

# ACI管理和核心服務故障排除 — Pod策略

## 目錄

[簡介](#)

[背景資訊](#)

[Pod策略概述](#)

[Pod策略](#)

[日期和時間策略](#)

[故障排除 workflow](#)

[BGP路由反射器策略](#)

[故障排除 workflow](#)

[SNMP](#)

[故障排除 workflow](#)

## 簡介

本文檔介紹瞭解ACI Pod策略並對其進行故障排除的步驟。

## 背景資訊

本文中的資料摘自 [思科以應用為中心的基礎設施第二版故障排除](#) 書，尤其是管理和核心服務 — POD策略 — BGP RR/日期和時間/SNMP 章節。

## Pod策略概述

使用Pod策略組在系統上應用BGP RR、日期和時間以及SNMP等管理服務。Pod策略組管理一組與ACI交換矩陣的基本功能相關的Pod策略。這些Pod策略與以下元件相關，其中很多元件預設在ACI交換矩陣中調配。

## Pod策略

Pod策略	需要手動配置
日期和時間	是
BGP路由反射器	是
SNMP ( 伺服器網路管理通訊協定 )	是
ISIS	否
COOP	否
管理訪問	否
MAC安全	是

即使在單個ACI交換矩陣中，也需要配置Pod策略組和Pod配置檔案。這並非特定於多Pod甚至多站點部署。該要求適用於所有ACI部署型別。

本章重點介紹這些基本的Pod策略以及如何驗證它們是否正確應用。

## 日期和時間策略

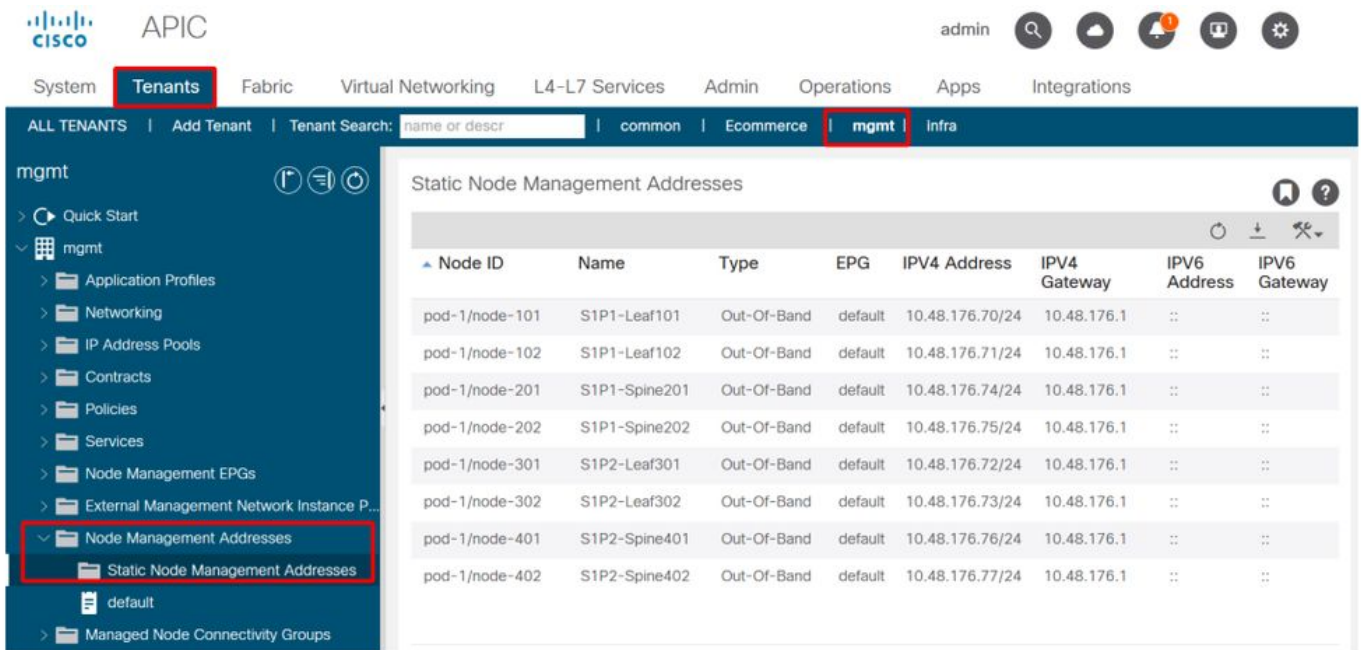
時間同步在ACI交換矩陣中扮演著重要角色。從驗證證書到保持APIC和交換機中的日誌時間戳一致，最好的做法是使用NTP將ACI交換矩陣中的節點同步到一個或多個可靠的時間源。

為了正確地將節點同步到NTP伺服器提供程式，需要依賴關係為節點分配管理地址。這可以在管理租戶下使用靜態節點管理地址或管理節點連線組完成。

## 故障排除 workflow

### 1. 驗證是否已將節點管理地址分配給所有節點

#### 管理租戶 — 節點管理地址



The screenshot shows the APIC interface for the 'mgmt' tenant. The 'Static Node Management Addresses' table is displayed, listing various nodes and their associated IP addresses and gateways.

Node ID	Name	Type	EPG	IPV4 Address	IPV4 Gateway	IPV6 Address	IPV6 Gateway
pod-1/node-101	S1P1-Leaf101	Out-Of-Band	default	10.48.176.70/24	10.48.176.1	::	::
pod-1/node-102	S1P1-Leaf102	Out-Of-Band	default	10.48.176.71/24	10.48.176.1	::	::
pod-1/node-201	S1P1-Spine201	Out-Of-Band	default	10.48.176.74/24	10.48.176.1	::	::
pod-1/node-202	S1P1-Spine202	Out-Of-Band	default	10.48.176.75/24	10.48.176.1	::	::
pod-1/node-301	S1P2-Leaf301	Out-Of-Band	default	10.48.176.72/24	10.48.176.1	::	::
pod-1/node-302	S1P2-Leaf302	Out-Of-Band	default	10.48.176.73/24	10.48.176.1	::	::
pod-1/node-401	S1P2-Spine401	Out-Of-Band	default	10.48.176.76/24	10.48.176.1	::	::
pod-1/node-402	S1P2-Spine402	Out-Of-Band	default	10.48.176.77/24	10.48.176.1	::	::

### 2. 驗證NTP伺服器是否已配置為NTP提供程式

如果有多個NTP提供程式，則使用「首選」覈取方塊將其中至少一個提供程式標籤為首選時間源，如下圖所示。

#### 日期和時間Pod策略下的NTP提供商/伺服器

### 3.在「系統設定」下驗證日期和時間格式

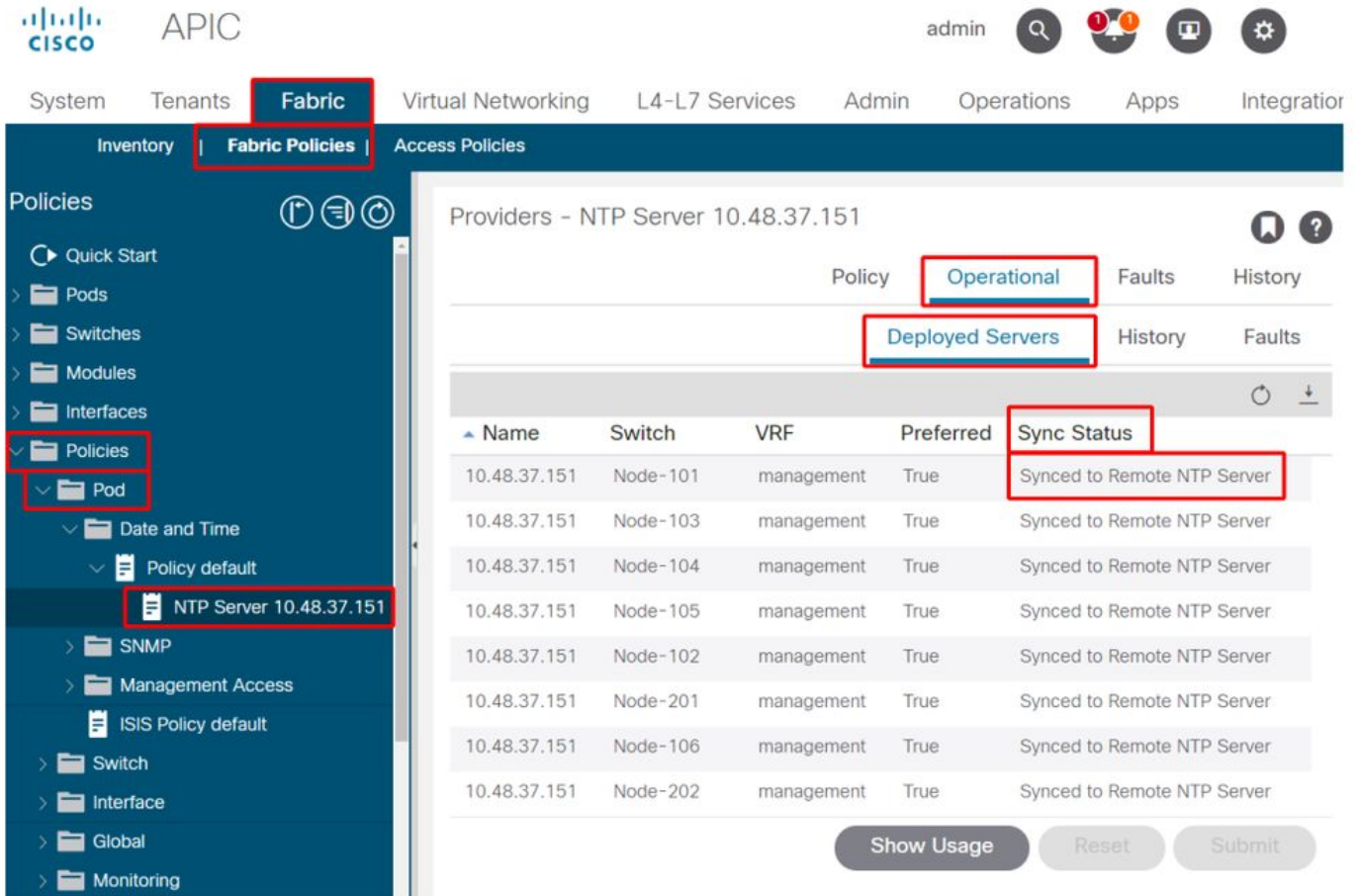
下圖顯示了一個示例，其中日期和時間格式已設定為UTC。

「系統設定」下的「日期和時間」設定

### 4.驗證所有節點的NTP提供程式的運行同步狀態

如下圖所示，「同步狀態」列應顯示「已同步到遠端NTP伺服器」。請注意，「同步狀態」可能需要幾分鐘才能正確收斂到.Synched to Remote NTP Server。狀態。

### NTP提供程式/伺服器同步狀態



或者，也可以在APIC和交換機上使用CLI方法驗證與NTP伺服器的正確時間同步。

### APIC - NX-OS CLI

下面的「refId」列根據層級顯示下次的NTP伺服器源。

```

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
```

## 交換器

使用「show ntp peers」命令確保NTP提供程式配置已正確推送到交換機。

```
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
```

此處的「\*」字元至關重要，因為它控制NTP伺服器是否實際用於同步。

在下面的命令中驗證傳送/接收的資料包數量，以確保ACI節點能夠連線到NTP伺服器。

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

## BGP路由反射器策略

ACI交換矩陣在枝葉和主幹節點之間使用多協定BGP(MP-BGP)，更具體地說，使用iBGP VPNv4，交換從外部路由器（連線到L3Outs）接收的租戶路由。為了避免全網狀iBGP對等拓撲，主幹節點將從枝葉節點接收的VPNv4字首反映到交換矩陣中的其他枝葉節點。

如果沒有BGP路由反射器(BGP RR)策略，則不會在交換機上建立BGP例項，並且不會建立BGP VPNv4會話。在多Pod部署中，每個Pod至少需要一個配置為BGP RR的主幹，並且實際上需要多個主幹以實現冗餘。

因此，BGP RR策略是每個ACI交換矩陣中一個必不可少的配置。BGP RR策略還包含ACI交換矩陣用於每台交換機上BGP進程的ASN。

## 故障排除 workflow

### 1. 驗證BGP RR策略是否配置了ASN和至少一個骨幹

以下示例涉及單個Pod部署。

## 系統設定下的BGP路由反射器策略

System Settings

- Quota
- APIC Connectivity Preferences
- System Alias and Banners
- System Response Time
- Global AES Passphrase Encrypt
- BD Enforced Exception List
- Fabric Security
- Control Plane MTU
- Endpoint Controls
- Fabric-Wide Settings
- Port Tracking
- System Global GIPo
- Date and Time
- Intersight
- APIC Passphrase
- BGP Route Reflector**
- COOP Group

BGP Route Reflector Policy - BGP Route Reflector

Policy | Faults | History

Properties

Name: default  
Description: optional

Autonomous System Number: 65001

Route Reflector Nodes:

Pod ID	Node ID	Node Name	Description
1	201	bdsol-aci12-spine1	
1	202	bdsol-aci12-spine2	

Show Usage | Reset | Submit

## 2. 驗證BGP RR策略是否在Pod策略組下應用

在Pod策略組下應用預設BGP RR策略。即使條目為空，預設BGP RR策略也將作為Pod策略組的一部分應用。

在Pod策略組下應用的BGP路由反射器策略

Name: All

Description: optional

Date Time Policy: default

Resolved Date Time Policy: default

ISIS Policy: select a value

Resolved ISIS Policy: default

COOP Group Policy: select a value

Resolved COOP Group Policy: default

BGP Route Reflector Policy: default

Show Usage

Reset

Submit

### 3. 驗證Pod策略組是否應用在Pod配置檔案下

在Pod配置檔案下應用的Pod策略組

admin

System Tenants **Fabric** Virtual Networking L4-L7 Services Admin Operations Apps Integration

Inventory | **Fabric Policies** | Access Policies

Policies

- Quick Start
- Pods
  - Policy Groups
  - Profiles
    - Pod Profile default**
      - default
  - Switches
  - Modules
  - Interfaces
  - Policies
  - Tags

Pod Profile - default

Policy Faults History

Properties

Name: default

Description: optional

Pod Selectors:

Name	Type	Blocks	Policy Group
default	ALL	ALL	All

Show Usage Reset Submit

#### 4.登入到主幹，並驗證BGP進程是否正在運行已建立的VPN4對等會話

```
spinel# 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              7
Active-peers       6
Routes             0
Paths              0
Networks           0
Aggregates         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 interleaf_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
```

如上所述，枝葉和主幹節點之間的MP-BGP僅承載VPNv4和VPNv6地址系列。IPv4地址系列僅用於枝葉節點上的MP-BGP。

使用下列命令還可以輕鬆觀察主幹和枝葉節點之間的BGP VPNv4和VPNv6會話。

```
spinel# 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

```
spinel# 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

```

注意上述輸出中的「Up/Down」列。它應列出一個持續時間，該持續時間表示BGP會話已建立的時間。另請注意，在示例中，「PfxRcd」列顯示每個BGP VPNv4/VPNv6對等點的0，因為此ACI交換矩陣尚未配置L3Outs，因此枝葉和主幹節點之間沒有交換外部路由/字首。

## 5. 登入到枝葉，並驗證BGP進程是否正在運行已建立的VPN4對等會話

```
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

```

上面的命令輸出顯示的BGP VPNv4會話數量等於ACI交換矩陣中存在的脊柱節點數量。這與主幹節點不同，因為它們會建立到每個枝葉和其他路由反射器主幹節點的會話。

## SNMP

必須從頭開始闡明本節介紹的SNMP功能的特定子集。ACI交換矩陣中的SNMP功能與SNMP Walk功能或SNMP Trap功能相關。這裡的重要區別是SNMP Walk管理UDP埠161上的輸入SNMP流量，而SNMP Trap管理傳出SNMP流量，SNMP Trap伺服器在UDP埠162上偵聽。

ACI節點上的入口管理流量需要節點管理EPG（帶內或帶外）提供必要的合約，以允許流量流動。因此，這也適用於輸入SNMP流量流。

本節將介紹進入ACI節點（APIC和交換機）的輸入SNMP流量（SNMP漫遊）。它將不包括出口SNMP流量流（SNMP陷阱），因為這會將本部分的範圍擴展到監控策略和監控策略依賴關係（例如，監控策略範圍、監控包等）。

本部分也不涵蓋ACI支援哪些SNMP MIB。該資訊可通過思科CCO網站中的以下連結獲得

：<https://www.cisco.com/c/dam/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/mib/list/mib-support.html>

## 故障排除 workflow

### 1. SNMP Pod策略 — 驗證是否配置了客戶端組策略

確保至少有一個SNMP客戶端配置為客戶端組策略的一部分，如下面的螢幕截圖所示。

## Pod策略 — SNMP策略 — 客戶端組策略

System Tenants **Fabric** Virtual Networking L4-L7 Services Admin Operations Apps Integrations

Inventory **Fabric Policies** Access Policies

Policies

- Quick Start
- Pods
- Switches
- Modules
- Interfaces
- Policies**
  - Pod**
    - Date and Time
    - SNMP**
      - default**
    - Management Access
      - ISIS Policy default
    - Switch
    - Interface
    - Global
    - Monitoring
    - Troubleshooting

**SNMP Policy - default**

Policy Faults History

Properties

Name: default  
Description: optional

Admin State:  Disabled  Enabled

Contact:   
Location:

Client Group Policies:

Name	Description	Client Entries	Associated Management EPG
snmpClientGrpProf		10.155.0.153	default (Out-of-Band)

Show Usage Reset Submit

## Pod策略 — SNMP策略 — 客戶端組策略

**SNMP Client Group Profile - snmpClientGrpProf**

Policy History

Properties

Name: snmpClientGrpProf  
Description: optional

Associated Management EPG: default (Out-of-Band)

Client Entries:

Name	Address
Server01	10.155.0.153

## 2. SNMP Pod策略 — 驗證是否至少配置了一個社群策略

## Pod策略 — SNMP策略 — 社群策略

The screenshot shows the Cisco APIC Fabric Policies configuration page. The left sidebar is expanded to show the 'Fabric Policies' section, with 'SNMP' and 'default' sub-items highlighted. The main panel displays the configuration for the 'SNMP Policy - default'. The 'Community Policies' section is expanded, showing a table with one entry: 'my-secret-SNMP-community'. The 'Trap Forward Servers' section is empty, with a message 'No items have been found. Select Actions to create a new item.' Below the table are buttons for 'Show Usage', 'Reset', and 'Submit'.

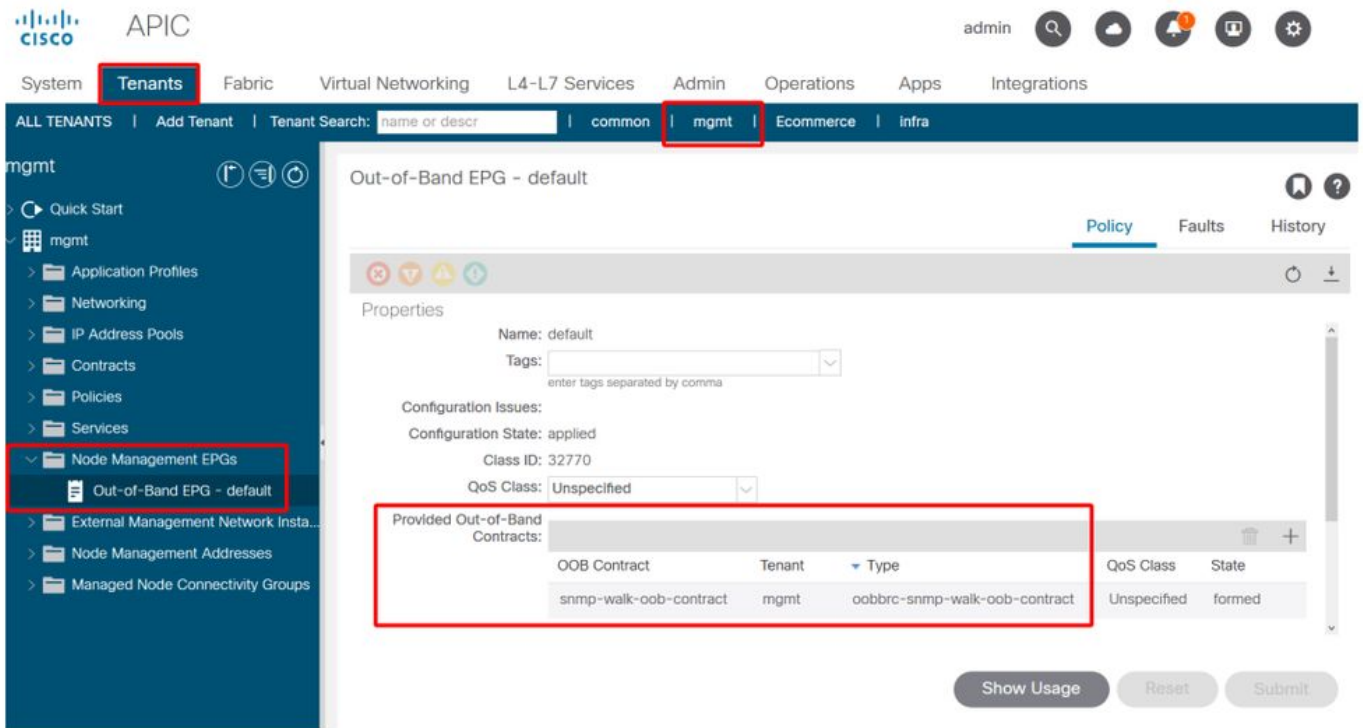
### 3. SNMP Pod策略 — 驗證管理狀態是否設定為「已啟用」

The screenshot shows the Cisco APIC Fabric Policies configuration page for the 'SNMP Policy - default'. The left sidebar is expanded to show the 'Fabric Policies' section, with 'SNMP' and 'default' sub-items highlighted. The main panel displays the configuration for the 'SNMP Policy - default'. The 'Admin State' is set to 'Enabled'. The 'Description' is 'optional'. The 'Client Group Policies' section is expanded, showing a table with one entry: 'snmpClientGrpProf' with IP address '10.155.0.153' and associated Management EPG 'default (Out-of-Ban...'. Below the table are buttons for 'Show Usage', 'Reset', and 'Submit'.

### 4. 管理租戶 — 驗證OOB EPG是否提供允許UDP埠161的OOB合約

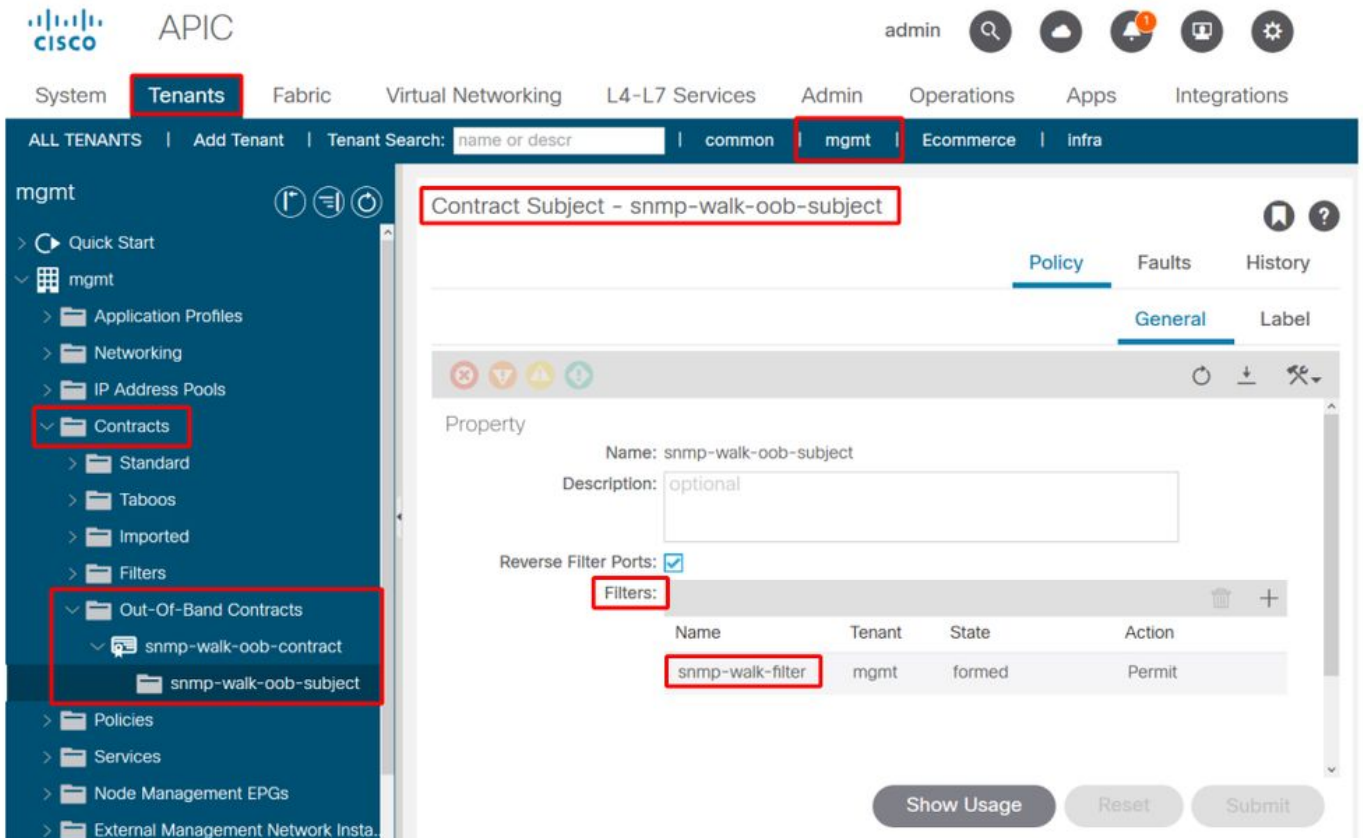
OOB EPG管理到APIC和交換機OOB管理埠的連線。因此，它會影響所有進入OOB埠的流量。

確保此處提供的合約包括所有必要的管理服務，而不僅僅是SNMP。例如：它還需要至少包括SSH ( TCP埠22 )。 否則，無法使用SSH登入交換機。請注意，這不適用於APIC，因為它們具有允許SSH、HTTP和HTTPS的機制來防止使用者完全鎖定。



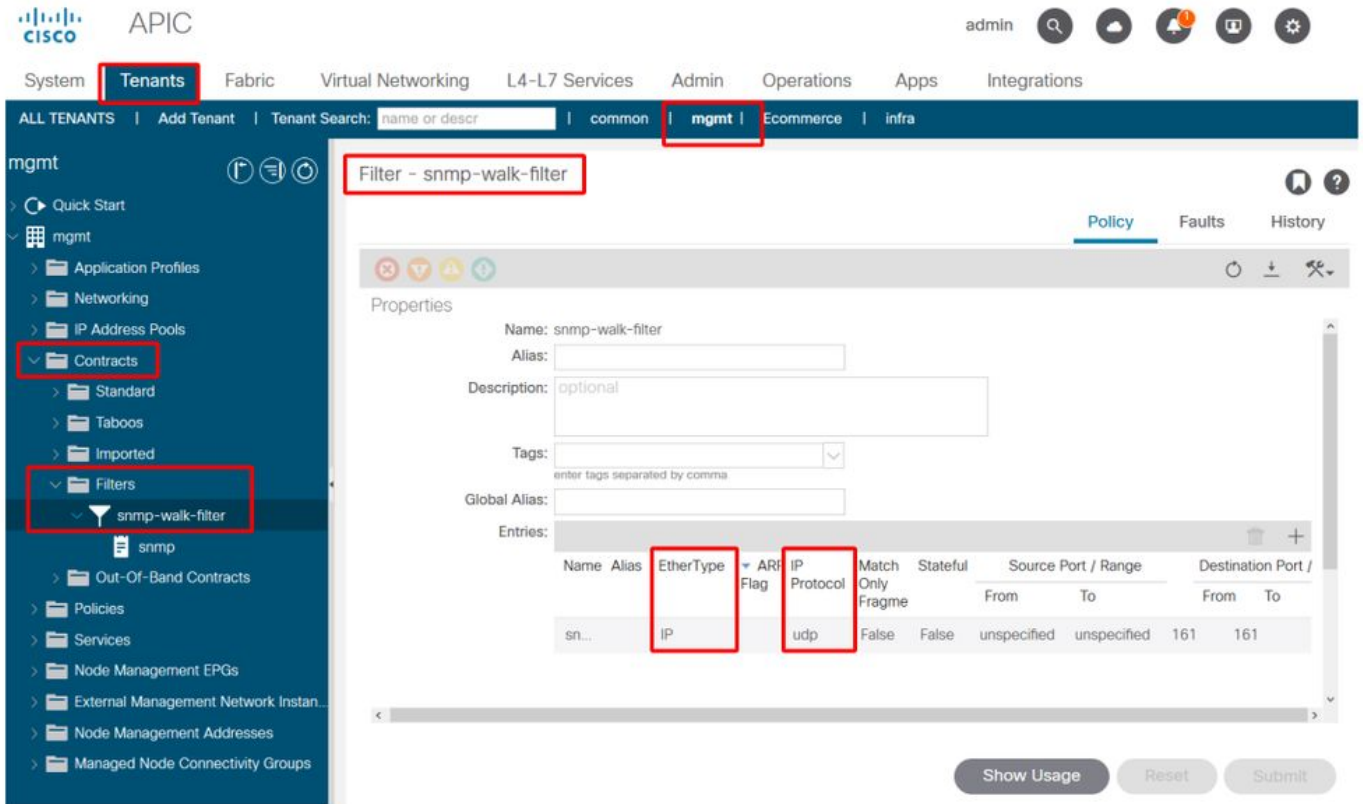
## 5.管理租戶 — 驗證OOB合約是否存在，並且其篩選器允許UDP埠161

### 管理租戶 — OOB EPG — 提供的OOB合約



在下圖中，並非只允許UDP埠161是強制性的。具有允許以任何方式使用UDP埠161的過濾器的合約

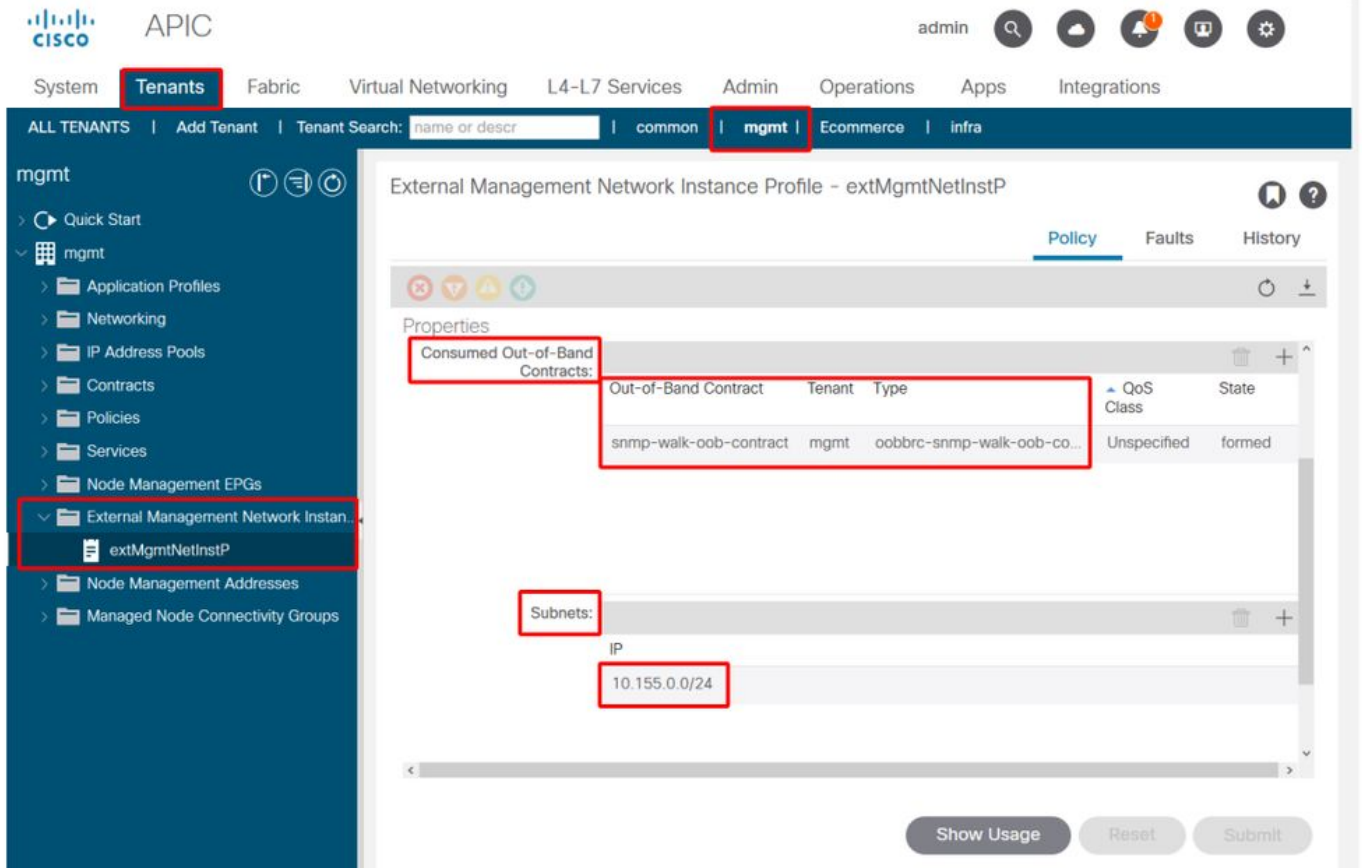
是正確的。這甚至可以是具有公共租戶預設篩選器的合約主題。在我們的示例中，為清楚起見，僅針對UDP埠161配置了特定過濾器。



## 6.管理租戶 — 驗證外部管理網路例項配置檔案是否存在使用OOB合約的有效子網

外部管理網路例項配置檔案(ExtMgmtNetInstP)表示需要使用通過OOB EPG可訪問的服務的「子網」定義的外部源。因此，ExtMgmtNetInstP使用由OOB EPG提供的同一OOB合約。這是允許UDP埠161的合約。此外，ExtMgmtNetInstP還指定了可能使用OOB EPG提供的服務的允許的子網範圍。

管理租戶 — ExtMgmtNetInstP，使用已使用的OOB合約和子網



如上圖所示，需要基於CIDR的子網表示法。圖中顯示了特定的/24子網。要求子網條目包括SNMP Pod策略中配置的SNMP客戶端條目（請參閱圖Pod策略 — SNMP策略 — 客戶端組策略）。

如前所述，請小心包括所有所需的外部子網，以防止其他必要的管理服務被鎖定。

## 7. 登入到交換機並執行tcpdump以觀察是否觀察到了SNMP Walk資料包 — UDP埠161

如果SNMP Walk資料包通過OOB埠進入交換機，這意味著所有必要的SNMP和OOB策略/引數都已正確配置。因此，這是一種正確的驗證方法。

枝葉節點上的Tcpdump利用其Linux shell和Linux netdevice。因此，必須按照以下示例在介面「eth0」上捕獲資料包。在本示例中，SNMP客戶端正在對OID .1.0.8802.1.1.2.1.1.1.0執行SNMP Get請求。

```
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
```

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。