

配置並檢驗ACI中的活動/活動L1 PBR

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[拓撲](#)

[為什麼ACI中需要L1服務圖？](#)

[關於L1裝置](#)

[活動/活動L1 PBR](#)

[L1服務圖的配置](#)

[在APIC GUI上驗證L1服務圖](#)

[在APIC CLI上驗證L1服務圖](#)

[流量驗證](#)

簡介

本文檔介紹如何在以應用為中心的基礎設施(ACI)中配置和驗證活動/活動L1服務圖。

必要條件

需求

思科建議您瞭解以下主題：

- 瞭解第3層服務圖在ACI中的工作方式
- 瞭解如何在ACI中配置終端策略組、橋接域和合約

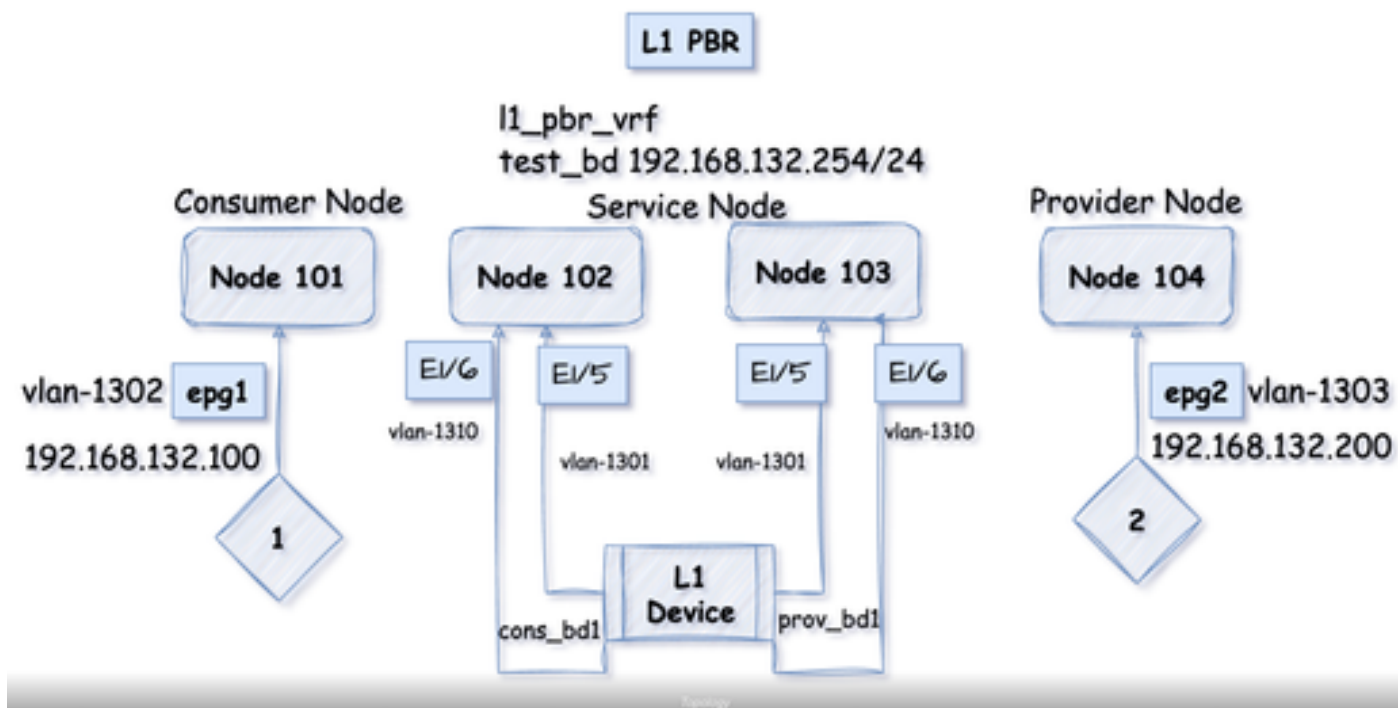
採用元件

本文中的資訊係根據以下軟體和硬體版本：

- APIC版本：5.3(2a)
- 枝葉H/W:N9K-C93180YC-FX、N9K-C93180YC-EX
- 枝葉S/W:n9000-15.3(2a)
- 葉節點101, 102, 103, 104

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響

拓撲



本文檔中未顯示EPG1和EPG2配置，必須在手動配置之前配置該配置，並且必須學習終結點。

1.驗證EPG1端點192.168.132.100 learned (節點101)。

MAC/IP	Endpoint Name	Learning Hosting Server Source	ReportingInterface (learned) Controller Name	Encap	ESG	Policy Tags
10-83-D5-14-13-02 192.168.132.100		learned	Pod-1/Node-101/eth1/5 (learned)	vlan-1302		

2.驗證EPG2已獲取端點192.168.132.200 (節點104)。

MAC/IP	Endpoint Name	Learning Hosting Server Source	ReportingInterface (learned) Controller Name	Encap	ESG	Policy Tags
10-83-D5-14-13-03 192.168.132.200		learned	Pod-1/Node-104/eth1/5 (learned)	vlan-1303		

為什麼ACI中需要L1服務圖？

在思科ACI中，您可以將L4-L7服務裝置插入為L3/L2/L1。第3層表示外部裝置能夠執行路由決策來轉發流量，而第2層表示僅根據MAC地址轉發流量。在ACI中，您可以插入第2層裝置，例如入侵防禦系統(IPS)/透明防火牆。現在考慮以下情況：您要重定向流量的裝置無法做出任何轉發決策，因此在這些情況下，您可以部署L1基於策略的路由(PBR)。

第3層和第2層PBR的流量轉發是相同的，唯一的區別是第3層PBR流量被重定向到IP地址，而第1/第2層PBR流量被重定向到MAC地址。這些MAC地址被靜態繫結到枝葉介面以用於轉發。你將會看到更多這方面的進展。

有關活動/備用或活動/活動L1/L2 PBR使用案例的詳細資訊，請參閱鏈路：[PBR白皮書](#)。

關於L1裝置

在此部署模型中，不會在服務裝置上執行VLAN轉換，並且服務裝置的兩個介面都在同一個VLAN上運行。此方法通常稱為內嵌模式或線路模式，通常用於防火牆和入侵防禦系統(IPS)。當服務裝置需要執行安全功能而不參與第2層或第3層轉發時，這是理想的。

活動/活動L1 PBR

從ACI版本5.0開始，支援以主用/主用模式部署L4-L7裝置的服務圖。這是通過為每個L4-L7裝置介面（具體介面）分配唯一的封裝並在隱藏服務EPG上利用自動配置「封裝中泛洪」的ACI來實現的。此隱藏服務EPG由ACI建立，以便將L4-L7裝置介面與服務橋域相關聯。

管理員不需要手動配置隱藏服務EPG，因為ACI會在服務圖形呈現過程中自動啟用「Flood in encap」。

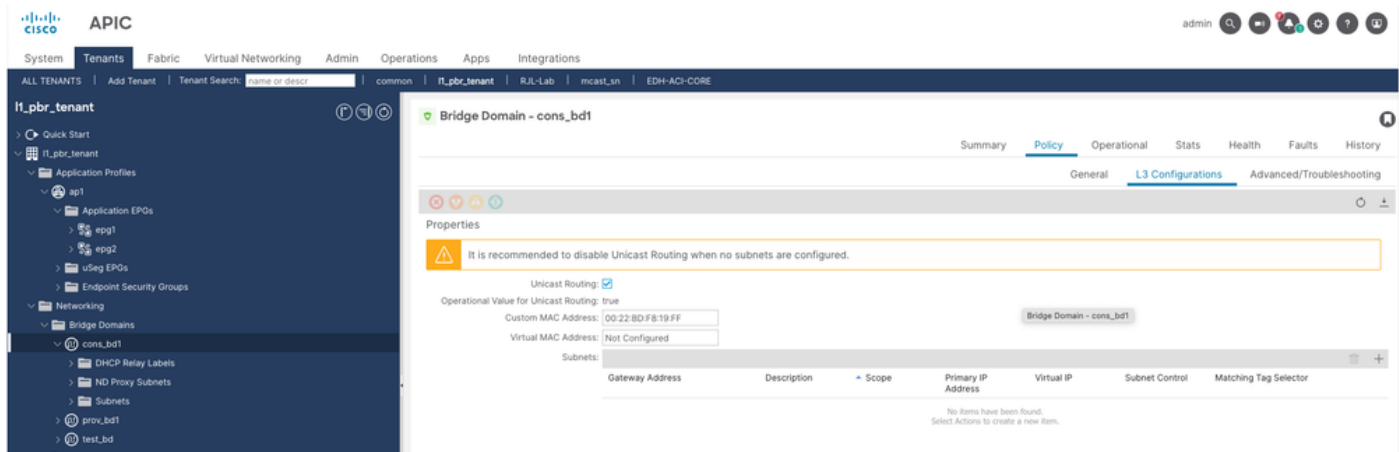
對於L1 PBR主動 — 主動部署，必須配置端口本地範圍。這要求將L4-L7裝置的消費者和提供商群集介面（聯結器）放在不同的物理域中，每個域都有自己的VLAN池，同時在兩個域中保持相同的VLAN範圍。

參考：[PBR白皮書](#)。

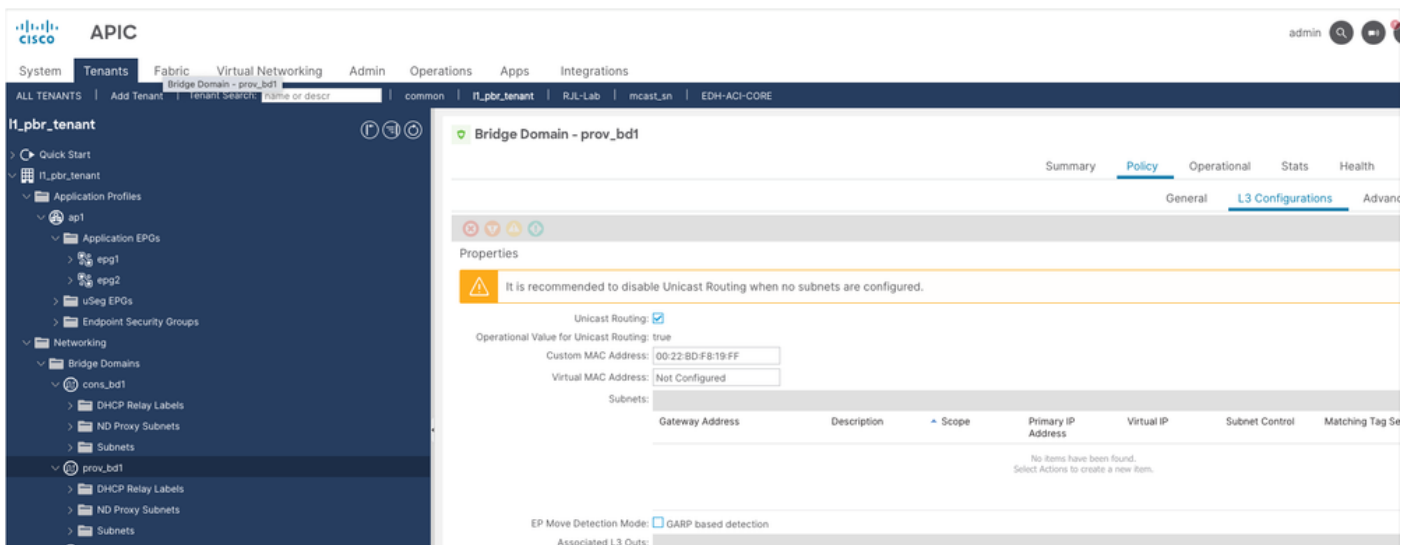
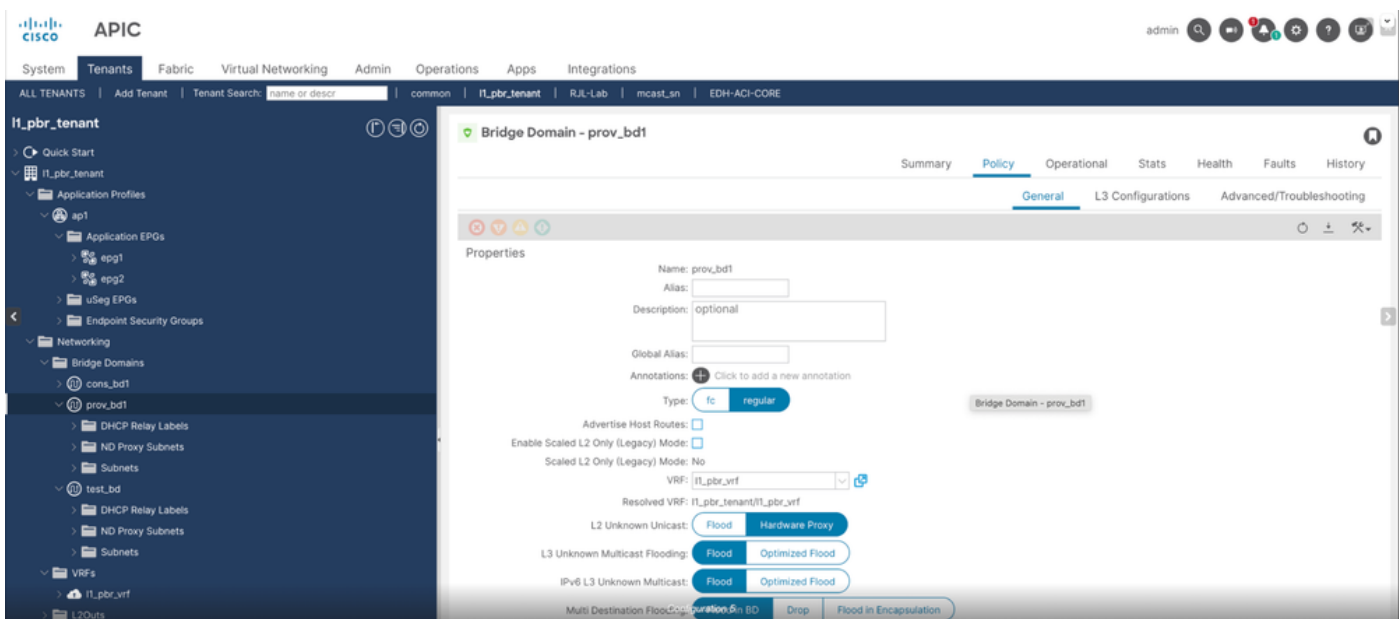
L1服務圖的配置

必須啟用單播路由，L2未知單播必須設定為Hardware proxy，並且不需要子網用於cons和prov網橋域。

步驟1.配置名為cons_bd1的使用者網橋域。

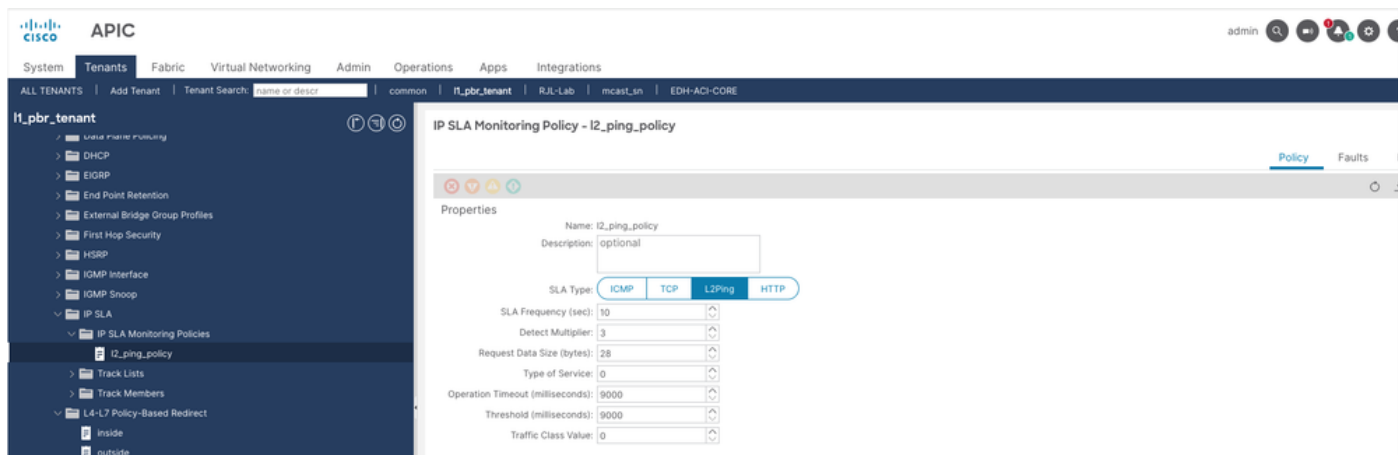


步驟2.配置名為prov-bd1的提供程式橋接域。



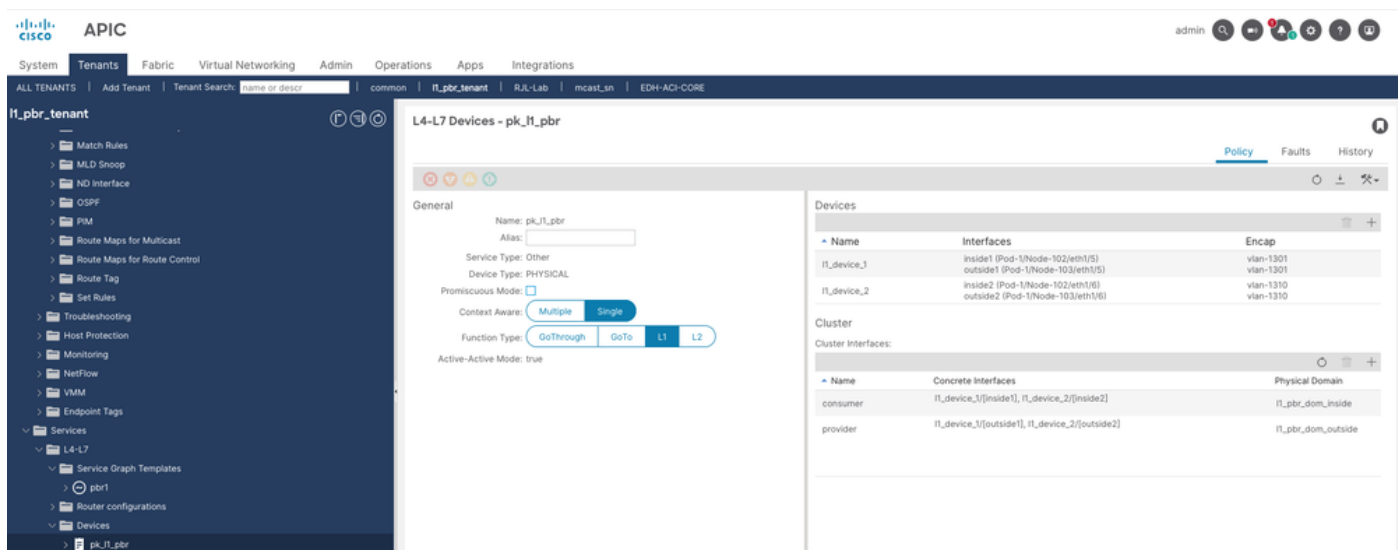
步驟3.使用SLA型別L2Ping配置IP服務級別協定(SLA)策略。

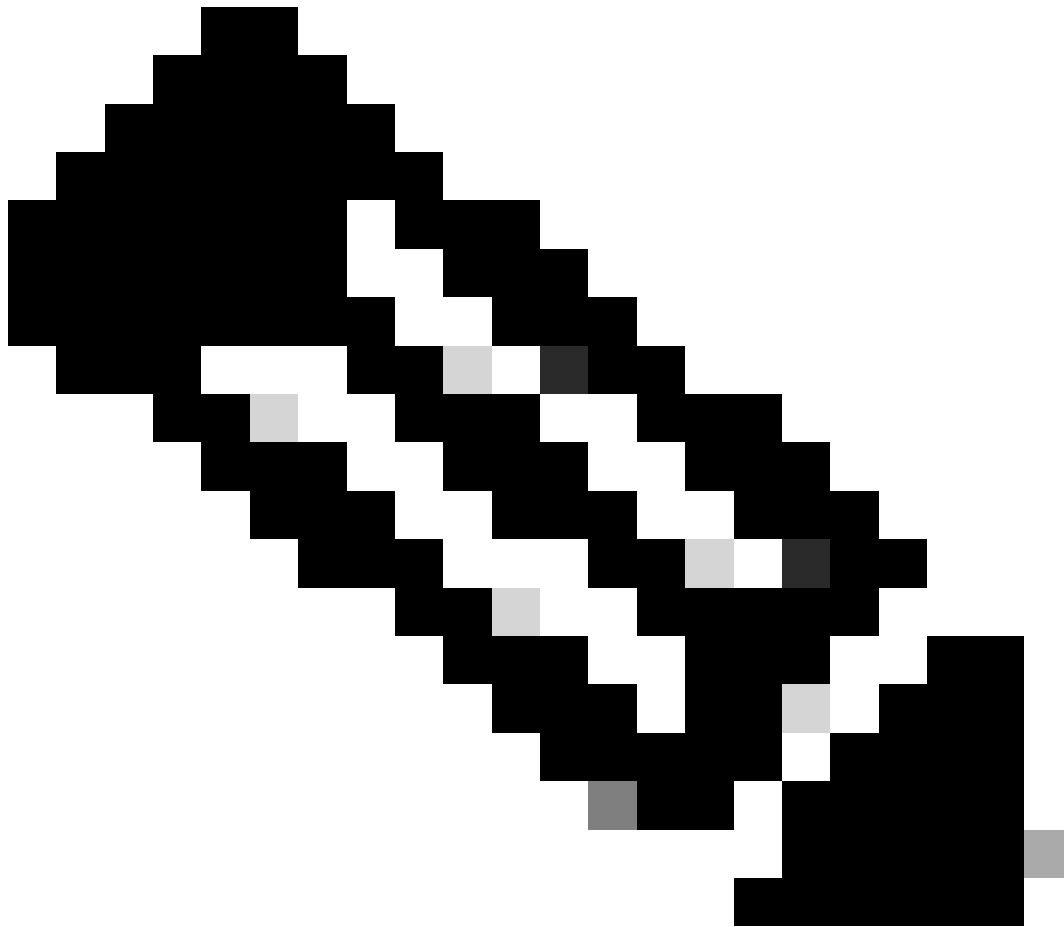
導航到Tenant > Policies > Protocol > IP SLA > IP SLA Monitoring Policies，然後按一下右鍵並建立策略。



步驟4.設定L4/L7裝置。

導航到Tenant > Services > Devices，然後按一下右鍵並建立L4-L7裝置。





附註：對於L1裝置，對於埠本地範圍，每個集群介面必須位於不同的物理域中。

步驟5. 為內部和外部介面配置基於L4-L7策略的重定向。

導航到Tenant > Policies > Protocol > L4-L7 Policy based redirect，然後按一下右鍵並建立策略。

++策略名稱在內部

++我們有兩個L1目標，每個L1裝置一個

Cisco APIC interface showing the configuration for L4-L7 Policy-Based Redirect - inside.

Properties:

- Name: inside
- Description: optional
- Destination Type: L1, L2, L3
- Rewrite source MAC: ☐
- IP SLA Monitoring Policy: i2_ping_policy
- Oper Status: Enabled
- Threshold Enable: ☒
- Min Threshold Percent (percentage): 40
- Max Threshold Percent (percentage): 100
- Threshold Down Action: bypass action, deny action, permit action
- Enable Pod ID Aware Redirection: ☐
- Hashing Algorithm: Destination IP, Source IP, Source IP, Destination IP and Protocol number
- Resilient Hashing Enabled: ☐
- L1/L2 Destinations:

Destination Name	IP	MAC	Redirect Health Group	CIF	Description	Oper Status
inside2	ceda:aaaa2d2-4c82-93ff-d533-76f3-4741	10-B3-D5-14-88-88	HG2	[inside2]		Enabled
inside	8301:bb59:e940-4233-81c6-e007-437e-45f	10-B3-D5-14-99-99	HG1	[inside1]		Enabled

++策略名稱外部

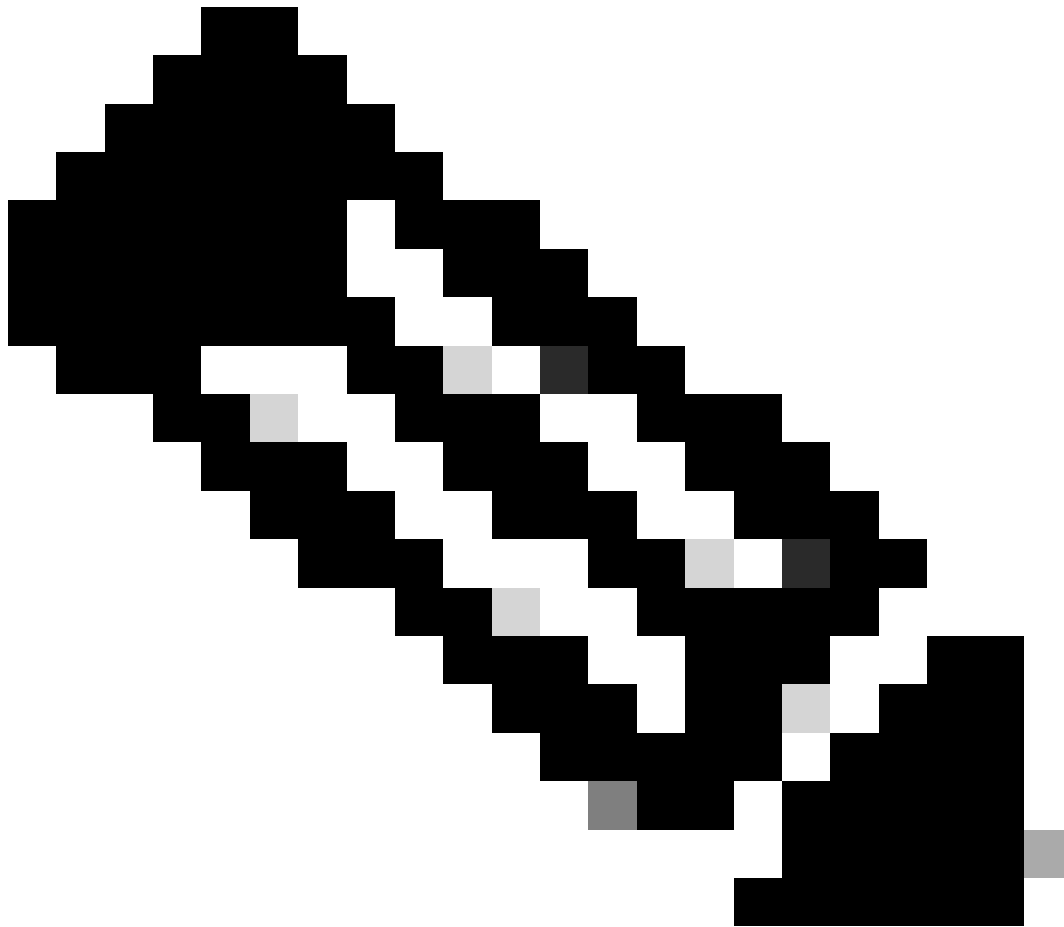
++我們有兩個L1目標，每個L1裝置一個

Cisco APIC interface showing the configuration for L4-L7 Policy-Based Redirect - outside.

Properties:

- Name: outside
- Description: optional
- Destination Type: L1, L2, L3
- Rewrite source MAC: ☐
- IP SLA Monitoring Policy: i2_ping_policy
- Oper Status: Enabled
- Threshold Enable: ☒
- Min Threshold Percent (percentage): 40
- Max Threshold Percent (percentage): 100
- Threshold Down Action: bypass action, deny action, permit action
- Enable Pod ID Aware Redirection: ☐
- Hashing Algorithm: Destination IP, Source IP, Source IP, Destination IP and Protocol number
- Resilient Hashing Enabled: ☐
- L1/L2 Destinations:

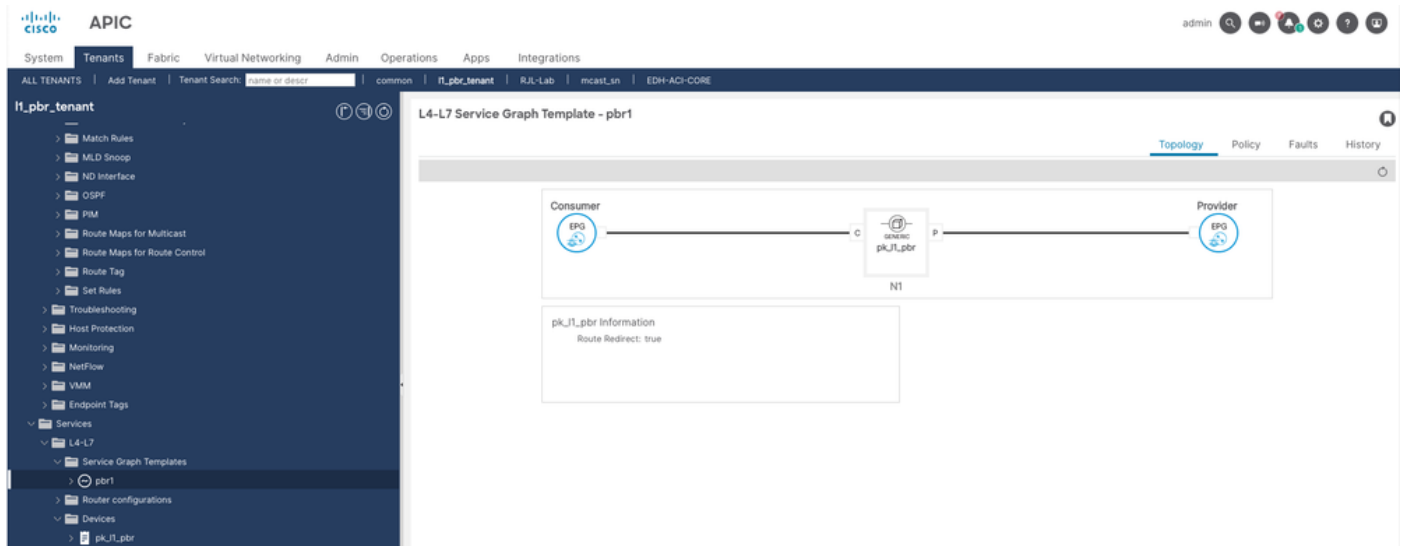
Destination Name	IP	MAC	Redirect Health Group	CIF	Description	Oper Status
outside	2958:ddd3:6eda-4ede-8bb4:1b66:8b19:1eb-4	10-B3-D5-14-66-66	HG1	[outside1]		Enabled
outside2	13fc:5458:d1ef-46a4-b17b-63b5-4946-ae3f	10-B3-D5-14-77-77	HG2	[outside2]		Enabled



附註：兩個L4-L7重定向策略的「閾值關閉」操作必須相同。

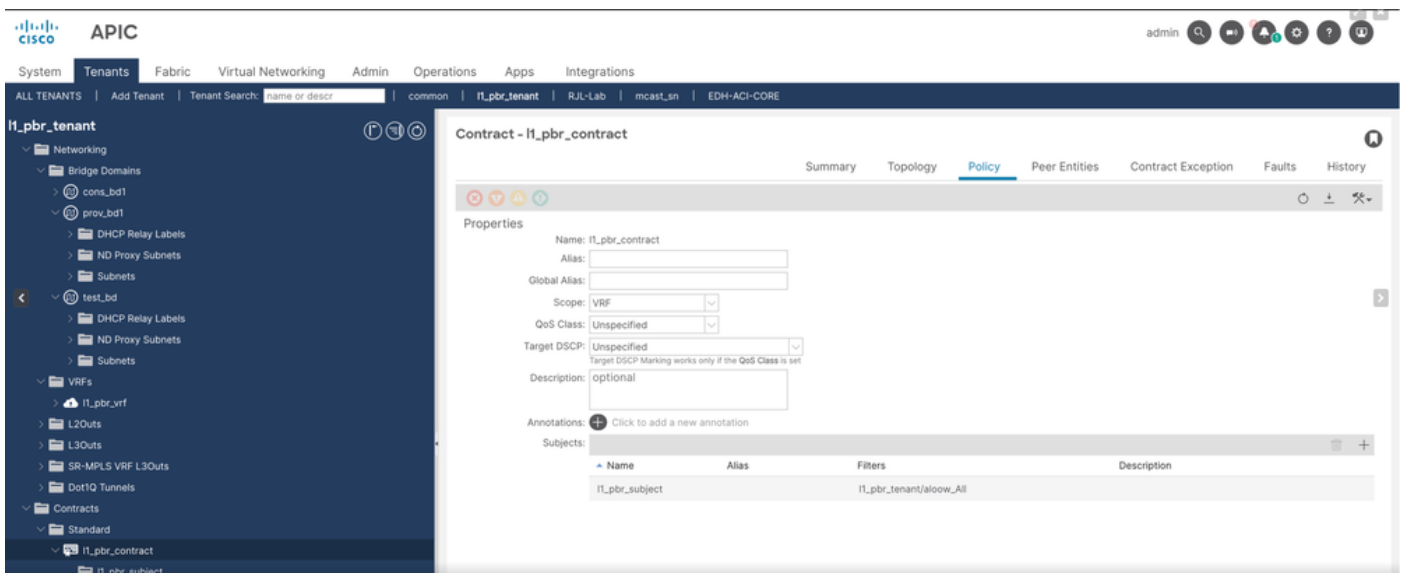
步驟6.配置服務圖模板。

導航到Tenant > Services > Service Graph Template，然後按一下右鍵並建立L4-L7服務圖形模板。

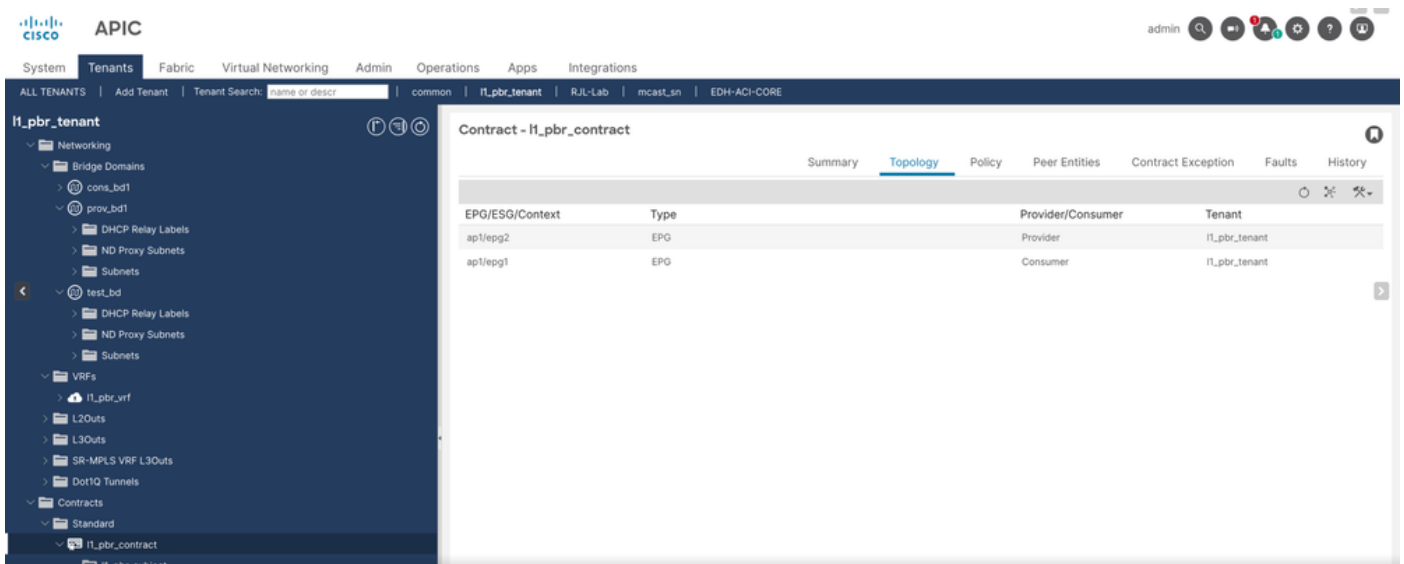


步驟7.建立合約。

導航到Tenant > Contract > Standard，然後按一下右鍵並建立合約。

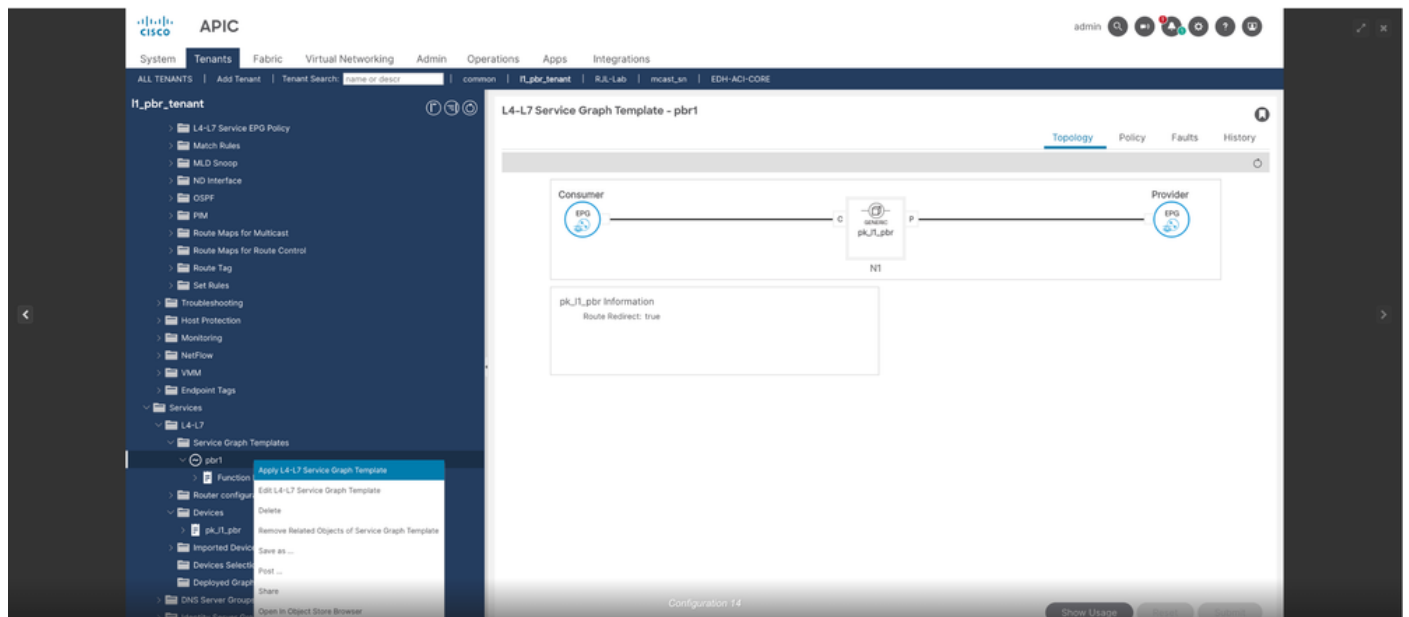


步驟8.將合約作為消費者和提供者分別應用於EPG1和EPG2。



步驟9.應用L4-L7服務圖模板。

導航到Tenant > Services > Service Graph Template，然後按一下右鍵PBR1並應用L4-L7服務圖形模板。



++新增消費者和提供商EPG

++指定合約

Apply L4-L7 Service Graph Template to EPG/ESG(s)

STEP 1 > Contract

1. Contract

2. Graph

Endpoint Group Type

Group Type: Endpoint Policy Group (EPG) Endpoint Security Group (ESG)

Endpoint Group Configuration

Configure an Intra-Endpoint Contract: ☐

Consumer EPG / External Network:

Provider EPG / Internal Network:

Contract Information

Contract Type: New Contract Select Existing Contract Subject

Existing Contracts with Subjects:

Configuration 15

Previous

Cancel

Next

++擊「下一步」

++指定使用者聯結器詳細資訊

Apply L4-L7 Service Graph Template to EPG/ESG(s)

STEP 2 > Graph

Service Graph Template:

Consumer EPG epg1 — C — [pk_l1_pbr] — P — Provider EPG epg2

N1

pk_l1_pbr Information
Policy-Based Redirect: true

Consumer Connector
Type: **General** Route Peering
BD:
BD that connects the two devices

L3 Destination (VIP): ☒
Redirect Policy:
Service EPG Policy:
Cluster Interface:

++指定提供程式連結器詳細資訊

Apply L4-L7 Service Graph Template to EPG/ESG(s)

STEP 2 > Graph

Service Graph Template:

Consumer EPG epg1 — C — [pk_l1_pbr] — P — Provider EPG epg2

N1

Service EPG Policy:
Cluster Interface:

Provider Connector
Type: **General** Route Peering
BD:
BD that connects the two devices

L3 Destination (VIP): ☒
Redirect Policy:
Service EPG Policy:
Cluster Interface:

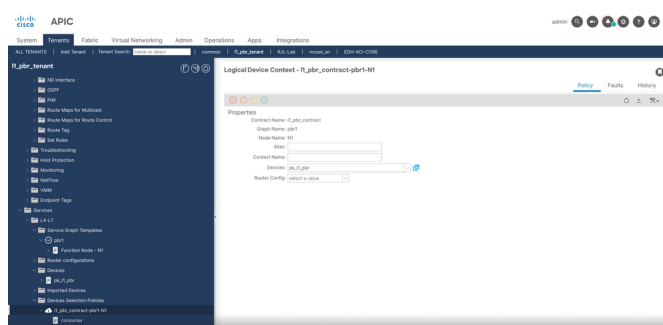
Configuration 17

Previous Cancel Finish

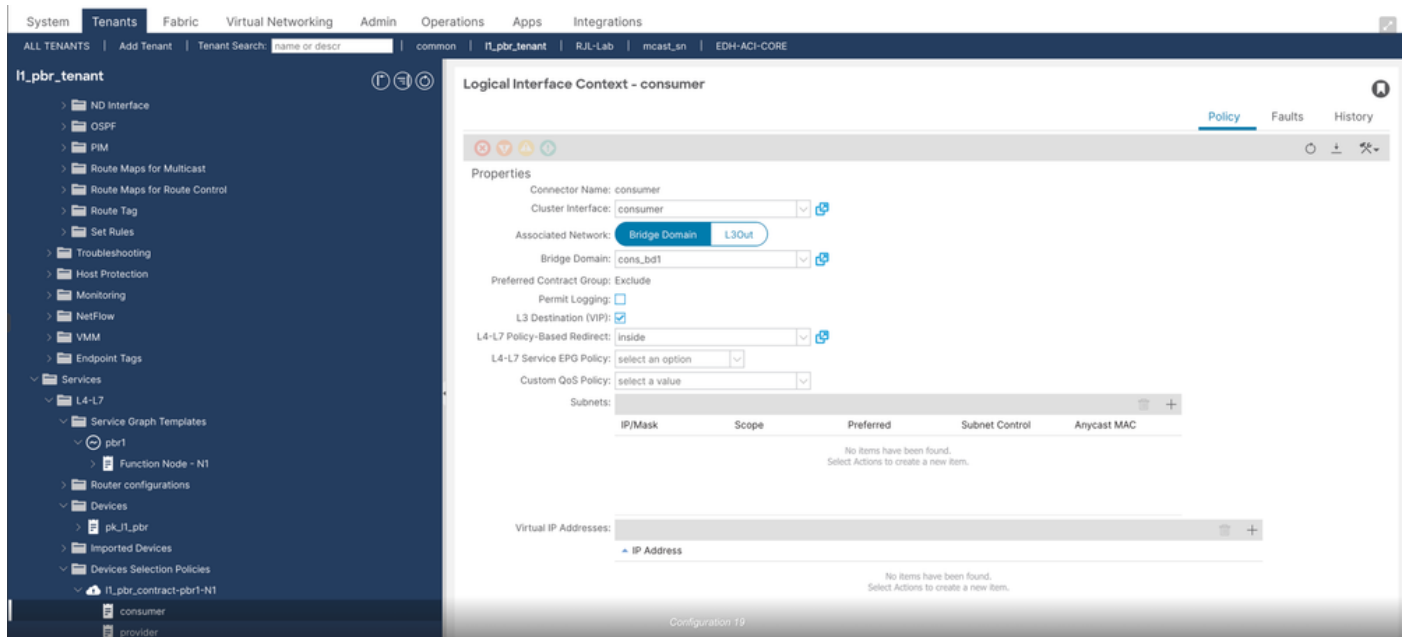
++按一下「完成」

在APIC GUI上驗證L1服務圖

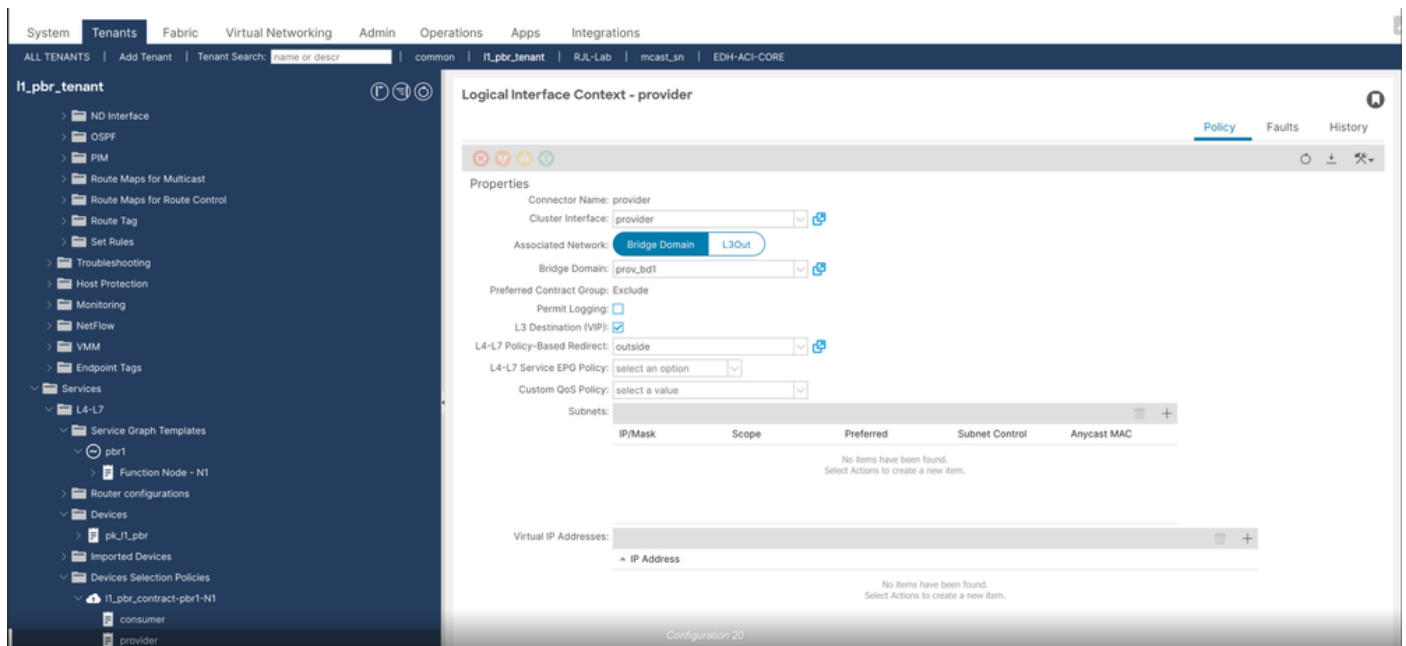
步驟1.驗證應用服務圖模板後建立的裝置選擇策略。



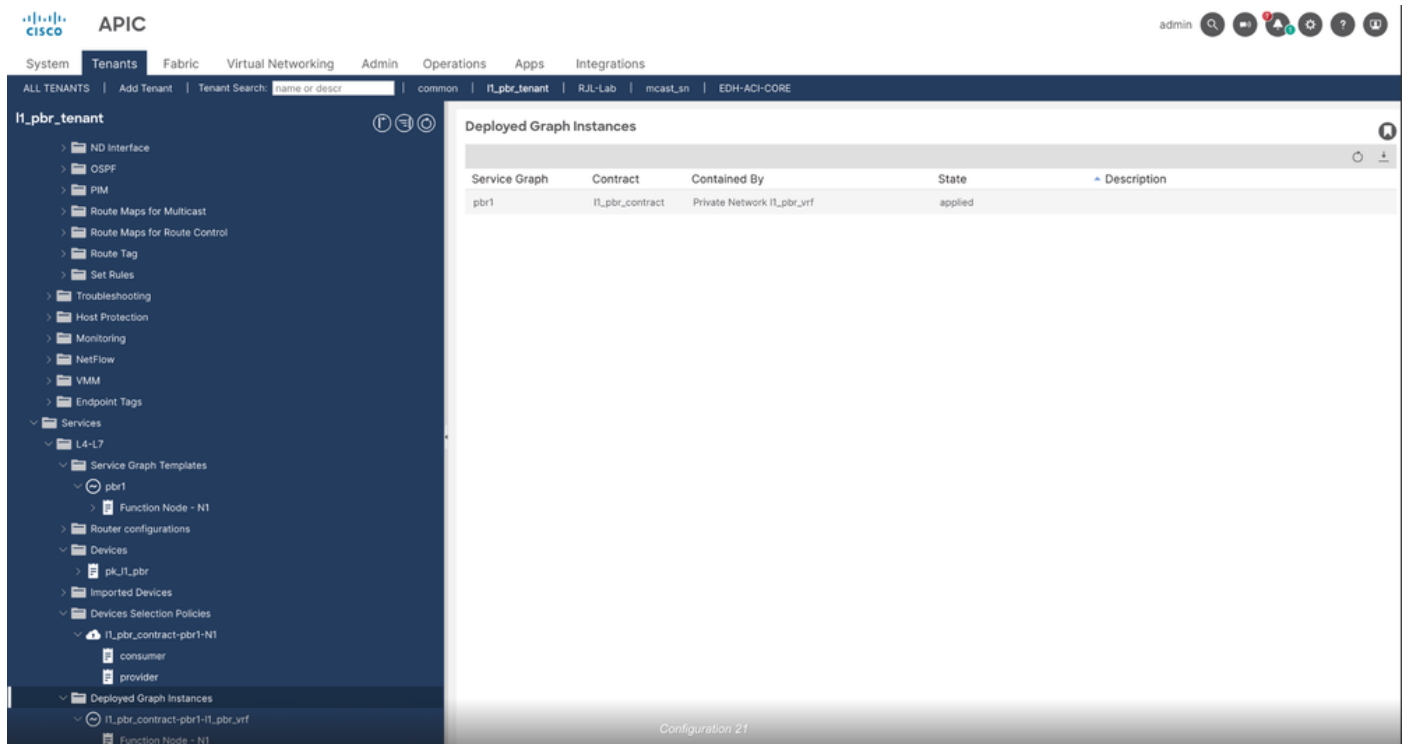
++驗證使用者聯結器



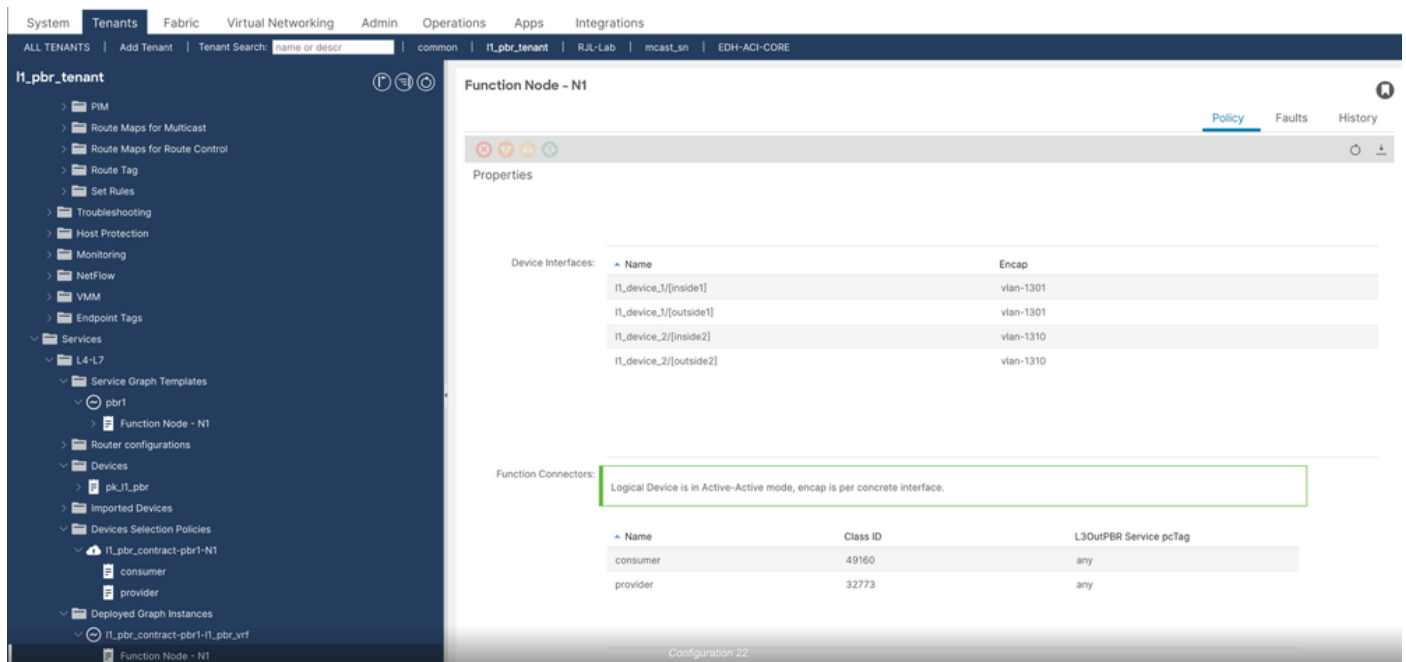
++配置提供程式聯結器



步驟2.驗證部署的圖形例項，您將在其中看到一個例項，該例項必須處於應用狀態。



++檢查裝置介面和功能聯結器，您將在其中看到與服務EPG關聯的PCTAG



在APIC CLI上驗證L1服務圖

步驟1.驗證服務圖是否與運行狀況組狀態一起應用於消費者和提供商節點。

```
<#root>
```

```
apic01#
```

```
fabric 101,104 show service redir info
```

Node 101

=====

LEGEND

TL: Threshold(Low) | TH: Threshold(High) | HP: HashProfile | HG: HealthGrp | BAC: Backup-Dest |

=====

List of Dest Groups

GrpID	Name	destination	HG-name
=====	=====	=====	=====
10	destgrp-10	dest-[476f:9be9:5aab:4454:a5d6:8c9e:7017:61eb]-[vlan-2490369]	11_pbr_tenant::HG2
		dest-[8301:bb59:e940:4233:81c6:e007:437e:45f]-[vlan-2490369]	11_pbr_tenant::HG1
2	destgrp-2	dest-[2958:ddd3:6eda:4ede:8bb4:1b66:8b19:1eb4]-[vlan-2490369]	11_pbr_tenant::HG1
		dest-[d438:790d:6fdb:4485:bab7:197d:ef61:9a59]-[vlan-2490369]	11_pbr_tenant::HG2

List of destinations

Name	bdVnid	vMac	vrfl
=====	=====	=====	=====
dest-[8301:bb59:e940:4233:81c6:e007:437e:45f]-[vlan-2490369]	vxlan-16252846	10:B3:D5:14:99:99	11_pbr_tenant::HG1
dest-[476f:9be9:5aab:4454:a5d6:8c9e:7017:61eb]-[vlan-2490369]	vxlan-16252846	10:B3:D5:14:77:77	11_pbr_tenant::HG2
dest-[2958:ddd3:6eda:4ede:8bb4:1b66:8b19:1eb4]-[vlan-2490369]	vxlan-15794150	10:B3:D5:14:66:66	11_pbr_tenant::HG1
dest-[d438:790d:6fdb:4485:bab7:197d:ef61:9a59]-[vlan-2490369]	vxlan-15794150	10:B3:D5:14:77:77	11_pbr_tenant::HG2

List of Health Groups

HG-Name	HG-OperSt	HG-Dest
=====	=====	=====
11_pbr_tenant::HG1	enabled	dest-[2958:ddd3:6eda:4ede:8bb4:1b66:8b19:1eb4]-[vlan-2490369] dest-[8301:bb59:e940:4233:81c6:e007:437e:45f]-[vlan-2490369]
11_pbr_tenant::HG2	enabled	dest-[d438:790d:6fdb:4485:bab7:197d:ef61:9a59]-[vlan-2490369] dest-[476f:9be9:5aab:4454:a5d6:8c9e:7017:61eb]-[vlan-2490369]

Node 104

=====

LEGEND

TL: Threshold(Low) | TH: Threshold(High) | HP: HashProfile | HG: HealthGrp | BAC: Backup-Dest |

=====

List of Dest Groups

GrpID	Name	destination	HG-name
=====	=====	=====	=====
3	destgrp-3	dest-[d438:790d:6fdb:4485:bab7:197d:ef61:9a59]-[vlan-2490369]	11_pbr_tenant::HG2
		dest-[2958:ddd3:6eda:4ede:8bb4:1b66:8b19:1eb4]-[vlan-2490369]	11_pbr_tenant::HG1
4	destgrp-4	dest-[476f:9be9:5aab:4454:a5d6:8c9e:7017:61eb]-[vlan-2490369]	11_pbr_tenant::HG2
		dest-[8301:bb59:e940:4233:81c6:e007:437e:45f]-[vlan-2490369]	11_pbr_tenant::HG1

List of destinations

Name	bdVnid	vMac	vrfl
=====	=====	=====	=====
dest-[2958:ddd3:6eda:4ede:8bb4:1b66:8b19:1eb4]-[vlan-2490369]	vxlan-15794150	10:B3:D5:14:66:66	11_pbr_tenant::HG1
dest-[d438:790d:6fdb:4485:bab7:197d:ef61:9a59]-[vlan-2490369]	vxlan-15794150	10:B3:D5:14:77:77	11_pbr_tenant::HG2
dest-[476f:9be9:5aab:4454:a5d6:8c9e:7017:61eb]-[vlan-2490369]	vxlan-16252846	10:B3:D5:14:77:77	11_pbr_tenant::HG2
dest-[8301:bb59:e940:4233:81c6:e007:437e:45f]-[vlan-2490369]	vxlan-16252846	10:B3:D5:14:99:99	11_pbr_tenant::HG1

List of Health Groups

HG-Name	HG-OperSt	HG-Dest
=====	=====	=====
l1_pbr_tenant::HG1	enabled	dest-[2958:ddd3:6eda:4ede:8bb4:1b66:8b19:1eb4]-[vx dest-[8301:bb59:e940:4233:81c6:e007:437e:45f]-[vx
l1_pbr_tenant::HG2	enabled	dest-[476f:9be9:5aab:4454:a5d6:8c9e:7017:61eb]-[vx dest-[d438:790d:6fdb:4485:bab7:197d:ef61:9a59]-[vx

步驟2.驗證是否已在服務節點 (102和103) 上建立靜態MAC繫結。

<#root>

apic01#

fabric 102-103 show endpoint vrf l1_pbr_tenant:l1_pbr_vrf

Node 102

Legend:

S - static s - arp L - local O - peer-attached
V - vpc-attached a - local-aged p - peer-aged M - span
B - bounce H - vtep R - peer-attached-r1 D - bounce-to-proxy
E - shared-service m - svc-mgr

VLAN/	Encap	MAC Address	MAC Info/	Interface
Domain	VLAN	IP Address	IP Info	
23/l1_pbr_tenant:l1_pbr_vrf	vlan-1310	10b3.d514.7777	LS	eth1/6
24/l1_pbr_tenant:l1_pbr_vrf	vlan-1301	10b3.d514.9999	LS	eth1/5

Node 103

Legend:

S - static s - arp L - local O - peer-attached
V - vpc-attached a - local-aged p - peer-aged M - span
B - bounce H - vtep R - peer-attached-r1 D - bounce-to-proxy
E - shared-service m - svc-mgr

VLAN/	Encap	MAC Address	MAC Info/	Interface
Domain	VLAN	IP Address	IP Info	
40/l1_pbr_tenant:l1_pbr_vrf	vlan-1310	10b3.d514.7777	LS	eth1/6
1/l1_pbr_tenant:l1_pbr_vrf	vlan-1301	10b3.d514.6666	LS	eth1/5

流量驗證

1.正在從EP1到EP2生成2000 ICMP ping資料包，這些資料包將被重定向到L1裝置。

```
switch1# ping 192.168.132.200 vrf l1_pbr1 count 2000 >>>>> sending 2000 packets
64 bytes from 192.168.132.200: icmp_seq=464 ttl=251 time=0.859 ms
64 bytes from 192.168.132.200: icmp_seq=465 ttl=251 time=0.872 ms
```

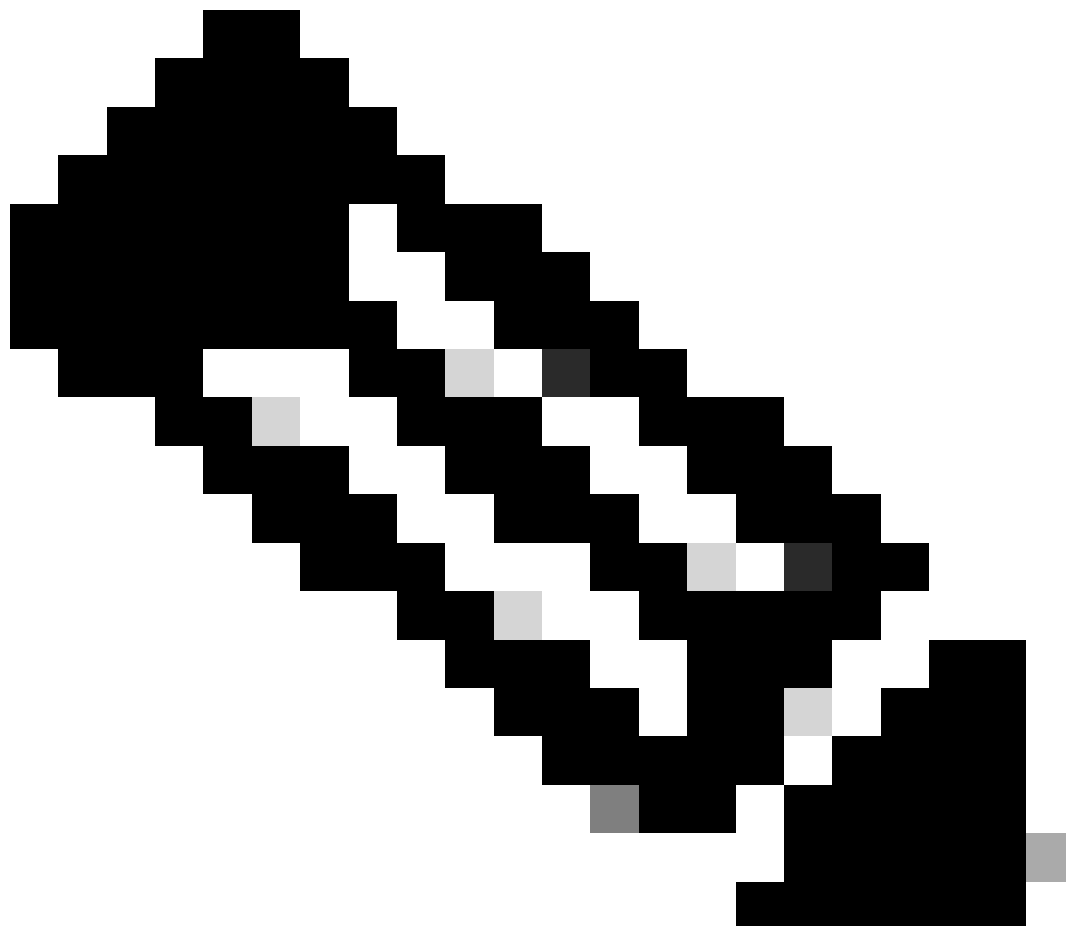
```
64 bytes from 192.168.132.200: icmp_seq=466 ttl=251 time=0.844 ms
64 bytes from 192.168.132.200: icmp_seq=467 ttl=251 time=0.821 ms
64 bytes from 192.168.132.200: icmp_seq=468 ttl=251 time=0.814 ms
64 bytes from 192.168.132.200: icmp_seq=469 ttl=251 time=0.846 ms
64 bytes from 192.168.132.200: icmp_seq=470 ttl=251 time=0.863 ms
64 bytes from 192.168.132.200: icmp_seq=471 ttl=251 time=0.819 ms
64 bytes from 192.168.132.200: icmp_seq=472 ttl=251 time=0.802 ms
64 bytes from 192.168.132.200: icmp_seq=473 ttl=251 time=0.851 ms
64 bytes from 192.168.132.200: icmp_seq=474 ttl=251 time=0.815 ms
```

2. 驗證連線到L1裝置的節點102和103上的介面計數器。

```
apic01# fabric 102-103 show interface ethernet 1/5-6 | grep "Node\|Ethernet\|RX\|packets\|TX"
Node 102
Ethernet1/5 is up
Hardware: 100/1000/10000/25000/auto Ethernet, address: 10b3.d5c5.8f25 (bia 10b3.d5c5.8f25)
30 seconds input rate 0 bits/sec, 0 packets/sec
30 seconds output rate 64 bits/sec, 0 packets/sec
RX
2008 unicast packets 2 multicast packets 0 broadcast packets >>>>>2000 packets recieved from L1 device
2010 input packets 213180 bytes
0 jumbo packets 0 storm suppression bytes
TX
2009 unicast packets 1 multicast packets 0 broadcast packets >>>>> 2000 packets transmitted towards L1
2010 output packets 213003 bytes
0 jumbo packets
Ethernet1/6 is up
Hardware: 100/1000/10000/25000/auto Ethernet, address: 10b3.d5c5.8f26 (bia 10b3.d5c5.8f26)
30 seconds input rate 0 bits/sec, 0 packets/sec
30 seconds output rate 64 bits/sec, 0 packets/sec
RX
9 unicast packets 2 multicast packets 0 broadcast packets
11 input packets 1286 bytes
0 jumbo packets 0 storm suppression bytes
TX
9 unicast packets 1 multicast packets 0 broadcast packets
10 output packets 1003 bytes
0 jumbo packets

Node 103
Ethernet1/5 is up
Hardware: 100/1000/10000/25000/auto Ethernet, address: a453.0e75.9a85 (bia a453.0e75.9a85)
30 seconds input rate 0 bits/sec, 0 packets/sec
30 seconds output rate 64 bits/sec, 0 packets/sec
RX
2009 unicast packets 1 multicast packets 0 broadcast packets >>>>> 2000 packets recieved from L1 device
2010 input packets 213003 bytes
0 jumbo packets 0 storm suppression bytes
TX
2008 unicast packets 1 multicast packets 0 broadcast packets >>> 2000 packets transmitted towards L1 de
2009 output packets 212897 bytes
0 jumbo packets
Ethernet1/6 is up
Hardware: 100/1000/10000/25000/auto Ethernet, address: a453.0e75.9a86 (bia a453.0e75.9a86)
30 seconds input rate 0 bits/sec, 0 packets/sec
30 seconds output rate 64 bits/sec, 0 packets/sec
RX
9 unicast packets 1 multicast packets 0 broadcast packets
```

10 input packets 1003 bytes
0 jumbo packets 0 storm suppression bytes
TX
9 unicast packets 1 multicast packets 0 broadcast packets
10 output packets 1003 bytes
0 jumbo packets



附註：在測試流量之前，已清除節點102和103上的介面計數器。

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）。