Solução de problemas de gerenciamento da ACI e Core Services - Políticas de Pod

Contents

Introduction

Este documento descreve as etapas para entender e solucionar problemas das políticas do ACI Pod.

Informações de Apoio

O material deste documento foi extraído do Solução de problemas da Cisco Application Centric Infrastructure, segunda edição , especificamente o Management and Core Services - **Políticas de POD - BGP RR/ Date&Time / SNMP** capítulo.

Visão geral das políticas de Pod

Serviços de gerenciamento como BGP RR, Data e Hora e SNMP são aplicados no sistema usando um Grupo de Políticas de Pod. Um grupo de políticas do Pod governa um grupo de políticas do Pod relacionadas às funções essenciais de uma estrutura da ACI. Essas Políticas de Pod se relacionam aos seguintes componentes, muitos dos quais são provisionados em uma estrutura da ACI por padrão.

Políticas de Pod

Política Pod	Requer configuração manual
Data e hora	Yes
Refletor de rota BGP	Yes
SNMP (protocolo de gerenciamento de rede de servidor)	Yes
ISIS	No
COOP	No

Acesso de gerenciamento	No
MAC Sec	Yes

Mesmo em uma única estrutura da ACI, o Grupo de políticas do Pod e o Perfil do Pod precisam ser configurados. Isso não é específico para uma implantação de vários pods ou mesmo de vários locais. O requisito se aplica a **todos os** tipos de implantação da ACI.

Este capítulo se concentra nessas Políticas de Pod essenciais e em como verificar se elas são aplicadas corretamente.

Política de data e hora

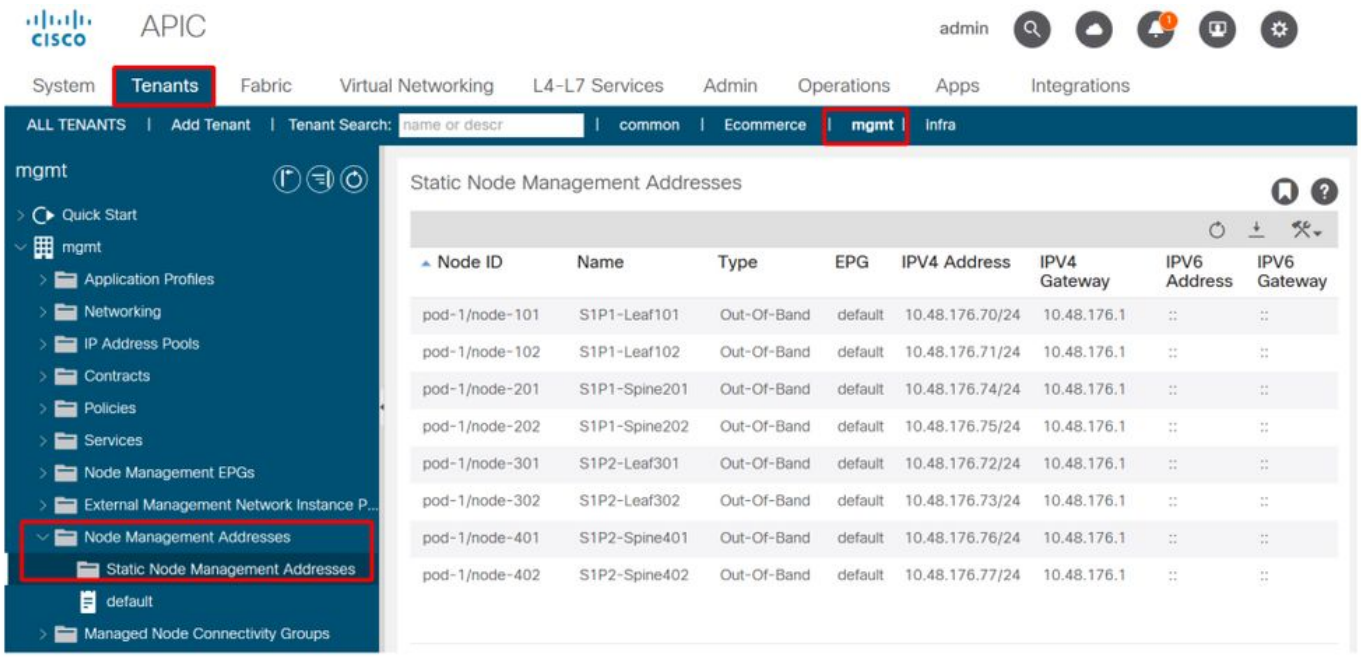
A sincronização de horário desempenha um papel fundamental na estrutura da ACI. Desde a validação de certificados até a manutenção de registros de data e hora em APICs e switches consistentes, é uma prática recomendada sincronizar os nós na estrutura da ACI para uma ou mais fontes de tempo confiáveis usando o NTP.

Para sincronizar corretamente os nós com um provedor de servidor NTP, há uma dependência para atribuir nós com endereços de gerenciamento. Isso pode ser feito no espaço de gerenciamento usando Endereços de Gerenciamento de Nó Estático ou Grupos de Conectividade de Nó de Gerenciamento.

Troubleshooting de Fluxo de Trabalho

1. Verifique se os Endereços de Gerenciamento de Nó estão atribuídos a todos os nós

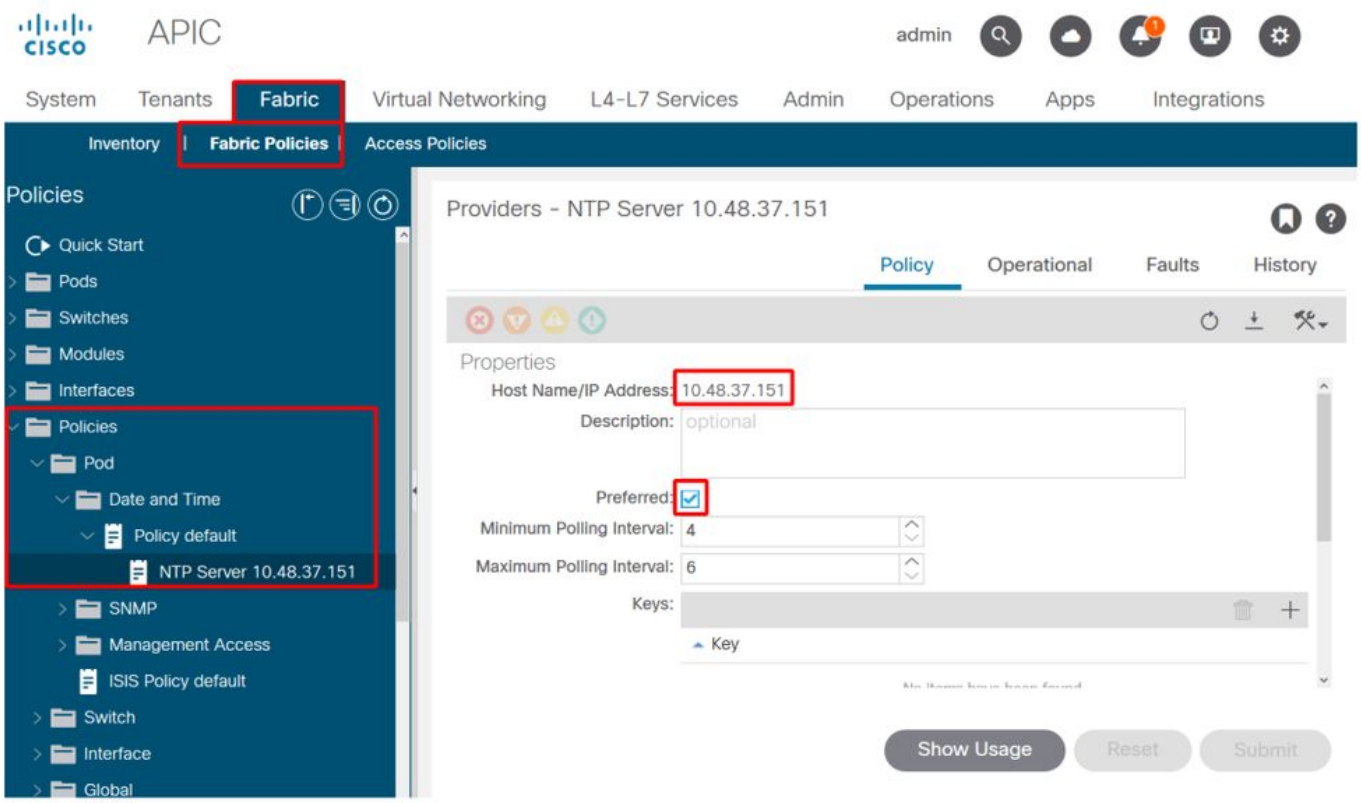
Locatário de gerenciamento - Endereços de gerenciamento de nó



2. Verifique se um servidor NTP foi configurado como provedor NTP

Se houver vários provedores NTP, sinalize pelo menos um deles como a origem de tempo preferencial usando a caixa de seleção 'Preferencial', conforme a figura abaixo.

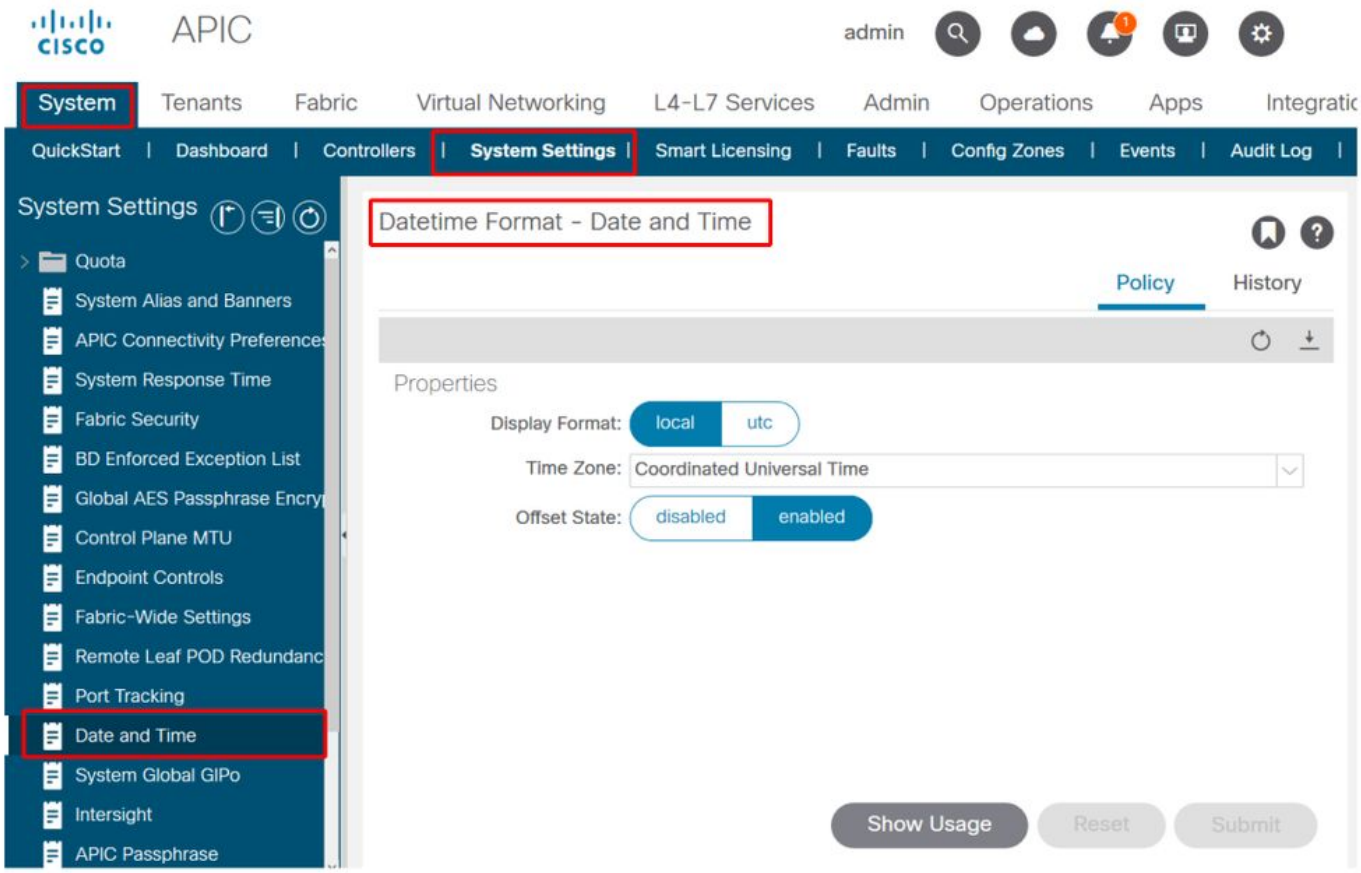
Provedor/Servidor NTP em Política de Pod de data e hora



3. Verifique o formato de Data e Hora em Configurações do Sistema

A figura abaixo mostra um exemplo em que o formato de Data e Hora foi definido como UTC.

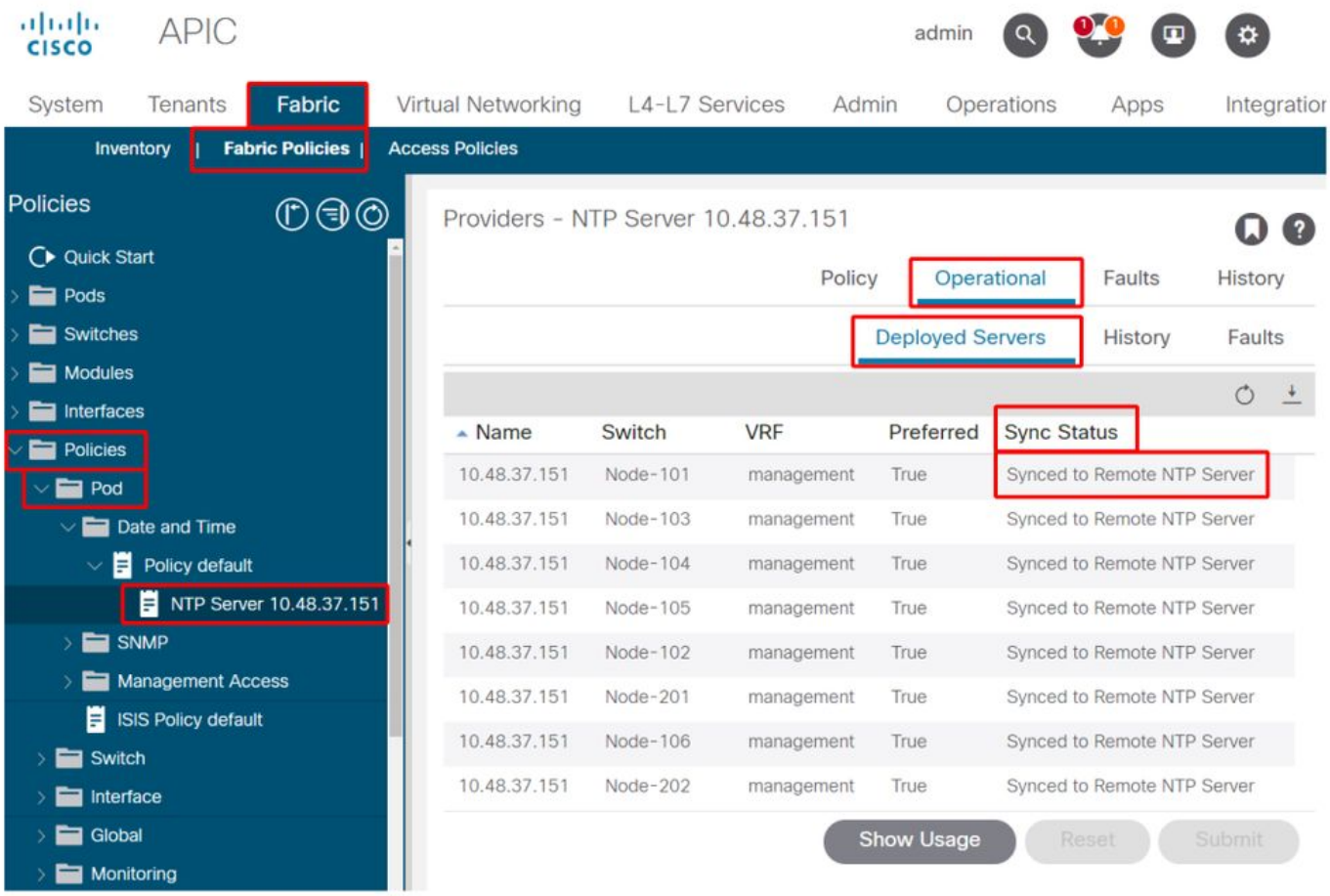
Configuração de data e hora em Configurações do sistema



4. Verifique o Status de Sincronização operacional do provedor de NTP para todos os nós

Como mostrado na figura abaixo, a coluna Status da sincronização deve mostrar 'Sincronizado com o servidor NTP remoto'. Esteja ciente de que pode levar vários minutos para que o Status de Sincronização convirja corretamente para o Servidor NTP Remoto. status.

Status de sincronização de provedor/servidor NTP



Como alternativa, os métodos CLI podem ser usados nos APICs e nos switches para verificar a sincronização de tempo correta em relação ao servidor NTP.

APIC - CLI NX-OS

A coluna 'refId' abaixo mostra a origem da próxima vez dos servidores NTP, dependendo da camada.

```
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

Use o comando 'show ntp peers' para certificar-se de que a configuração do provedor de NTP tenha sido enviada corretamente ao 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
```

O caractere '*' é essencial aqui, pois controla se o servidor NTP está realmente sendo usado para sincronização.

Verifique o número de pacotes enviados/recebidos no seguinte comando para certificar-se de que os nós da ACI tenham acessibilidade ao servidor NTP.

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

Política de Refletor de Rota BGP

Uma estrutura ACI usa o BGP multiprotocolo (MP-BGP) e, mais especificamente, o iBGP VPNv4 entre os nós de folha e coluna para trocar rotas de locatário recebidas de roteadores externos (conectados em L3Outs). Para evitar uma topologia de peer iBGP de malha completa, os nós spine refletem os prefixos VPNv4 recebidos de uma folha para outros nós leaf na estrutura.

Sem a Política de Refletor de Rota BGP (BGP RR), nenhuma instância BGP será criada nos switches e as sessões BGP VPNv4 não serão estabelecidas. Em uma implantação de vários pods, cada pod requer pelo menos um spine configurado como um BGP RR e essencialmente mais de um para redundância.

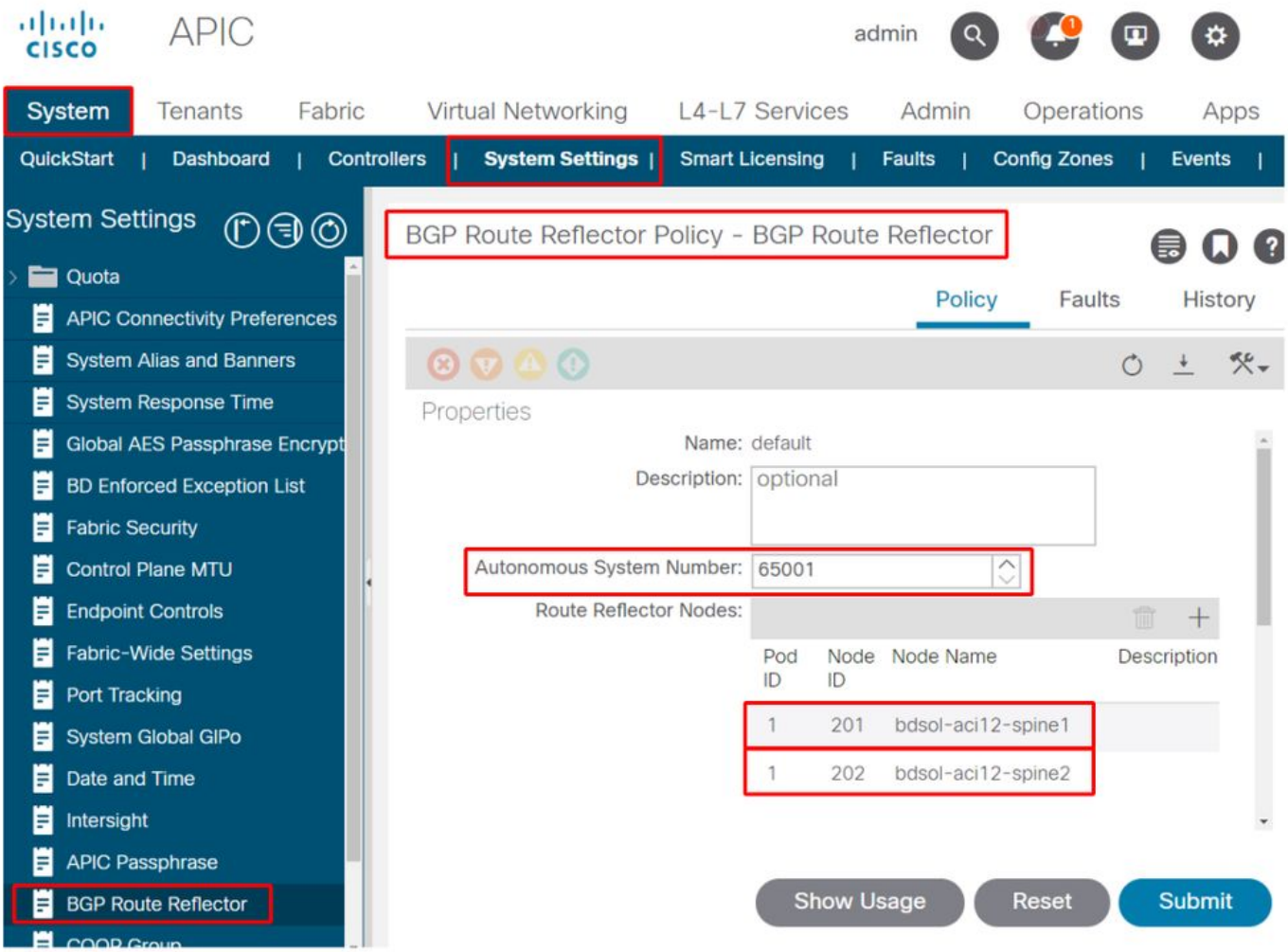
Como resultado, a política BGP RR é uma parte essencial da configuração em cada estrutura da ACI. A Política de RR do BGP também contém o ASN que a estrutura da ACI usa para o processo BGP em cada switch.

Troubleshooting de Fluxo de Trabalho

1. Verifique se a Política BGP RR tem um ASN e pelo menos um spine configurado

O exemplo abaixo refere-se a uma única implantação de Pod.

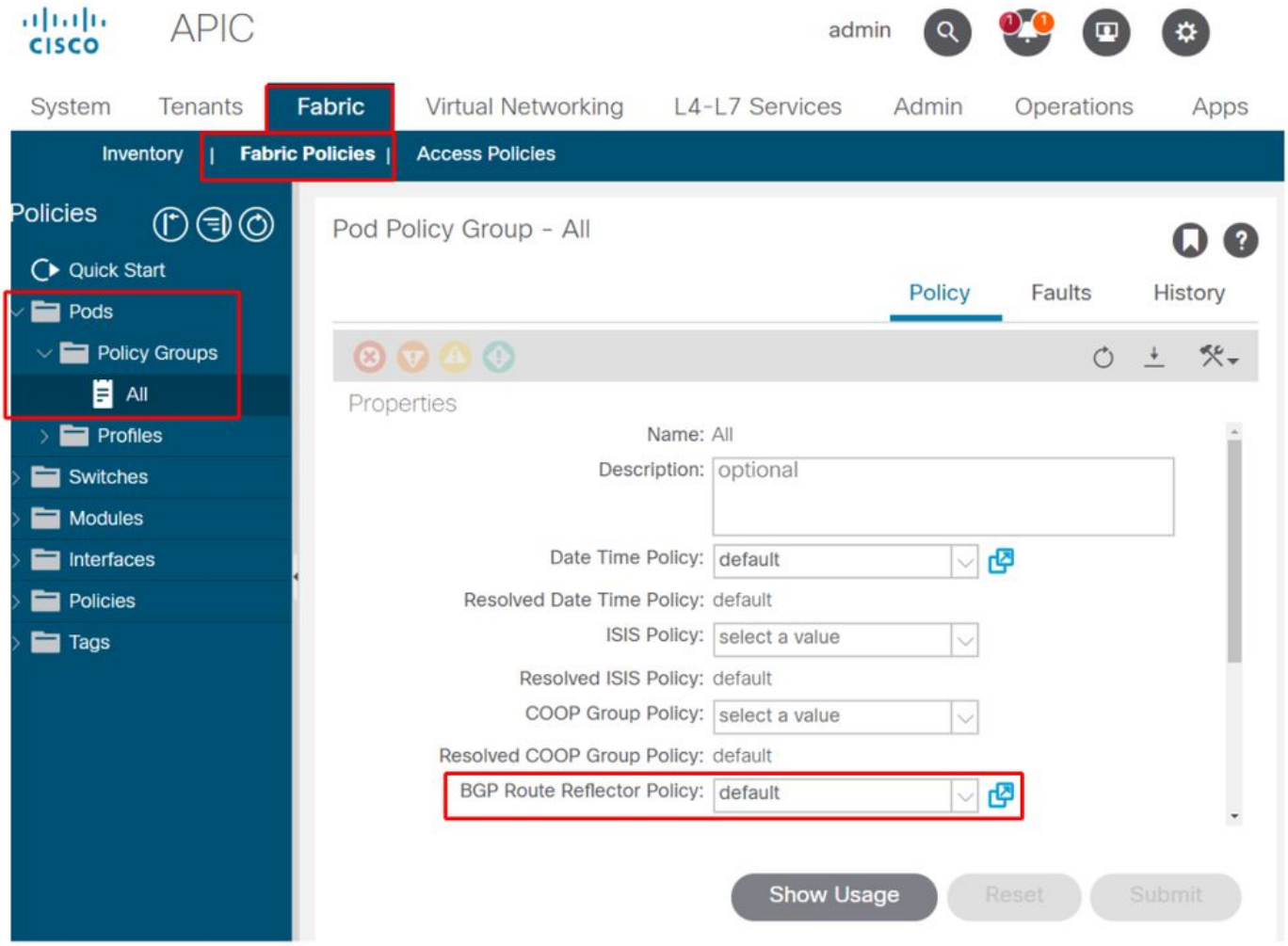
Política de Refletor de Rota BGP em Configurações do Sistema



2. Verifique se a Política de RR do BGP é aplicada no Grupo de Políticas do Pod

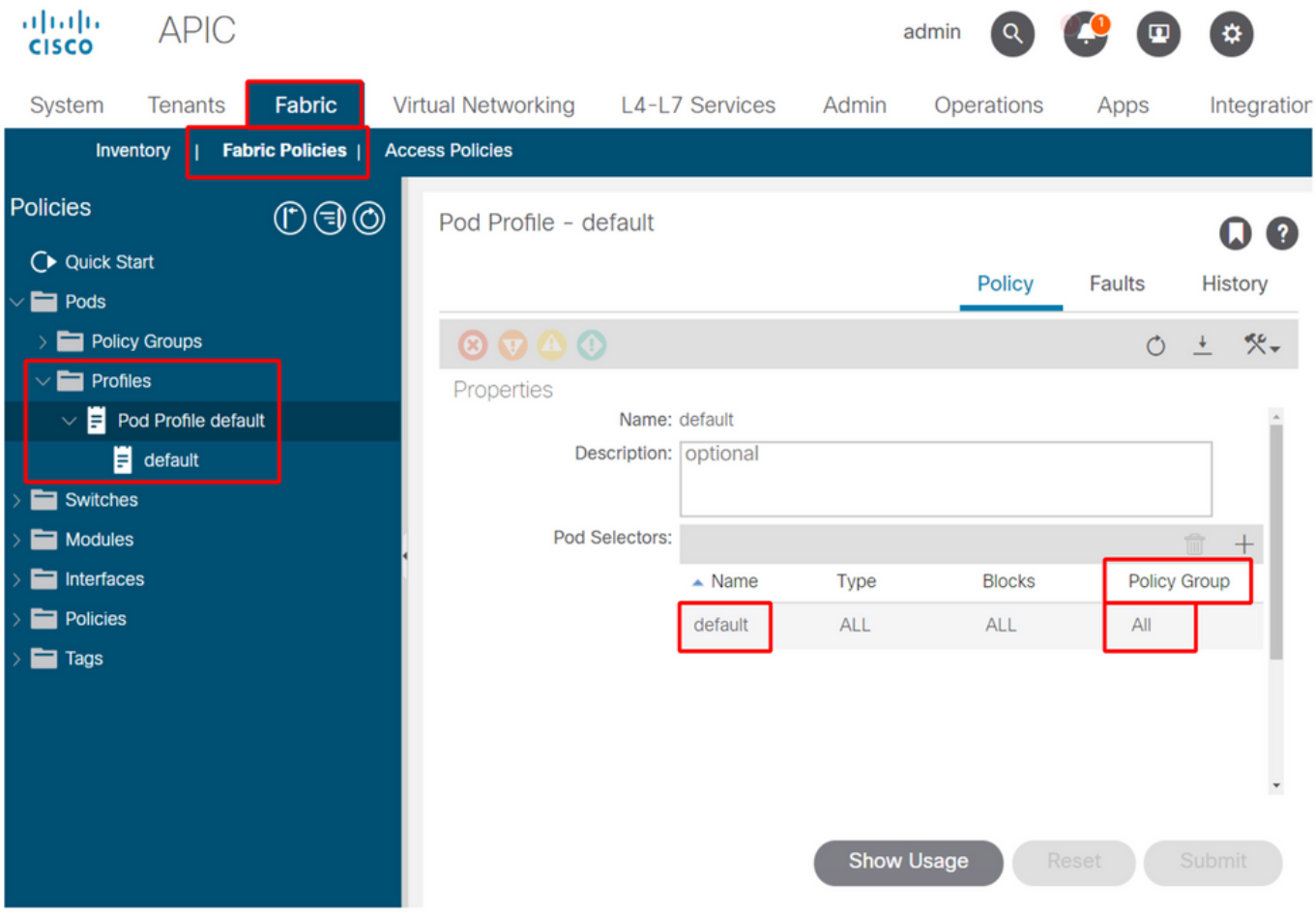
Aplique uma Política de RR de BGP padrão no Grupo de Políticas de Pod. Mesmo se a entrada estiver em branco, a Política de RR de BGP padrão será aplicada como parte do Grupo de Políticas de Pod.

Política de Refletor de Rota BGP aplicada no Grupo de Política Pod



3. Verifique se o Grupo de Políticas do Pod está aplicado no Perfil do Pod

Grupo de Políticas Pod aplicado sob o Perfil Pod



4. Faça login em um spine e verifique se o processo BGP está sendo executado com sessões de pares VPN4 estabelecidas

```
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 mostrado acima, o MP-BGP entre nós de folha e coluna transporta somente famílias de endereços VPNv4 e VPNv6. A família de endereços IPv4 é usada em MP-BGP somente em nós folha.

As sessões BGP VPNv4 e VPNv6 entre os nós spine e leaf também podem ser facilmente observadas usando o seguinte 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 a coluna 'Up/Down' na saída acima. Ele deve listar um tempo de duração que denota o tempo em que a sessão BGP foi estabelecida. Observe também no exemplo que a coluna 'PfxRcd' mostra 0 para cada par BGP VPNv4/VPNv6, pois essa estrutura ACI ainda não tem L3Outs configurados e, como tal, nenhuma rota/prefixo externo são trocas entre os nós de folha e coluna.

5. Faça login em uma folha e verifique se o Processo BGP está sendo executado com sessões de pares VPN4 estabelecidas

```
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
```

As saídas do comando acima mostram uma quantidade de sessões BGP VPNv4 igual ao número de nós spine presentes na estrutura da ACI. Isso difere dos nós spine porque eles estabelecem sessões para cada folha e para os outros nós spine do refletor de rota.

SNMP

Éimportante esclarecer desde o início que subconjunto específico de funções SNMP esta seção abrange. As funções SNMP em uma estrutura ACI se relacionam à função Walk SNMP ou à função Trap SNMP. A distinção importante aqui é que o SNMP Walk governa os fluxos de tráfego SNMP de **ingresso** na porta UDP 161, enquanto o SNMP Trap governa os fluxos de **tráfego SNMP de saída** com um servidor de interceptação SNMP ouvindo na porta UDP 162.

O tráfego de gerenciamento de entrada em nós ACI exige que os EPGs de gerenciamento de nó (dentro ou fora da banda) forneçam os contratos necessários para permitir o fluxo do tráfego. Como tal, isso também se aplica aos fluxos de tráfego SNMP de entrada.

Esta seção abordará os fluxos de tráfego SNMP de entrada (caminhadas de SNMP) em nós ACI (APICs e switches). Ele não abrangerá os fluxos de tráfego SNMP de saída (interceptações SNMP), pois isso expandiria o escopo desta seção em Políticas de monitoramento e dependências de política de monitoramento (ou seja, escopo da Política de monitoramento, Pacotes de monitoramento etc.).

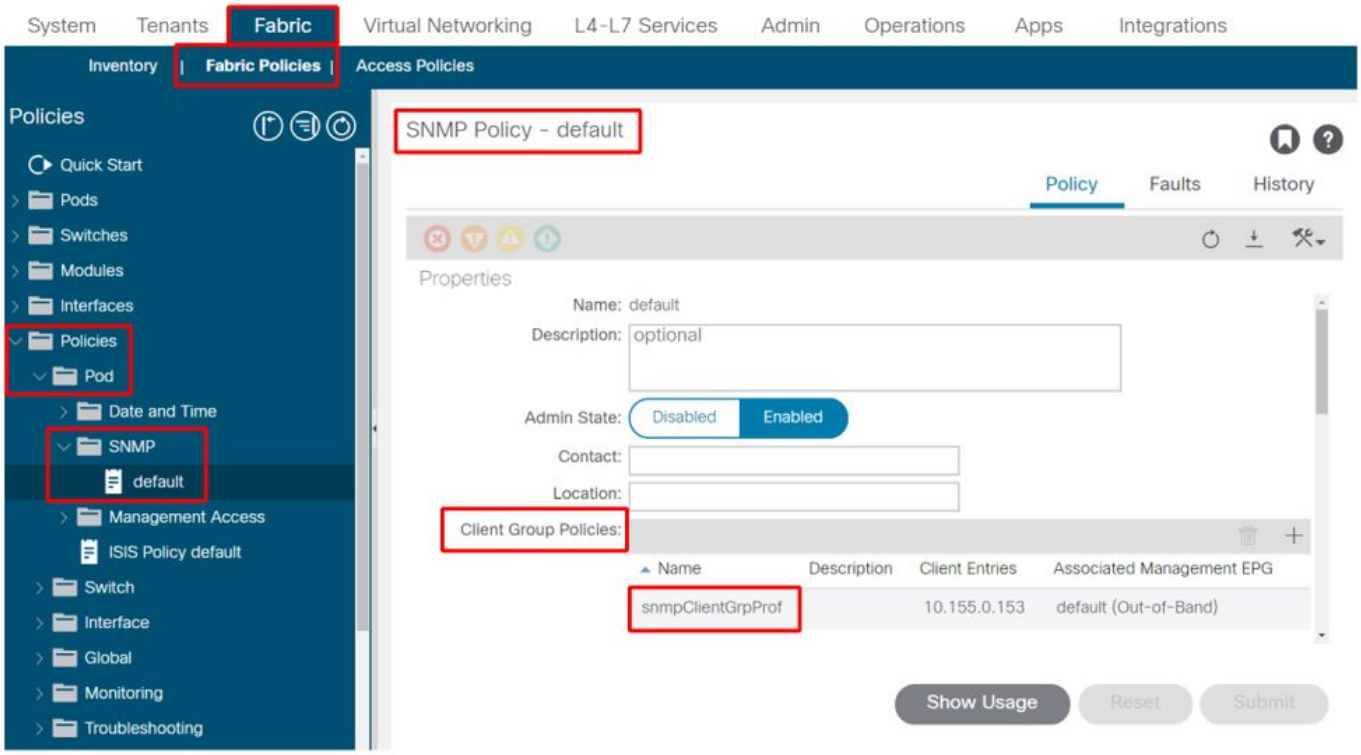
Esta seção também não abordará quais MIBs SNMP são suportados pela ACI. Essas informações estão disponíveis no site do Cisco CCO no seguinte link: https://www.cisco.com/c/dam/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/mib/list/mib-support.html

Troubleshooting de Fluxo de Trabalho

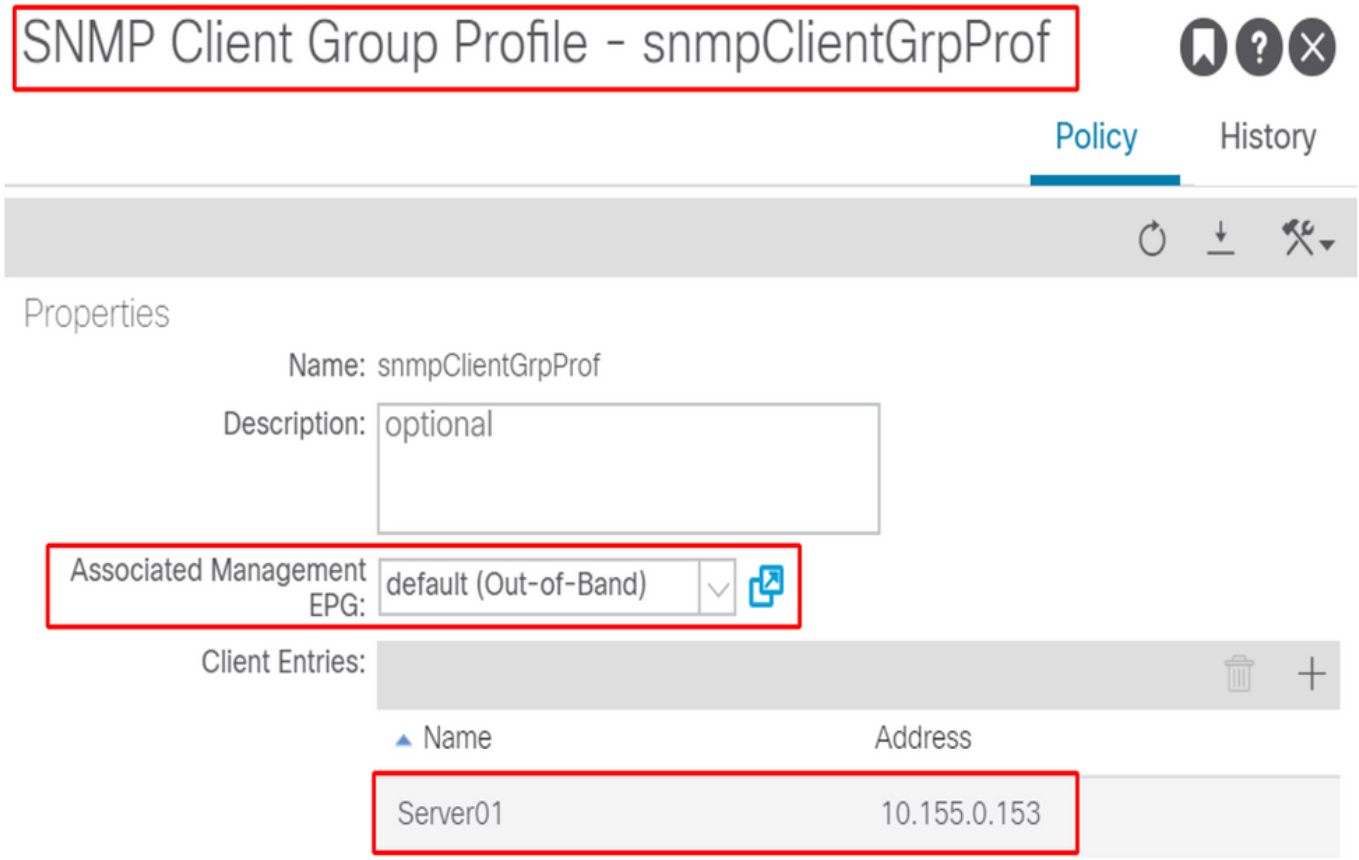
1. Política de Pod SNMP — Verificar se uma Política de Grupo do Cliente está configurada

Certifique-se de que pelo menos um único cliente SNMP esteja configurado como parte da Política de grupo do cliente conforme as capturas de tela abaixo.

Políticas de Pod — Política SNMP — Políticas de grupo do cliente

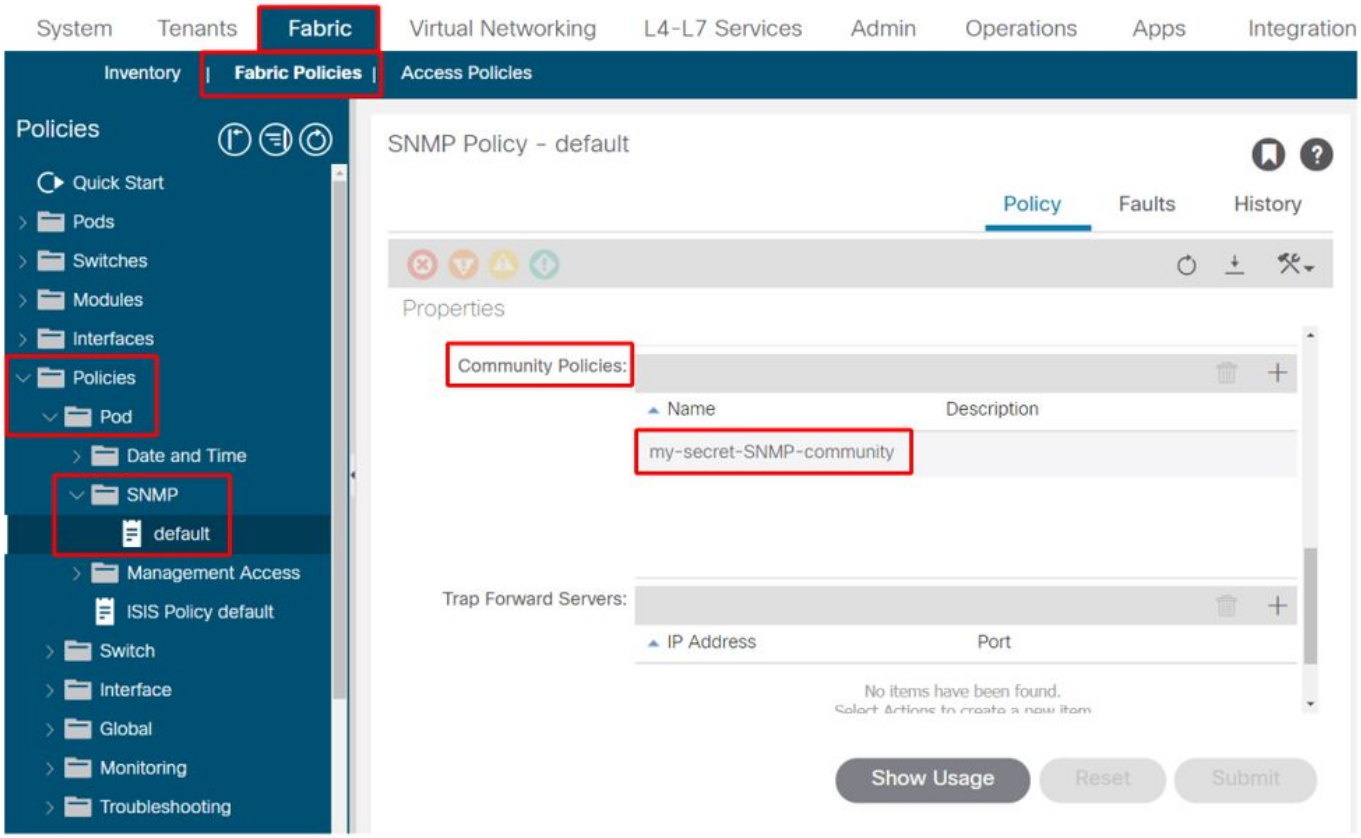


Políticas de Pod — Política SNMP — Políticas de grupo do cliente

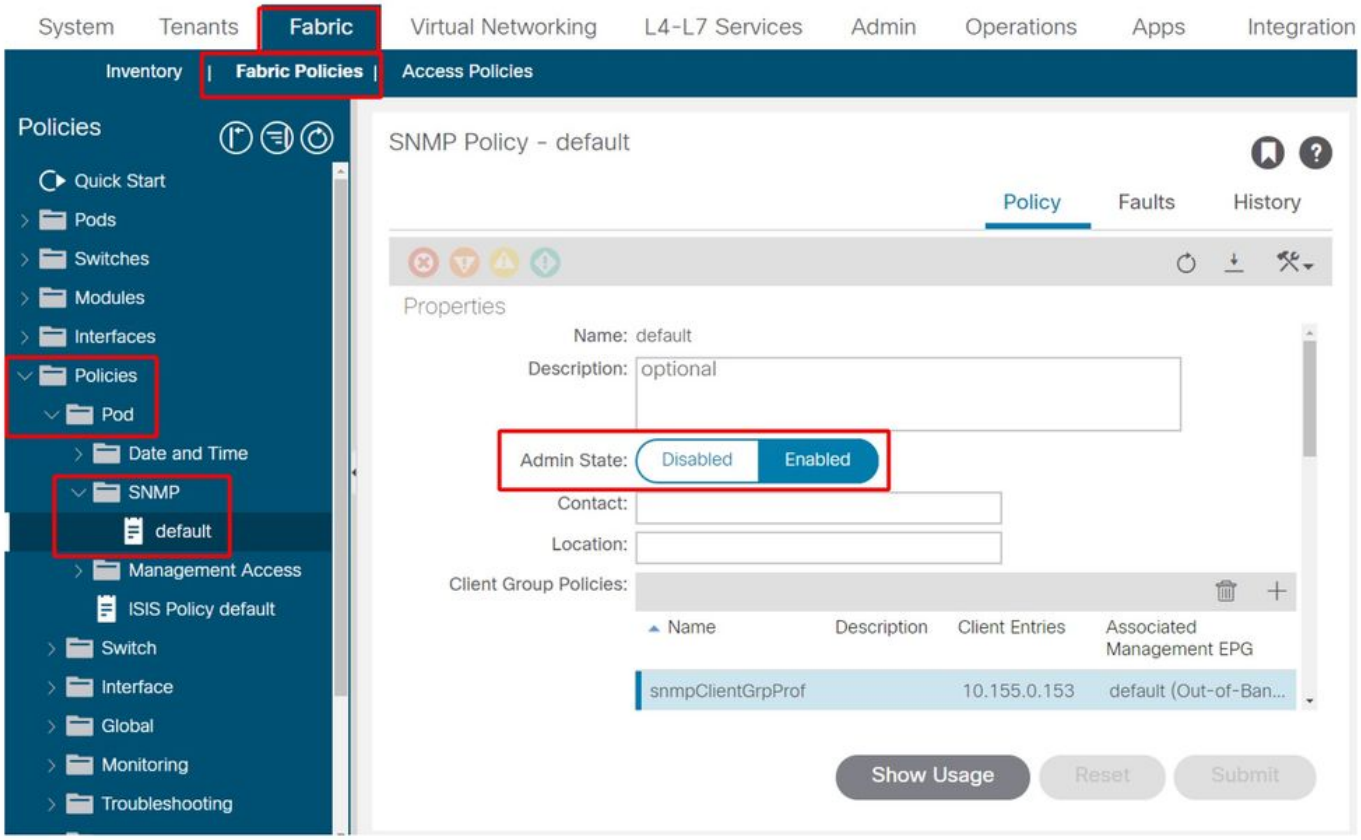


2. Política de Pod SNMP — Verifique se pelo menos uma Política de Comunidade está configurada

Políticas Pod — Política SNMP — Políticas da Comunidade



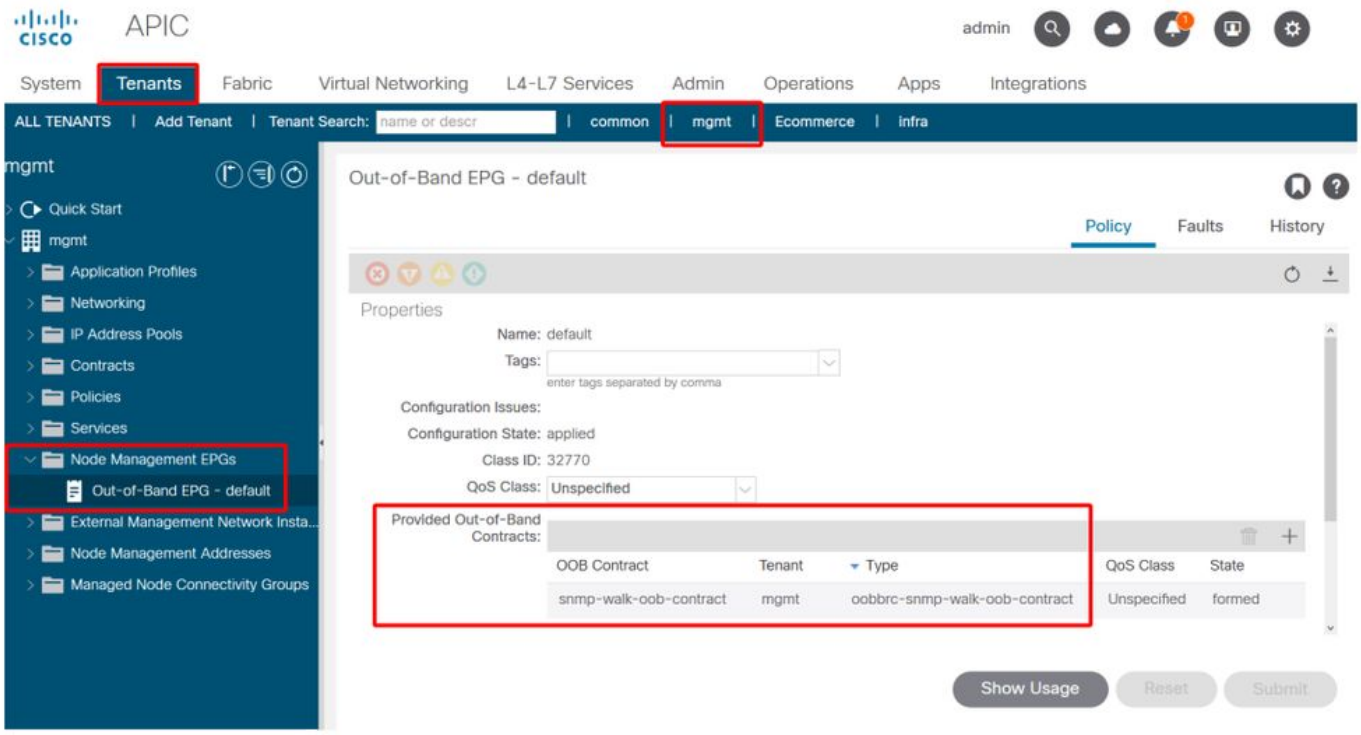
3. Política de Pod SNMP — Verifique se o Estado do Admin está definido como 'Habilitado'



4. Locatário de gerenciamento — verifique se o EPG OOB está fornecendo um Contrato OOB que permite a porta UDP 161

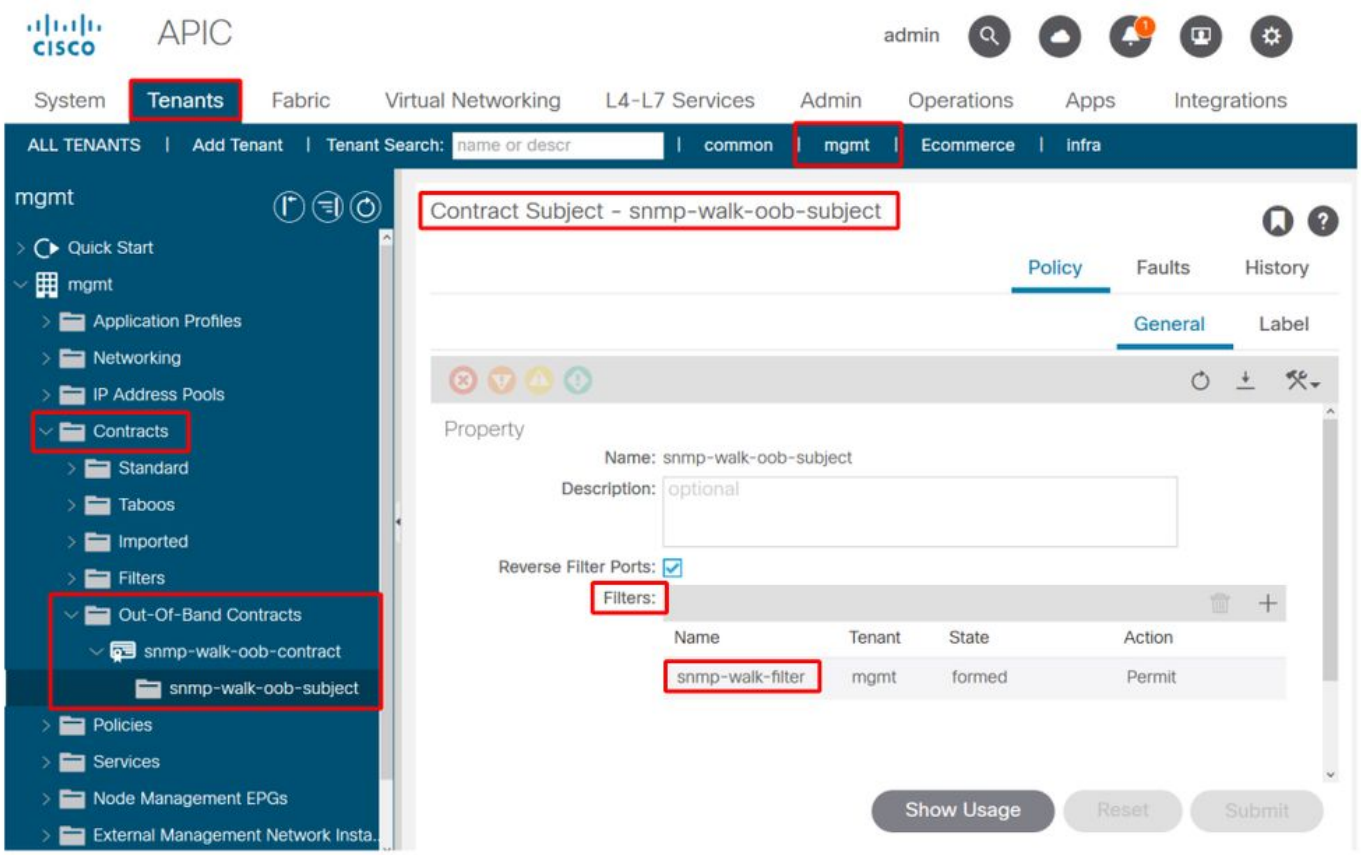
O EPG OOB controla a conectividade no APIC e nas portas de gerenciamento OOB do switch. Como tal, ela afeta todos os fluxos de tráfego que entram nas portas OOB.

Certifique-se de que o contrato fornecido aqui inclua todos os serviços de gerenciamento necessários em vez de apenas SNMP. Por exemplo: também precisa incluir pelo menos SSH (porta TCP 22). Sem isso, não é possível fazer login nos switches usando SSH. Observe que isso não se aplica aos APICs, pois eles têm um mecanismo para permitir SSH, HTTP, HTTPS para evitar que os usuários sejam bloqueados completamente.

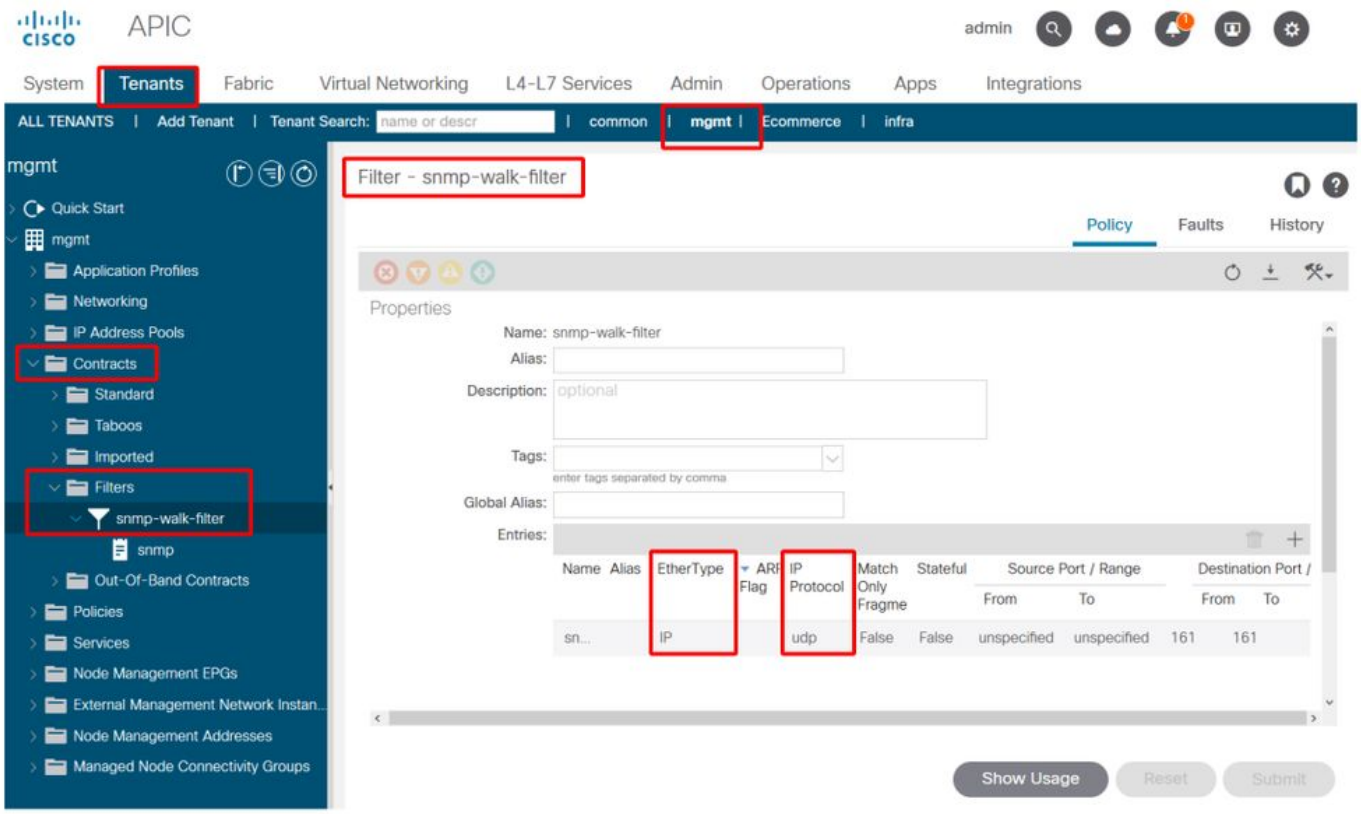


5. Locatário de gerenciamento — verifique se o Contrato OOB está presente e se tem um filtro que permita a porta UDP 161

Locatário de gerenciamento — OOB EPG — Contrato OOB fornecido



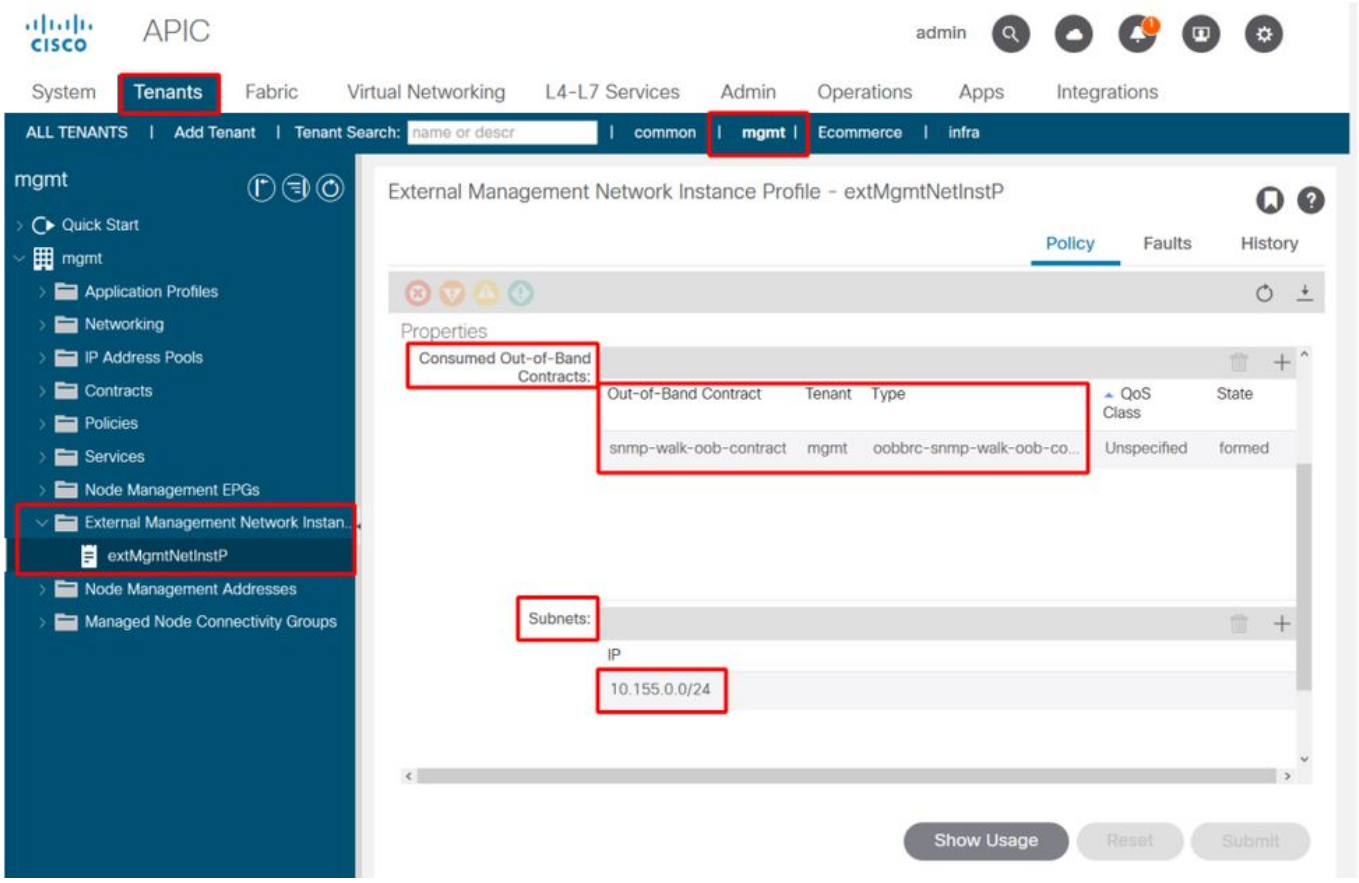
Na figura abaixo, não é obrigatório permitir apenas a porta UDP 161. Um contrato que tem um filtro que permite a porta UDP 161 de qualquer maneira está correto. Isso pode até ser um sujeito de contrato com o filtro padrão do espaço comum. Em nosso exemplo, para fins de clareza, um filtro específico foi configurado apenas para a porta UDP 161.



6. Locatário de gerenciamento — verifique se um Perfil de Instância de Rede de Gerenciamento Externo está presente com uma Sub-rede válida consumindo o Contrato OOB

O perfil da instância de rede de gerenciamento externo (ExtMgmtNetInstP) representa as fontes externas definidas pelas 'Sub-redes' que precisam consumir serviços acessíveis por meio do EPG OOB. Assim, o ExtMgmtNetInstP consome o mesmo contrato OOB fornecido pelo OOB EPG. Este é o contrato que permite a porta UDP 161. Além disso, ExtMgmtNetInstP também especifica os intervalos de sub-rede permitidos que podem consumir os serviços fornecidos pelo EPG OOB.

Locatário de gerenciamento — ExtMgmtNetInstP com contrato OOB e sub-rede consumidos



Como mostrado na figura acima, uma notação de sub-rede baseada em CIDR é necessária. A figura mostra uma sub-rede /24 específica. O requisito é que as entradas de sub-rede cubram as Entradas do Cliente SNMP conforme configurado na Política de Pod SNMP (consulte a Figura Políticas de Pod — Política SNMP — Políticas de grupo do cliente).

Como mencionado anteriormente, tenha cuidado ao incluir todas as sub-redes externas necessárias para evitar que outros serviços de gerenciamento necessários sejam bloqueados.

7. Faça login em um switch e execute um tcpdump para observar se os pacotes Walk SNMP — porta UDP 161 — são observados

Se os pacotes Walk de SNMP estiverem entrando em um switch através da porta OOB, isso significa que todas as políticas/parâmetros necessários baseados em SNMP e OOB foram configurados corretamente. Portanto, é um método de verificação adequado.

O Tcpdump nos nós de folha aproveita o shell do Linux e os dispositivos de rede do Linux. Portanto, é necessário capturar os pacotes na interface 'eth0' conforme o exemplo abaixo. No exemplo, um cliente SNMP está executando uma solicitação SNMP Get no OID .1.0.802.1.1.2.1.1.1.0.

```
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
```

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.