ACI管理とコアサービスのトラブルシューティング：ポッドポリシー

内容

概要

このドキュメントでは、ACIポッドポリシーの理解とトラブルシューティングの手順について説明します。

背景説明

このドキュメントの内容は、 Troubleshooting Cisco Application Centric Infrastructure, Second Edition 特にManagement and Core Servicesについて説明します **PODポリシー：BGP RR/日時/SNMP** 章

ポッドポリシーの概要

BGP RR、日時、SNMPなどの管理サービスは、ポッドポリシーグループを使用してシステムに適用されます。ポッドポリシーグループは、ACIファブリックの重要な機能に関連するポッドポリシーのグループを管理します。これらのポッドポリシーは次のコンポーネントに関連しており、その多くはデフォルトでACIファブリックでプロビジョニングされます。

ポッドポリシー

ポッドポリシー	手動設定が必要
日時	Yes
BGPルートリフレクタ	Yes
SNMP（サーバネットワーク管理プロトコル）	Yes
ISIS	No
クープ	No
管理アクセス	No
MAC秒	Yes

単一のACIファブリックでも、ポッドポリシーグループとポッドプロファイルを設定する必要があります。これは、マルチポッドやマルチサイト展開に固有のものではありません。この要件は、**すべての** ACI導入タイプに適用されます。

この章では、これらの重要なポッドポリシーと、それらが正しく適用されていることを確認する方法について説明します。

日時ポリシー

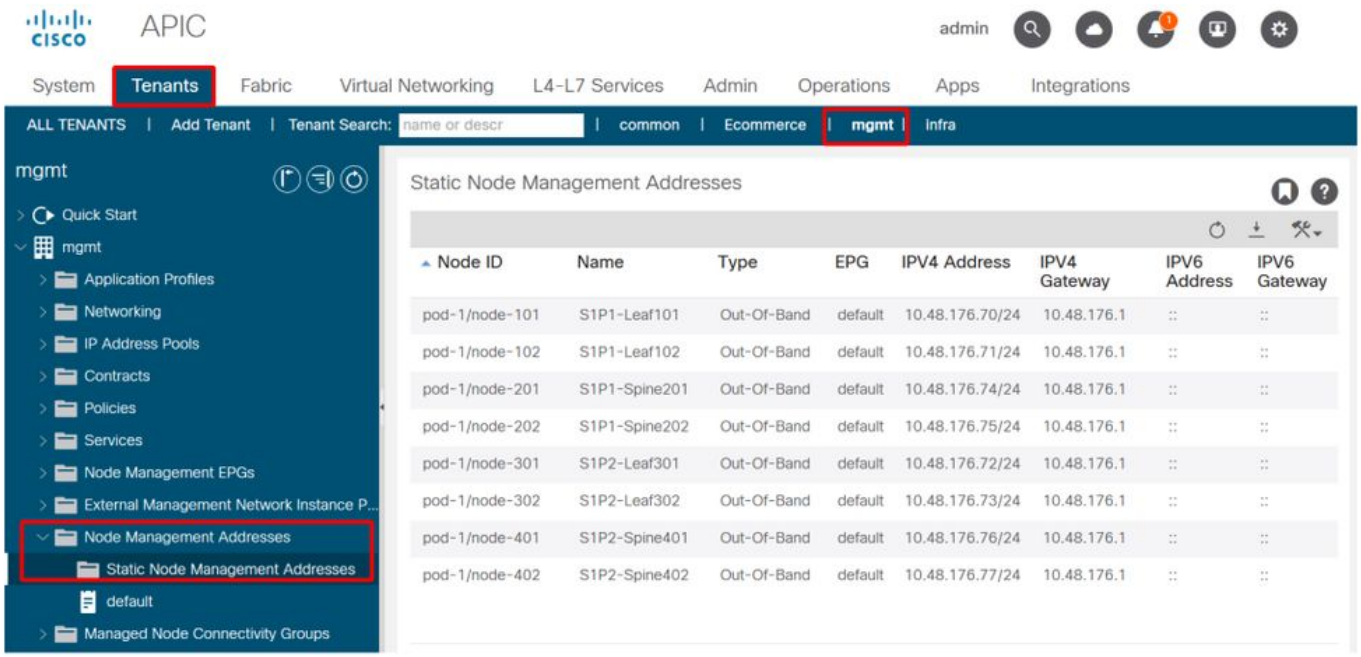
時刻の同期は、ACIファブリックにおいて重要な役割を果たします。証明書の検証から、APICおよびスイッチのログタイムスタンプの一貫性の維持まで、NTPを使用してACIファブリック内のノードを1つ以上の信頼できる時刻源と同期させることがベストプラクティスです。

ノードをNTPサーバプロバイダーに正しく同期させるには、ノードに管理アドレスを割り当てる依存関係があります。これは、管理テナントで静的ノード管理アドレスまたは管理ノード接続グループを使用して実行できます。

トラブルシューティングワークフロー

1.ノード管理アドレスがすべてのノードに割り当てられているかどうかを確認する

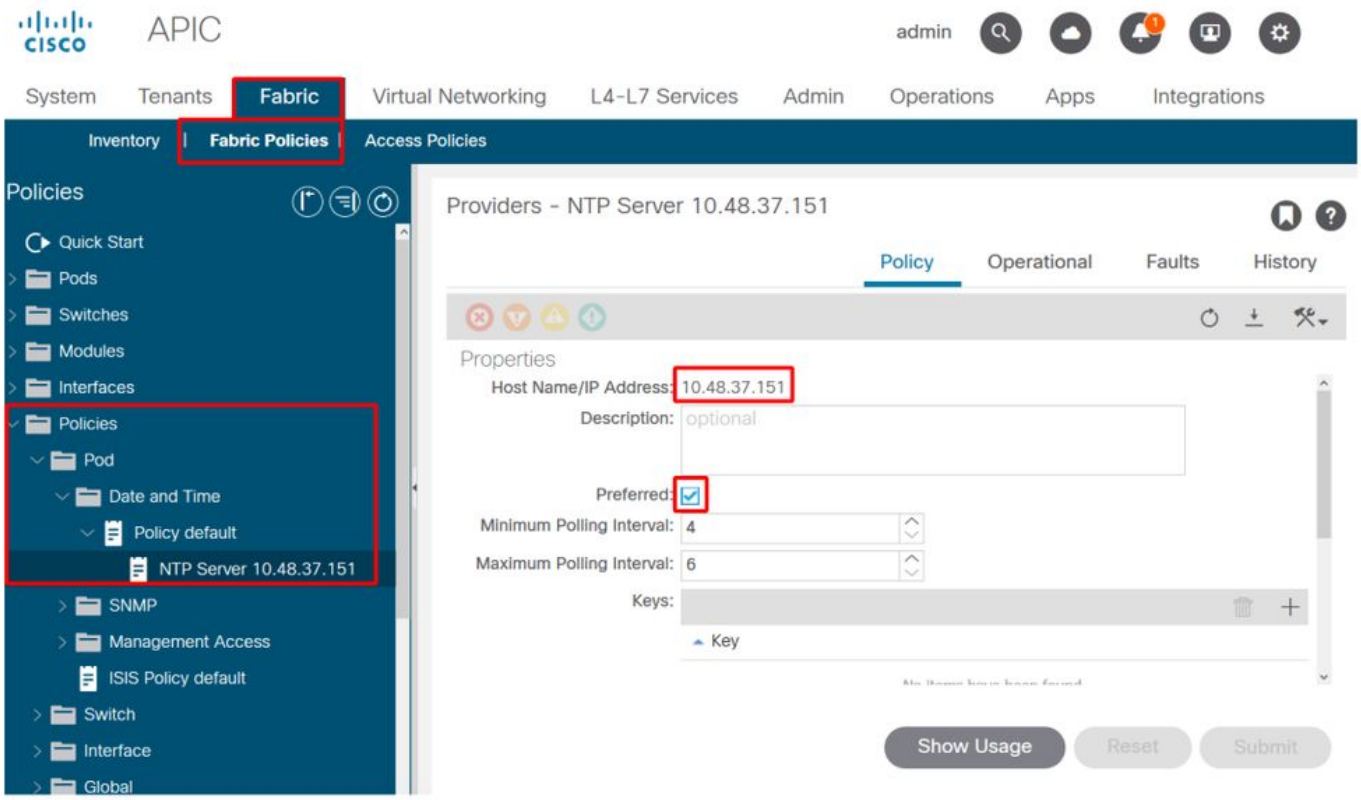
管理テナント – ノード管理アドレス



2. NTPサーバがNTPプロバイダーとして設定されているかどうかを確認する

複数のNTPプロバイダーが存在する場合は、次の図に示すように、[Preferred]チェックボックスを使用して、そのうちの少なくとも1つを優先タイムソースとしてフラグ付けします。

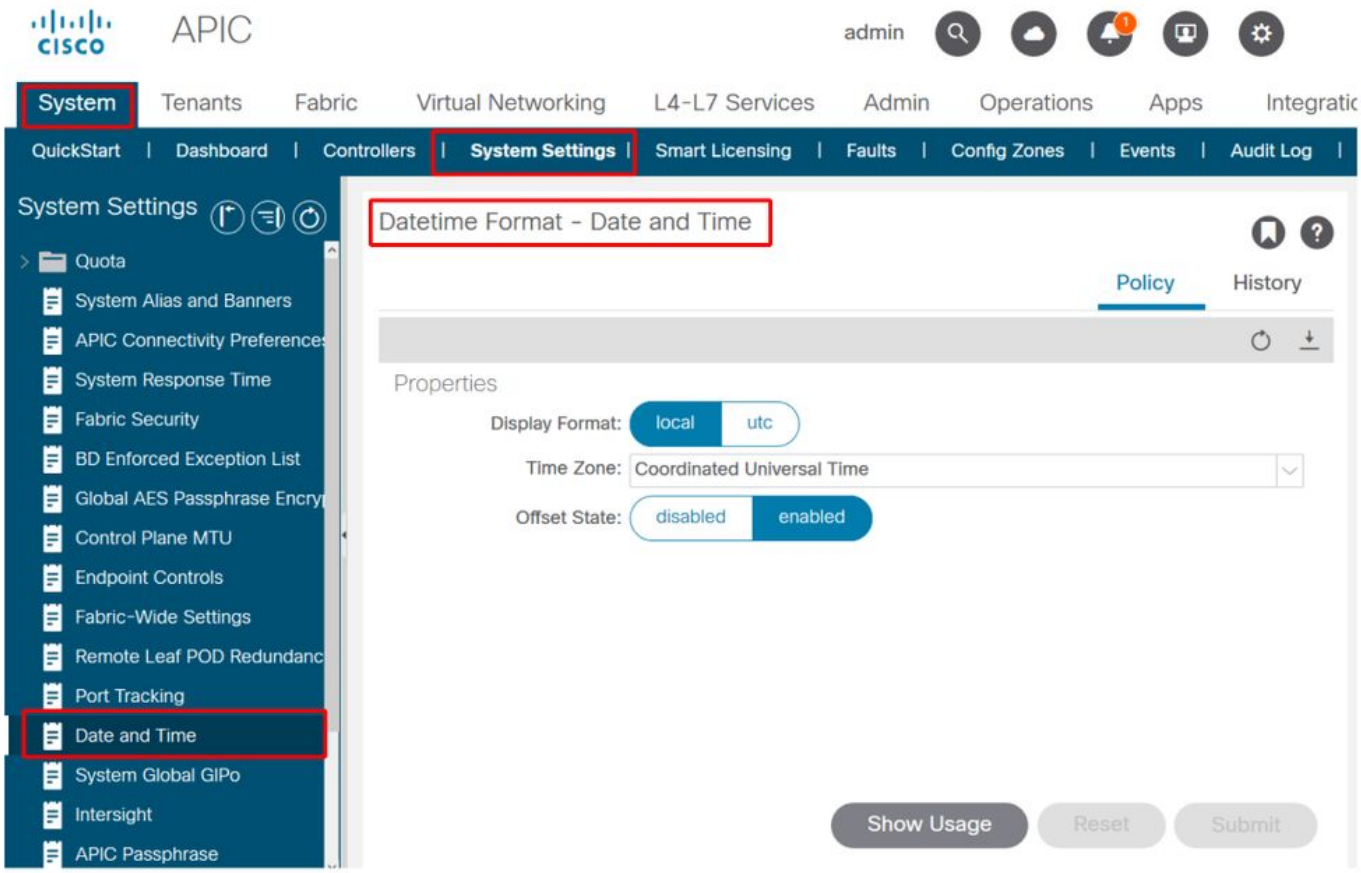
日時ポッドポリシーの下のNTPプロバイダー/サーバ



3.システム設定で日付と時刻の形式を確認します

次の図は、日付と時刻の形式がUTCに設定されている例を示しています。

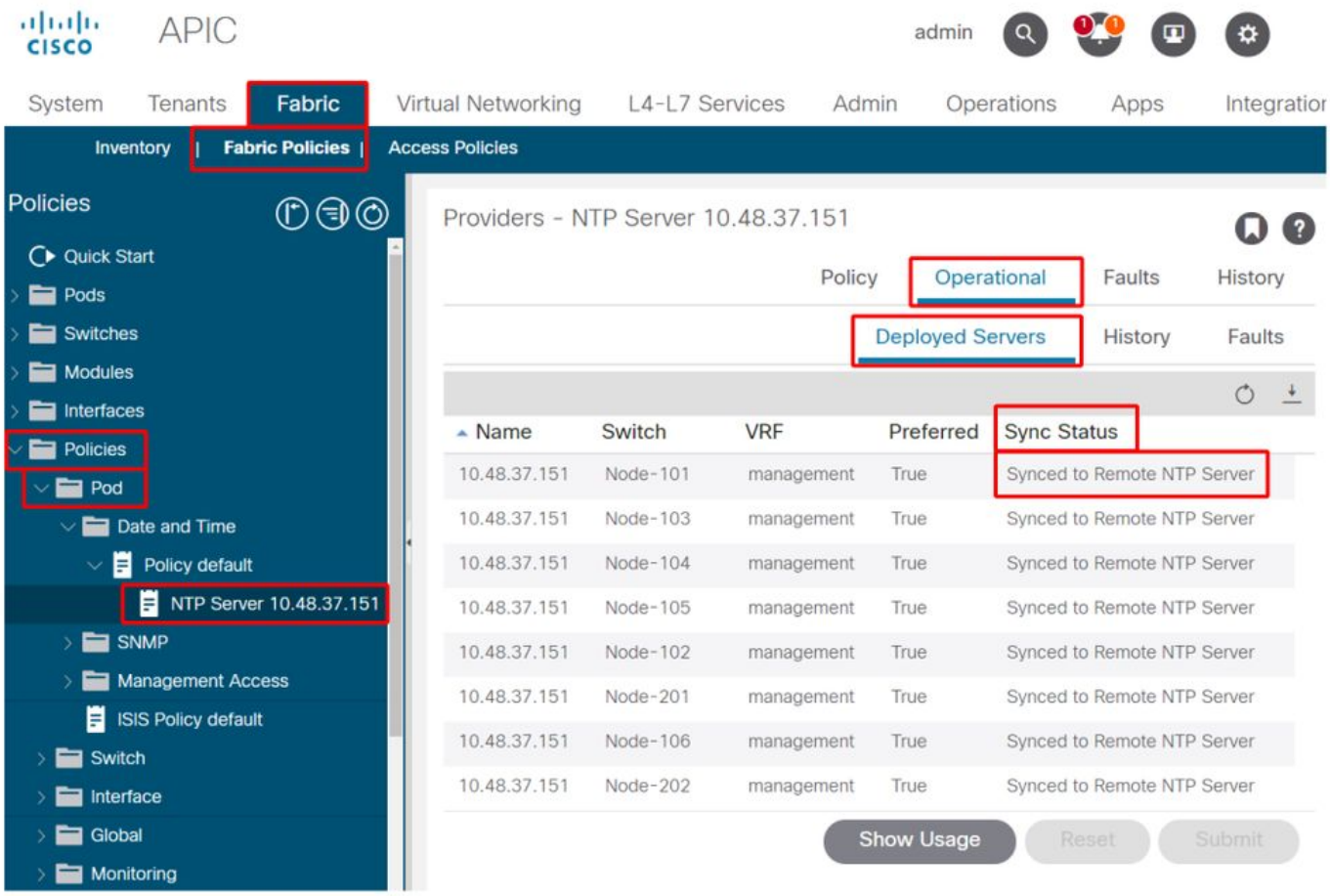
[システム設定]の[日付と時刻]の設定



4.すべてのノードに対するNTPプロバイダーの動作同期ステータスの確認

次の図に示すように、[Sync Status]列に[Synced to Remote NTP Server]と表示されます。 同期ステータスがリモートNTPサーバに正しく収束するまで数分かかることがあります。ステータス.

NTPプロバイダー/サーバの同期ステータス



また、APICとスイッチでCLI方式を使用して、NTPサーバに対する正しい時刻同期を確認することもできます。

APIC:NX-OS CLI

次の「refId」列は、ストラタムに応じてNTPサーバの次のタイムソースを示します。

```
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
```

最大 300 のアクセス ポイント グループ

「show ntp peers」コマンドを使用して、NTPプロバイダーの設定がスイッチに正しくプッシュされたことを確認します。

```
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
```

「*」文字は、NTPサーバが実際に同期に使用されているかどうかを制御するため、ここでは必須です。

次のコマンドで送受信されたパケットの数を確認し、ACIノードがNTPサーバに到達できることを確認します。

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

BGPルートリフレクタポリシー

ACIファブリックは、マルチプロトコルBGP(MP-BGP)、具体的にはリーフノードとスパインノード間のiBGP VPNv4を使用して、外部ルータ（L3Outに接続）から受信したテナントルートを交換します。 フルメッシュiBGPピアトポロジを回避するために、スパインノードはリーフからファブリック内の他のリーフノードに受信したVPNv4プレフィックスを反映します。

BGPルートリフレクタ(BGP RR)ポリシーがないと、BGPインスタンスはスイッチ上に作成されず、BGP VPNv4セッションは確立されません。マルチポッド導入では、各ポッドにBGP RRとして設定された少なくとも1つのスパインと、冗長性を確保するための実質的に複数のスパインが必要です。

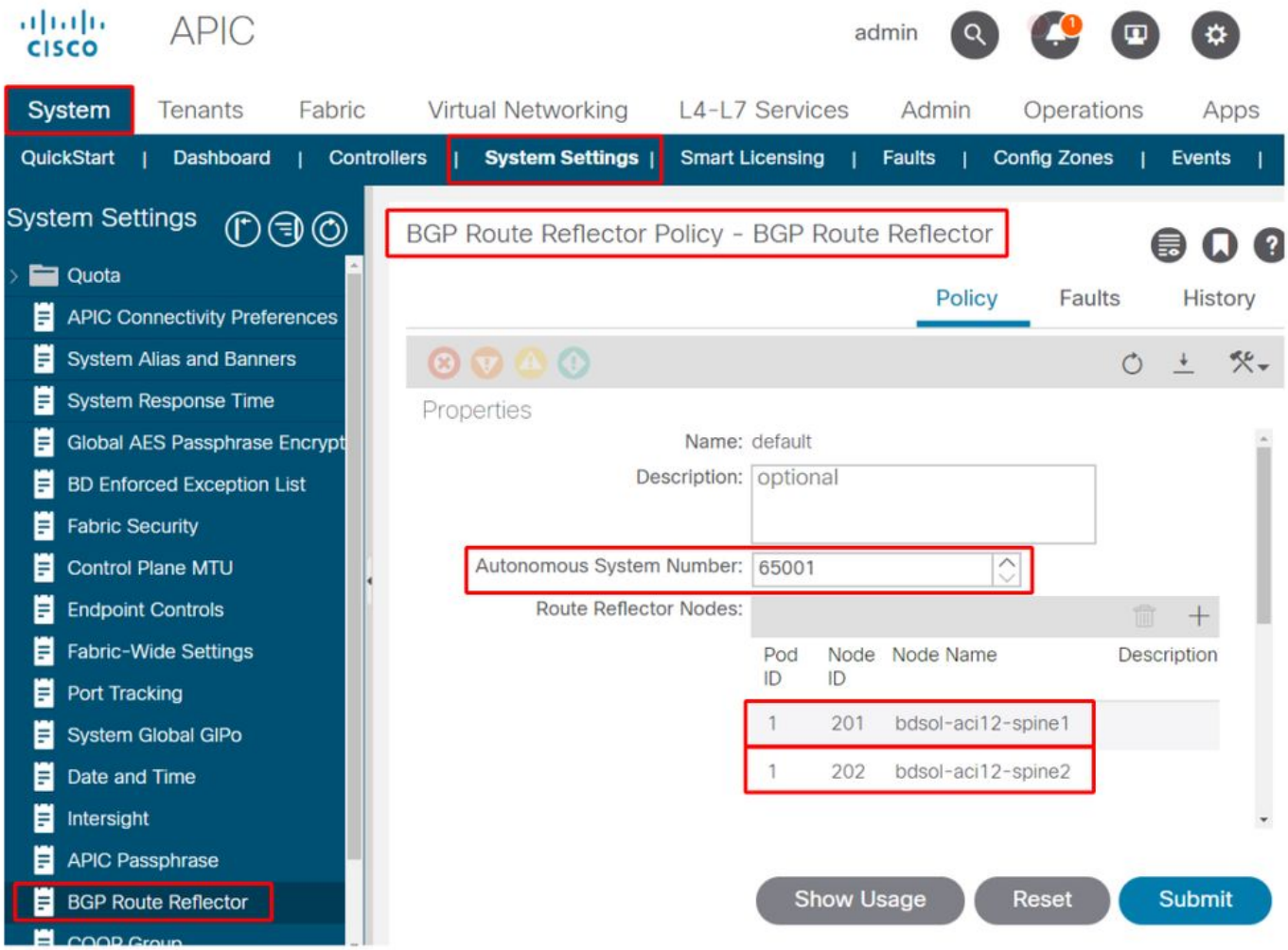
その結果、BGP RRポリシーは、すべてのACIファブリックの設定に不可欠な要素となります。BGP RRポリシーには、ACIファブリックが各スイッチのBGPプロセスに使用するASNも含まれています。

トラブルシューティングワークフロー

1. BGP RRポリシーにASNがあり、少なくとも1つのスパインが設定されているかどうかを確認します

次の例は、単一のPod導入を示しています。

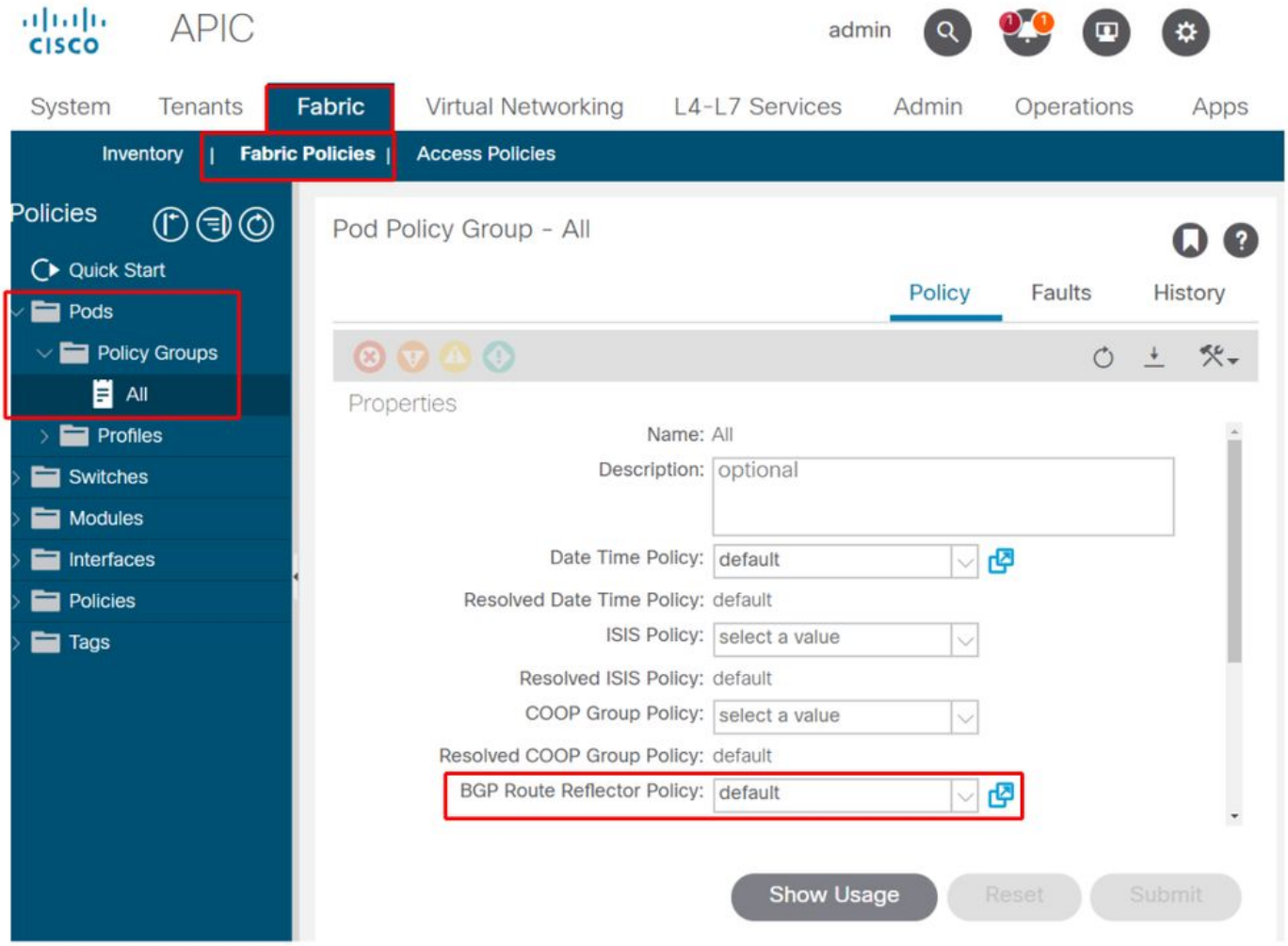
[System Settings]の[BGP Route Reflector Policy]



2. BGP RRポリシーがポッドポリシーグループに適用されているかどうかを確認します

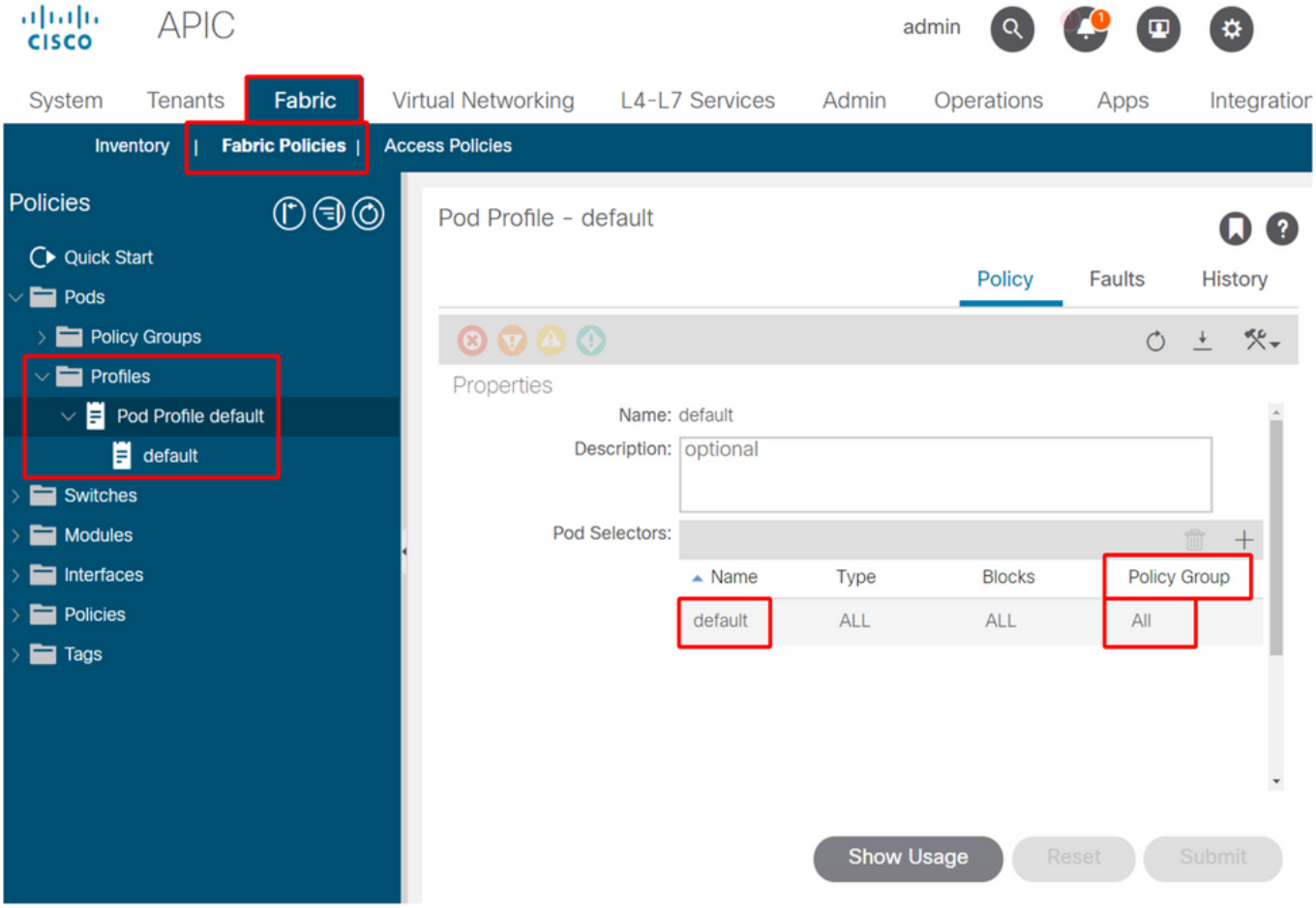
ポッドポリシーグループの下でデフォルトのBGP RRポリシーを適用します。エントリが空白の場合でも、デフォルトのBGP RRポリシーはポッドポリシーグループの一部として適用されます。

ポッドポリシーグループで適用されるBGPルートリフレクタポリシー



3.ポッドポリシーグループがポッドプロファイルに適用されているかどうかを確認します

ポッドプロファイルで適用されるポッドポリシーグループ



4.スパインにログインし、確立されたVPN4ピアセッションでBGPプロセスが実行されているかどうかを確認します

```
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
```

上に示すように、リーフノードとスパインノード間のMP-BGPは、VPNv4およびVPNv6アドレスファミリのみを伝送します。IPv4アドレスファミリは、リーフノード上のMP-BGPでのみ使用されます。

スパインノードとリーフノード間のBGP VPNv4およびVPNv6セッションも、次のコマンドを使用して簡単に確認できます。

```
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
```

上記の出力の「Up/Down」列に注目してください。BGPセッションが確立された時間を示すduration timeが表示されます。また、このACIファブリックにはL3Outsがまだ設定されていないため、外部ルート/プレフィクスがリーフノードとスパインノード間で交換されないため、例の「PfxRcd」列には、各BGP VPNv4/VPNv6ピアに対して0が表示されています。

5.リーフにログインし、確立されたVPN4ピアセッションでBGPプロセスが実行されているかどうかを確認します

```
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
```

上記のコマンド出力は、ACIファブリックに存在するスパインノードの数に等しいBGP VPNv4セッションの量を示しています。これは、スパインノードとは異なり、各リーフおよび他のルートリフレクタスパインノードへのセッションを確立します。

SNMP

このセクションで扱うSNMP機能の特定のサブセットを最初から明確にすることが重要です。ACIファブリックのSNMP機能は、SNMP Walk機能またはSNMP Trap機能に関連しています。ここでの重要な違いは、SNMP WalkがUDPポート161での**入力** SNMPトラフィックフローを制御するのに対し、SNMP TrapはUDPポート162でリスニングしているSNMP Trapサーバでの**発信** SNMPトラフィックフローを制御することです。

ACIノードの入力管理トラフィックでは、トラフィックのフローを許可するために必要なコントラクトを提供するために、ノード管理EPG（インバンドまたはアウトオブバンド）が必要です。したがって、これは入力SNMPトラフィックフローにも適用されます。

このセクションでは、ACIノード（APICおよびスイッチ）への入力SNMPトラフィックフロー（SNMPウォーク）について説明します。 出力SNMPトラフィックフロー（SNMPトラップ）については説明しません。出力SNMPトラフィックフロー（SNMPトラップ）については説明しません。出力SNMPトラフィックフローは、このセクションの範囲をモニタリングポリシーとモニタリングポリシーの依存関係（モニタリングポリシースコープ、モニタリングパッケージなど）に拡張します。

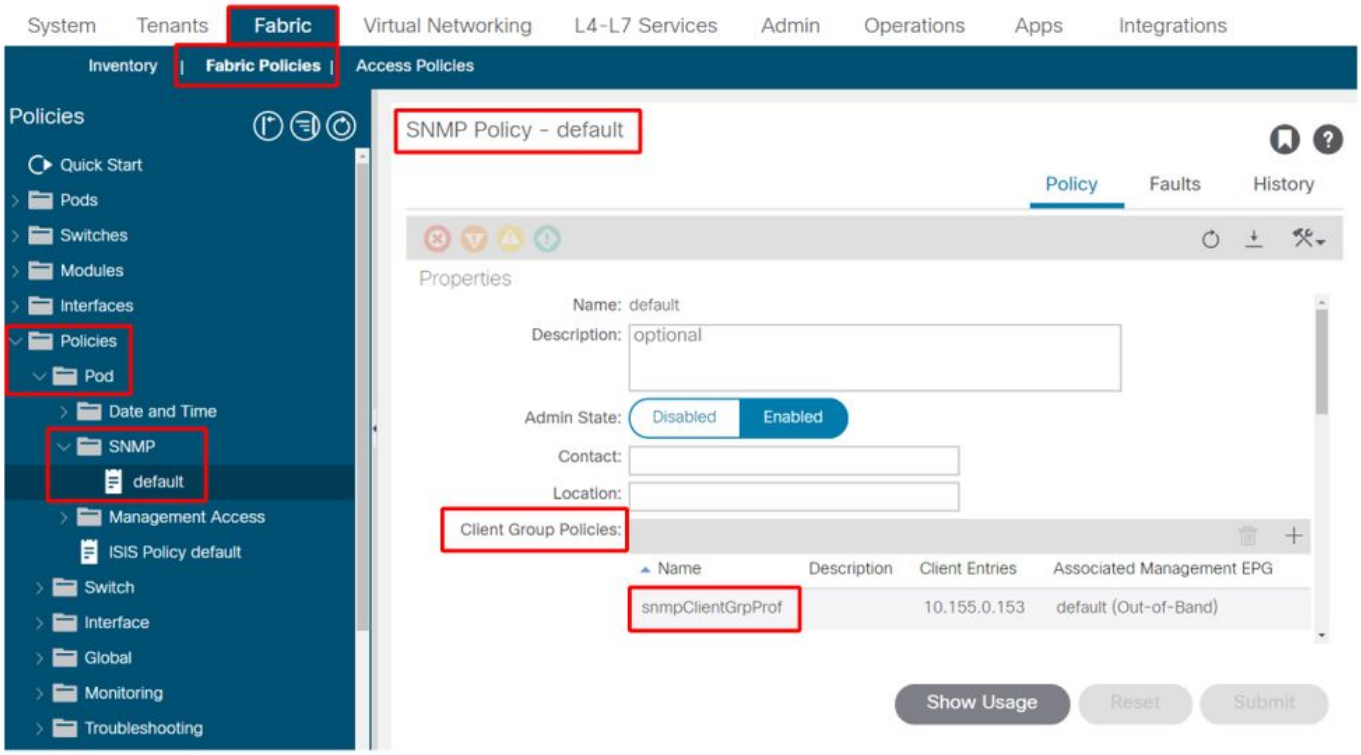
また、ACIでサポートされているSNMP MIBについても説明しません。この情報は、Cisco CCOのWebサイト(https://www.cisco.com/c/dam/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/mib/list/mib-support.html)で入手できます。

トラブルシューティングワークフロー

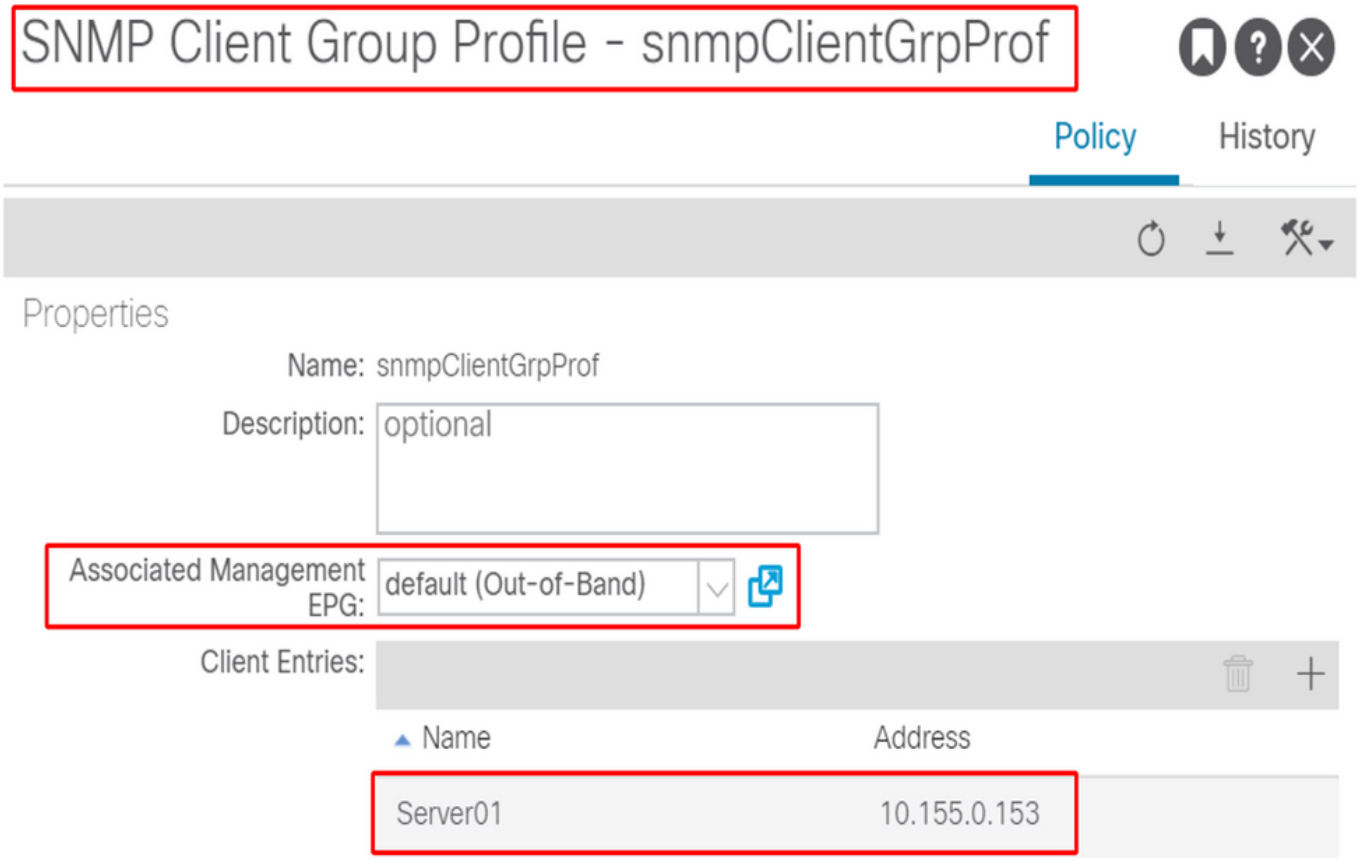
1. SNMPポッドポリシー：クライアントグループポリシーが設定されているかどうかを確認します

次のスクリーンショットに示すように、少なくとも1つのSNMPクライアントがクライアントグループポリシーの一部として設定されていることを確認します。

ポッドポリシー – SNMPポリシー – クライアントグループポリシー

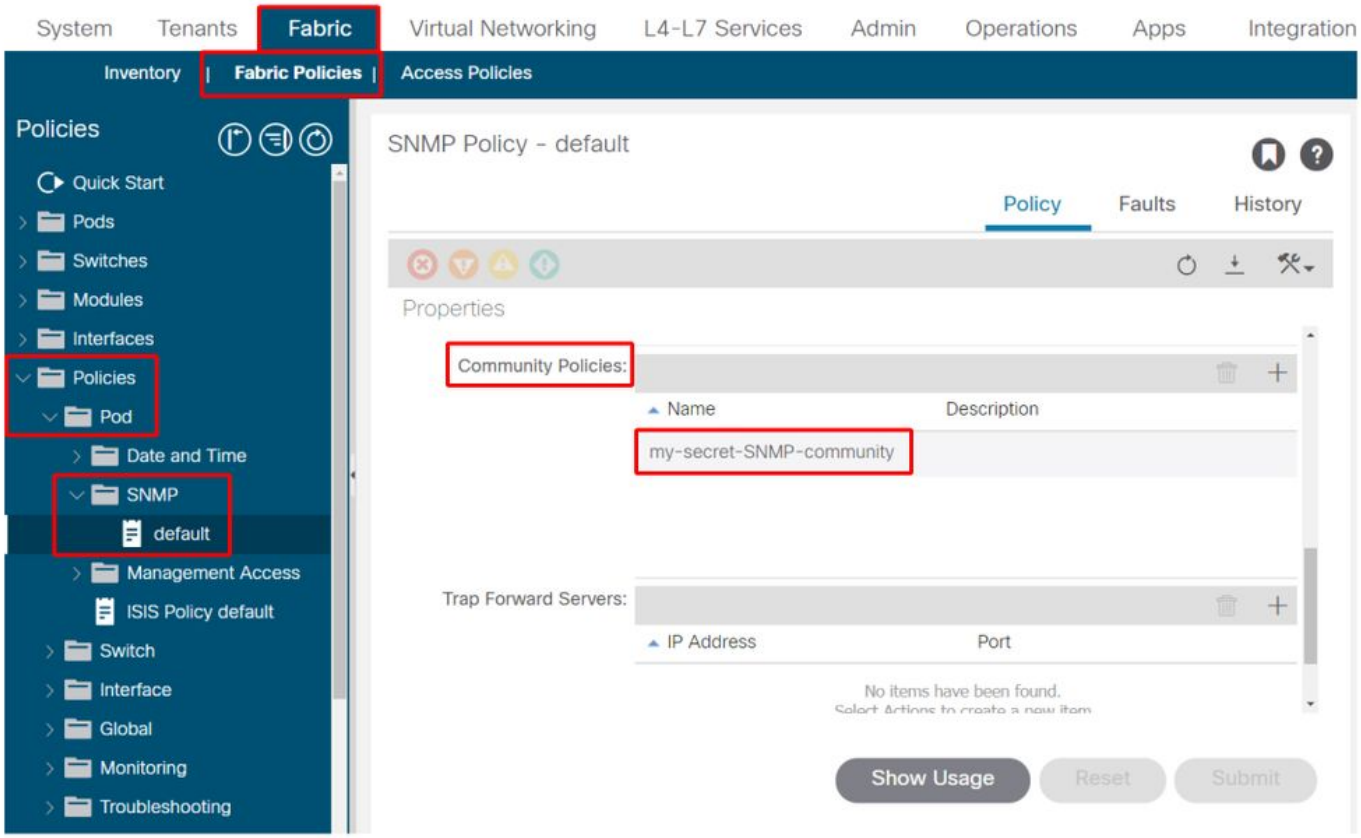


ポッドポリシー – SNMPポリシー – クライアントグループポリシー

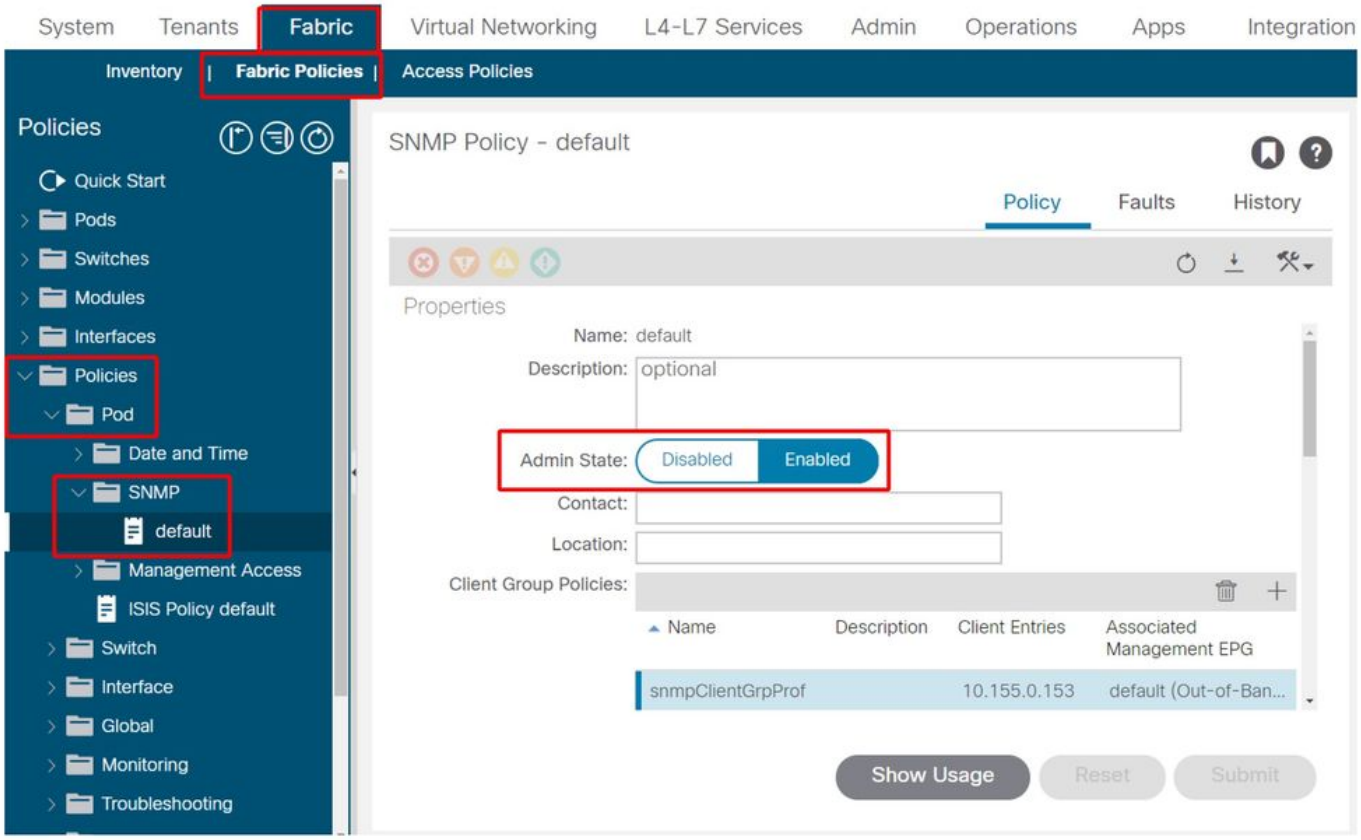


2. SNMPポッドポリシー：少なくとも1つのコミュニティポリシーが設定されているかどうかを確認します

ポッドポリシー：SNMPポリシー：コミュニティポリシー



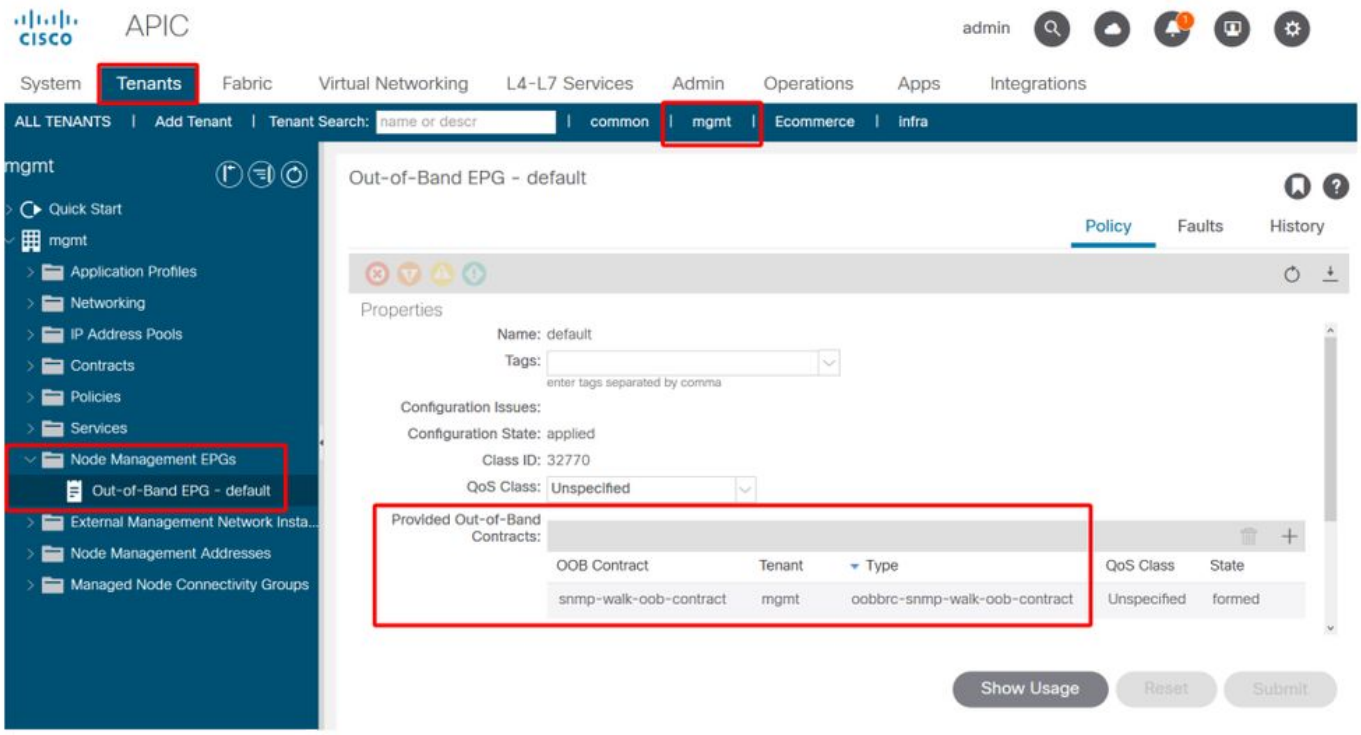
3. SNMPポッドポリシー：Admin Stateが[Enabled]に設定されているかどうかを確認します。



4.管理テナント：OOB EPGがUDPポート161を許可するOOBコントラクトを提供しているかどうかを確認します

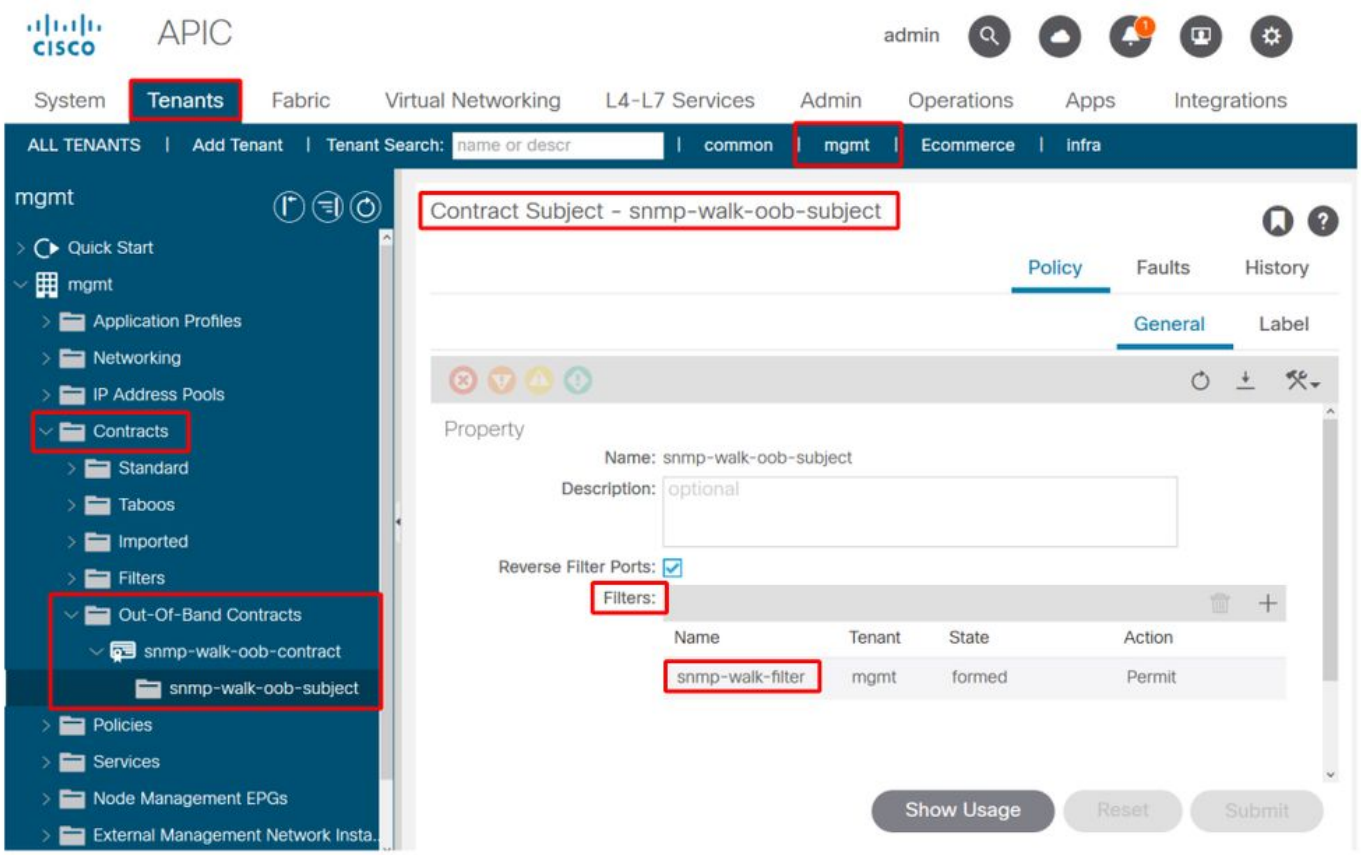
OOB EPGは、APICおよびスイッチのOOB管理ポートへの接続を管理します。そのため、OOBポートに入ってくるすべてのトラフィックフローに影響します。

ここで提供される契約に、SNMPだけでなく、必要なすべての管理サービスが含まれていることを確認します。以下に、いくつかの例を示します。また、少なくともSSH（TCPポート22）を含める必要があります。 これがないと、SSHを使用してスイッチにログインできません。APICにはSSH、HTTP、HTTPSを許可するメカニズムがあり、ユーザが完全にロックされるのを防ぐことができるため、これはAPICには適用されないことに注意してください。

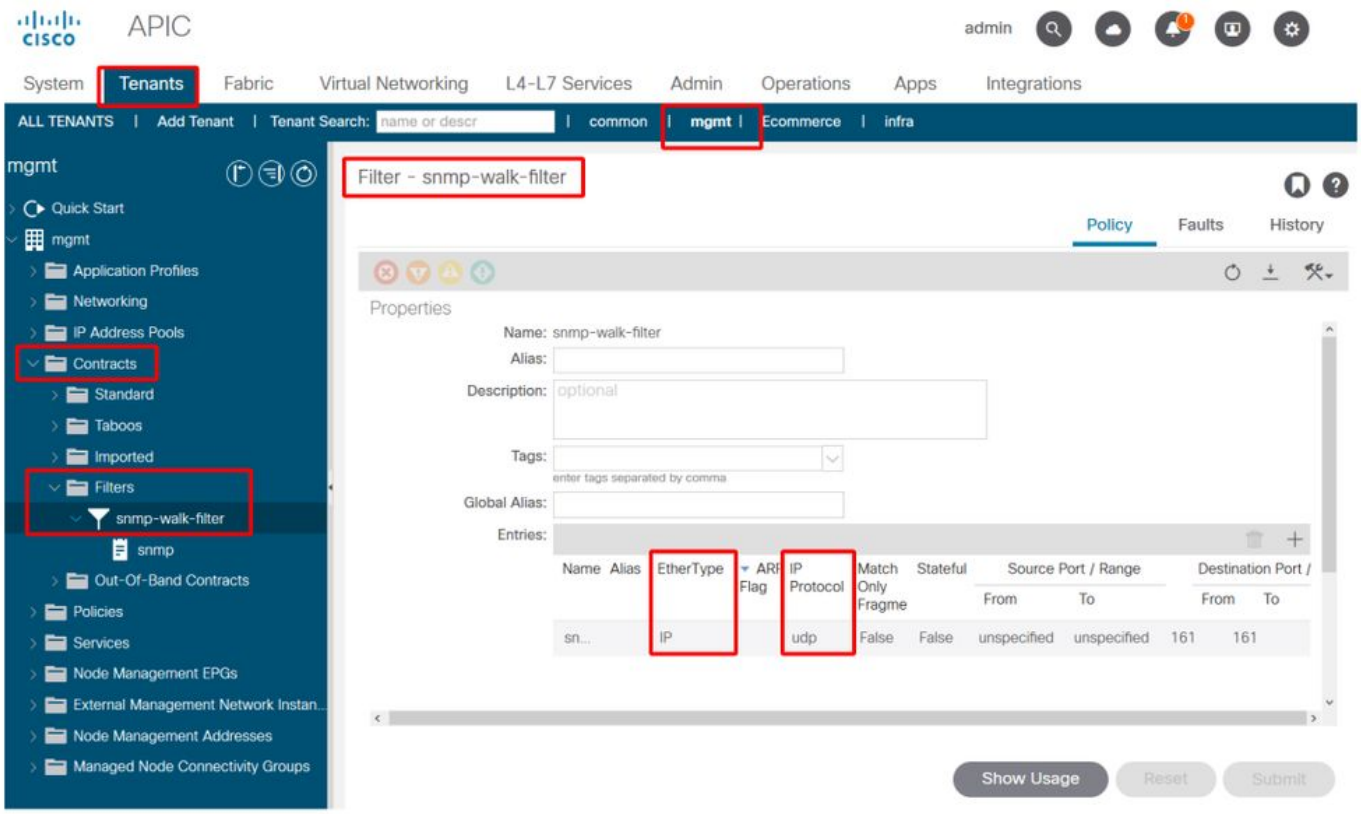


5.管理テナント：OOBコントラクトが存在し、UDPポート161を許可するフィルタが設定されていることを確認します

管理テナント – OOB EPG – 提供されたOOBコントラクト



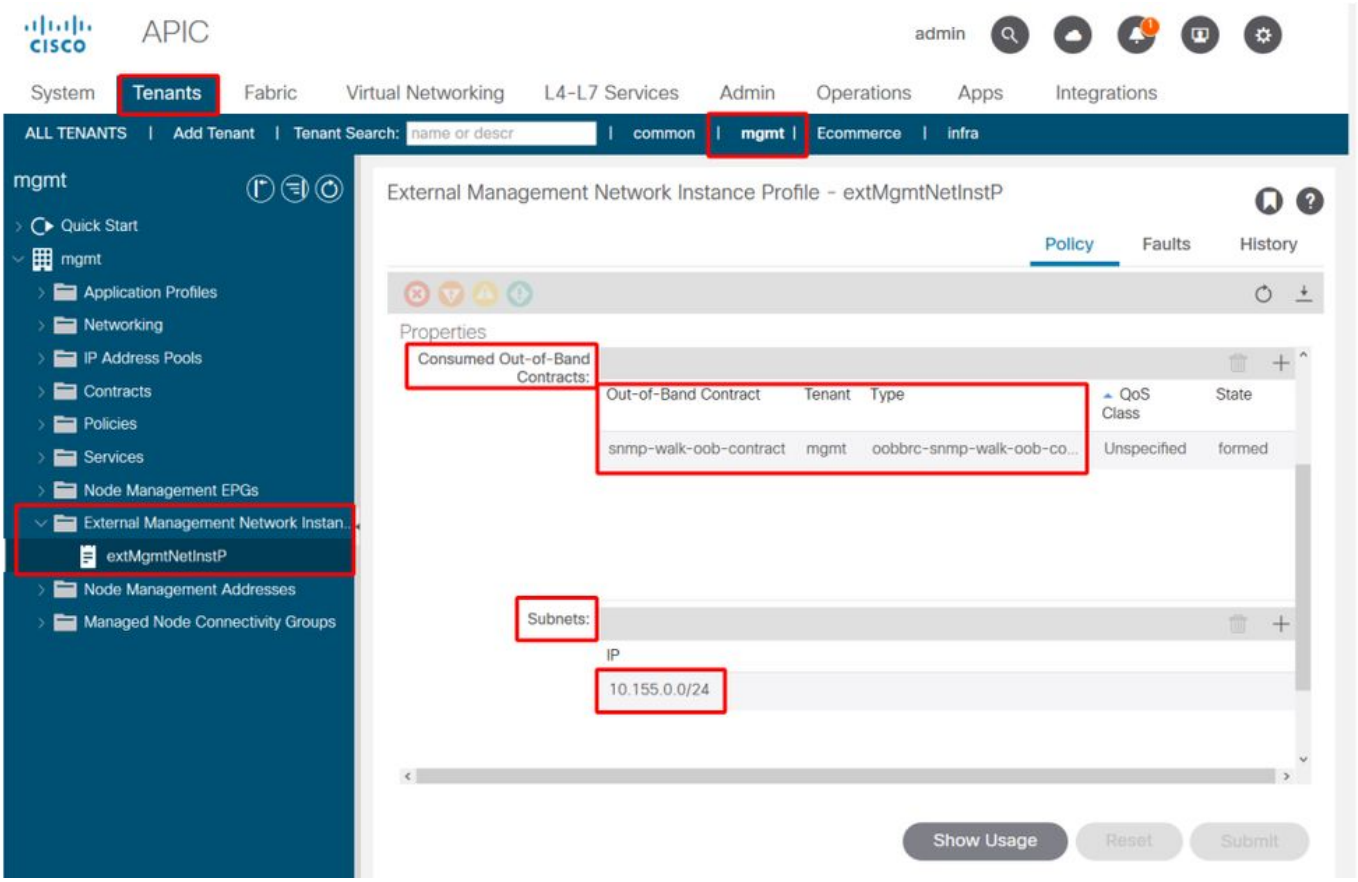
次の図では、UDPポート161だけを許可することは必須ではありません。どのような方法でもUDPポート161を許可するフィルタを持つコントラクトが正しいものです。これは、共通テナントのデフォルトフィルタを使用したコントラクト対象である場合もあります。この例では、分かりやすくするために、特定のフィルタはUDPポート161だけに設定されています。



6.管理テナント：外部管理ネットワークインスタンスプロファイルが、OOBコントラクトを使用する有効なサブネットに存在するかどうかを確認します

外部管理ネットワークインスタンスプロファイル(ExtMgmtNetInstP)は、OOB EPG経由で到達可能なサービスを消費する必要がある、内部の「サブネット」によって定義された外部ソースを表します。したがって、ExtMgmtNetInstPはOOB EPGによって提供されるのと同じOOB契約を消費します。これはUDPポート161を許可するコントラクトです。さらに、ExtMgmtNetInstPは、OOB EPGによって提供されるサービスを消費する可能性のある許可されたサブネット範囲も指定します。

管理テナント：使用されたOOBコントラクトとサブネットを持つExtMgmtNetInstP



上の図に示すように、CIDRベースのサブネット表記が必要です。図は、特定の/24サブネットを示しています。要件は、サブネットエントリが、SNMPポッドポリシーで設定されたSNMPクライアントエントリをカバーすることです（図「ポッドポリシー – SNMPポリシー – クライアントグループポリシー」を参照）。

前述したように、他の必要な管理サービスがロックアウトされないように、必要なすべての外部サブネットを含めるよう注意してください。

7.スイッチにログインし、tcpdumpを実行して、SNMP Walkパケット（UDPポート161）が観察されるかどうかを確認します

SNMP WalkパケットがOOBポートを介してスイッチに入る場合、これは必要なすべてのSNMPおよびOOBベースのポリシー/パラメータが適切に設定されていることを意味します。したがって、これは適切な検証方法です。

リーフノードのtcpdumpは、LinuxシェルとLinuxネットデバイスを利用します。したがって、次の例のように、インターフェイス「eth0」上のパケットをキャプチャする必要があります。この例では、SNMPクライアントがOID .1.0.8802.1.1.2.1.1.1.0に対してSNMP Get要求を実行しています。

```
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
```

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。