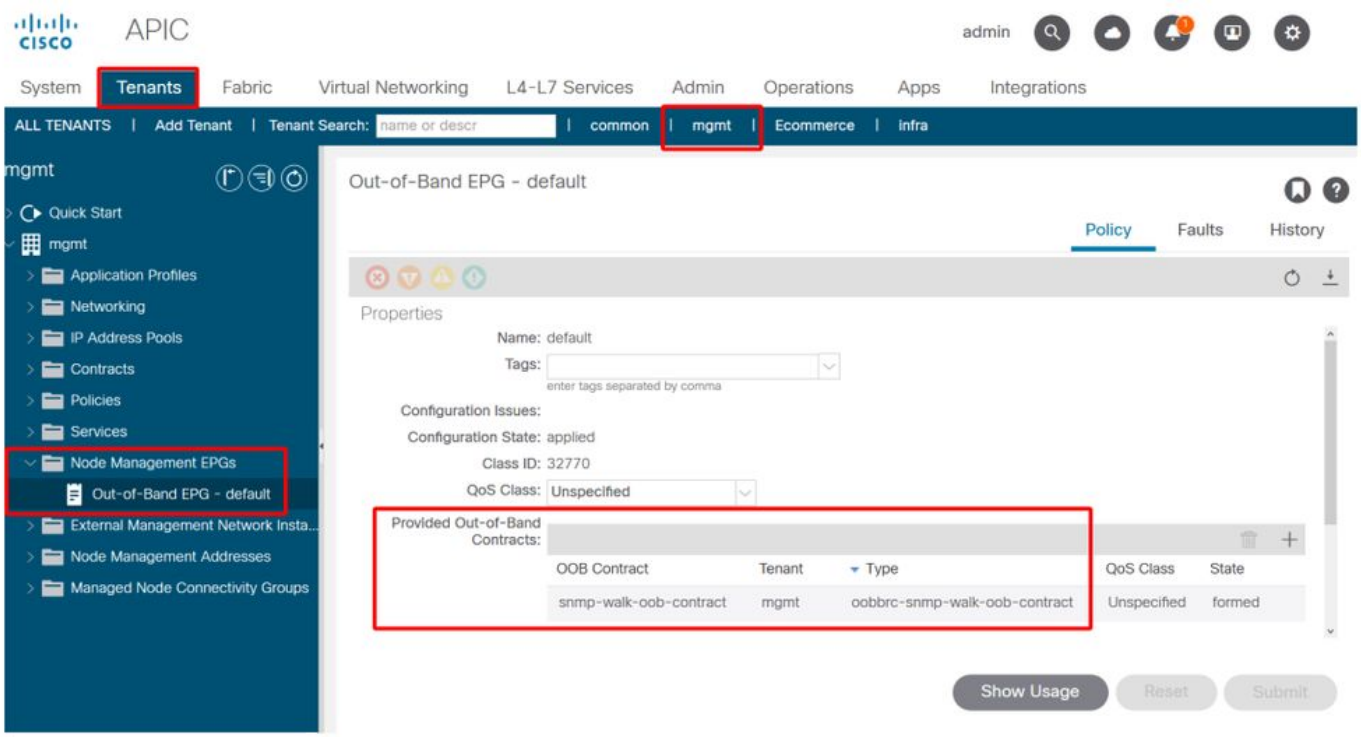
3. Política de Pod SNMP: verifique si el estado del administrador está configurado en 'Habilitado'



4. Arrendatario de administración: verifique si el EPG OOB proporciona un contrato OOB que permite el puerto UDP 161

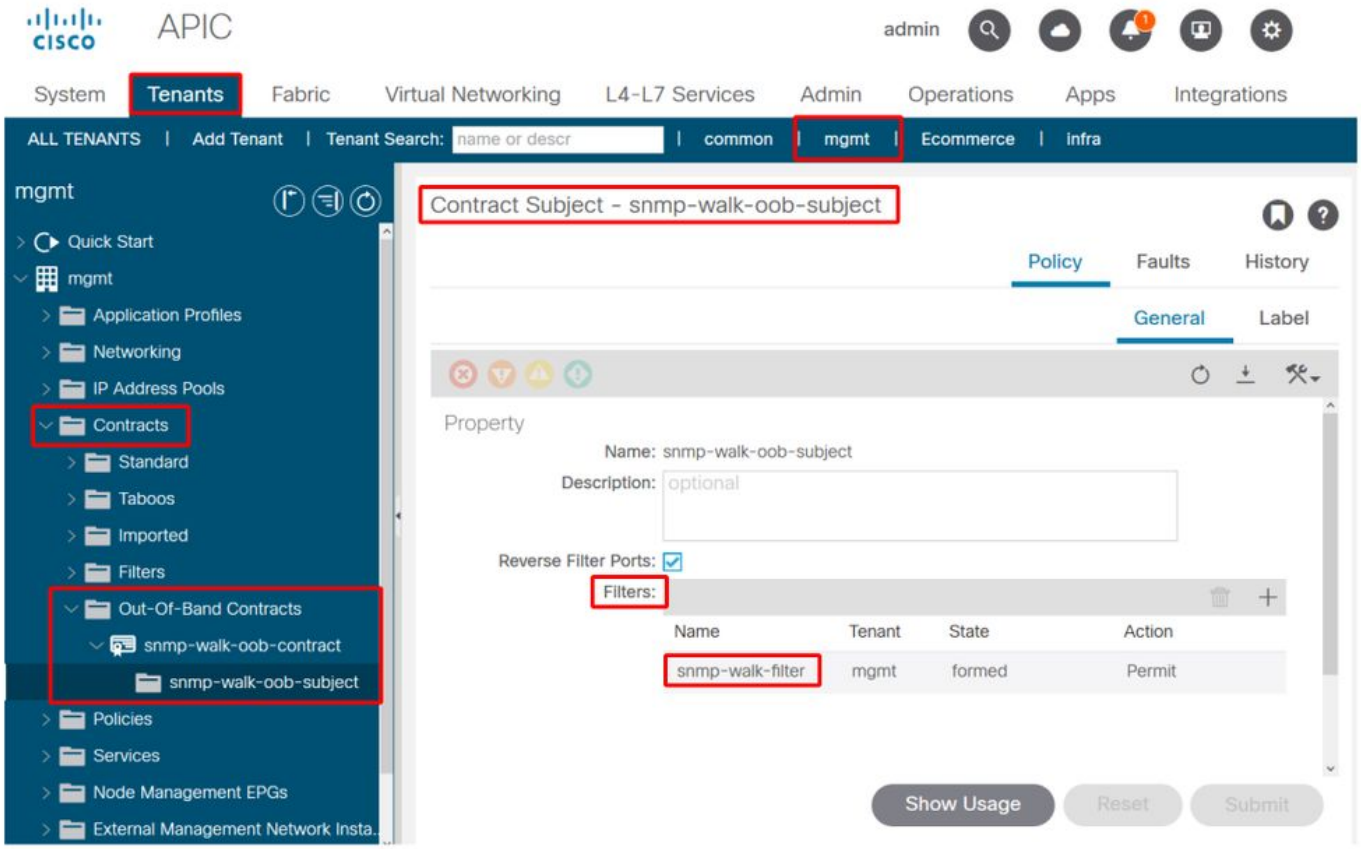
El EPG OOB controla la conectividad en el APIC y los puertos de gestión OOB del switch. Como tal, afecta a todos los flujos de tráfico que ingresan a los puertos OOB.

Asegúrese de que el contrato que se proporciona aquí incluye todos los servicios de gestión necesarios en lugar de solo SNMP. Por ejemplo: también debe incluir al menos SSH (puerto TCP 22). Sin esto no es posible iniciar sesión en los switches usando SSH. Tenga en cuenta que esto no se aplica a los APIC, ya que disponen de un mecanismo que permite SSH, HTTP y HTTPS para evitar que los usuarios se bloqueen completamente.

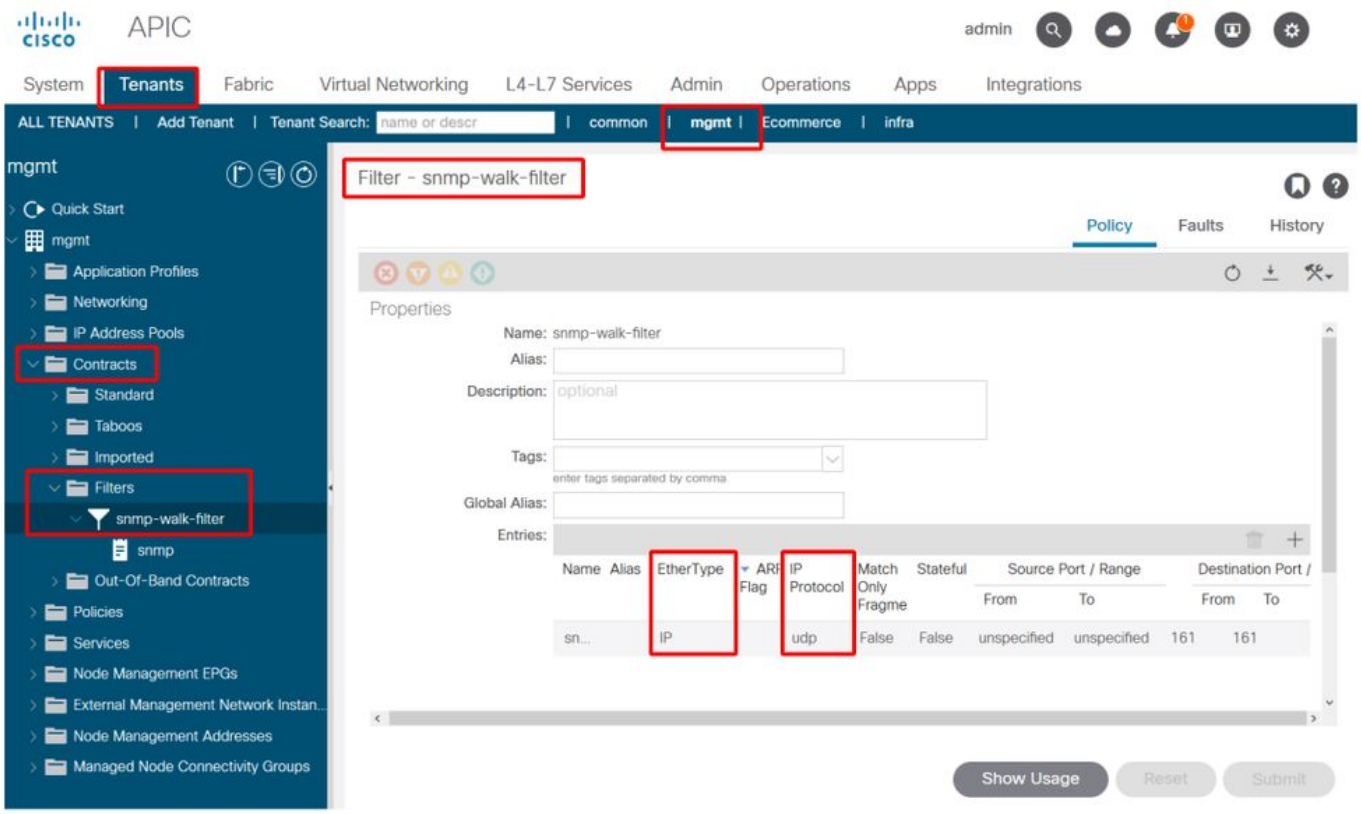


5. Arrendatario de administración: verifique si el Contrato OOB está presente y tiene un filtro que permite el puerto UDP 161

Arrendatario de gestión — EPG OOB — Contrato OOB proporcionado



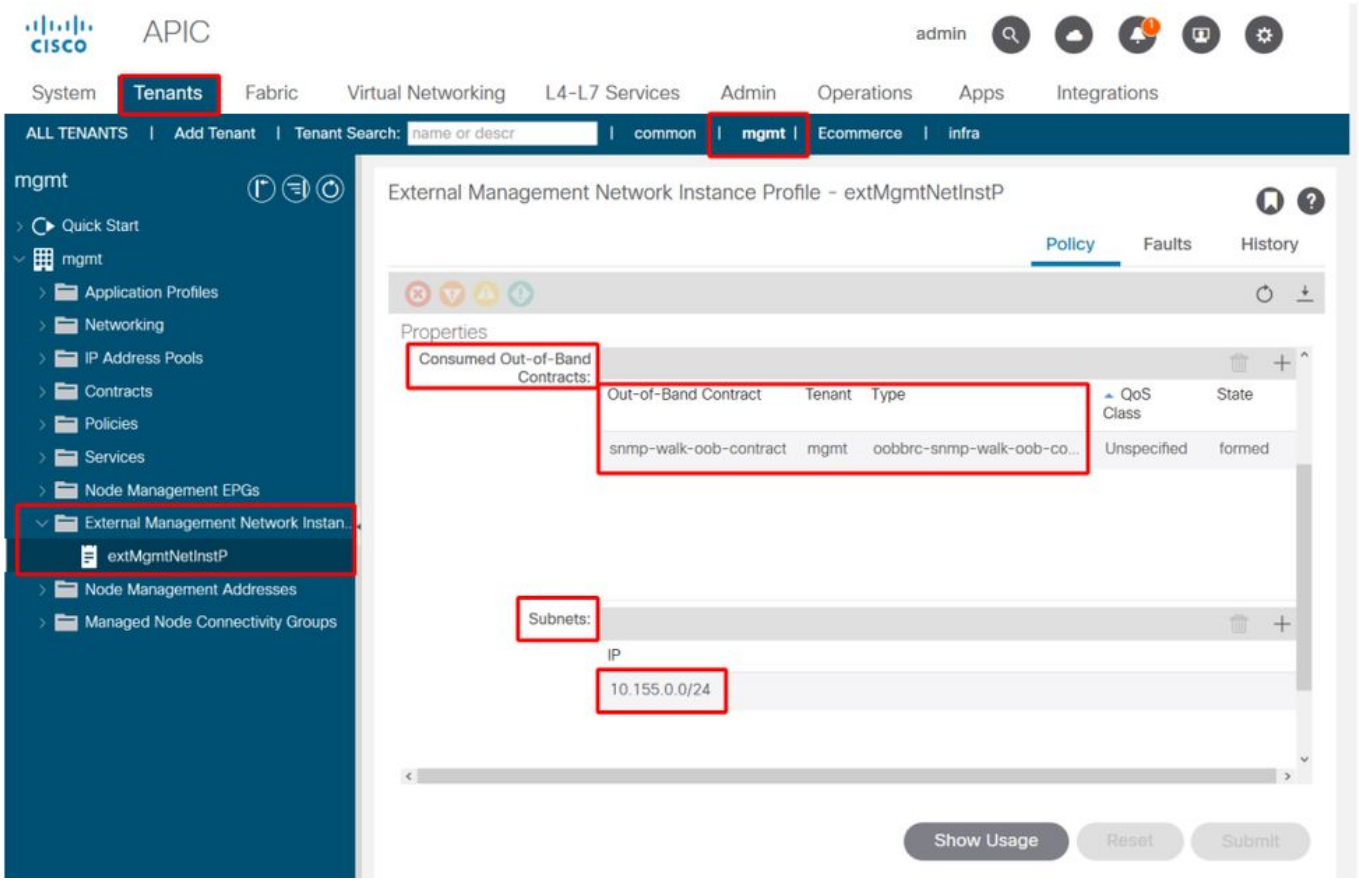
En la siguiente figura, no es obligatorio permitir solamente el puerto UDP 161. Un contrato que tiene un filtro que permite el puerto UDP 161 de cualquier manera es correcto. Puede ser incluso un asunto de contrato con el filtro predeterminado del arrendatario común. En nuestro ejemplo, por motivos de claridad, se configuró un filtro específico sólo para el puerto UDP 161.



6. Arrendatario de gestión: verifique si hay un perfil de instancia de red de gestión externa con una subred válida que consume el contrato OOB.

El perfil de instancia de red de administración externa (ExtMgmtNetInstP) representa los orígenes externos definidos por las "subredes" que se encuentran en el sitio y que necesitan consumir servicios accesibles a través de la EPG OOB. Por lo tanto, ExtMgmtNetInstP utiliza el mismo contrato OOB que proporciona el EPG OOB. Este es el contrato que permite el puerto UDP 161. Además, ExtMgmtNetInstP también especifica los rangos de subred permitidos que pueden consumir los servicios proporcionados por el EPG OOB.

Arrendatario de administración: ExtMgmtNetInstP con contrato OOB y subred consumidos



Como se muestra en la figura anterior, se requiere una notación de subred basada en CIDR. La figura muestra una subred /24 específica. El requisito es que las entradas de subred cubran las entradas de cliente SNMP configuradas en la directiva de grupo SNMP (consulte la figura Directivas de grupo — Directiva SNMP — Directivas de grupo de clientes).

Como se ha mencionado anteriormente, tenga cuidado de incluir todas las subredes externas necesarias para evitar que se bloqueen otros servicios de gestión necesarios.

7. Inicie sesión en un switch y realice un tcpdump para observar si se observan los paquetes SNMP Walk, el puerto UDP 161

Si los paquetes SNMP Walk ingresan a un switch a través del puerto OOB, esto significa que todas las políticas/parámetros necesarios basados en SNMP y OOB se han configurado correctamente. Por lo tanto, es un método de verificación adecuado.

Tcpdump en los nodos de hoja aprovecha su shell Linux y los netdevices Linux. Por lo tanto, es necesario capturar los paquetes en la interfaz 'eth0' según el siguiente ejemplo. En el ejemplo, un cliente SNMP está realizando una solicitud Get SNMP contra OID .1.0.8802.1.1.2.1.1.1.0.

```
leaf1# ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
   link/ether f4:cf:e2:28:fc:ac brd ff:ff:ff:ff:ff:ff
   inet 10.48.22.77/24 brd 10.48.22.255 scope global eth0
       valid_lft forever preferred_lft forever
   inet6 fe80::f6cf:e2ff:fe28:fcac/64 scope link
       valid_lft forever preferred_lft forever


leaf1# tcpdump -i eth0 udp port 161
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
```

```
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
22:18:10.204011 IP 10.155.0.153.63392 > 10.48.22.77.snmp:  C=my-snmp-community
GetNextRequest(28)  .iso.0.8802.1.1.2.1.1.1.0
22:18:10.204558 IP 10.48.22.77.snmp > 10.155.0.153.63392:  C=my-snmp-community GetResponse(29)
.iso.0.8802.1.1.2.1.1.2.0=4
```

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).