ACI 관리 및 코어 서비스 문제 해결 - 포드 정책

목차

소개

이 문서에서는 ACI 포드 정책을 이해하고 문제를 해결하는 단계에 대해 설명합니다.

배경 정보

이 문서의 자료는 Cisco Application Centric Infrastructure, Second Edition 트러블슈팅 특히 관리 및 코어 서비스, **POD 정책 - BGP RR/날짜 및 시간/SNMP** 장.

Pod 정책 개요

BGP RR, Date & Time 및 SNMP와 같은 관리 서비스는 포드 정책 그룹을 사용하여 시스템에 적용됩니다. Pod 정책 그룹은 ACI 패브릭의 필수 기능과 관련된 Pod 정책 그룹을 제어합니다. 이러한 Pod 정책은 다음 구성 요소와 관련되며, 그중 상당수는 기본적으로 ACI 패브릭에서 프로비저닝됩니다.

포드 정책

Pod 정책	수동 컨피그레이션 필요
날짜 및 시간	예
BGP 경로 리플렉터	예
SNMP(서버 네트워크 관리 프로토콜)	예
ISIS	아니요
우리	아니요
관리 액세스	아니요
MAC Sec	예

단일 ACI 패브릭에서도 포드 정책 그룹 및 포드 프로필을 구성해야 합니다. 이는 멀티 포드 또는 멀티 사이트 구축에 국한되지 않습니다. 이 요건은 **모든** ACI 구축 유형에 적용됩니다.

이 장에서는 이러한 필수 포드 정책 및 해당 정책이 올바르게 적용되었는지 확인하는 방법에 대해

중점적으로 설명합니다.

날짜 및 시간 정책

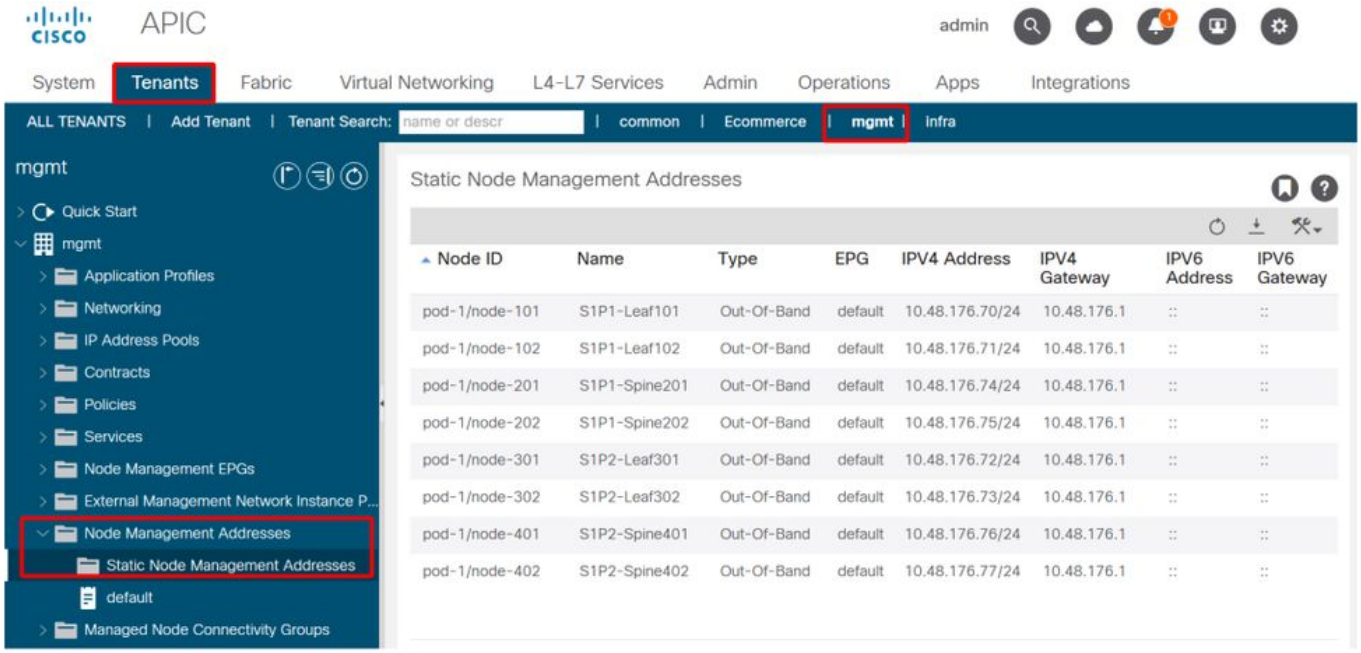
시간 동기화는 ACI 패브릭에서 중요한 역할을 합니다. 인증서 검증에서 APIC 및 스위치의 로그 타임스탬프를 일관되게 유지하는 것까지, NTP를 사용하여 ACI 패브릭의 노드를 하나 이상의 신뢰할 수 있는 시간 소스에 동기화하는 것이 모범 사례입니다.

노드를 NTP 서버 공급자에 올바르게 동기화하려면 관리 주소가 있는 노드를 할당해야 합니다. 이 작업은 관리 테넌트에서 고정 노드 관리 주소 또는 관리 노드 연결 그룹을 사용하여 수행할 수 있습니다.

문제 해결 워크플로

1. 노드 관리 주소가 모든 노드에 할당되었는지 확인합니다

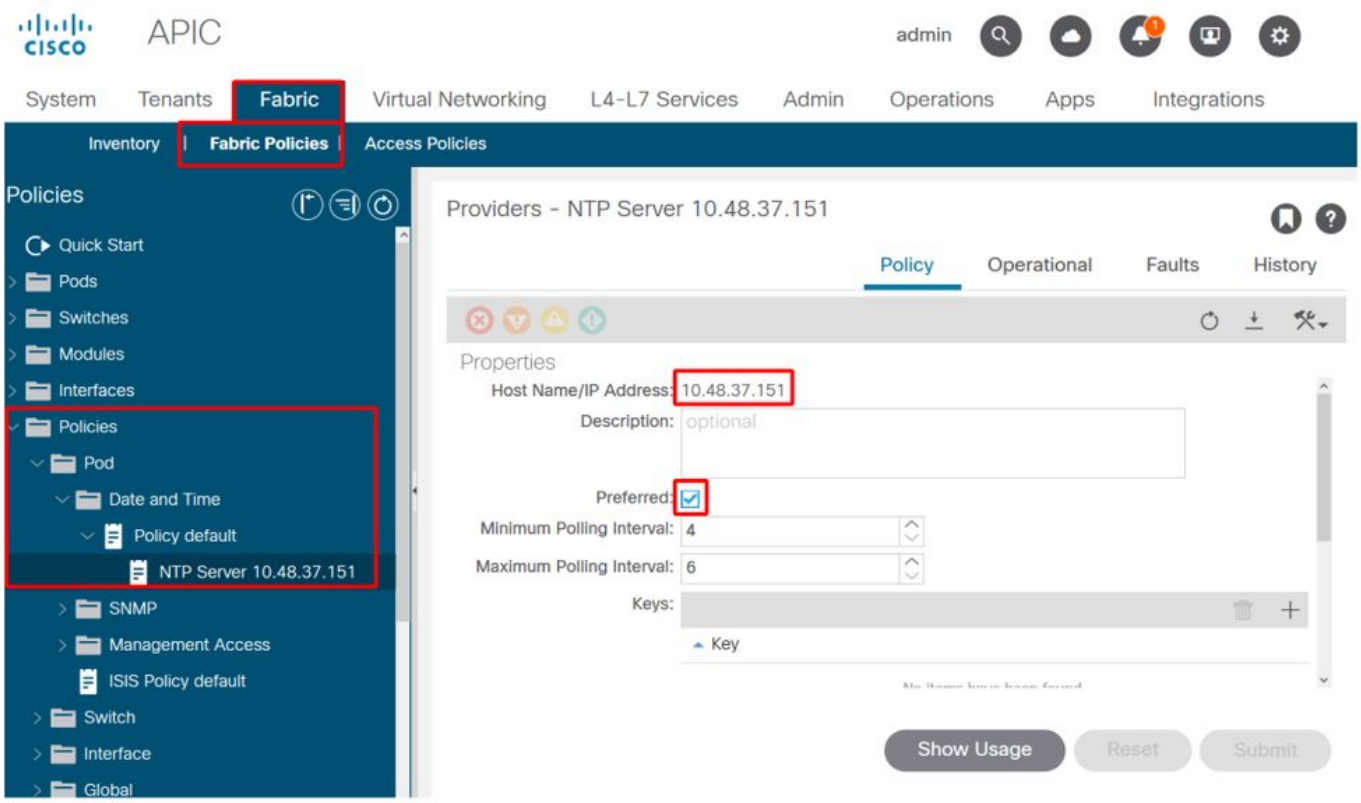
관리 테넌트 - 노드 관리 주소



2. NTP 서버가 NTP 제공자로 구성되었는지 확인합니다

여러 NTP 제공자가 있는 경우 아래 그림에 따라 '기본 설정' 확인란을 사용하여 하나 이상을 기본 설정 시간 소스로 플래그 지정합니다.

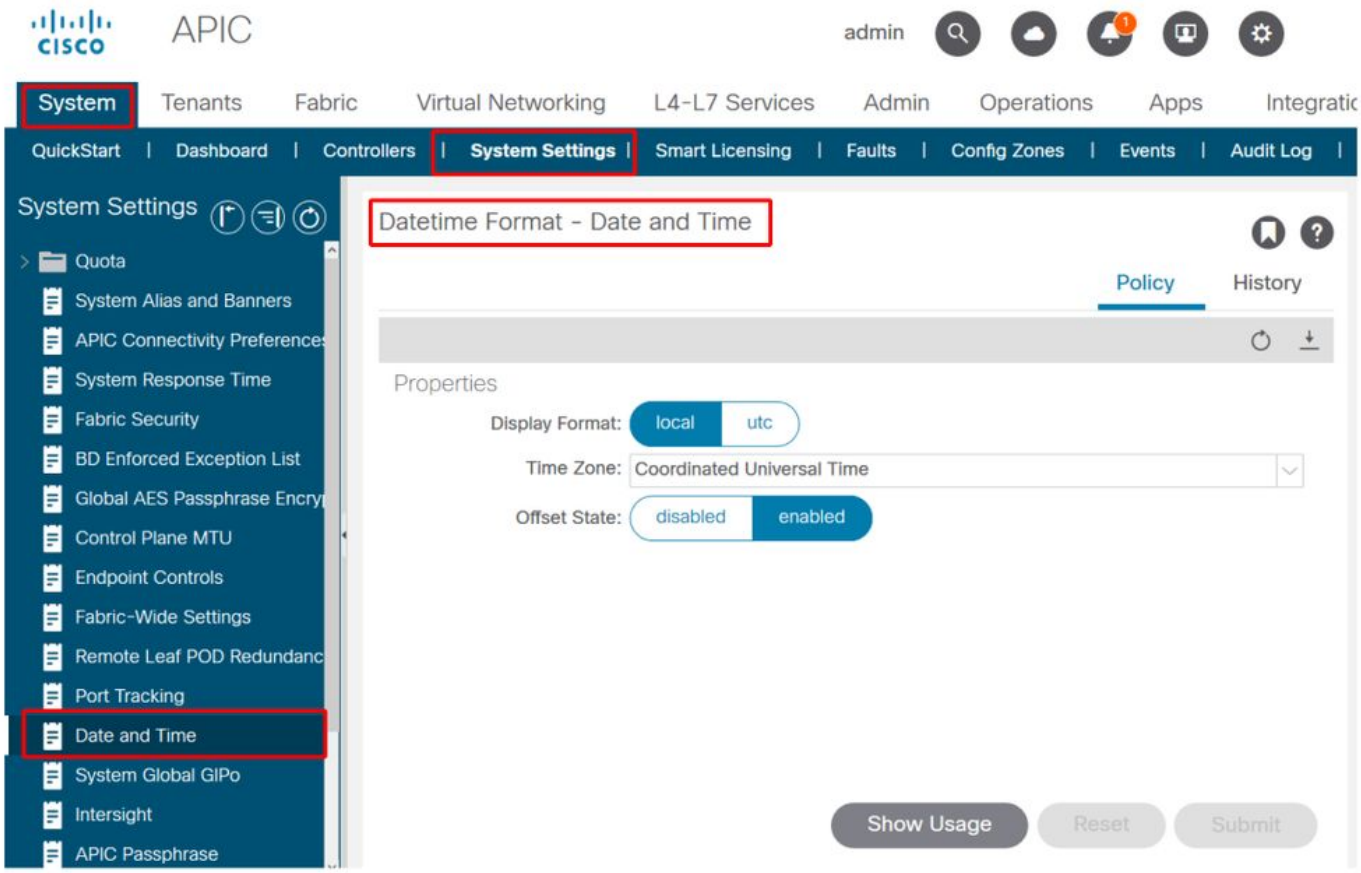
날짜 및 시간 포드 정책의 NTP 제공자/서버



3. 시스템 설정에서 날짜 및 시간 형식을 확인합니다

아래 그림에서는 날짜 및 시간 형식이 UTC로 설정된 예를 보여 줍니다.

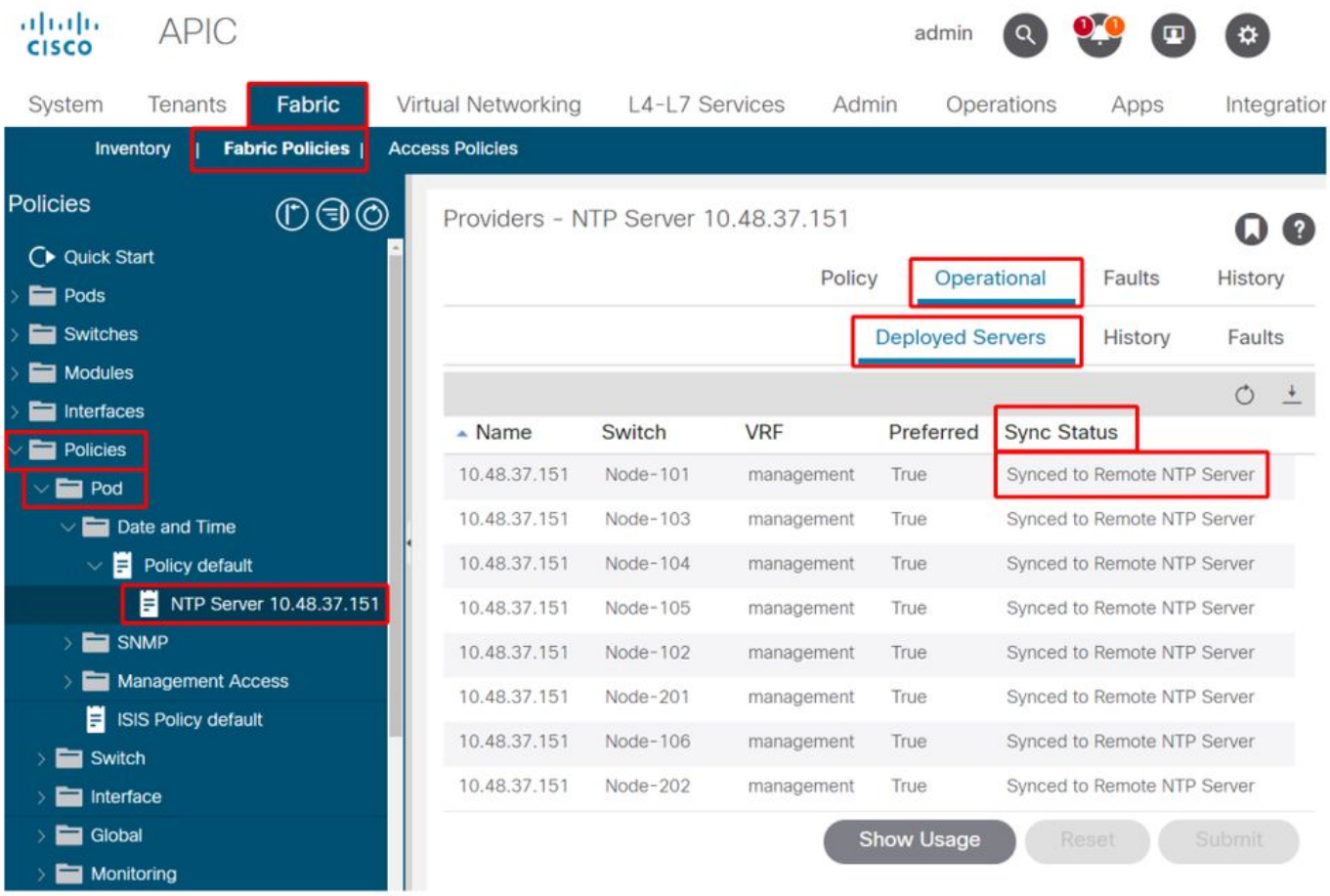
시스템 설정의 날짜 및 시간 설정



4. 모든 노드에 대한 NTP 제공자의 작동 동기화 상태를 확인합니다

아래 그림과 같이 Sync Status(동기화 상태) 열에 'Synced to Remote NTP Server(원격 NTP 서버에 동기화됨)'가 표시되어야 합니다. 동기화 상태가 .Synced to Remote NTP Server(원격 NTP 서버에 동기화됨)로 올바르게 통합되는 데 몇 분 정도 걸릴 수 있습니다. 상태.

NTP 제공자/서버 동기화 상태



또는 APIC 및 스위치에서 CLI 방법을 사용하여 NTP 서버에 대한 올바른 시간 동기화를 확인할 수 있습니다.

APIC - NX-OS CLI

아래의 'refId' 열은 계층에 따라 다음 번에 NTP 서버를 표시합니다.

```
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 - 바시

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

스위치

NTP 제공자 컨피그레이션이 스위치에 올바르게 푸시되었는지 확인하려면 'show ntp peers' 명령을 사용합니다.

```
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
```

'*' 문자는 NTP 서버가 실제로 동기화에 사용되는지 여부를 제어하므로 여기에서 반드시 사용해야 합니다.

ACI 노드가 NTP 서버에 연결할 수 있는지 확인하려면 다음 명령에서 전송/수신된 패킷 수를 확인합니다.

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

BGP 경로 리플렉터 정책

ACI 패브릭은 MP-BGP(Multi-Protocol BGP), 특히 leaf 노드와 spine 노드 간의 iBGP VPNv4를 사용하여 외부 라우터(L3Outs에 연결됨)에서 수신한 테넌트 경로를 교환합니다. 풀 메시 iBGP 피어 토폴로지를 피하기 위해 스파인 노드는 leaf에서 패브릭의 다른 leaf 노드로 수신된 VPNv4 접두사를 반영합니다.

BGP RR(Route Reflector) 정책이 없으면 스위치에서 BGP 인스턴스가 생성되지 않으며 BGP VPNv4 세션이 설정되지 않습니다. 멀티 포드 구축에서 각 포드에는 BGP RR로 구성된 스파인이 하나 이상 필요하며 이중화를 위해 하나 이상 필요합니다.

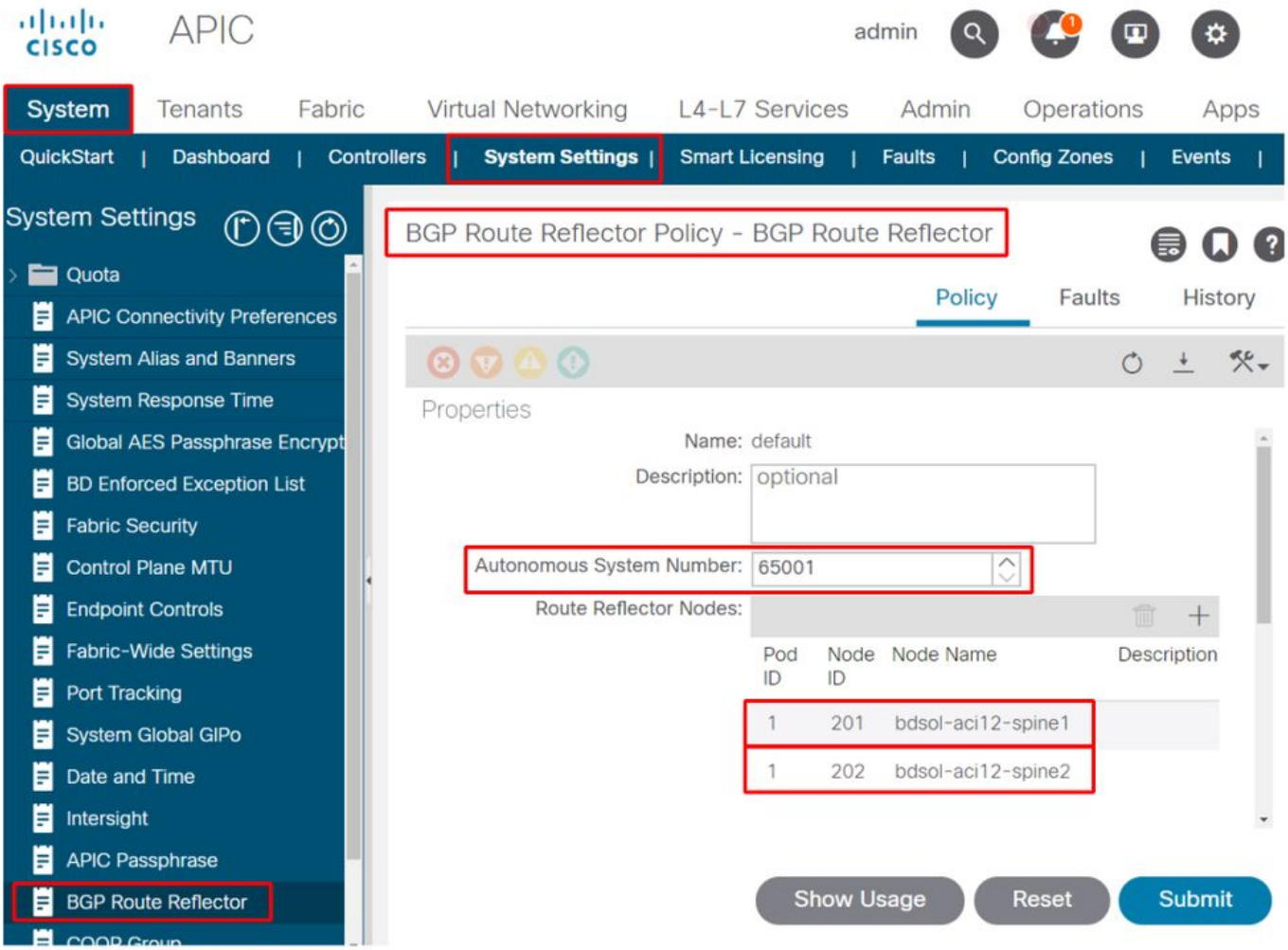
따라서 BGP RR 정책은 모든 ACI 패브릭에서 필수적인 컨피그레이션입니다. BGP RR 정책에는 ACI 패브릭이 각 스위치의 BGP 프로세스에 사용하는 ASN도 포함됩니다.

문제 해결 워크플로

1. BGP RR 정책에 ASN 및 하나 이상의 스파인이 구성되어 있는지 확인합니다

아래 예는 단일 Pod 구축을 가리킵니다.

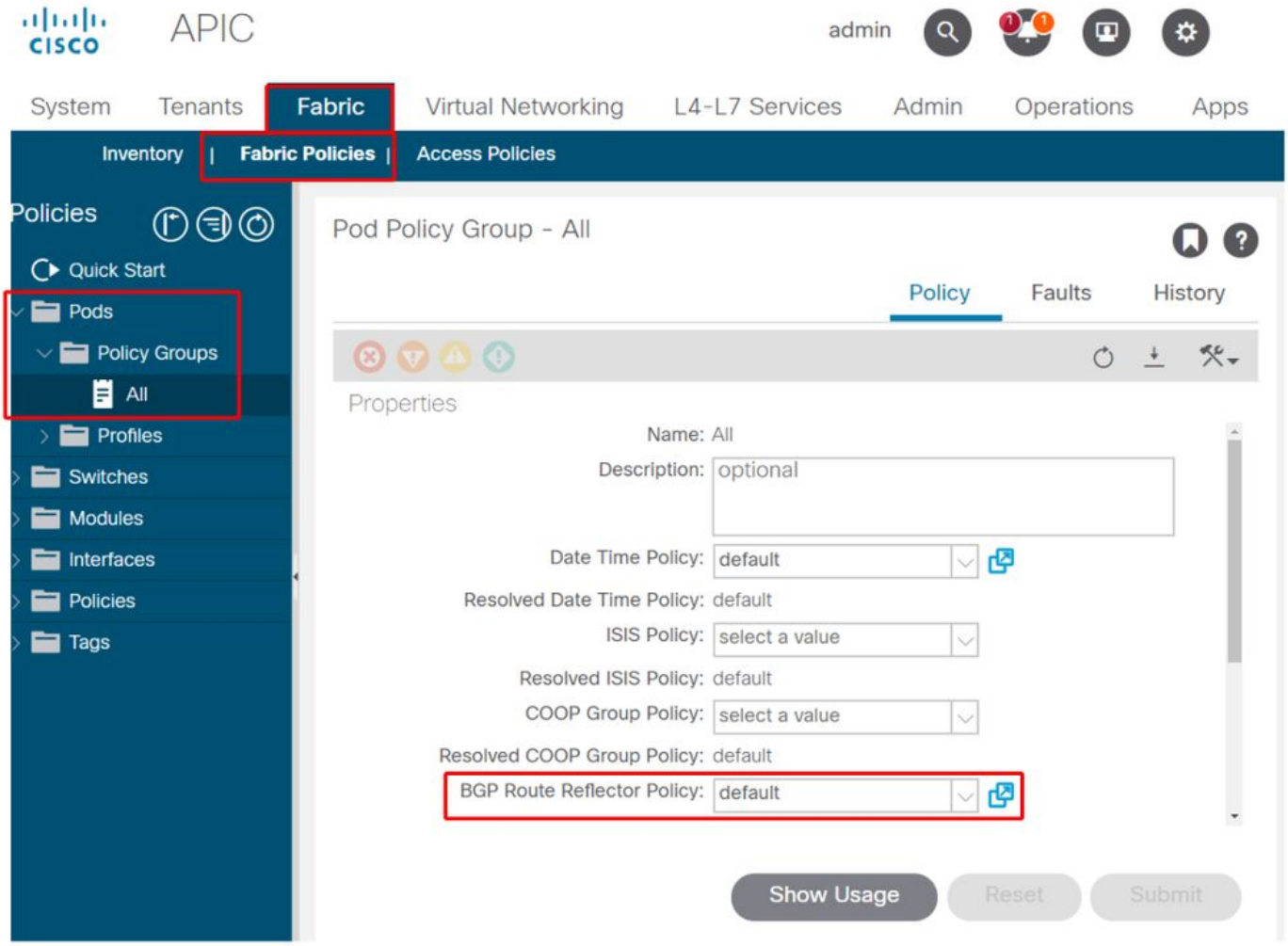
시스템 설정의 BGP 경로 리플렉터 정책



2. BGP RR 정책이 포드 정책 그룹 아래에 적용되는지 확인합니다

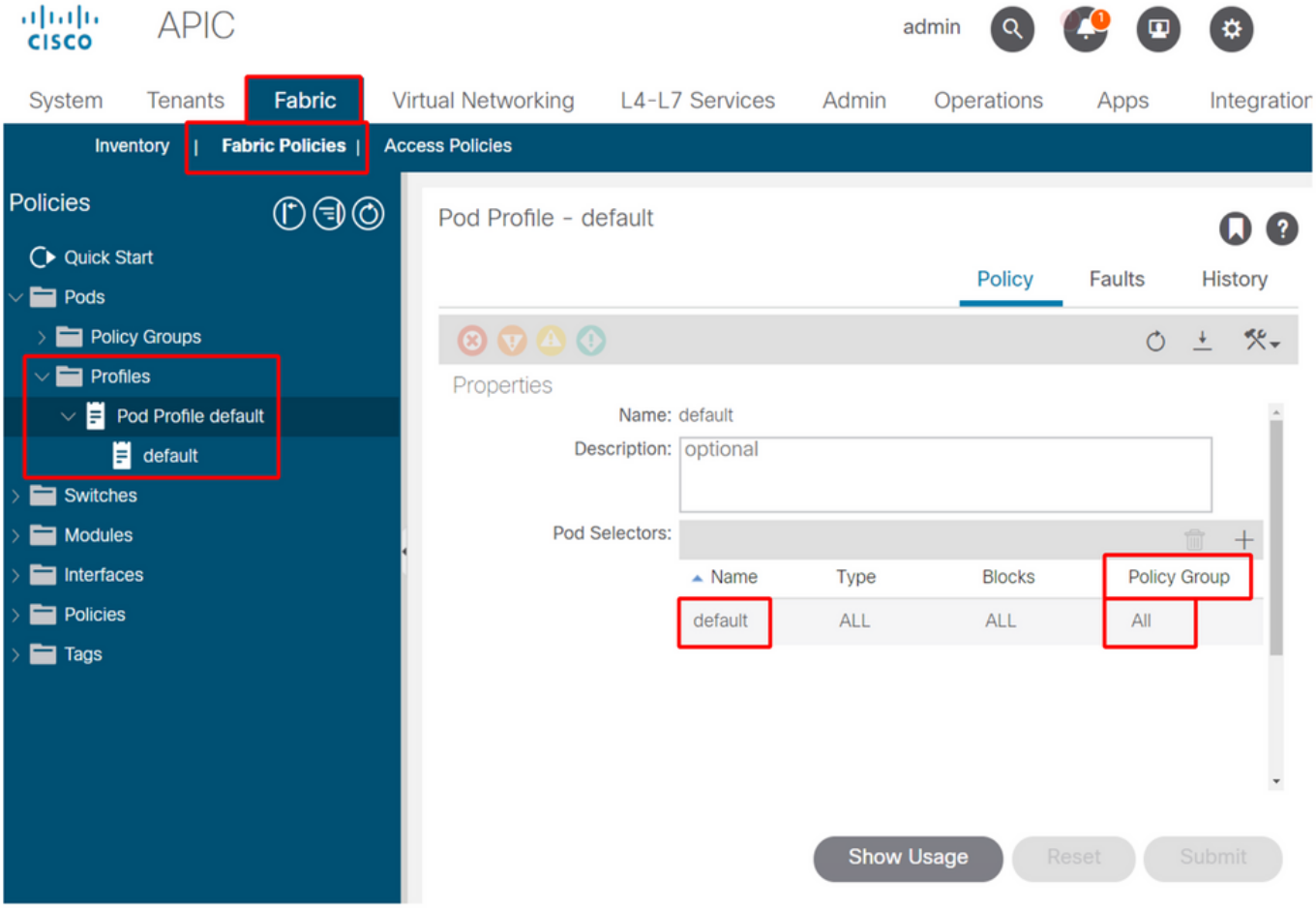
Pod Policy Group(포드 정책 그룹) 아래에 기본 BGP RR 정책을 적용합니다. 항목이 비어 있는 경우에도 기본 BGP RR 정책이 Pod Policy 그룹의 일부로 적용됩니다.

BGP 경로 리플렉터 정책이 포드 정책 그룹 아래에 적용됨



3. Pod Policy Group(Pod 정책 그룹)이 Pod Profile(Pod 프로필)에 적용되었는지 확인합니다

Pod 프로필에 Pod 정책 그룹이 적용됨



4. 스파인에 로그인하여 설정된 VPN4 피어 세션으로 BGP 프로세스가 실행 중인지 확인합니다

```
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
```

위에 표시된 것처럼 리프 노드와 스파인 노드 간의 MP-BGP는 VPNv4 및 VPNv6 주소 패밀리만 전달합니다. IPv4 주소군은 리프 노드의 MP-BGP에서만 사용됩니다.

스파인 노드와 리프 노드 간의 BGP VPNv4 및 VPNv6 세션도 다음 명령을 사용하여 쉽게 확인할 수 있습니다.

```
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
```

위의 출력에서 'Up/Down' 열을 확인합니다. BGP 세션이 설정된 시간을 나타내는 지속 시간을 나열해야 합니다. 또한 이 예에서는 'PfxRcd' 열에 각 BGP VPNv4/VPNv6 피어에 대해 0이 표시됩니다. 이 ACI 패브릭에는 아직 구성된 L3Outs가 없으며 외부 경로/접두사가 리프 노드와 스파인 노드 간의 교환이 없기 때문입니다.

5. leaf에 로그인하여 설정된 VPN4 피어 세션으로 BGP 프로세스가 실행 중인지 확인합니다

```
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
```

위 명령 출력은 ACI 패브릭에 있는 스파인 노드 수와 동일한 BGP VPNv4 세션의 양을 보여줍니다. 이는 각 리프 및 다른 경로 리플렉터 스파인 노드에 대한 세션을 설정하기 때문에 스파인 노드와 다릅니다.

SNMP

이 섹션에서 다루는 SNMP의 특정 하위 집합을 처음부터 명확히 하는 것이 중요합니다. ACI 패브릭의 SNMP 기능은 SNMP Walk 기능 또는 SNMP Trap 기능과 관련이 있습니다. 여기서 중요한 차이점은 SNMP Walk는 UDP 포트 161의 **인그레스(ingress) SNMP** 트래픽 흐름을 제어하는 반면, SNMP Trap은 UDP 포트 162에서 수신하는 SNMP 트랩 서버로 **발신** SNMP 트래픽 흐름을 제어한다는 것입니다.

ACI 노드의 인그레스 관리 트래픽에서는 노드 관리 EPG(대역 내 또는 대역 외)가 트래픽 흐름을 허용하는 데 필요한 계약을 제공해야 합니다. 따라서 인그레스 SNMP 트래픽 플로우에도 적용됩니다.

이 섹션에서는 ACI 노드(APIC 및 스위치)로의 인그레스 SNMP 트래픽 흐름(SNMP Walk)에 대해 설명합니다. 이 섹션의 범위를 모니터링 정책 및 모니터링 정책 종속성(예: 모니터링 정책 범위, 모니터링 패키지 등)으로 확장하므로 이그레스 SNMP 트래픽 흐름(SNMP 트랩)은 다루지 않습니다.

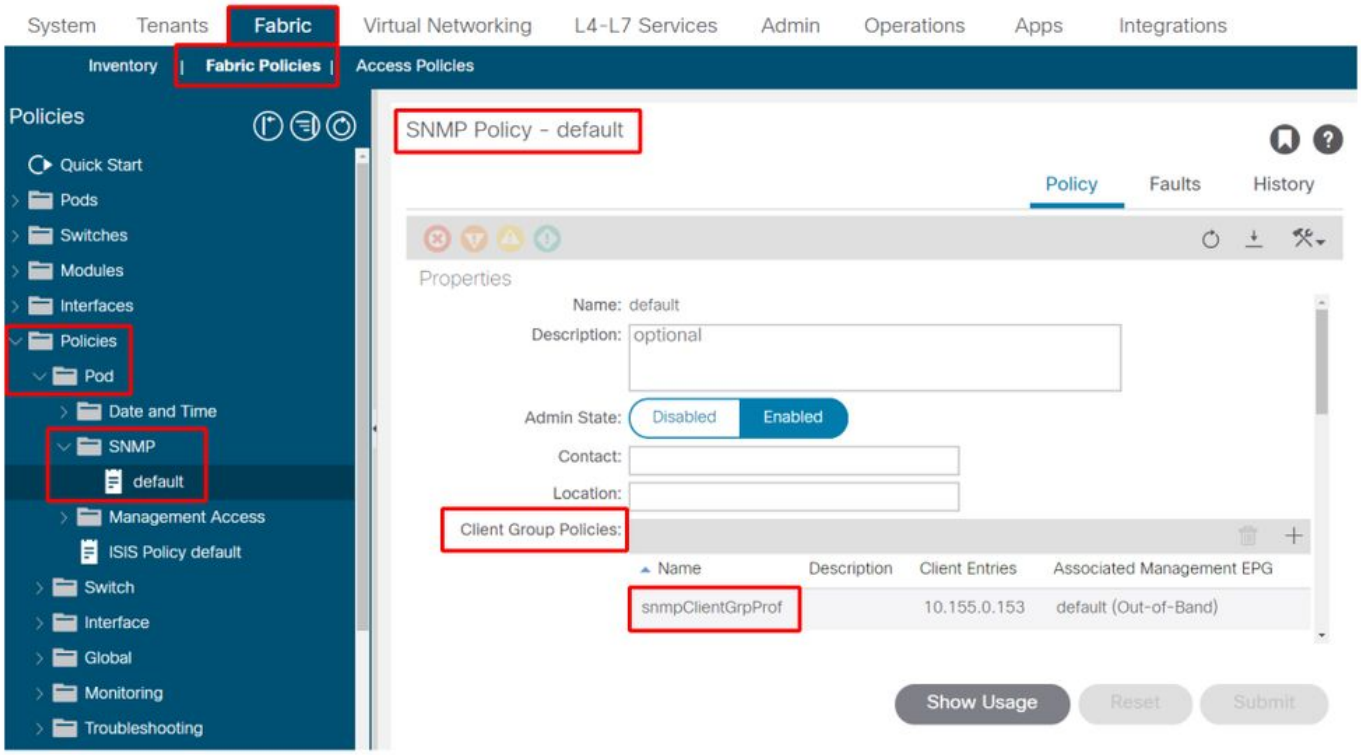
이 섹션에서는 ACI에서 지원되는 SNMP MIB에 대해서도 다루지 않습니다. 이 정보는 Cisco CCO 웹 사이트(https://www.cisco.com/c/dam/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/mib/list/mib-support.html 링크)에서 확인할 수 있습니다.

문제 해결 워크플로

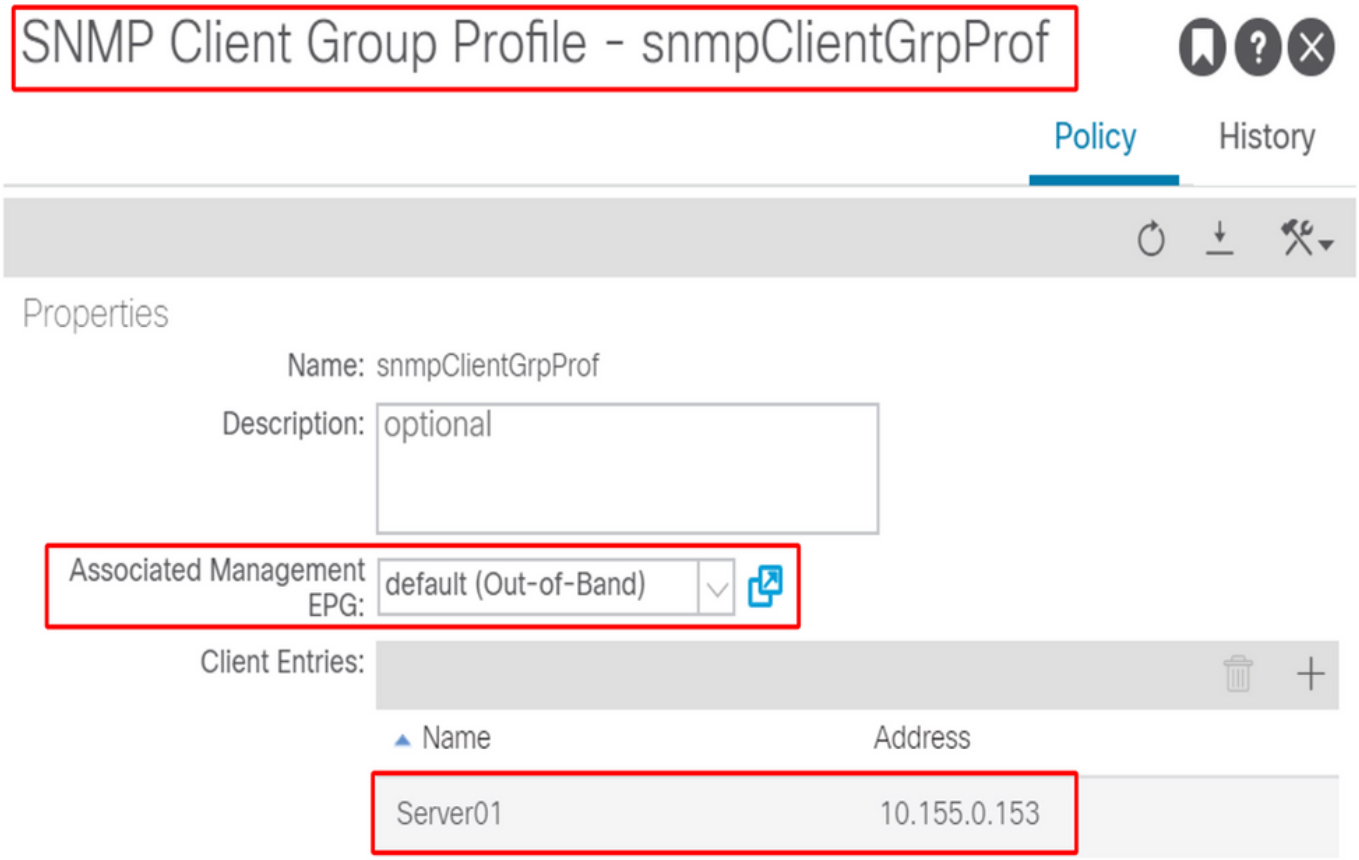
1. SNMP 포드 정책 — 클라이언트 그룹 정책이 구성되었는지 확인

아래 스크린샷에 따라 클라이언트 그룹 정책의 일부로 하나 이상의 SNMP 클라이언트가 구성되어 있는지 확인합니다.

포드 정책 — SNMP 정책 — 클라이언트 그룹 정책

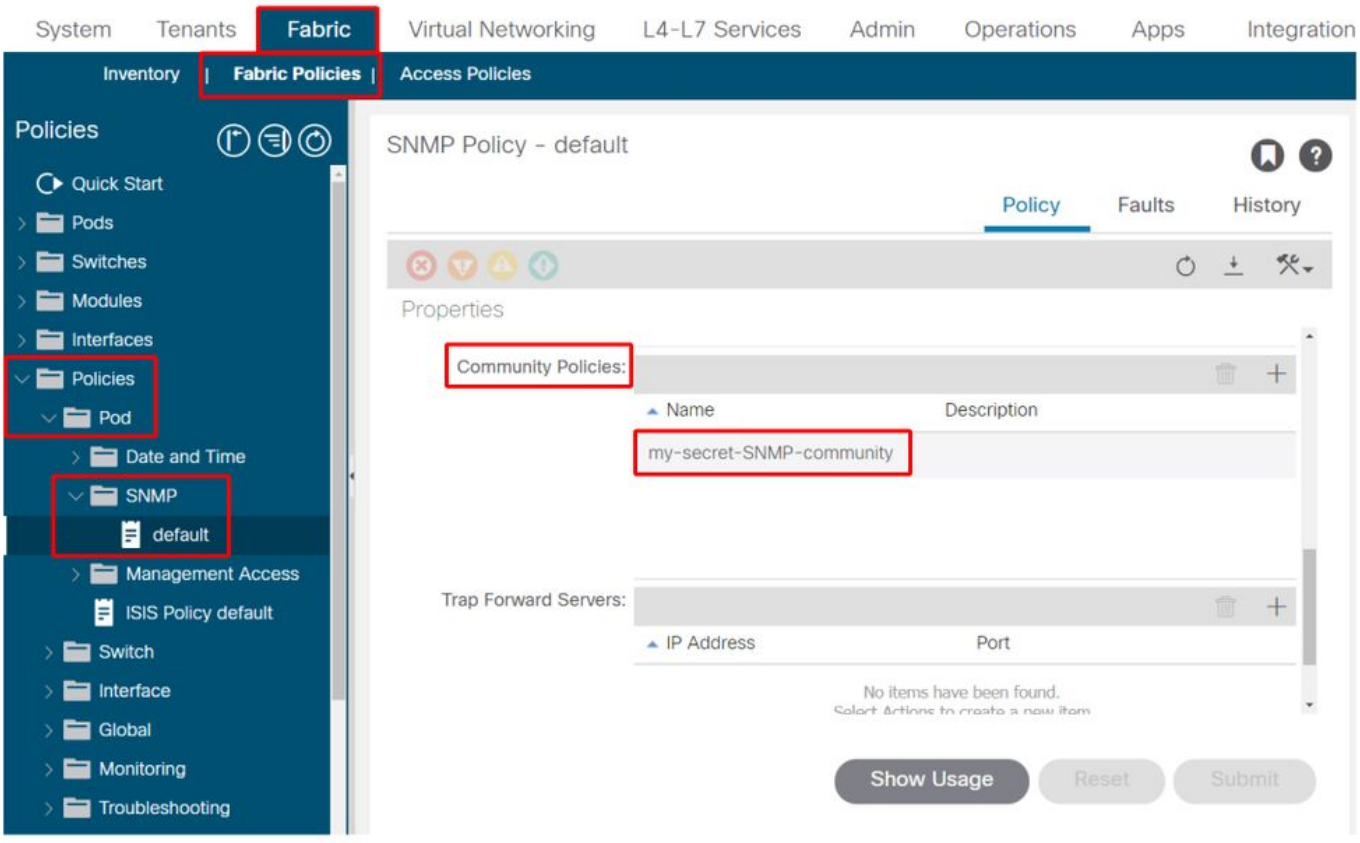


포드 정책 — SNMP 정책 — 클라이언트 그룹 정책

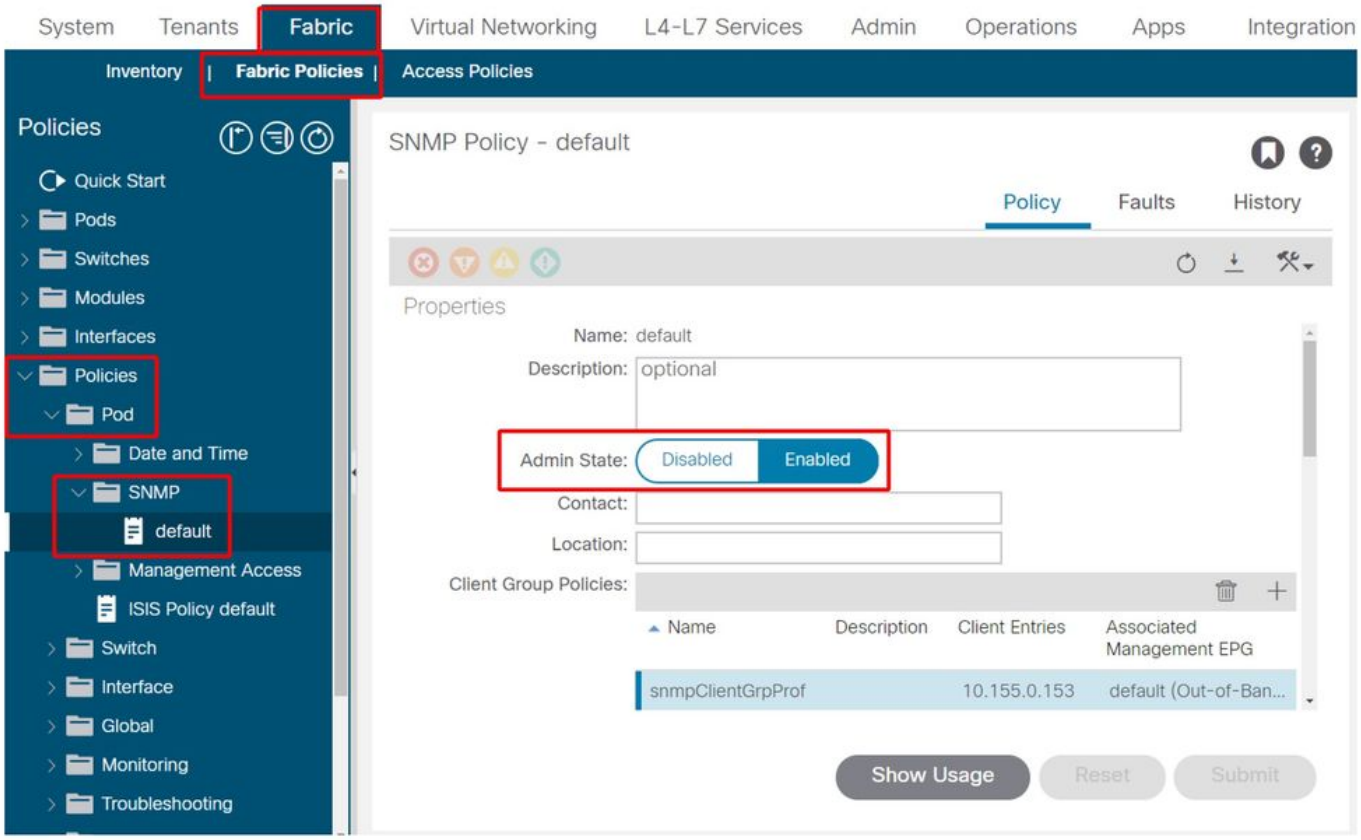


2. SNMP 포드 정책 — 하나 이상의 커뮤니티 정책이 구성되었는지 확인합니다.

포드 정책 — SNMP 정책 — 커뮤니티 정책



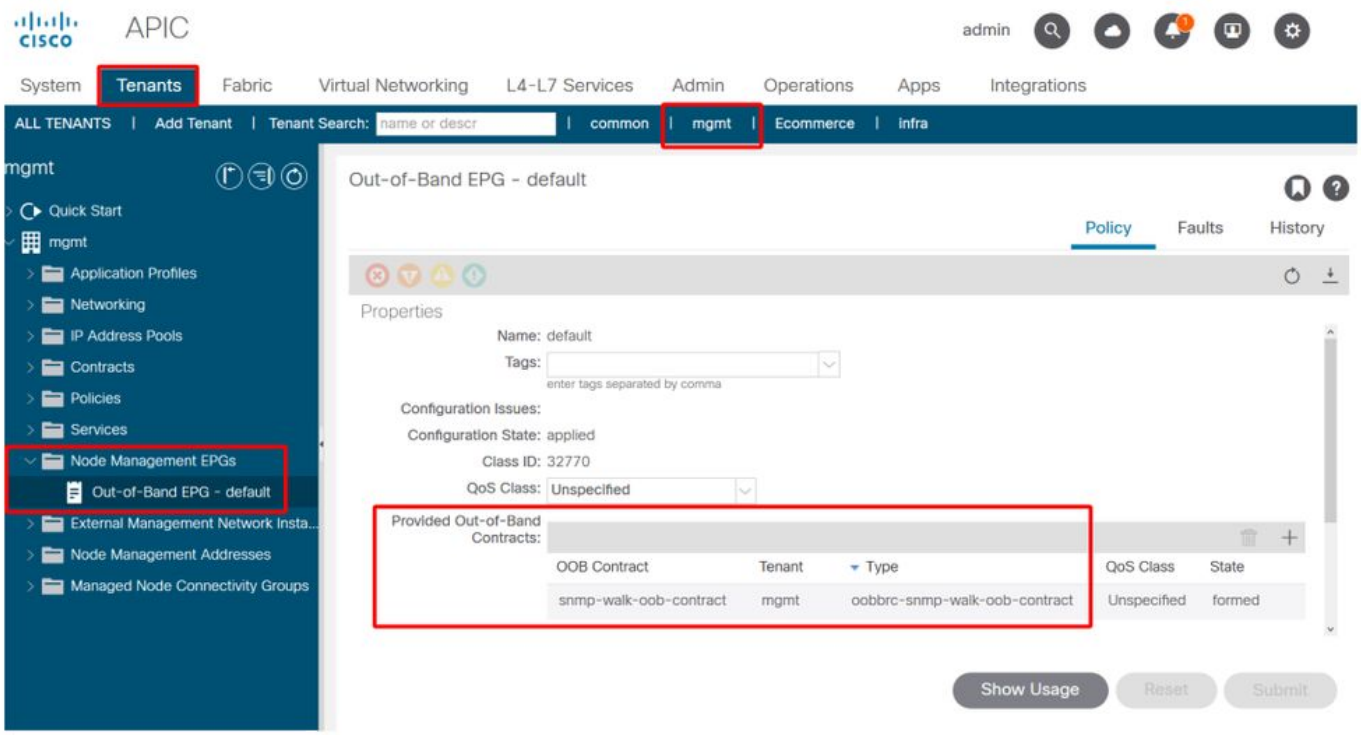
3. SNMP 포드 정책 — 관리 상태가 '사용'으로 설정되어 있는지 확인



4. 관리 테넌트 — OOB EPG가 UDP 포트 161을 허용하는 OOB 계약을 제공하는지 확인합니다.

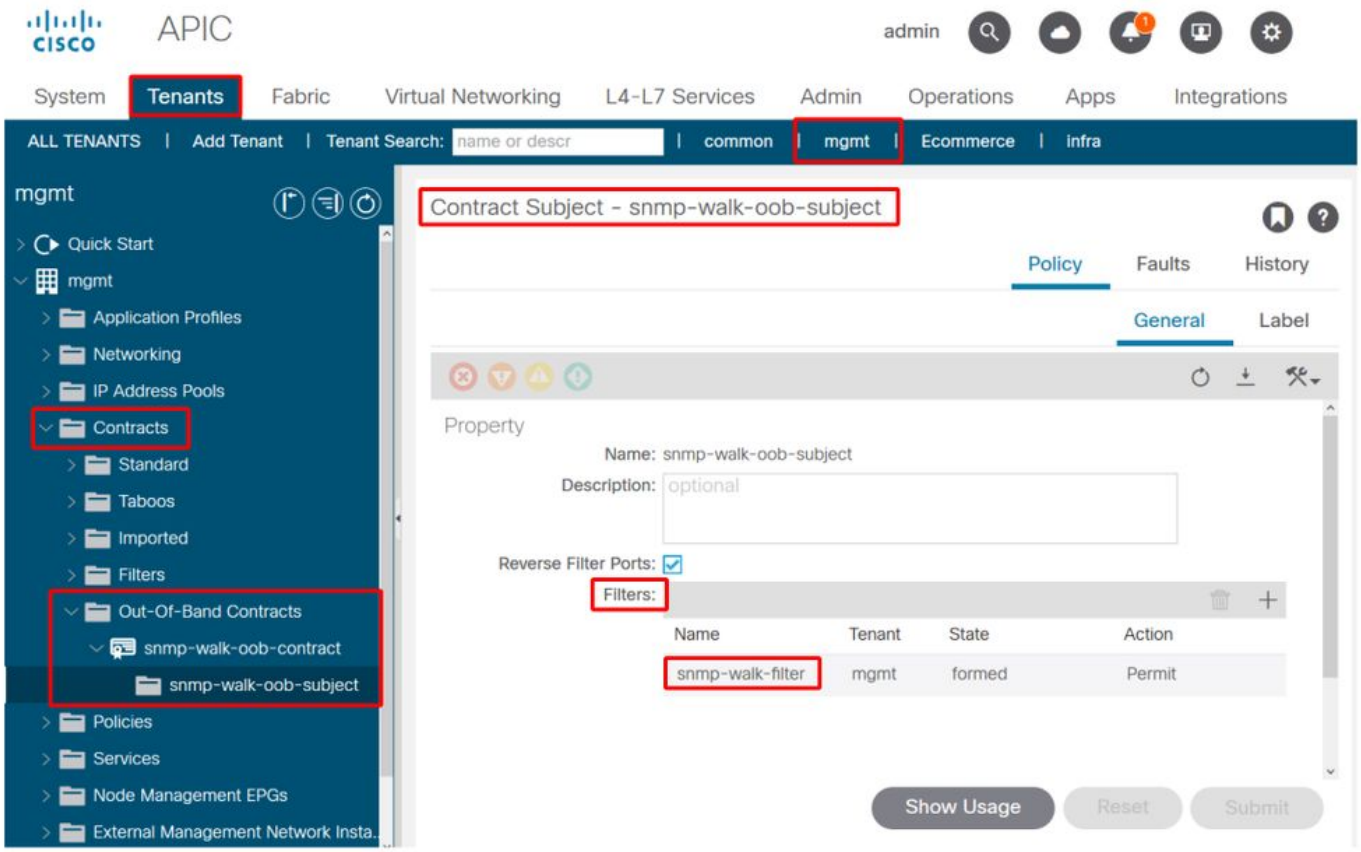
OOB EPG는 APIC 및 스위치 OOB 관리 포트로의 연결을 제어합니다. 따라서 OOB 포트로 들어오는 모든 트래픽 흐름에 영향을 미칩니다.

여기에 제공된 계약에는 SNMP만 포함된 것이 아니라 필요한 모든 관리 서비스가 포함되어 있는지 확인하십시오. 예를 들면 다음과 같습니다. 또한 SSH(TCP 포트 22) 이상을 포함해야 합니다. 이 기능이 없으면 SSH를 사용하여 스위치에 로그인할 수 없습니다. APIC에는 사용자가 완전히 잠기지 않도록 SSH, HTTP, HTTPS를 허용하는 메커니즘이 있으므로 이 기능이 적용되지 않습니다.

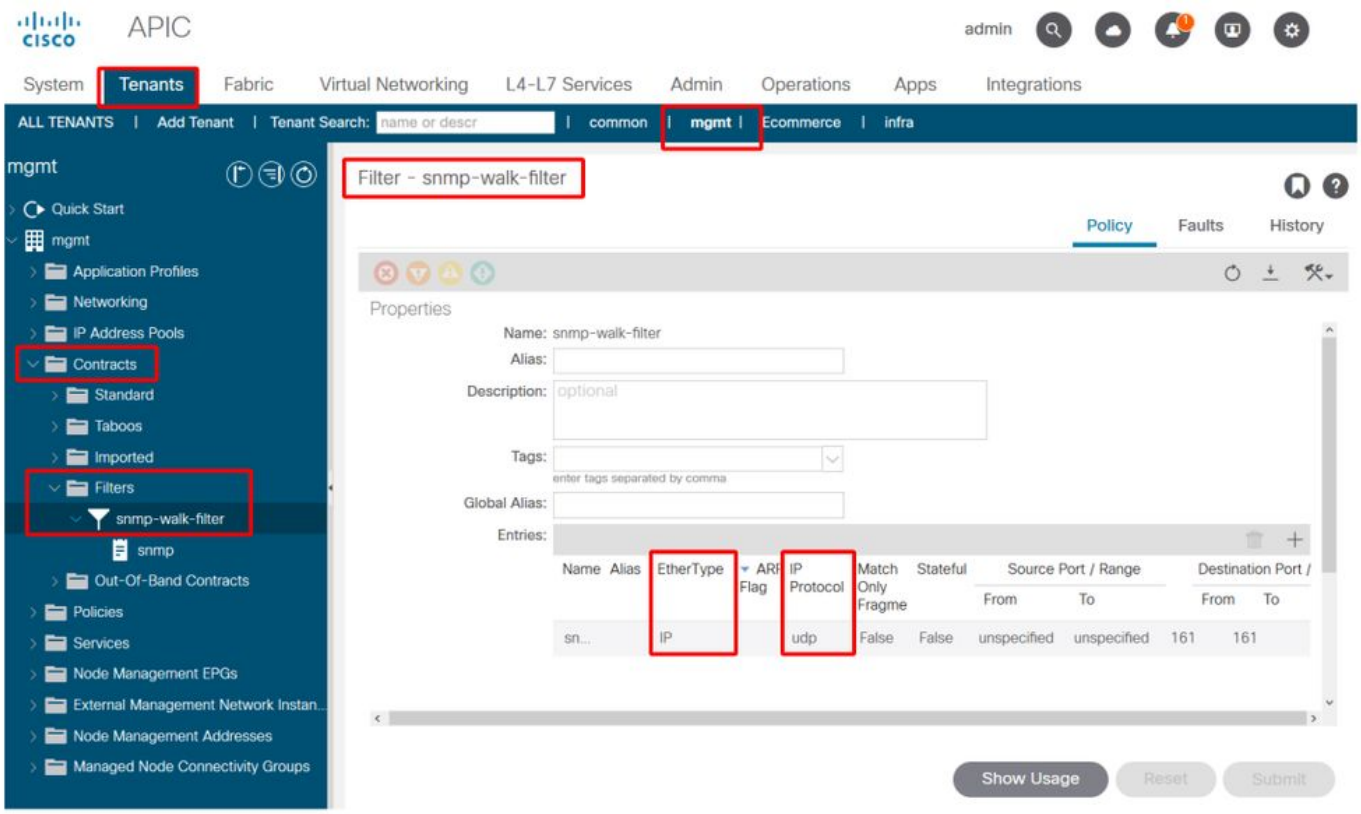


5. 관리 테넌트 — OOB 계약이 있고 UDP 포트 161을 허용하는 필터가 있는지 확인합니다.

관리 테넌트 — OOB EPG — OOB 계약 제공



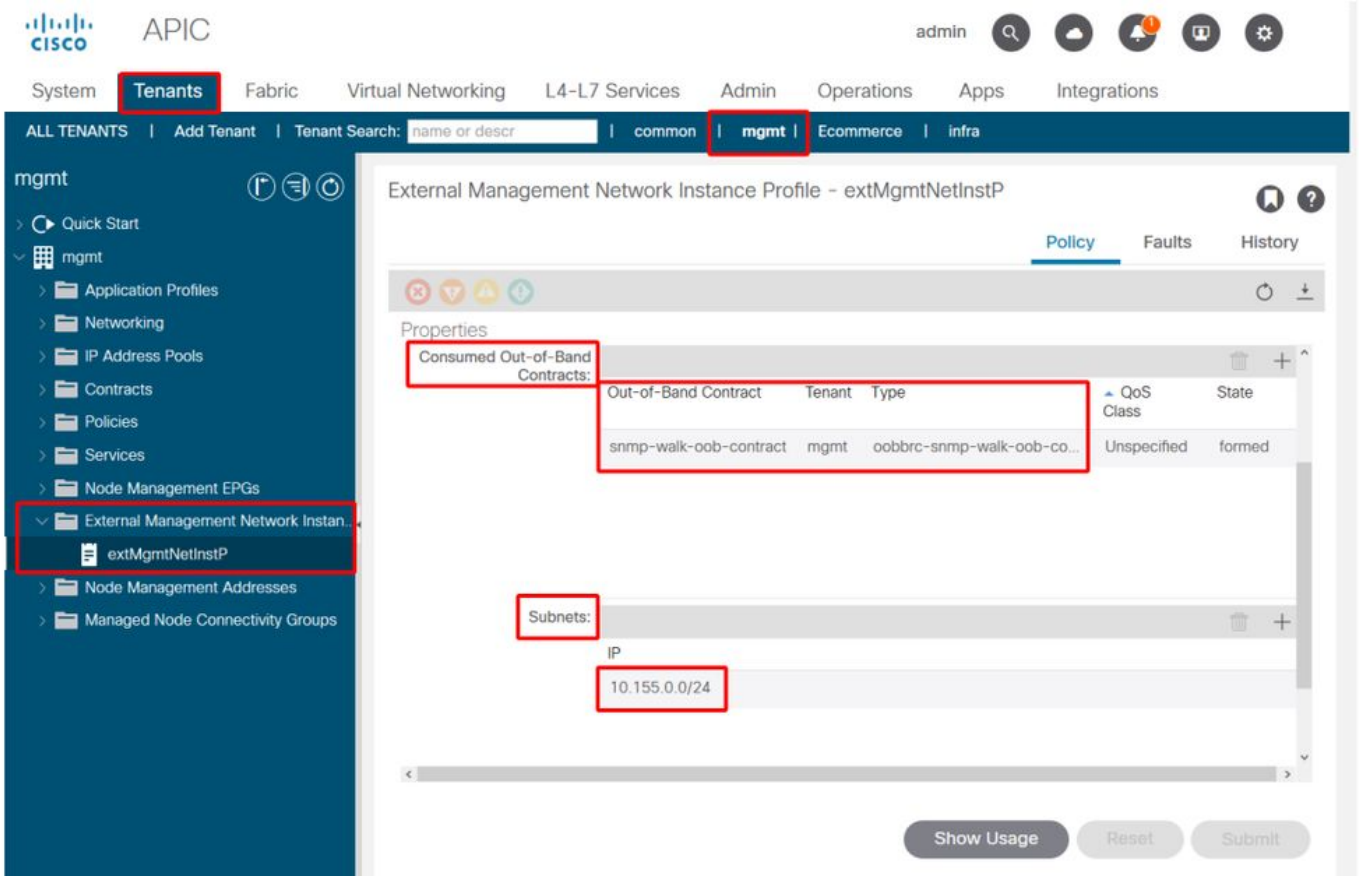
아래 그림에서는 UDP 포트 161만 허용하는 것이 필수는 아닙니다. 어떤 방식으로든 UDP 포트 161을 허용하는 필터가 있는 계약은 정확합니다. 이는 공통 테넌트의 기본 필터를 사용하는 계약 주체가 될 수도 있습니다. 이 예에서는 명확성을 위해 UDP 포트 161에 대해서만 특정 필터를 구성했습니다.



6. 관리 테넌트 — 외부 관리 네트워크 인스턴스 프로파일이 OOB 계약을 사용하는 유효한 서브넷과 함께 있는지 확인합니다.

외부 관리 네트워크 인스턴스 프로필(ExtMgmtNetInstP)은 OOB EPG를 통해 연결할 수 있는 서비스를 사용해야 하는 '서브넷'에 의해 정의된 외부 소스를 나타냅니다. 따라서 ExtMgmtNetInstP는 OOB EPG에서 제공하는 동일한 OOB 계약을 소비합니다. 이는 UDP 포트 161을 허용하는 계약입니다. 또한 ExtMgmtNetInstP는 OOB EPG에서 제공하는 서비스를 사용할 수 있는 허용된 서브넷 범위도 지정합니다.

관리 테넌트 — OOB 계약 및 서브넷이 사용된 ExtMgmtNetInstP



위 그림에 나와 있는 것처럼 CIDR 기반 서브넷 표기법이 필요합니다. 그림에는 특정 /24 서브넷이 나와 있습니다. 서브넷 항목이 SNMP 포드 정책에 구성된 SNMP 클라이언트 항목을 포함해야 합니다(그림 포드 정책 — SNMP 정책 — 클라이언트 그룹 정책 참조).

앞서 언급했듯이 필요한 다른 관리 서비스가 잠기지 않도록 필요한 모든 외부 서브넷을 포함하도록 주의하십시오.

7. 스위치에 로그인하고 tcpdump를 수행하여 SNMP Walk 패킷(UDP 포트 161)이 관찰되는지 확인합니다

SNMP Walk 패킷이 OOB 포트를 통해 스위치에 들어가는 경우, 이는 필요한 모든 SNMP 및 OOB 기반 정책/매개변수가 올바르게 구성되었음을 의미합니다. 따라서 적절한 확인 방법입니다.

리프 노드의 Tcpdump는 Linux 셸 및 Linux 넷디바이스를 활용합니다. 따라서 아래 예에 따라 인터페이스 'eth0'에서 패킷을 캡처해야 합니다. 이 예에서 SNMP 클라이언트는 OID .1.0.8802.1.1.2.1.1.0에 대해 SNMP Get 요청을 수행합니다.

```
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
```

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.