ACI管理和核心服務故障排除 — 帶內和帶外管理

目錄

簡介

本文檔介紹對ACI帶外(OOB)和帶內(INB)管理進行故障排除的步驟。

背景資訊

本文檔中的資料摘自思科以應用為中心的基礎架構故障排除第二版書，特別是**管理和核心服務 — 帶內和帶外管理**一章。

帶內和帶外管理

ACI交換矩陣節點有兩種管理連線選項；帶外(OOB)管理裝置背面的專用物理管理埠，帶內(INB)使用管理租戶中的特定EPG/BD/VRF調配並帶有一定程度的可配置引數。管理(「mgmt」)租戶中存在一個OOB EPG，但預設情況下該租戶存在且無法修改。僅允許配置提供的OOB合約。在APIC上，在「ifconfig」命令輸出中觀察到OOB介面為「oobmgmt」，帶內介面將由「bond.x」介面表示，其中是為帶內EPG配置的封裝VLAN。

```
apic1# ifconfig oobmgmt
oobmgmt: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.4.20  netmask 255.255.255.0  broadcast 192.168.4.255
        inet6 fe80::7269:5aff:feca:2986  prefixlen 64  scopeid 0x20
        ether 70:69:5a:ca:29:86  txqueuelen 1000  (Ethernet)
        RX packets 495815  bytes 852703636 (813.2 MiB)
```

```
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 432927  bytes 110333594 (105.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


apic1# ifconfig bond0.300
bond0.300: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1496
        inet 10.30.30.254  netmask 255.255.255.0  broadcast 10.30.30.255
        inet6 fe80::25d:73ff:fec1:8d9e  prefixlen 64  scopeid 0x20
        ether 00:5d:73:c1:8d:9e  txqueuelen 1000  (Ethernet)
        RX packets 545  bytes 25298 (24.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6996  bytes 535314 (522.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

在枝葉上，OOB介面在「ifconfig」命令輸出中視為「eth0」，INB被視為專用SVI。使用者可以用「ifconfig」或「show ip interface vrf mgmt：」檢視介面，其中是為帶內VRF選擇的名稱。

```
leaf101# show interface mgmt 0
mgmt0 is up
admin state is up,
  Hardware: GigabitEthernet, address: 00fc.baa8.2760 (bia 00fc.baa8.2760)
  Internet Address is 192.168.4.23/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec
  reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, medium is broadcast
  Port mode is routed
  full-duplex, 1000 Mb/s
  Beacon is turned off
  Auto-Negotiation is turned on
  Input flow-control is off, output flow-control is off
  Auto-mdix is turned off
  EtherType is 0x0000
  30 seconds input rate 3664 bits/sec, 4 packets/sec
  30 seconds output rate 4192 bits/sec, 4 packets/sec
  Rx
    14114 input packets 8580 unicast packets 5058 multicast packets
    476 broadcast packets 2494768 bytes
  Tx
    9701 output packets 9686 unicast packets 8 multicast packets
    7 broadcast packets 1648081 bytes


leaf101# show ip interface vrf mgmt:inb
  IP Interface Status for VRF "mgmt:inb-vrf"
  vlan16, Interface status: protocol-up/link-up/admin-up, iod: 4, mode: pervasive
    IP address: 10.30.30.1, IP subnet: 10.30.30.0/24
    secondary IP address: 10.30.30.3, IP subnet: 10.30.30.0/24
    IP broadcast address: 255.255.255.255
  IP primary address route-preference: 0, tag: 0
```

'show ip interface vrf mgmt:'將顯示帶內管理BD子網IP作為輔助IP地址；這是預期輸出。

在脊柱交換機上，帶內管理IP地址被新增為「mgmt：」VRF中的專用環回介面。因此，此實施與枝葉交換機上的帶內管理IP實施不同。觀察主**乾交換機上下面的「show ip int vrf mgmt**：」命令輸出

```
spine201# show ip interface vrf mgmt:inb
```

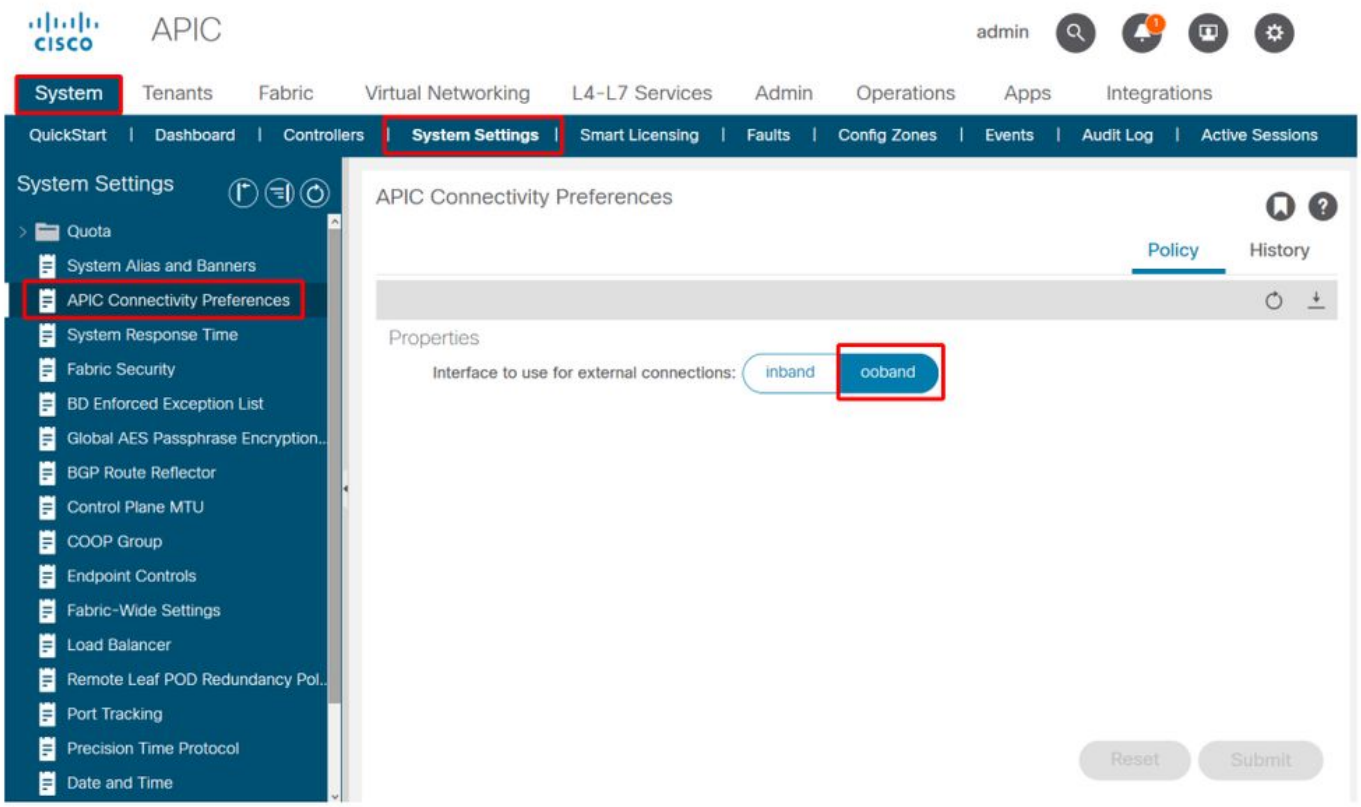
```
  IP Interface Status for VRF "mgmt:inb"
  lo10, Interface status: protocol-up/link-up/admin-up, iod: 98, mode: pervasive
    IP address: 10.30.30.12, IP subnet: 10.30.30.12/32
    IP broadcast address: 255.255.255.255
 IP primary address route-preference: 0, tag: 0
```

在System Settings（系統設定）下，有一個設定用於選擇APIC的帶內或帶外連線首選項。

只有從APIC傳送的流量將使用「APIC連線首選項」中選擇的管理首選項。 APIC仍可以在帶內或帶外接收流量（假設已配置其中之一）。APIC使用以下轉發邏輯：

- 傳入介面並流出同一介面的資料包。
- 源自APIC且目的地為直連網路的資料包從直連介面發出。
- 根據APIC連線首選項，源自APIC、目的地為遠端網路的資料包優先選擇帶內或帶外。

APIC連線首選項



已選擇OOB的APIC路由表。觀察oobmgmt介面的度量值16，該度量值低於bond0.300帶內管理介面度量32。這意味著oobmgmt帶外管理介面將用於傳出管理流量。

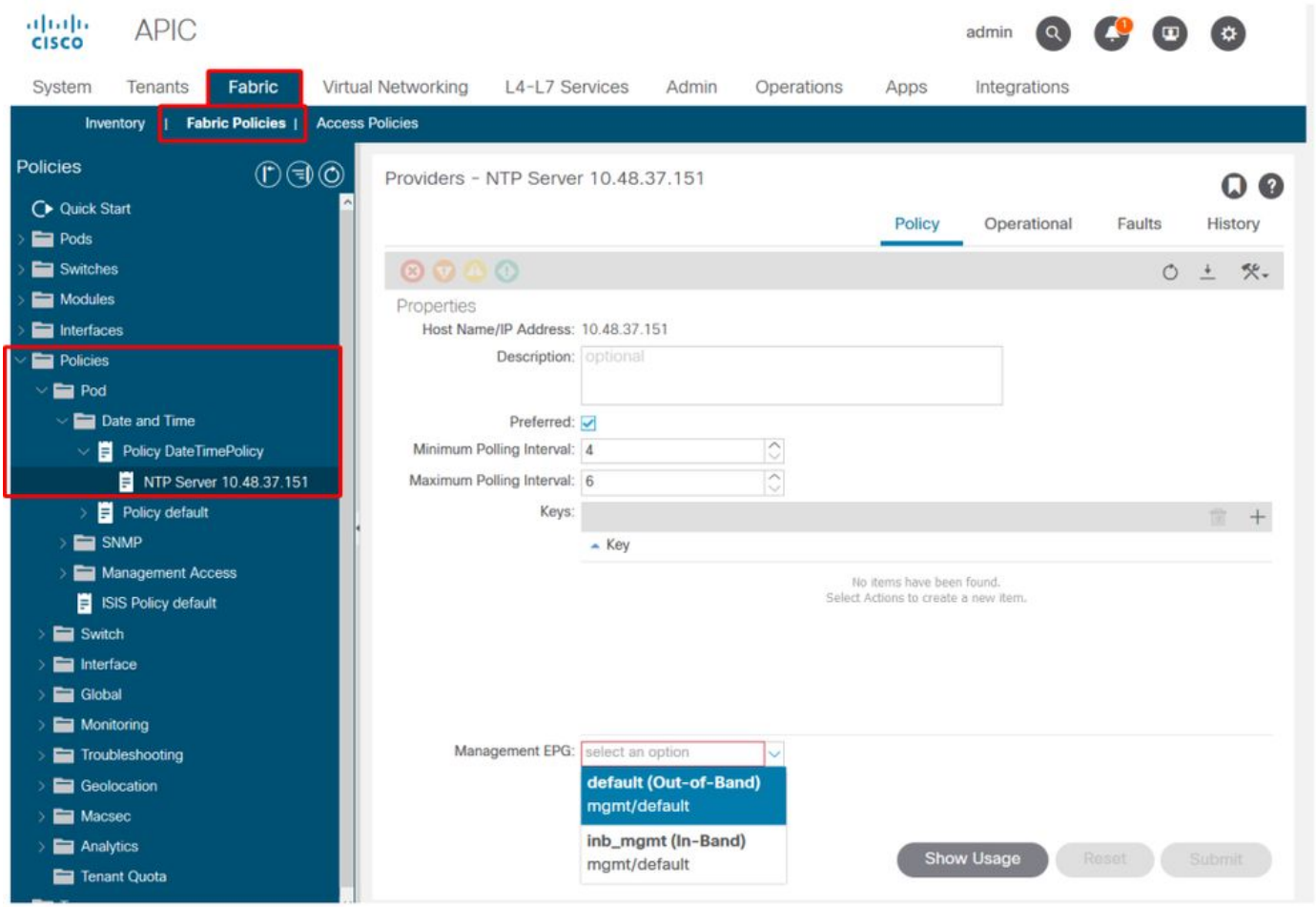
```
apic1# bash
admin@apic1:~> route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.4.1     0.0.0.0         UG    16     0        0 oobmgmt
0.0.0.0         10.30.30.1      0.0.0.0         UG    32     0        0 bond0.300
```

選擇帶內的APIC路由表。觀察bond0.300帶內管理介面的度量（如果為8，現在該度量低於oobmgmt介面度量16）。這意味著bond0.300帶內管理介面將用於傳出管理流量。

```
admin@apic1:~> route -n
```

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.30.30.1      0.0.0.0         UG    8      0        0 bond0.300
0.0.0.0         192.168.4.1     0.0.0.0         UG    16     0        0 oobmgmt
```

枝葉和主幹節點管理首選項不受此設定的影響。這些連線首選項是在協定策略下選擇的。以下是NTP的示例。



如果在「APIC連線首選項」下選擇了帶內，但在協定下選擇了帶外，則協定資料包使用哪個介面？

- APIC連線首選項將始終優先於APIC上的協定選擇。
- 枝葉節點則相反，它們只引用協定下的選擇。

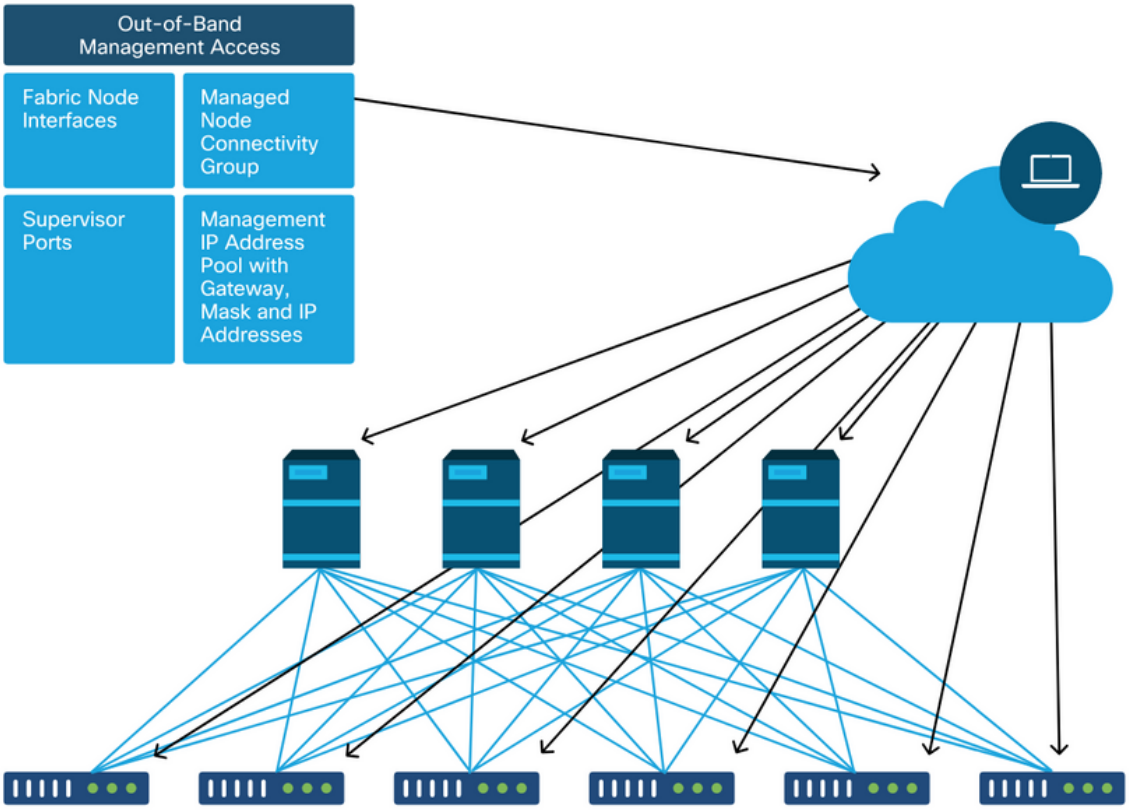
案例：無法訪問管理網路

如果使用者無法訪問管理網路，則可能是因為存在許多不同的問題，但他們始終可以使用相同的方法隔離問題。此案例的假設是使用者無法從L3Out後面到達管理網路中的任何裝置。

- 檢驗APIC連線首選項。圖「APIC連線首選項」中對此進行了概述，選項為OOB或帶內。
- 根據所選的首選項，驗證配置是否正確、介面是否處於啟用狀態、預設網關能否通過所選介面訪問，以及資料包路徑上是否沒有丟包。

不要忘記在GUI中檢查每個配置部分的故障。但是，某些配置錯誤可能會在意外狀態中顯示，但錯誤可能在使用者最初考慮的其他部分中生成。

帶外管理訪問



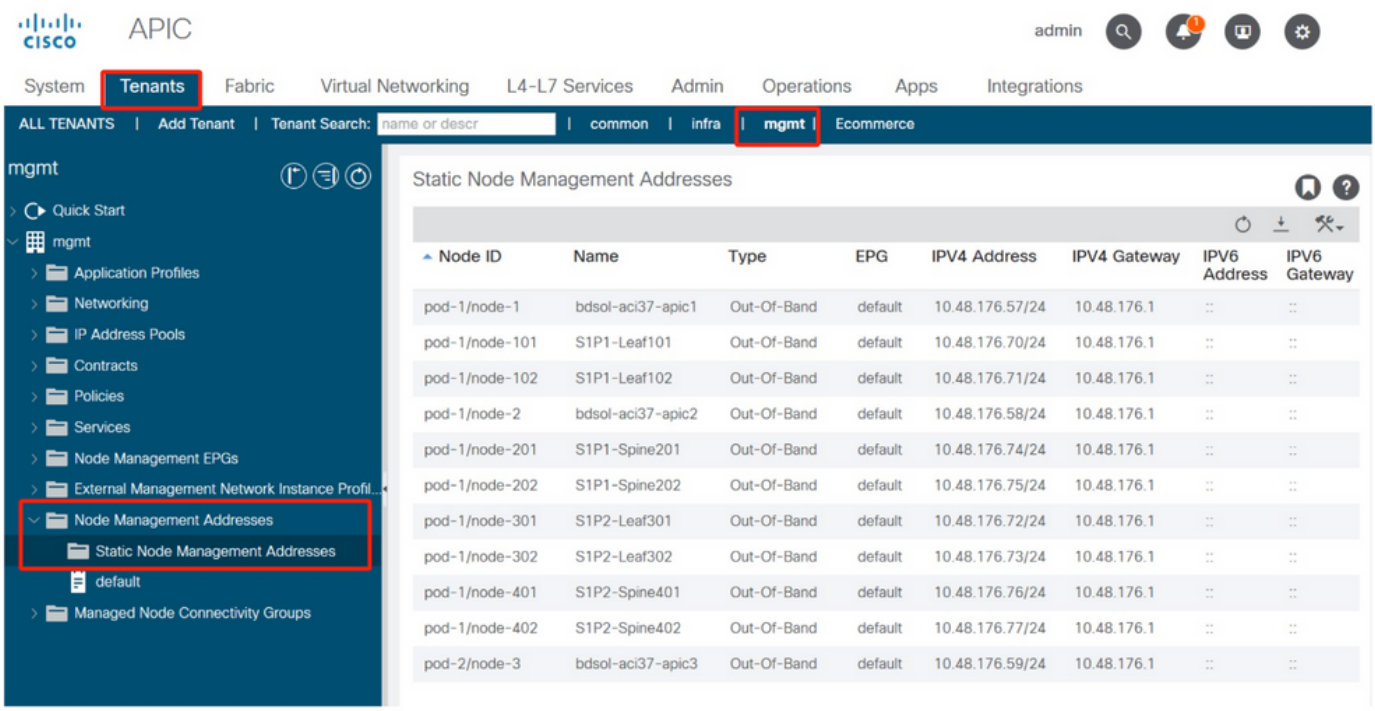
帶外配置驗證

對於帶外配置，需要在名為「mgmt」的特殊租戶下驗證四個資料夾：

- 節點管理地址。
- 節點管理EPG。
- 帶外合約（根據合約）。
- 外部網路例項配置檔案。

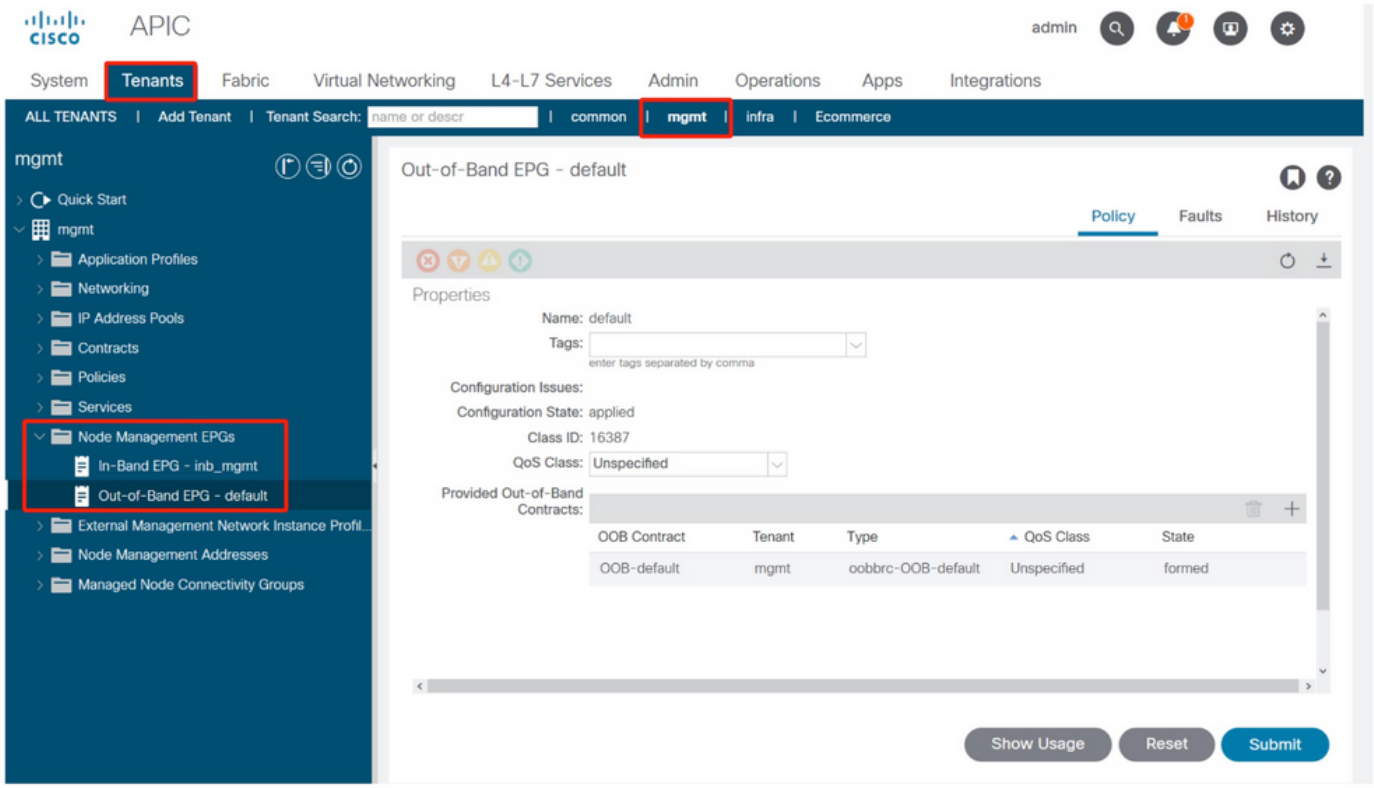
節點管理地址可以靜態分配，也可以從池中分配。以下是靜態地址分配的示例。驗證是否分配了帶外IP地址型別以及預設網關是否正確。

靜態節點管理地址GUI驗證



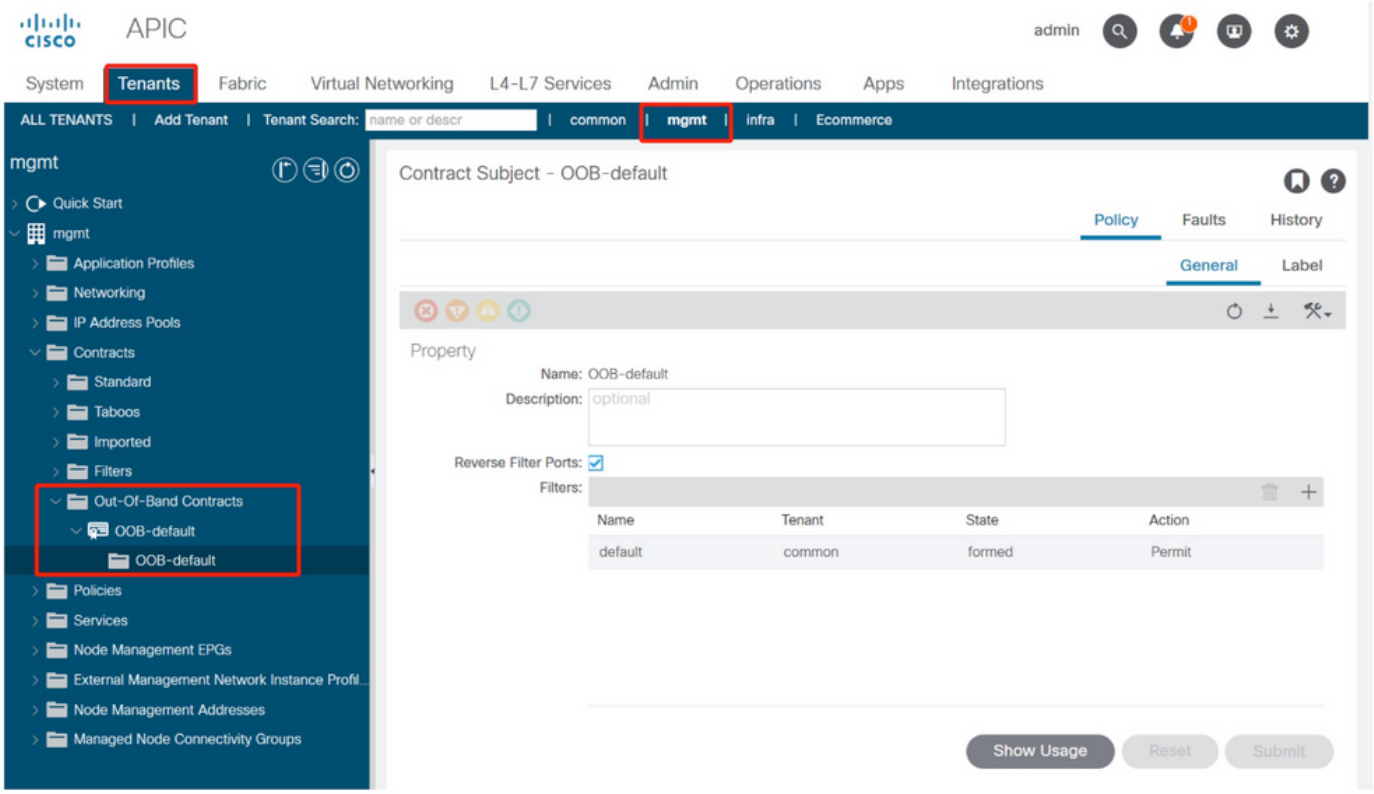
帶外EPG應位於節點管理EPG資料夾下。

帶外EPG — 預設



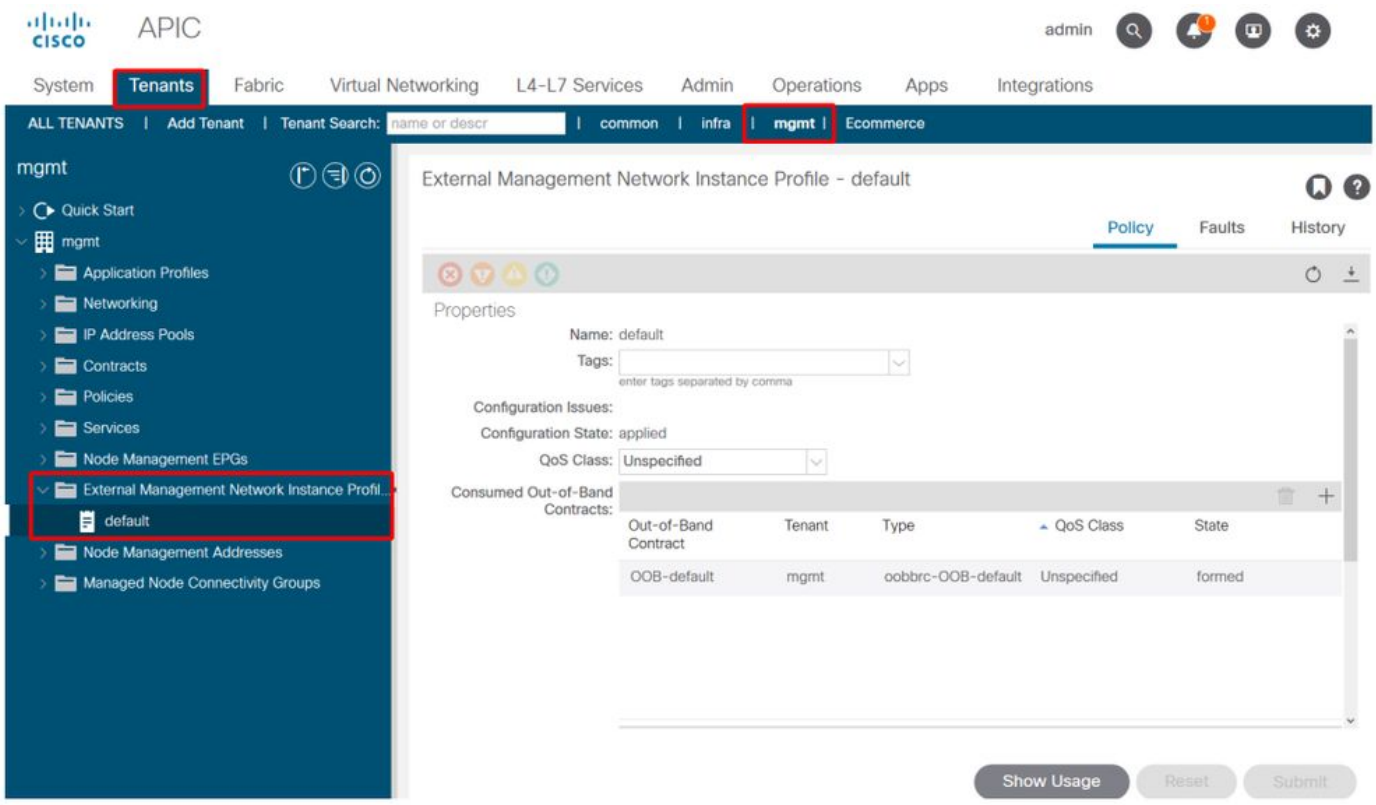
管理哪些管理服務從帶外EPG提供的合約是在帶外合約資料夾中配置的特殊合約。

帶外合約



接下來，驗證是否建立了外部管理網路例項配置檔案，以及是否將正確的帶外合約配置為「使用的帶外合約」。

外部管理網路例項配置檔案



接下來要檢驗的專案是介面狀態和佈線，然後是到網關的連線。

- 要檢查oobmgmt介面是否開啟，請在APIC CLI上輸入「ifconfig oobmgmt」。確認介面標誌為「UP」和「RUNNING」，配置正確的IP地址，以及資料包在RX和TX計數器中增加。如果缺少

任何檢查，請驗證使用的電纜是否正確，以及它們是否連線到APIC上正確的物理管理埠。管理埠將被標籤為Eth1-1和Eth1-2，並且最近的硬體具有帶外介面的oobmgmt標籤。有關APIC背面的物理帶外管理埠的詳細資訊，請參閱「交換矩陣發現」一章中的「初始交換矩陣設定」部分。

```
apic1# ifconfig oobmgmt
oobmgmt: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
inet 192.168.4.20  netmask 255.255.255.0  broadcast 192.168.4.255
inet6 fe80::7269:5aff:feca:2986  prefixlen 64  scopeid 0x20
ether 70:69:5a:ca:29:86  txqueuelen 1000  (Ethernet)
RX packets 295605  bytes 766226440 (730.7 MiB)
RX errors 0  dropped 0  overruns 0  frame 0
TX packets 253310  bytes 38954978 (37.1 MiB)
TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- 要通過OOB檢查網路連線，請使用ping測試資料包通過帶外網路的路徑。

```
apic1# ping 192.168.4.1
PING 192.168.4.1 (192.168.4.1) 56(84) bytes of data.
64 bytes from 192.168.4.1: icmp_seq=1 ttl=255 time=0.409 ms
64 bytes from 192.168.4.1: icmp_seq=2 ttl=255 time=0.393 ms
64 bytes from 192.168.4.1: icmp_seq=3 ttl=255 time=0.354 ms
```

在APIC的bash shell中使用traceroute跟蹤與終端使用者的連線。如果traceroute不完整，請登入此裝置（如果可訪問），ping管理介面並ping主機。根據故障方向，將問題作為傳統網路問題進行故障排除。

Traceroute的工作方式是以1開始，以遞增的TTL傳送UDP封包。如果路由器收到含有TTL 1的封包並需要對其進行路由，便會捨棄該訊框，並向傳送者傳回ICMP無法到達訊息。每個躍點在當前TTL傳送3個UDP資料包，星號表示未收到ICMP無法到達/TTL超出資料包的嘗試。由於某些路由裝置已停用ICMP無法到達/超過TTL訊息，因此當它們收到需要路由的TTL 1封包時，只會捨棄封包而不將訊息傳送回傳送者，因此大多數網路預期會收到這3個星號區塊。

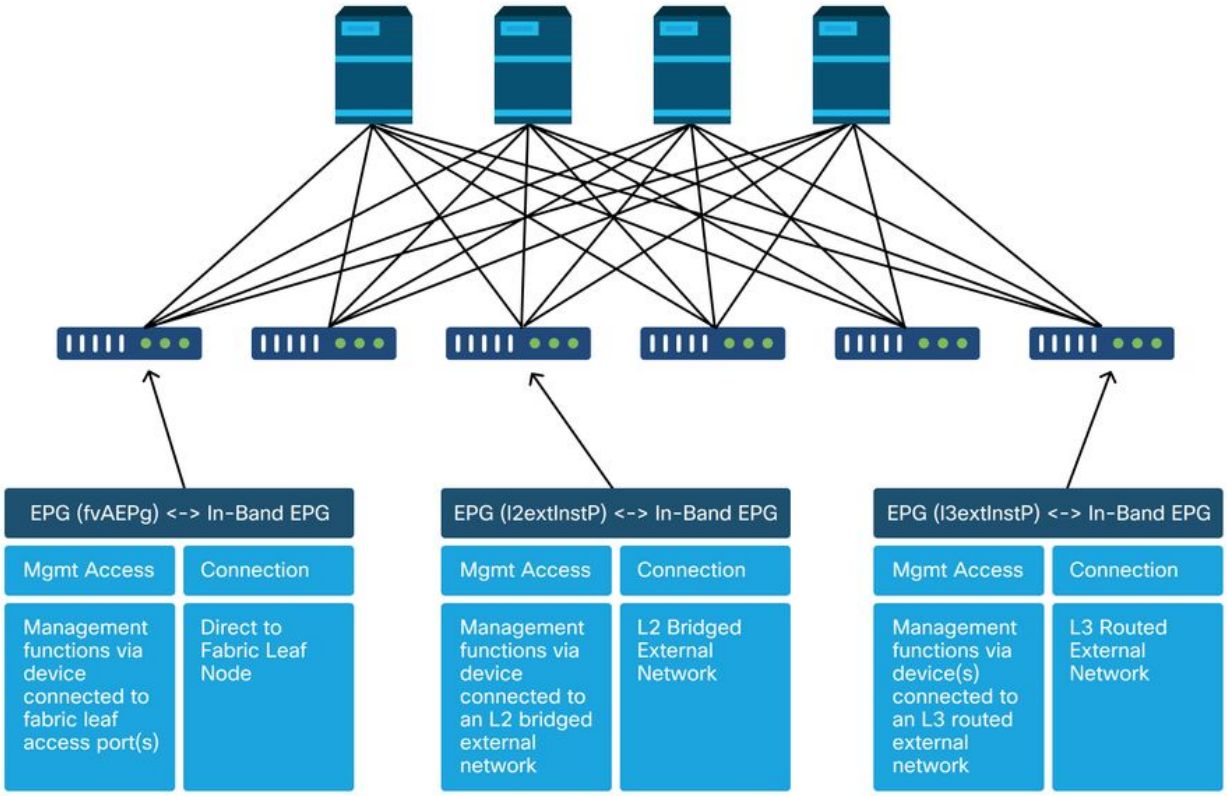
```
apic1# bash
admin@apic1:~> traceroute 10.55.0.16
traceroute to 10.55.0.16 (10.55.0.16), 30 hops max, 60 byte packets
    1  192.168.4.1 (192.168.4.1)  0.368 ms  0.355 ms  0.396 ms
    2  * * *
    3  * * *
    4  10.0.255.221 (10.0.255.221)  6.419 ms 10.0.255.225 (10.0.255.225)  6.447 ms *
    5  * * *
    6  * * *
    7  10.55.0.16 (10.55.0.16)  8.652 ms  8.676 ms  8.694 ms
```

枝葉交換機可以訪問tcpdump命令，該命令可用於驗證哪些資料包通過oobmgmt介面。以下示例捕獲枝葉和主幹交換機上使用的oobmgmt介面「eth0」，並使用「 — n」選項為tcpdump指定IP地址而不是DNS名稱，然後專門為NTP資料包（UDP埠123）進行過濾。 回想一下，在上一個示例中，枝葉正在輪詢NTP伺服器172.18.108.14。下面，使用者可以驗證是否正在通過帶外介面傳輸NTP資料包，以及枝葉正在接收來自伺服器的響應。

```
fab1-leaf101# tcpdump -n -i eth0 dst port 123
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
16:49:01.431624 IP 192.168.4.23.123 > 172.18.108.14.123: NTPv4, Client, length 48
16:49:01.440303 IP 172.18.108.14.123 > 192.168.4.23.123: NTPv4, Server, length 48
```

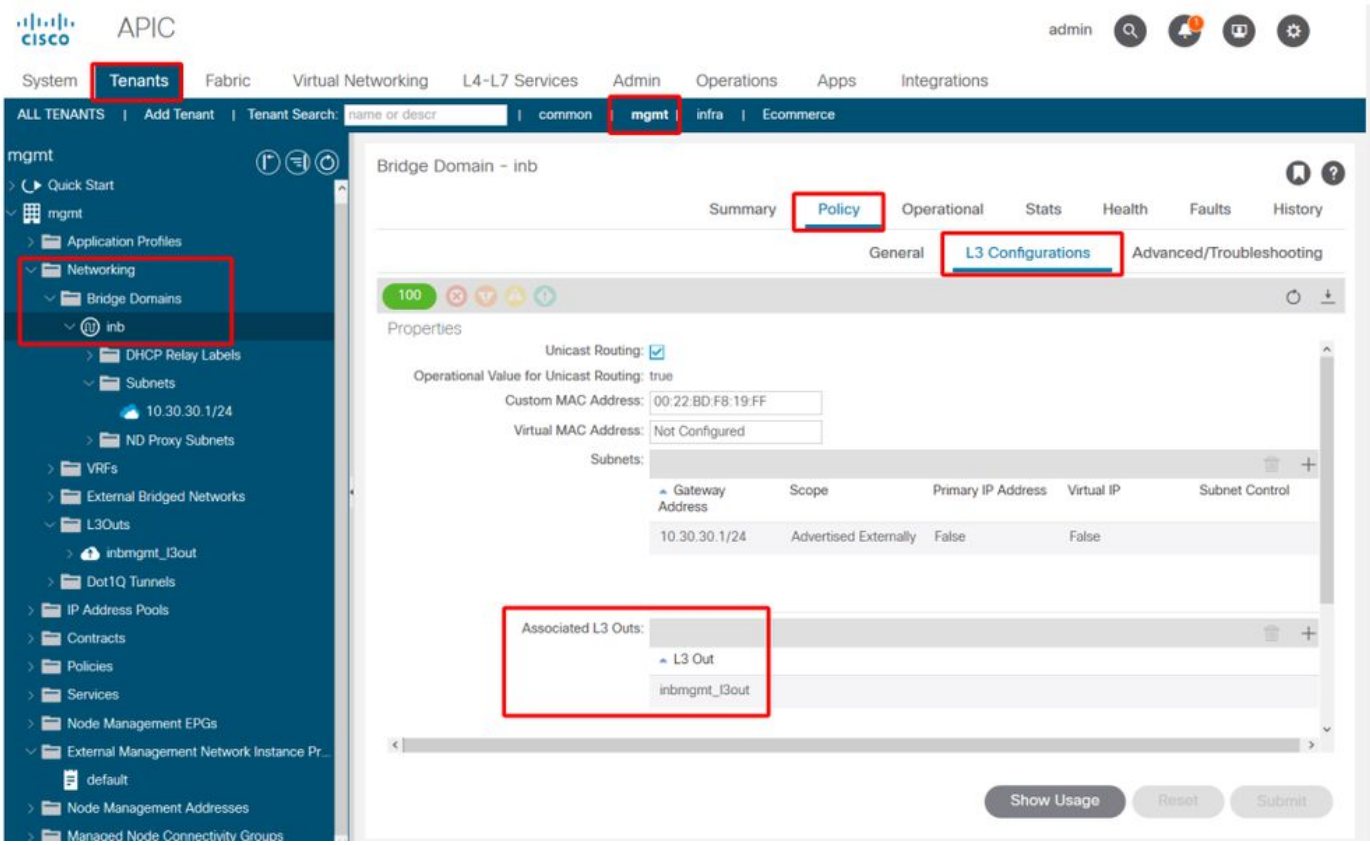
帶內管理配置需要第2層或第3層部署的特定注意事項。本示例僅介紹第3層部署和故障排除。

帶內管理配置



驗證具有子網的管理租戶中是否存在BD，從該子網將帶內節點管理地址分配給交換矩陣節點進行帶內連線，並確保L3Out在帶內管理BD下相關聯。

將充當帶內管理網關的網橋域子網



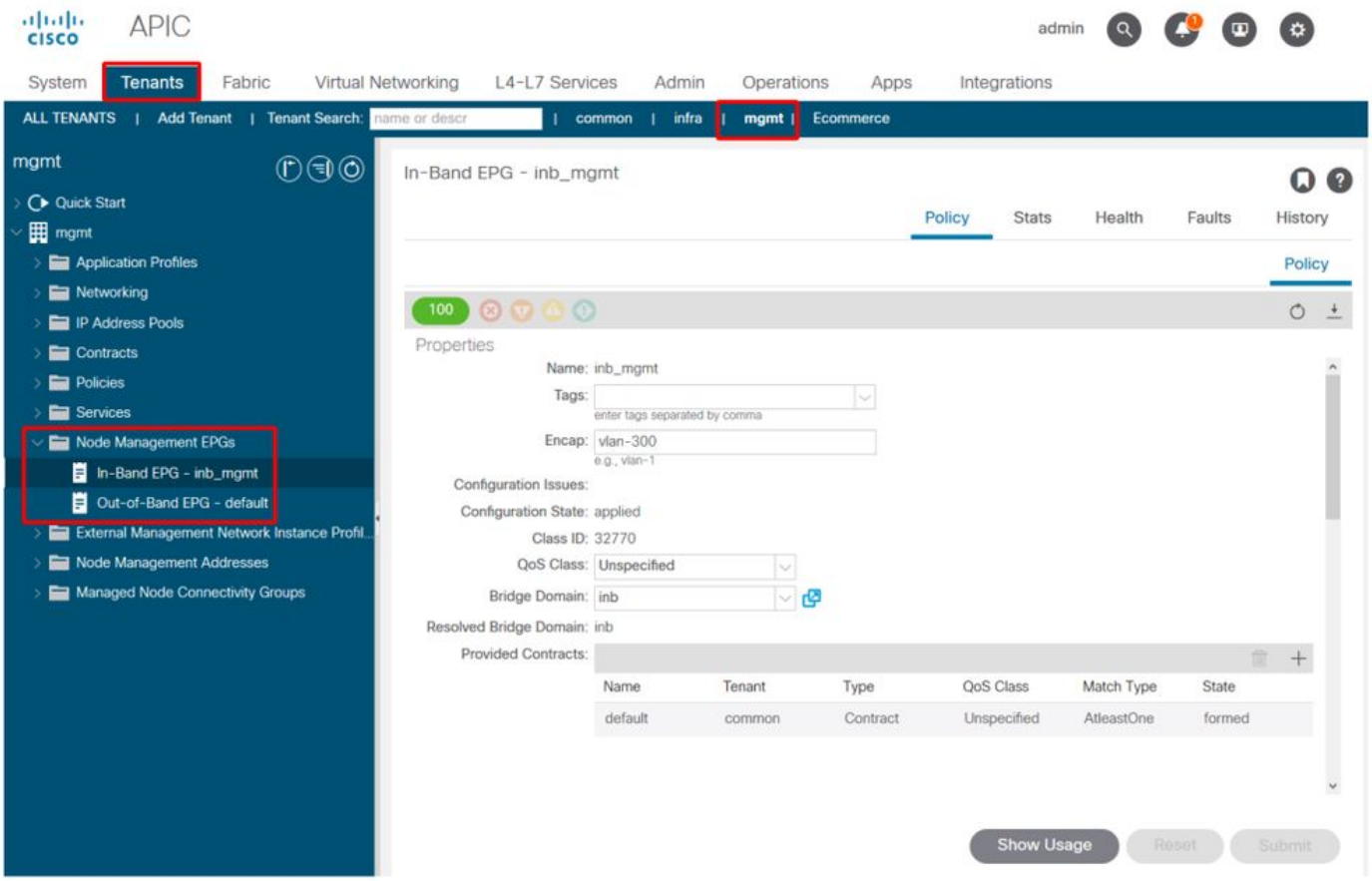
驗證是否存在帶內節點管理EPG。根據下面的螢幕截圖，帶內EPG名稱在GUI中標有字首「inb —」。 驗證帶內EPG封裝VLAN是否與VLAN池正確關聯。

接入策略需要允許帶內管理EPG中配置的封裝VLAN:'inb mgmt EPG encap VLAN > VLAN Pool > Domain > AEP > Interface Policy Group > Leaf Interface Profile > Switch Profile'。 如果未配置支援訪問策略，則會根據下面的螢幕截圖引發代碼F0467的故障。

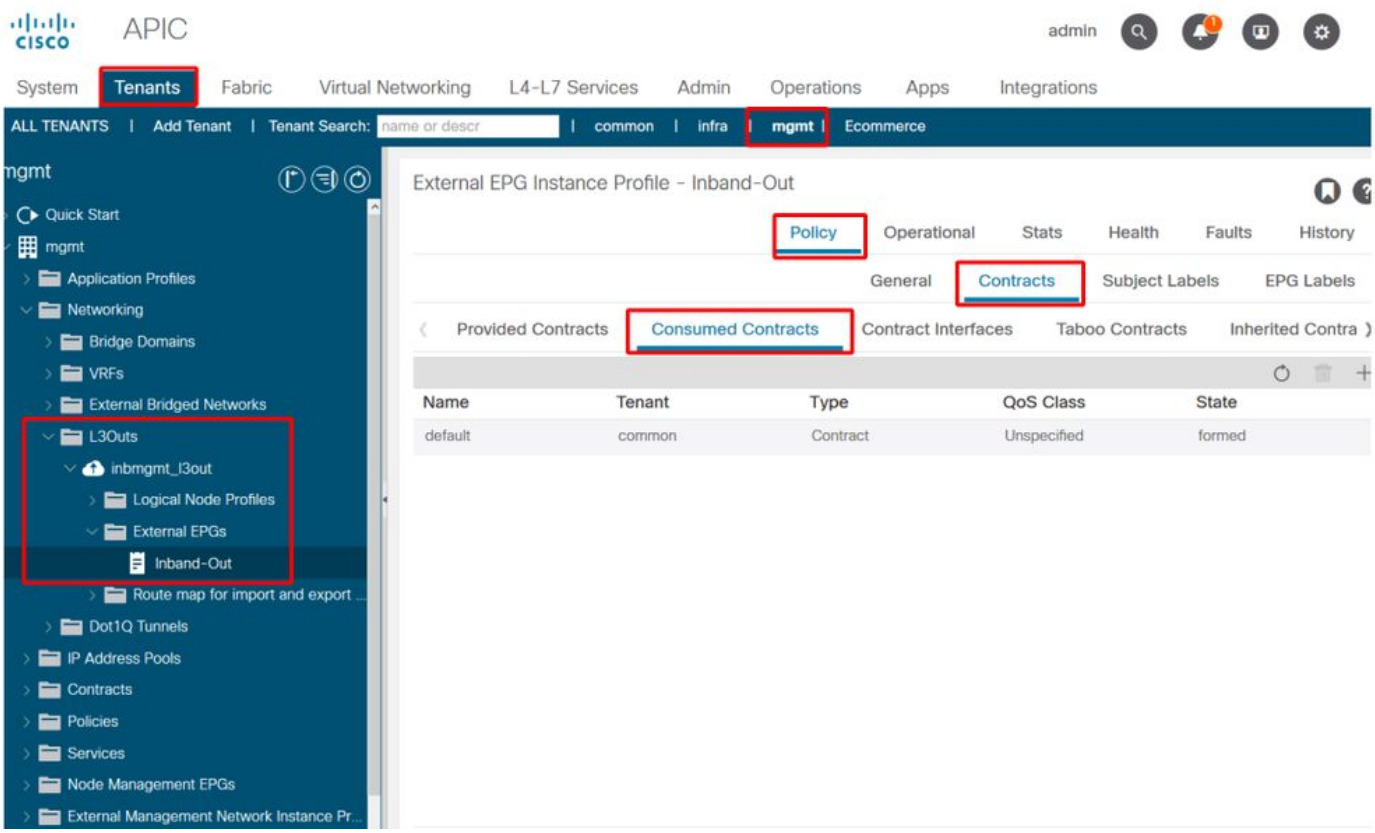
故障F0467 - inb EPG

驗證網橋域是否與上面為帶內子網建立的域相同。最後，驗證帶內管理EPG上是否配置了由外部EPG使用的提供的合約。

帶內EPG

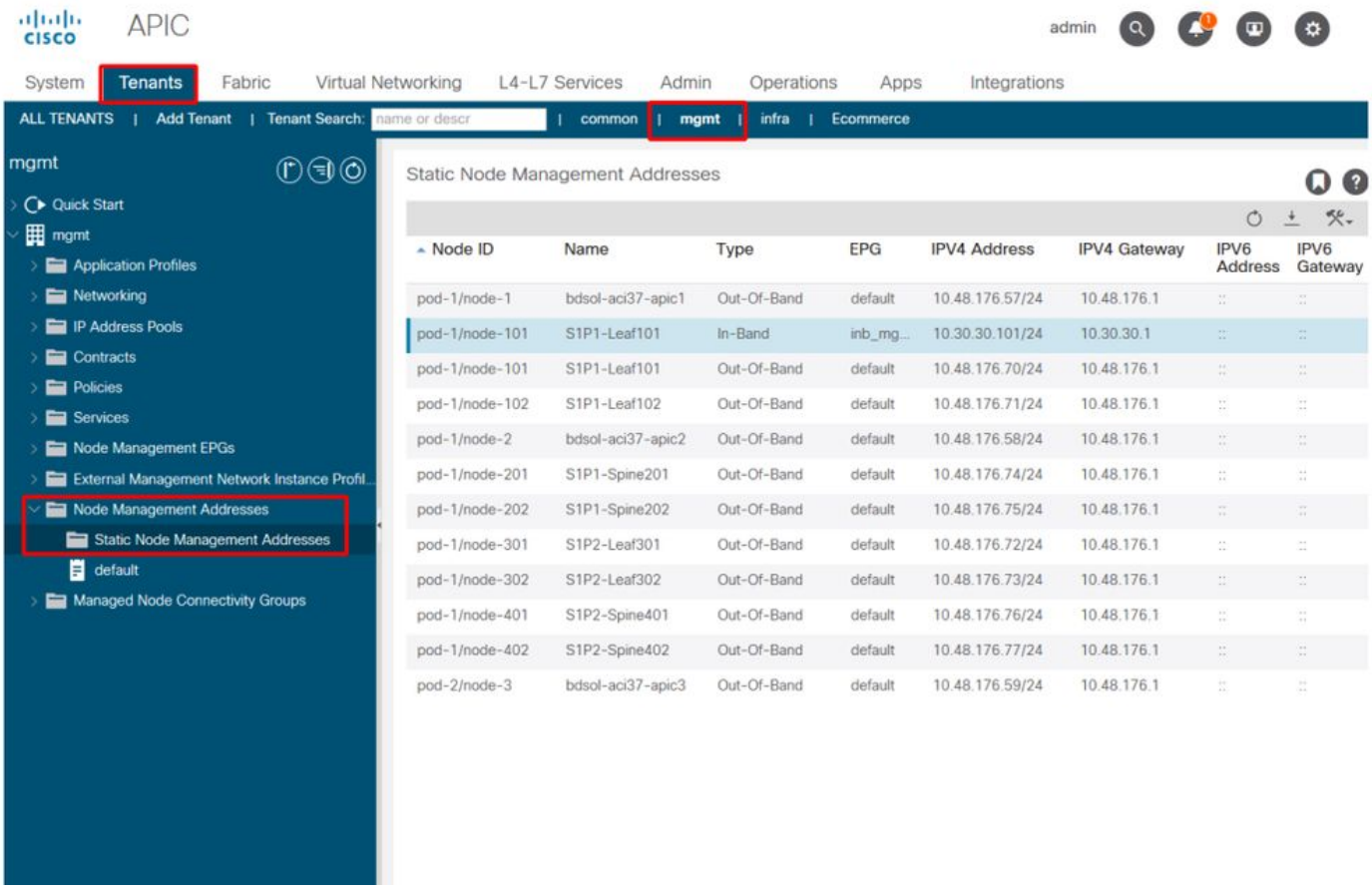


外部EPG例項配置檔案



與帶外類似，交換矩陣節點帶內管理IP地址可以靜態分配，也可以從預先選擇的範圍動態分配。驗證應用於帶內型別的地址是否與之前配置的BD子網匹配。此外，請確認預設網關是否正確。

靜態節點管理地址



如果所有配置都正確，並且上述任何部分都沒有故障，則下一步是在交換機和/或APIC之間執行

ping操作以驗證帶內連線在ACI中是否正常工作。

> 主幹節點不會響應帶內中的ping，因為它們使用環回介面進行連線，而環回介面不會響應ARP。

枝葉交換機上使用的帶內介面為kpm_inb。使用類似的tcpdump捕獲，檢驗資料包是否從帶內CPU介面發出。

```
fab2-leaf101# tcpdump -n -i kpm_inb dst port 123
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on kpm_inb, link-type EN10MB (Ethernet), capture size 65535 bytes
16:46:50.431647 IP 10.30.30.3.123 > 172.18.108.14.123: NTPv4, Client, length 48
16:47:19.431650 IP 10.30.30.3.123 > 172.18.108.15.123: NTPv4, Client, length 48
```

驗證用於帶內的SVI是「protocol-up/link-up/admin-up」。

```
fab1-leaf101# show ip interface vrf mgmt:inb-vrf
IP Interface Status for VRF "mgmt:inb-vrf"
vlan16, Interface status: protocol-up/link-up/admin-up, iod: 4, mode: pervasive
    IP address: 10.30.30.1, IP subnet: 10.30.30.0/24 secondary
    IP address: 10.30.30.3, IP subnet: 10.30.30.0/24
    IP broadcast address: 255.255.255.255
    IP primary address route-preference: 0, tag: 0
```

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）。