Configuración y verificación de PBR L1 activo/activo en ACI

Contenido

Introducción

Este documento describe cómo configurar y verificar Active/Active L1 Service Graph en Application Centric Infrastructure (ACI).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Comprensión del funcionamiento de Layer 3 Service Graph en ACI
- Información sobre cómo configurar el grupo de políticas de terminales, los dominios de puente y los contratos en ACI

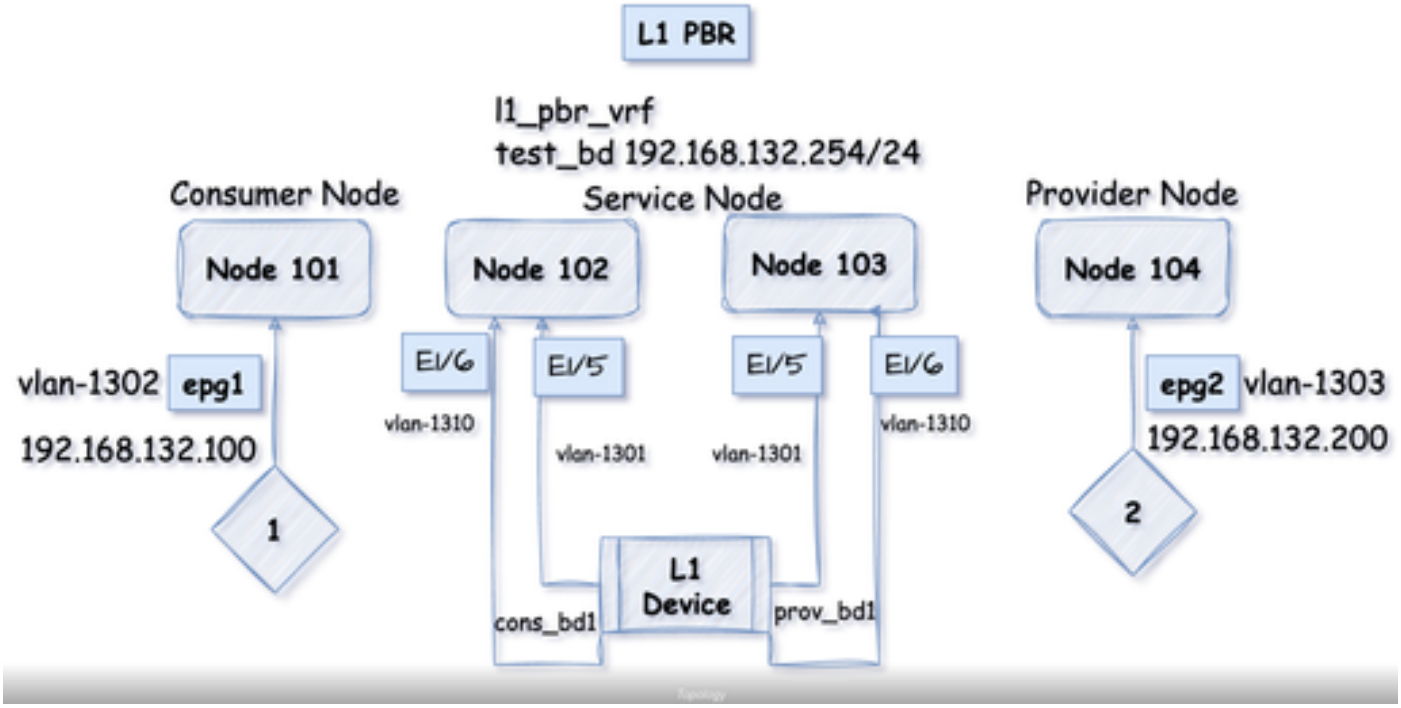
Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión de APIC: 5.3(2a)
- Hoja H/W: N9K-C93180YC-FX , N9K-C93180YC-EX
- S/W de hoja: n9000-15.3(2a)
- Nodo de hoja 101, 102 , 103 ,104

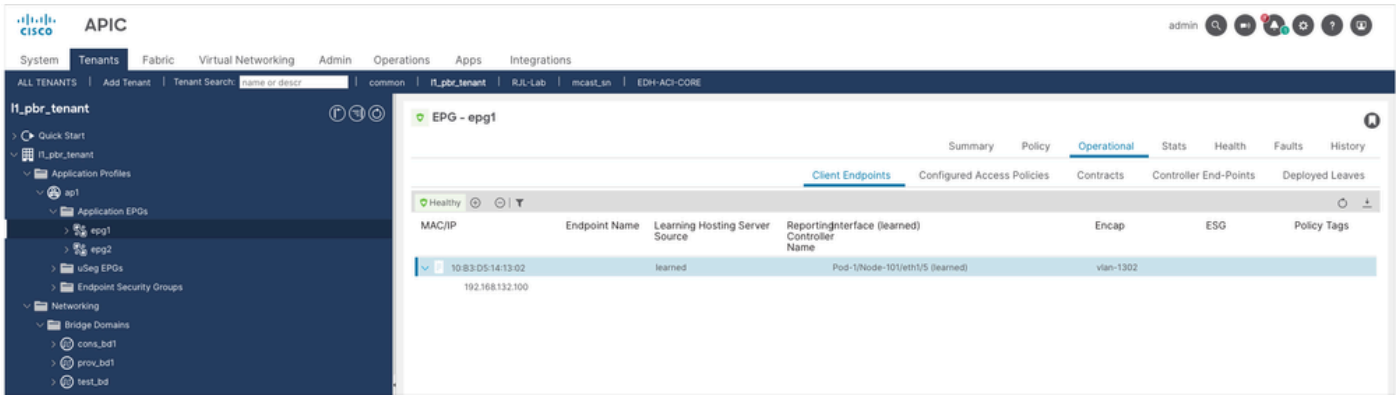
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando

Topología

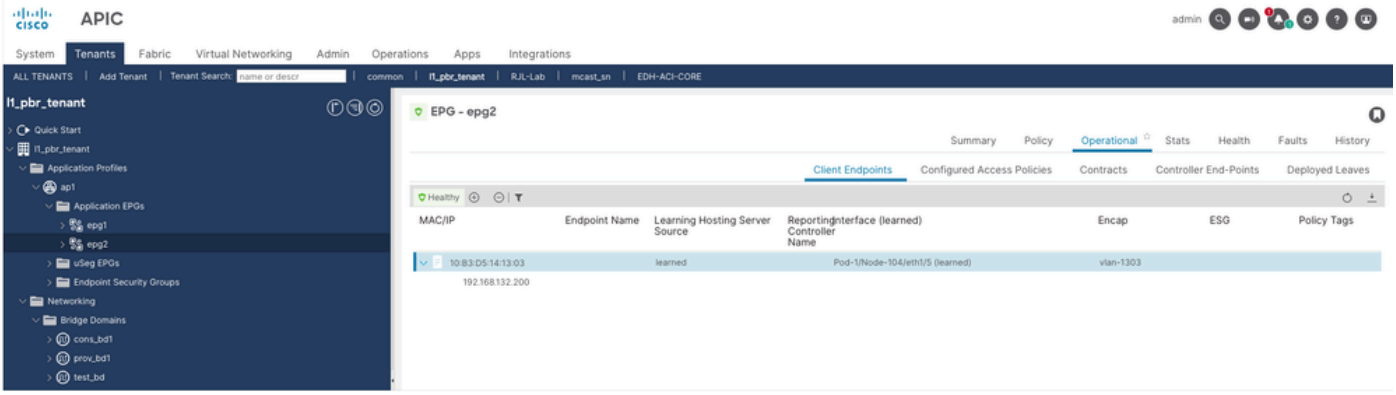


La configuración de EPG1 y EPG2 no se muestra en este documento, se debe configurar antes de aprender manualmente y el terminal.

1. Valide el punto final 192.168.132.100 de haș del EPG1 detectado (nodo 101).



2. Validar EPG2 tiene el punto final 192.168.132.200 detectado (Nodo 104).



¿Por qué se necesita L1 Service Graph en ACI?

En Cisco ACI, puede insertar un dispositivo de servicio L4-L7 como L3/L2/L1. La capa 3 significa que un dispositivo externo es capaz de realizar decisiones de routing para reenviar el tráfico, mientras que la capa 2 significa que el tráfico se reenvía únicamente en función de la dirección MAC. En ACI, puede insertar un dispositivo de nivel 2 como, por ejemplo, el sistema de prevención de intrusiones (IPS) o el firewall transparente. Piense ahora en un escenario en el que el dispositivo al que va a redirigir el tráfico no sea capaz de tomar ninguna decisión de reenvío, por lo que, en esos casos, puede implementar el routing basado en políticas (PBR) de capa 1.

El reenvío de tráfico es el mismo para los casos de PBR L3 y L2, la única diferencia es que en el caso del tráfico PBR L3 se redirige a una dirección IP, mientras que para el tráfico PBR L1/L2 se redirige a la dirección MAC. Estas direcciones MAC están enlazadas estáticamente a la interfaz de hoja para fines de reenvío. Verán más sobre esto si van más allá.

Para obtener más información sobre casos de uso de PBR L1/L2 Activo/En espera o Activo/Activo, consulte el enlace; Informe técnico de PBR.

Acerca del dispositivo L1

En este modelo de implementación, no se realiza ninguna traducción de VLAN en el dispositivo de servicio y ambas interfaces funcionan en la misma VLAN. Este enfoque se conoce comúnmente como modo en línea o modo de cable y se utiliza normalmente para firewalls y sistemas de prevención de intrusiones (IPS). Resulta ideal cuando se espera que el dispositivo de servicio realice funciones de seguridad sin participar en el reenvío de capa 2 o capa 3.

PBR L1 activo/activo

A partir de la versión 5.0 de ACI, se admite la implementación de un gráfico de servicios con dispositivos L4-L7 en modo activo/activo. Esto se consigue asignando un encapsulado único a cada interfaz de dispositivo L4-L7 (interfaz concreta) y aprovechando la configuración automática de ACI de "desbordamiento en encapsulado" en el EPG de servicio oculto. ACI crea este EPG de servicio oculto para asociar la interfaz de dispositivo L4-L7 con el dominio de puente de servicio.

Los administradores no necesitan configurar manualmente el EPG de servicio oculto, ya que ACI

activa automáticamente la opción "Inundación en la encapsulación" durante el proceso de representación del gráfico de servicios.

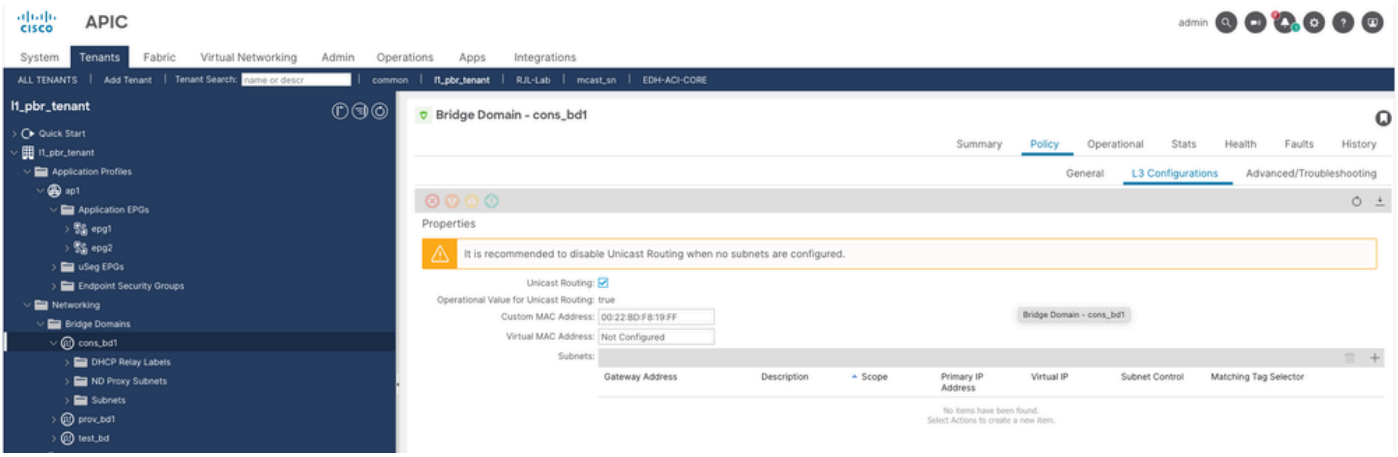
Para las implementaciones L1 PBR activo-activo, se debe configurar el ámbito local del puerto. Para ello, es necesario colocar las interfaces de clúster de proveedor y consumidor (conectores) del dispositivo L4-L7 en dominios físicos independientes, cada uno con su propio grupo de VLAN, a la vez que se mantiene el mismo intervalo de VLAN en ambos dominios.

Referencia: Informe técnico de PBR.

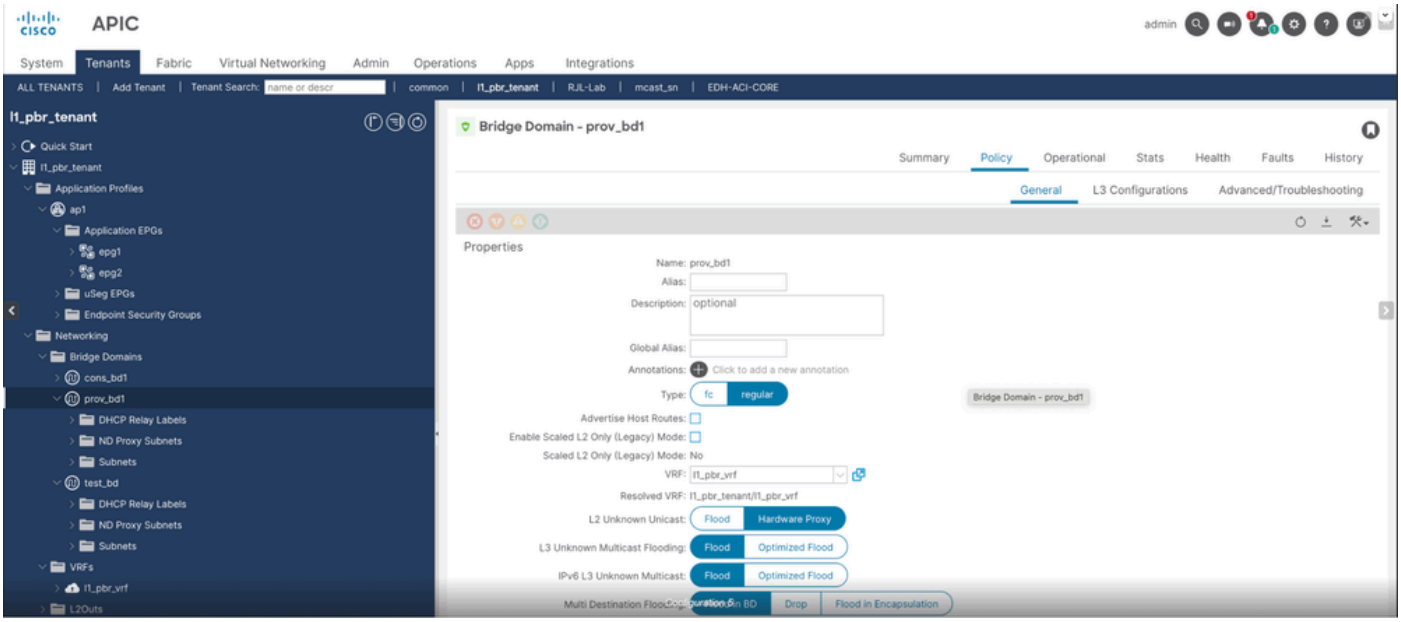
Configuración de L1 Service Graph

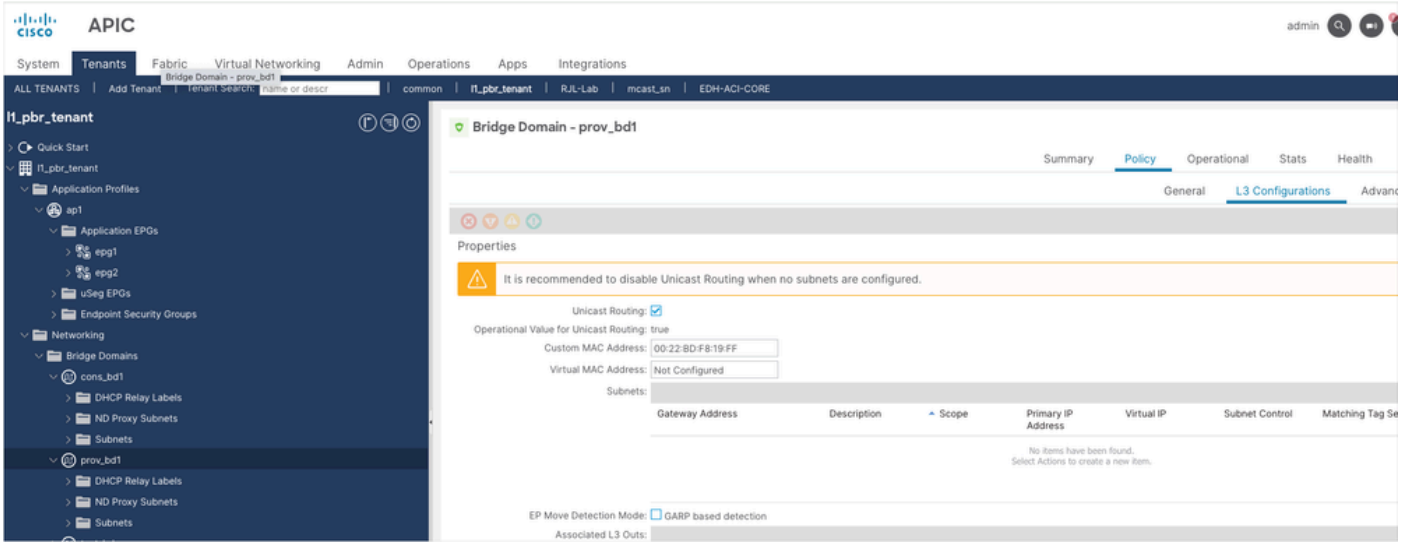
El ruteo de unidifusión debe estar habilitado, la unidifusión desconocida de L2 debe configurarse en el proxy de hardware y no se requiere subred para los dominios cons y prov bridge.

Paso 1. Configure el dominio de bridge de consumidor denominado cons_bd1.



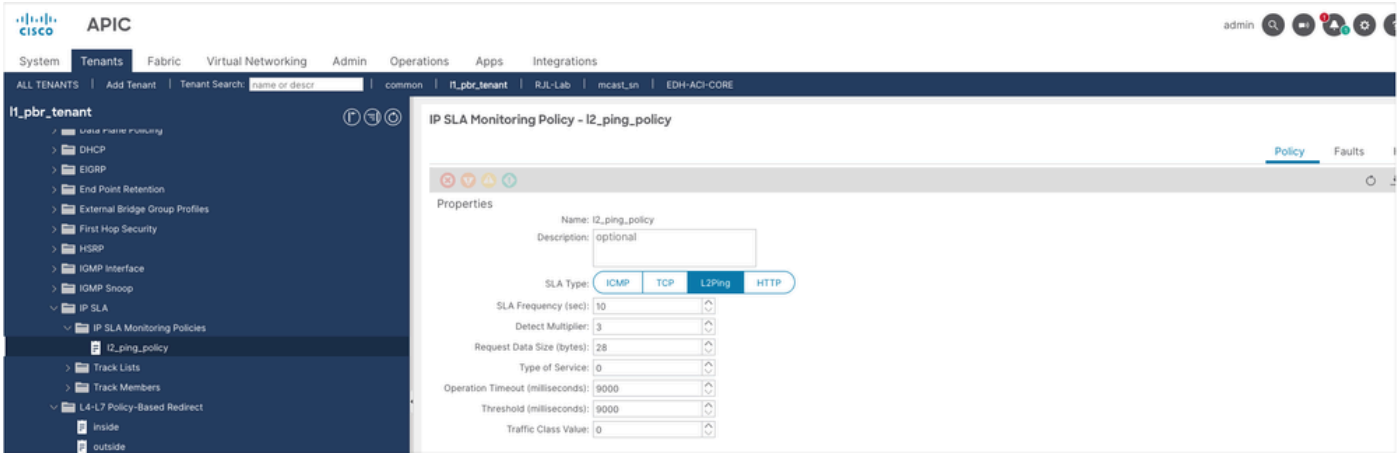
Paso 2. Configure el dominio de bridge del proveedor denominado prov-bd1.





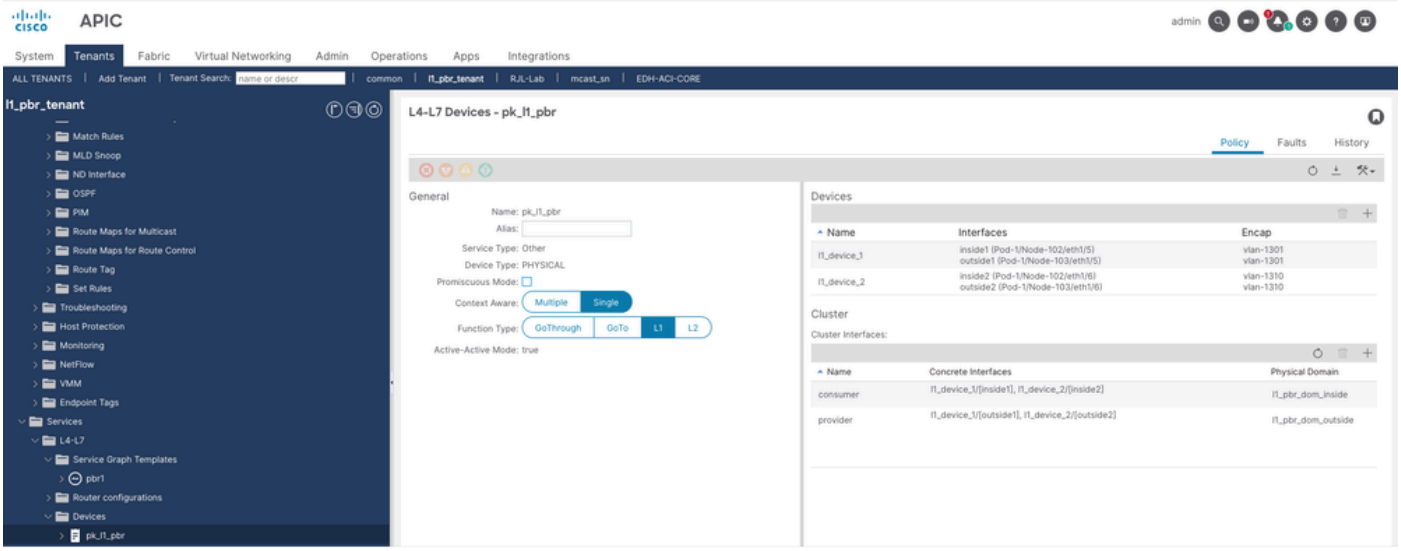
Paso 3. Configuración de la política de acuerdo de nivel de servicio (SLA) de IP con el tipo de SLA L2Ping.

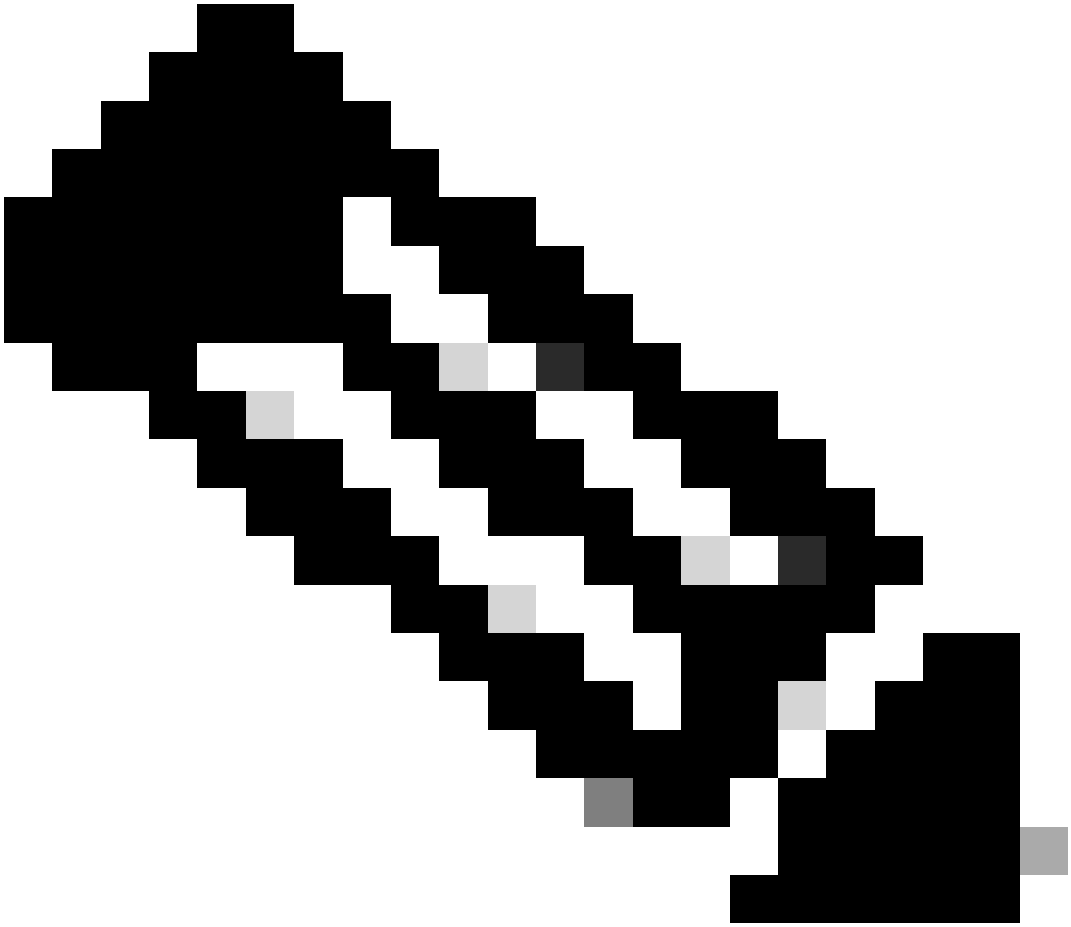
Navegue hasta Arrendatario > Políticas > Protocolo > IP SLA > Políticas de monitoreo de IP SLA, luego haga clic con el botón derecho y cree la política.



Paso 4. Configure el dispositivo L4/L7.

Navegue hasta Arrendatario > Servicios > Dispositivos, luego haga clic con el botón derecho y cree un dispositivo L4-L7.



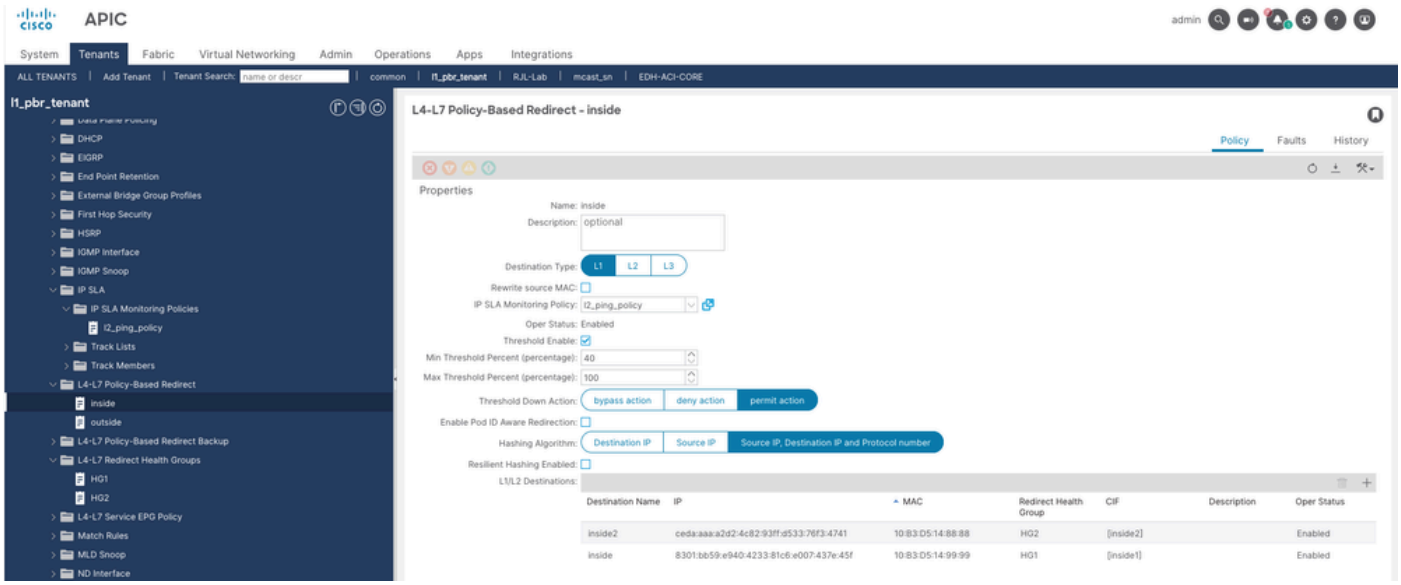


Nota: Para el dispositivo L1, cada interfaz de clúster debe estar en diferentes dominios físicos para el ámbito local del puerto.

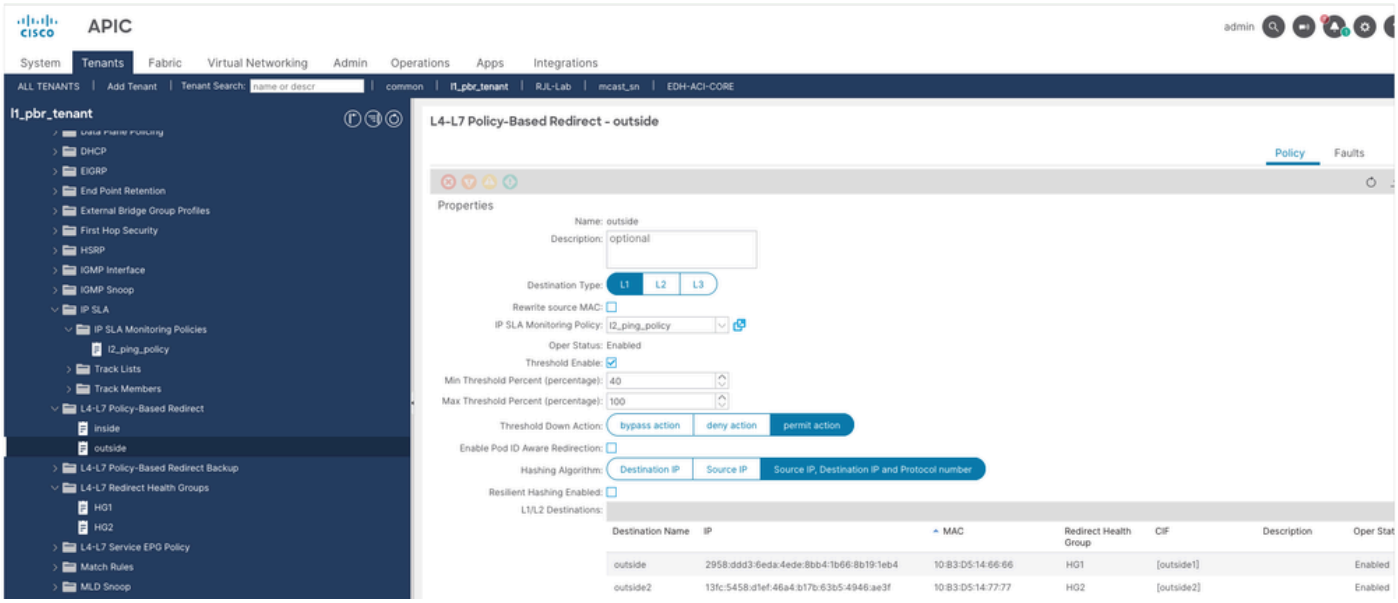
Paso 5. Configure el redireccionamiento basado en políticas L4-L7 para la interfaz interna y externa.

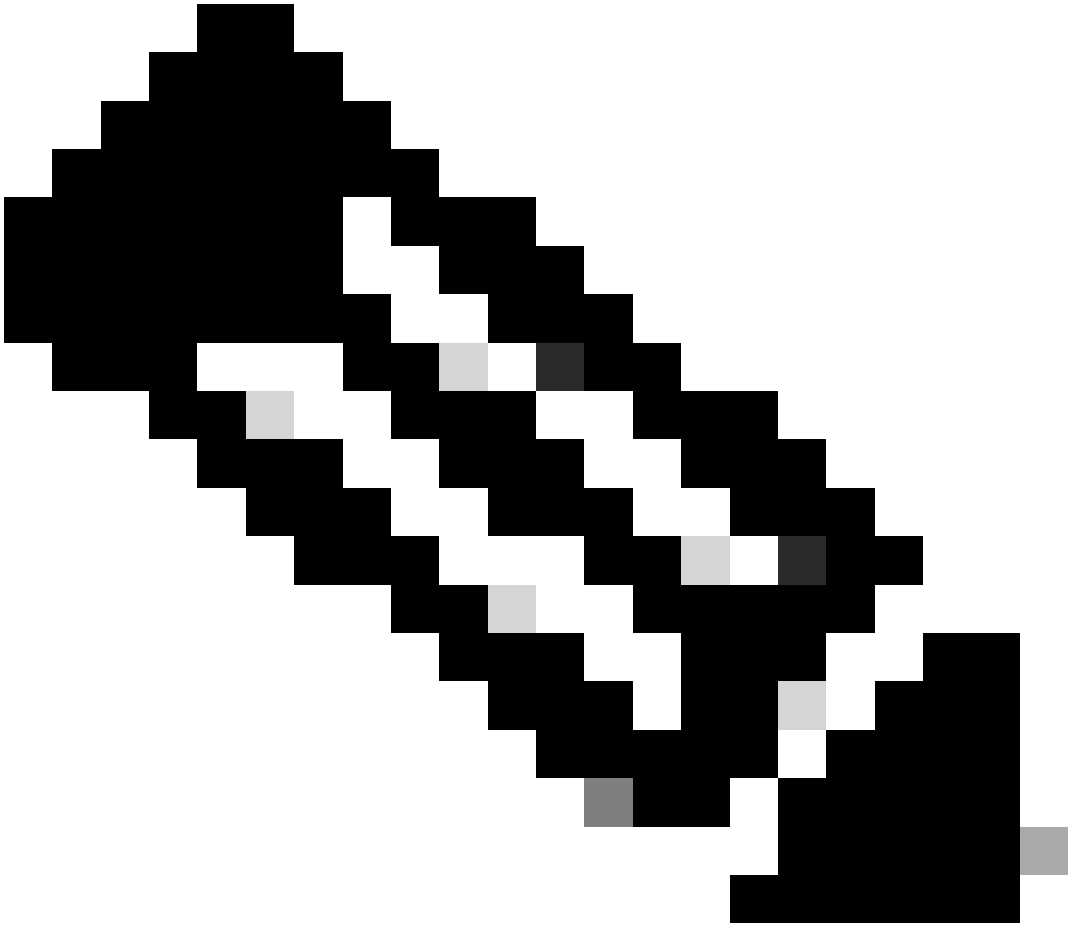
Navegue hasta Arrendatario > Políticas > Protocolo > Redirección basada en políticas L4-L7, luego haga clic con el botón derecho y cree la política.

++ El nombre de la política está dentro
++ Tenemos dos destinos L1, uno para cada dispositivo L1



++ El nombre de la política está fuera
++ Tenemos dos destinos L1, uno para cada dispositivo L1

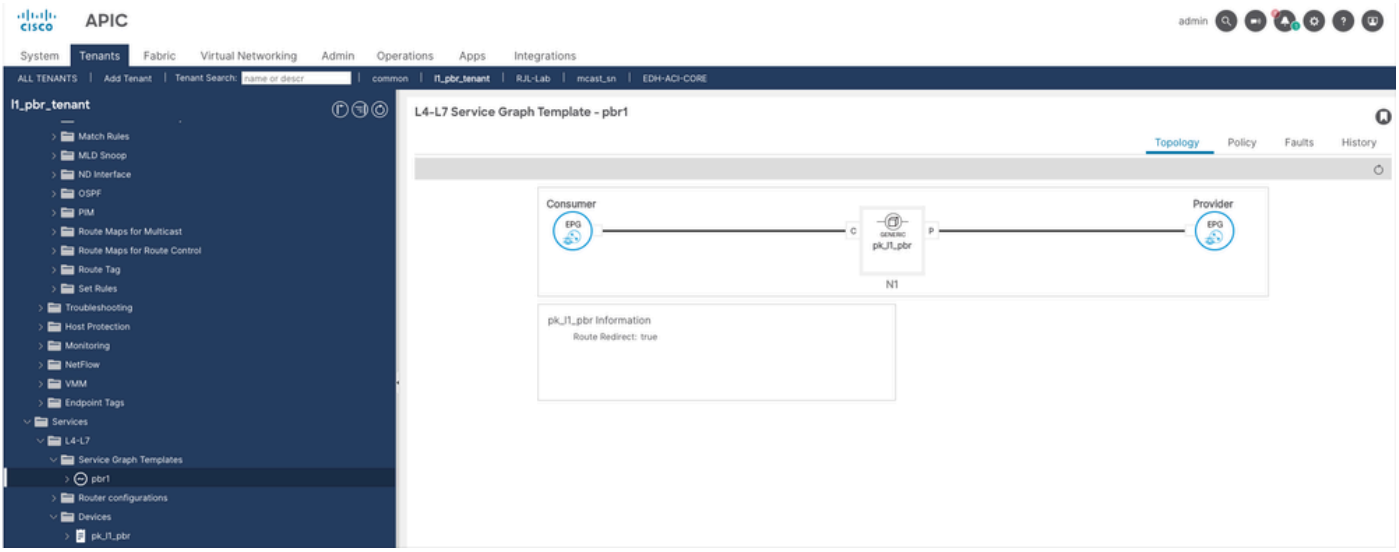




Nota: La acción de reducción del umbral debe ser la misma para ambas políticas de redirección L4-L7.

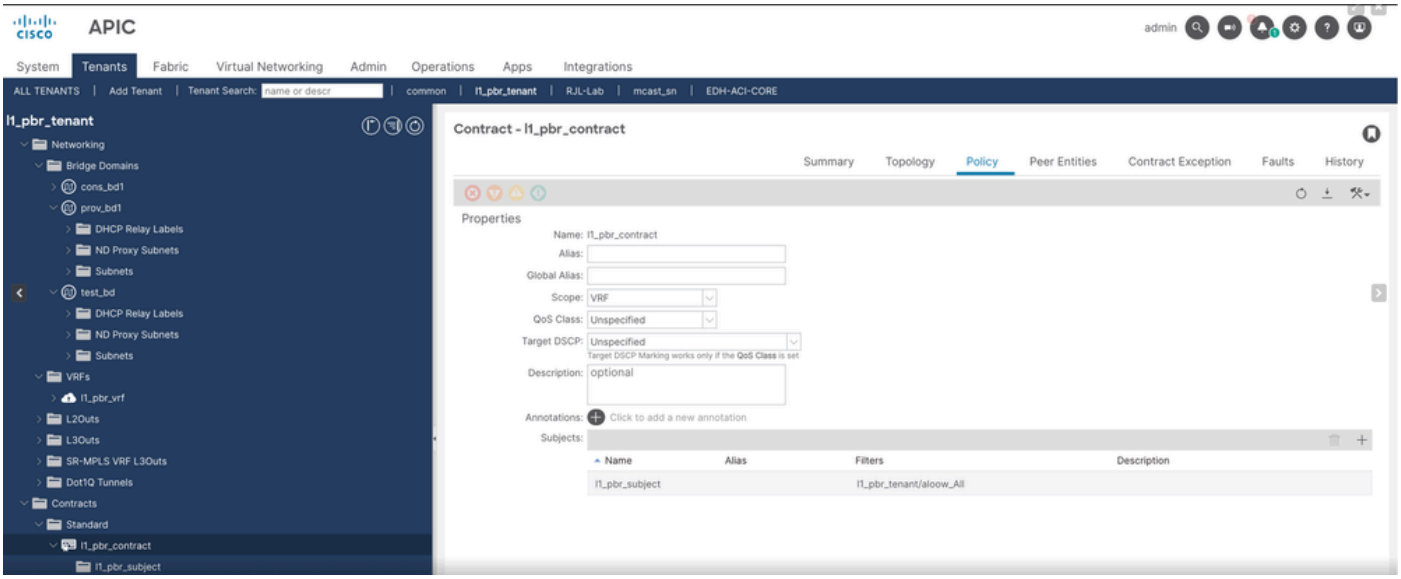
Paso 6. Configure la plantilla de gráfico de servicios.

Navegue hasta Arrendatario > Servicios > Plantilla de Service Graph, luego haga clic con el botón derecho y cree una plantilla de gráfico de servicio L4-L7.

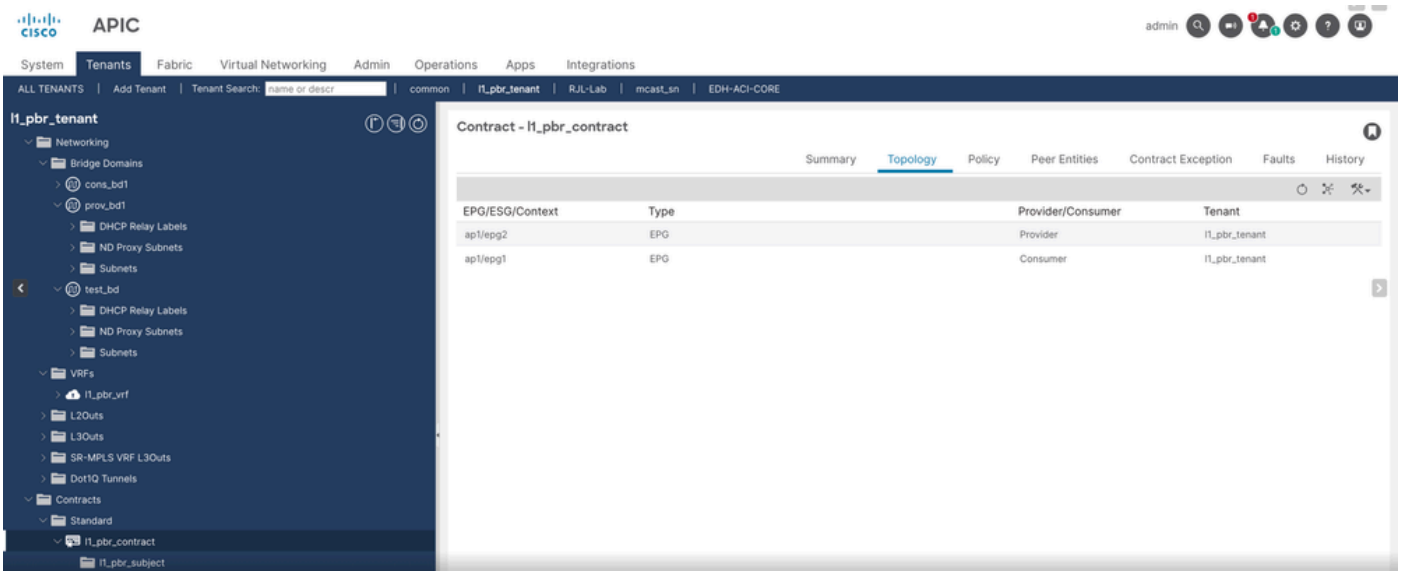


Paso 7. Creación de un contrato.

Navegue hasta Arrendatario > Contrato > Estándar, luego haga clic con el botón derecho y cree el contrato.

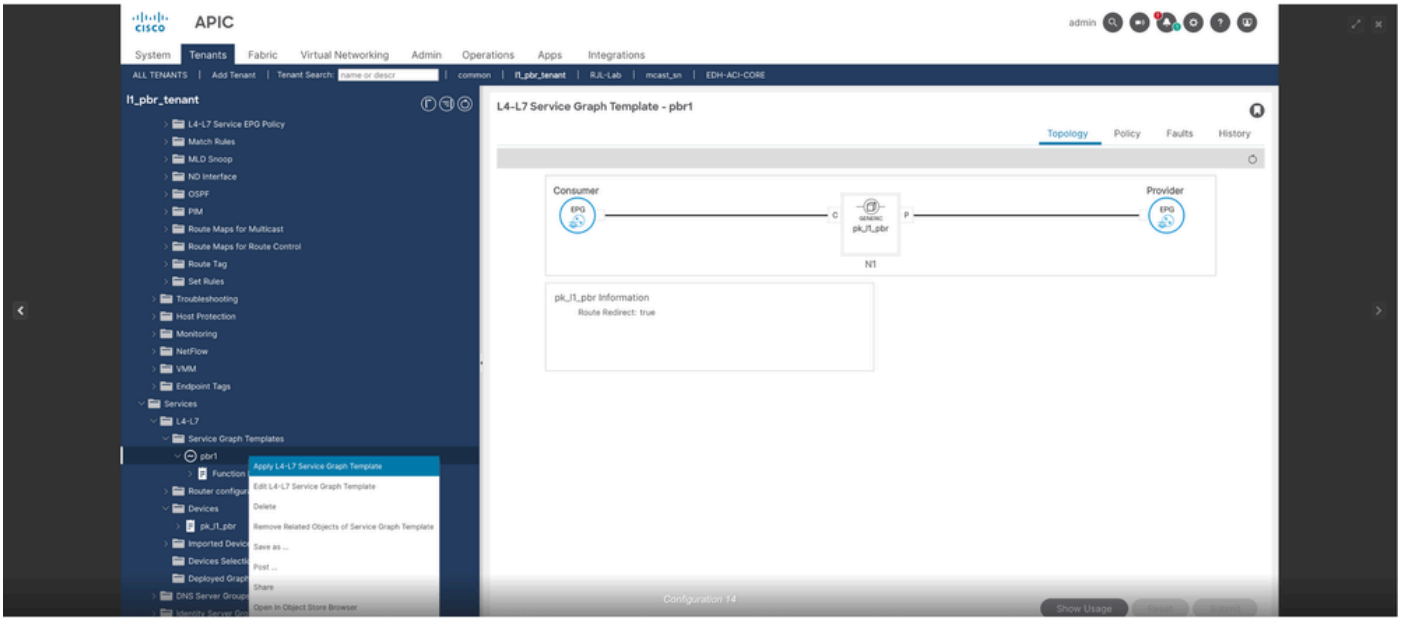


Paso 8. Aplique el contrato como consumidor y proveedor a EPG1 y EPG2 respectivamente.

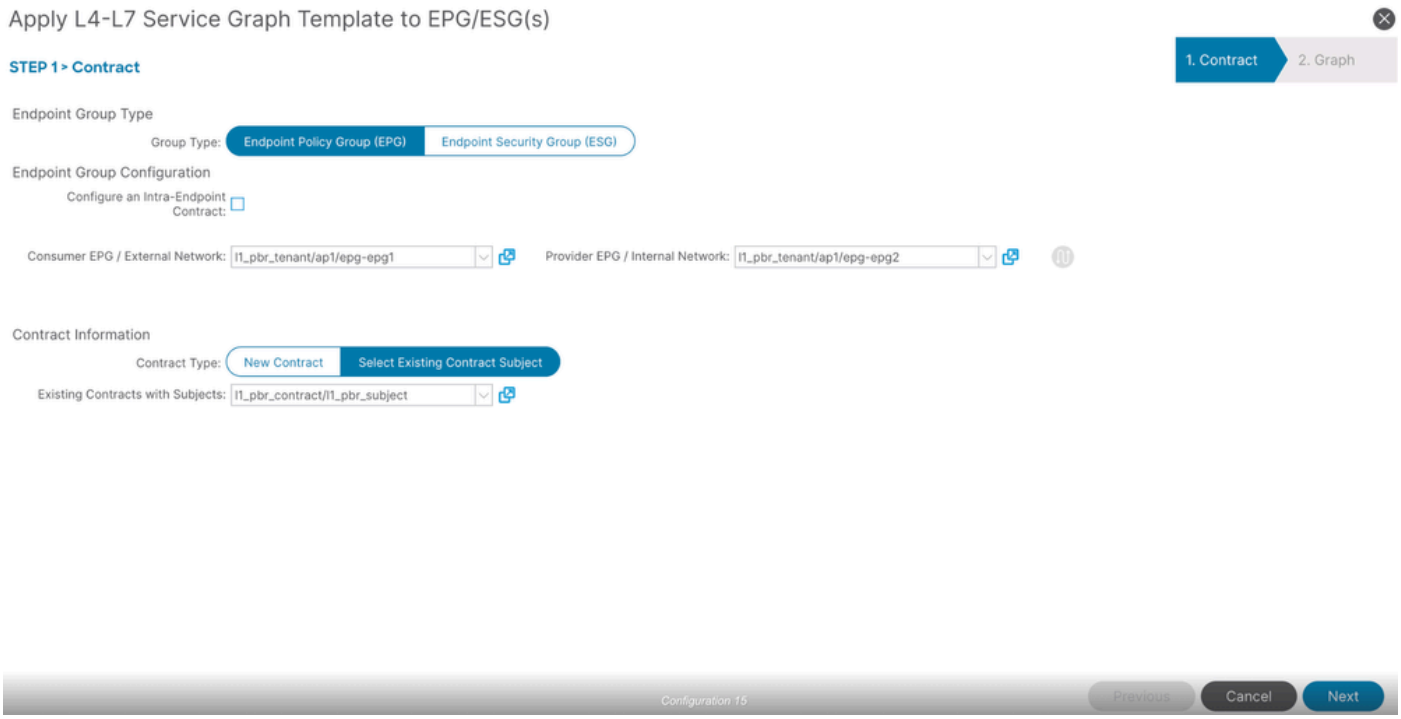


Paso 9. Aplicar plantilla de gráfico de servicio L4-L7.

Navegue hasta Arrendatario > Servicios > Plantilla de Service Graph, luego haga clic con el botón derecho en PBR1 y aplique la plantilla de gráfico de servicio L4-L7.

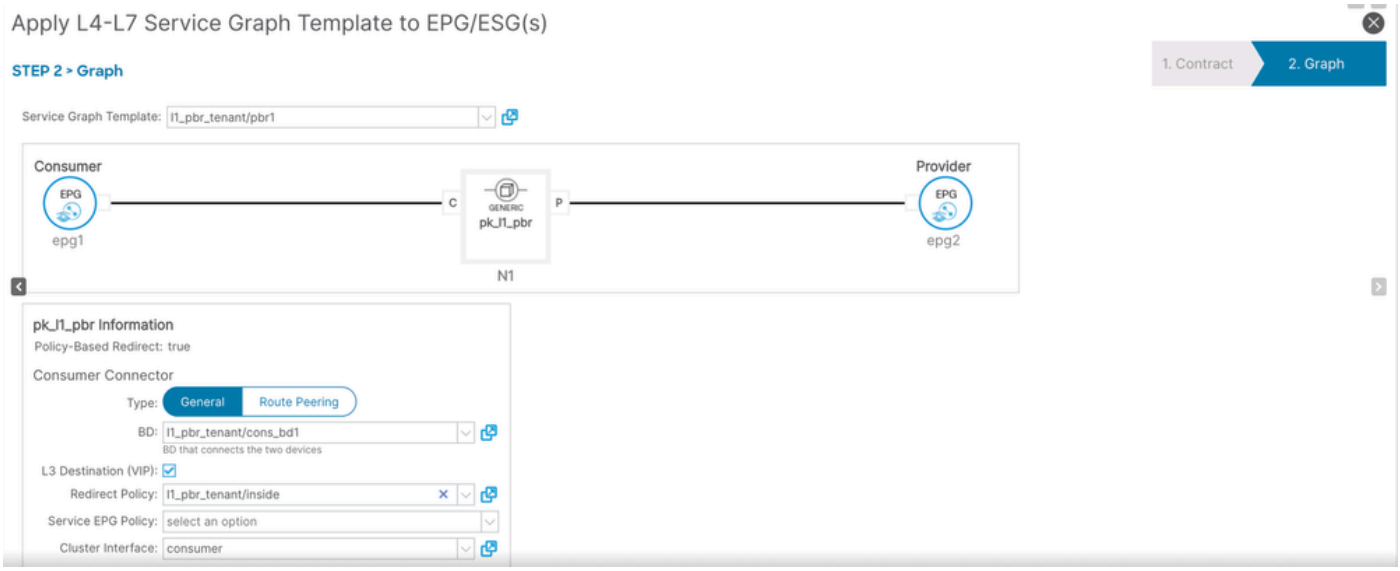


++ Adición de EPG de proveedor y consumidor
++ Especificar contrato

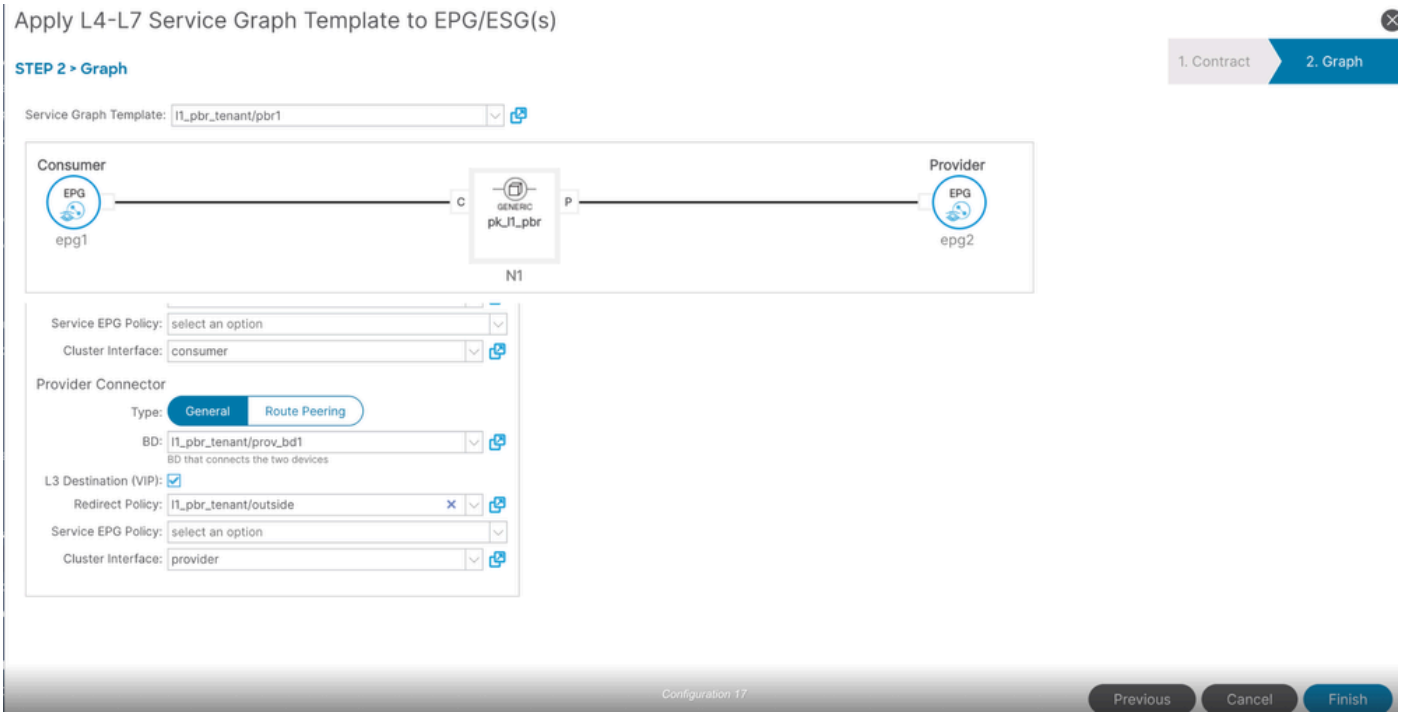


++ haga clic en Siguiente

++ Especificar detalles del conector de consumidor



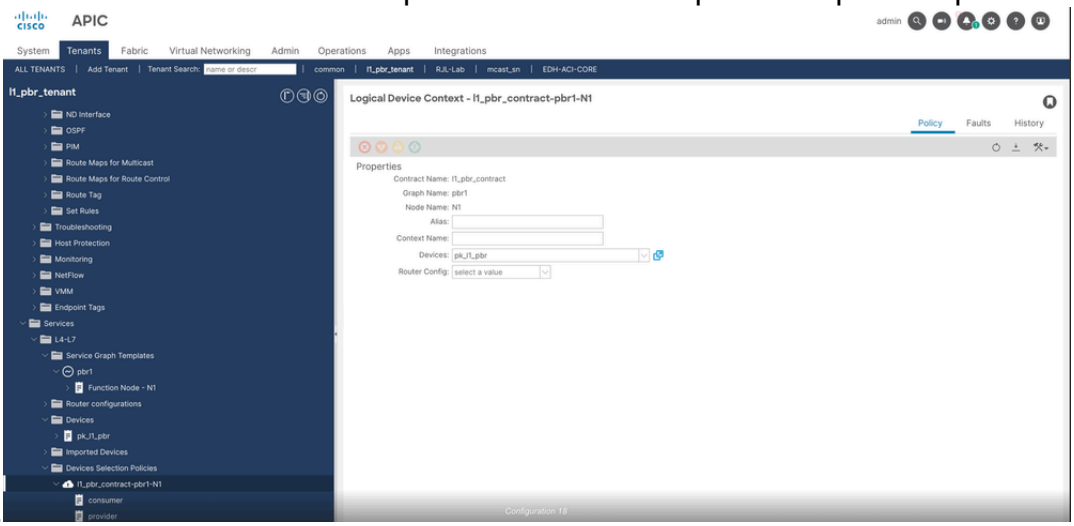
++ Especificar detalles del conector del proveedor



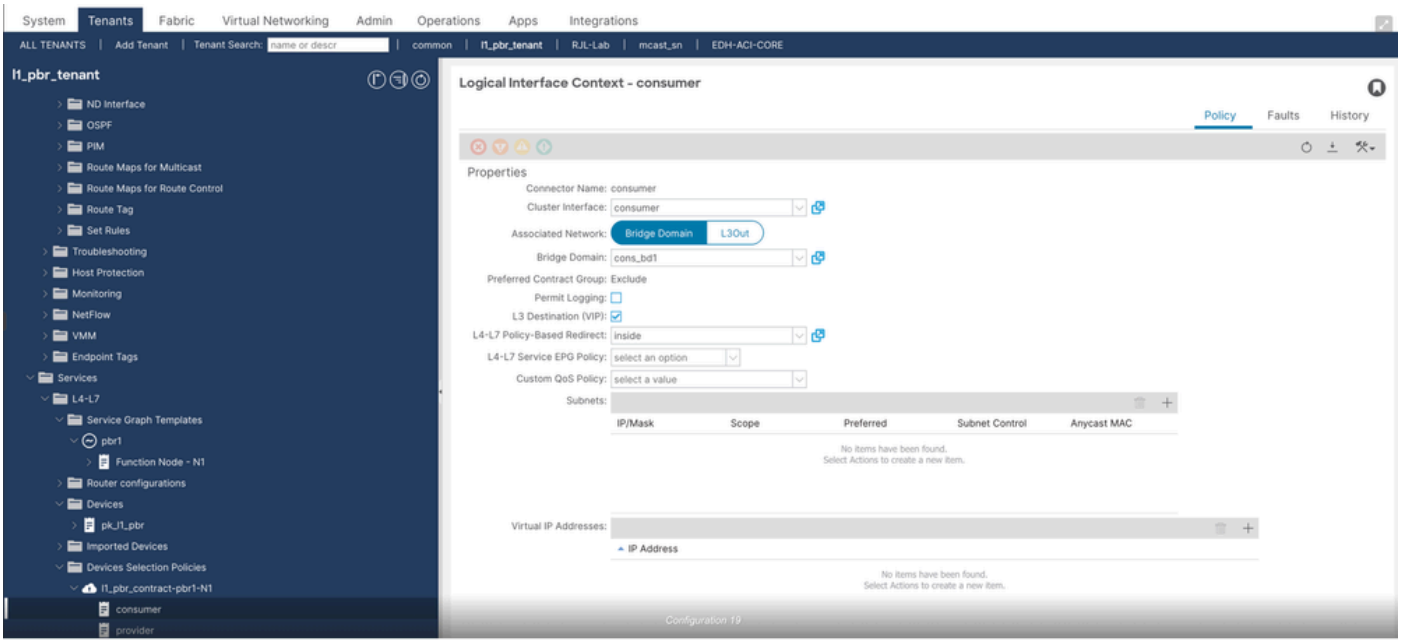
++ Haga clic en Finalizar

Verificación de L1 Service Graph en APIC GUI

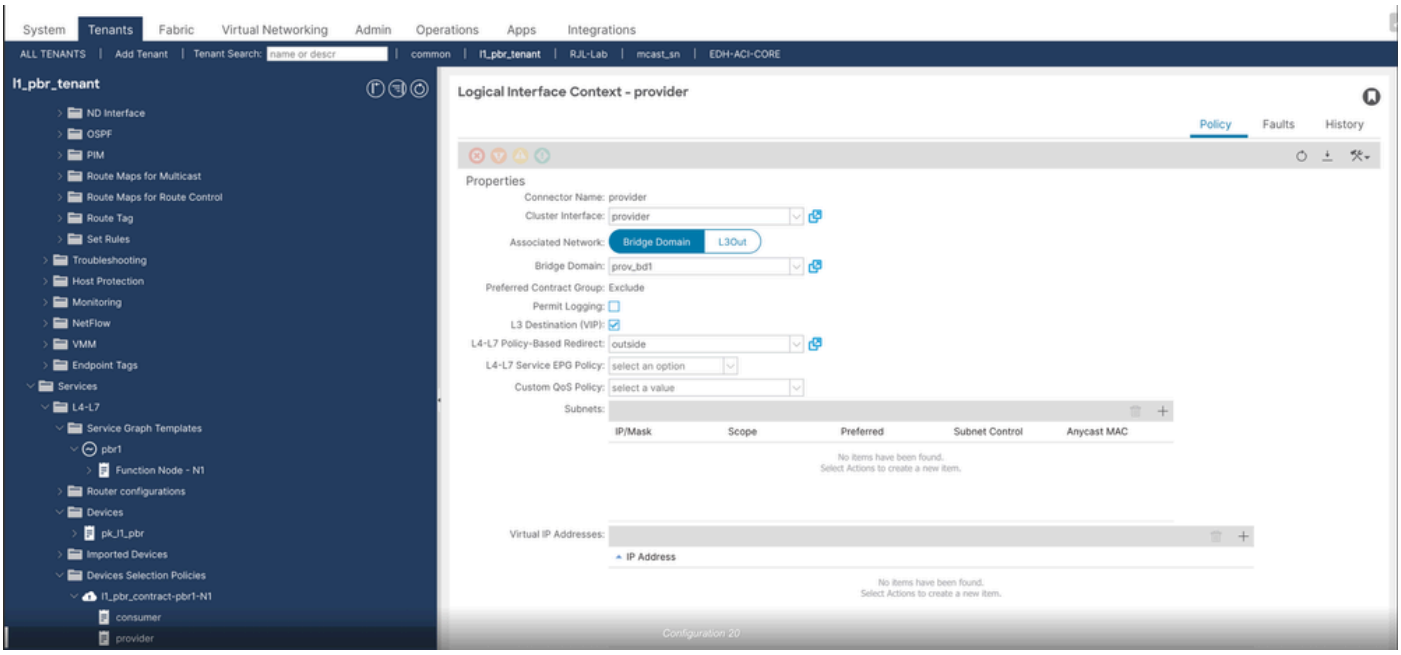
Paso 1. Compruebe la directiva de selección de dispositivos creada después de aplicar la plantilla de gráfico de servicios.



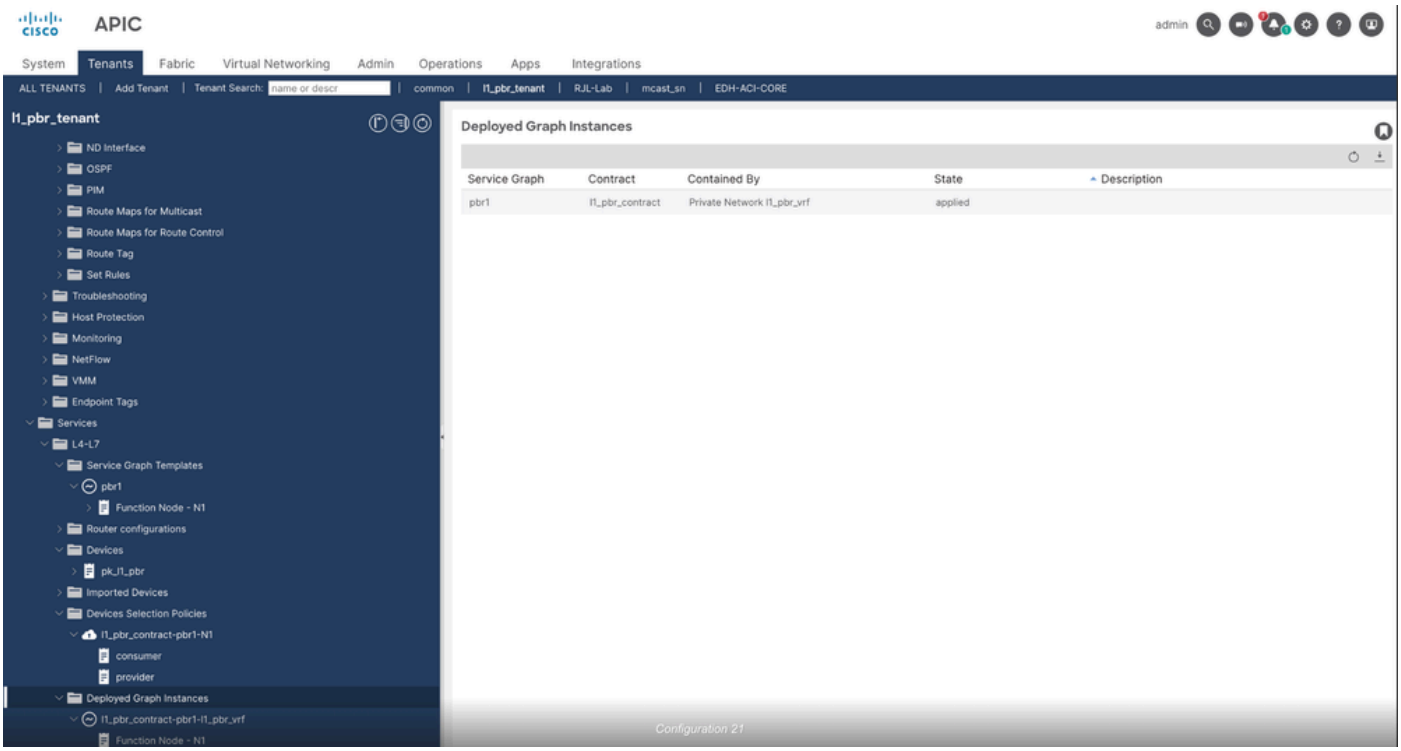
++ Verificar conector de consumidor



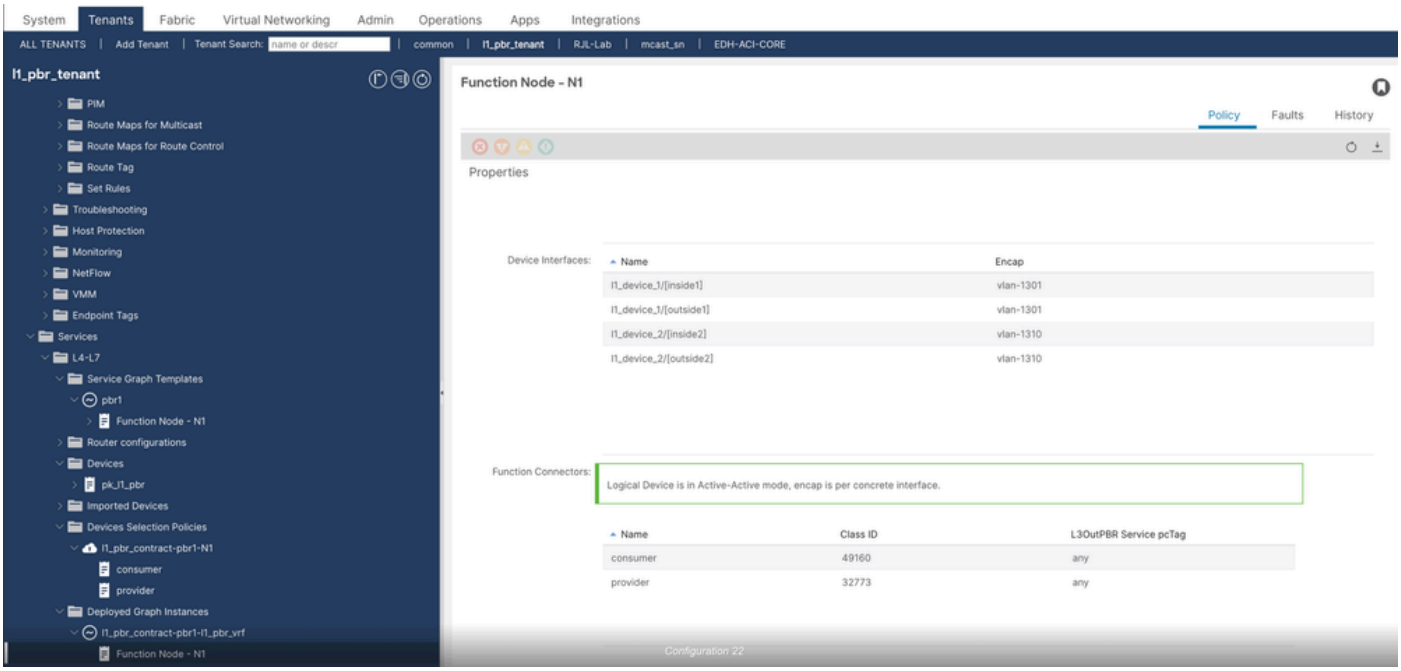
++ Configurar el conector del proveedor



Paso 2. Verificar las instancias del gráfico desplegado, allí va a ver una instancia, debe estar en estado aplicado.



++ Compruebe las interfaces de los dispositivos y los conectores de funciones donde vaya a ver el PCTAG asociado con los EPG de servicio



Verificación de L1 Service Graph en APIC CLI

Paso 1. Compruebe si el gráfico de servicios se aplica en el nodo de consumidor y proveedor junto con el estado del grupo de estado.

<#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]-[vxlan-2490369] l1_pbr_tenant::HG2
                      dest-[8301:bb59:e940:4233:81c6:e007:437e:45f]-[vxlan-2490369]  l1_pbr_tenant::HG1
2     destgrp-2       dest-[2958:ddd3:6eda:4ede:8bb4:1b66:8b19:1eb4]-[vxlan-2490369] l1_pbr_tenant::HG1
                      dest-[d438:790d:6fdb:4485:bab7:197d:ef61:9a59]-[vxlan-2490369] l1_pbr_tenant::HG2

List of destinations
Name                                                          bdVnid          vMac                vrf
====                                                          ======          ====                ===
dest-[8301:bb59:e940:4233:81c6:e007:437e:45f]-[vxlan-2490369]  vxlan-16252846  10:B3:D5:14:99:99    l1_
dest-[476f:9be9:5aab:4454:a5d6:8c9e:7017:61eb]-[vxlan-2490369] vxlan-16252846  10:B3:D5:14:77:77    l1_
dest-[2958:ddd3:6eda:4ede:8bb4:1b66:8b19:1eb4]-[vxlan-2490369] vxlan-15794150  10:B3:D5:14:66:66    l1_
dest-[d438:790d:6fdb:4485:bab7:197d:ef61:9a59]-[vxlan-2490369] vxlan-15794150  10:B3:D5:14:77:77    l1_

List of Health Groups

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

------------------------------------------------------------
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]-[vxlan-2490369] l1_pbr_tenant::HG2
                      dest-[2958:ddd3:6eda:4ede:8bb4:1b66:8b19:1eb4]-[vxlan-2490369] l1_pbr_tenant::HG1
4     destgrp-4       dest-[476f:9be9:5aab:4454:a5d6:8c9e:7017:61eb]-[vxlan-2490369] l1_pbr_tenant::HG2
                      dest-[8301:bb59:e940:4233:81c6:e007:437e:45f]-[vxlan-2490369]  l1_pbr_tenant::HG1

List of destinations

Name                                                          bdVnid          vMac                vrf
====                                                          ======          ====                ===
dest-[2958:ddd3:6eda:4ede:8bb4:1b66:8b19:1eb4]-[vxlan-2490369] vxlan-15794150  10:B3:D5:14:66:66    l1_
dest-[d438:790d:6fdb:4485:bab7:197d:ef61:9a59]-[vxlan-2490369] vxlan-15794150  10:B3:D5:14:77:77    l1_
dest-[476f:9be9:5aab:4454:a5d6:8c9e:7017:61eb]-[vxlan-2490369] vxlan-16252846  10:B3:D5:14:77:77    l1_
dest-[8301:bb59:e940:4233:81c6:e007:437e:45f]-[vxlan-2490369]  vxlan-16252846  10:B3:D5:14:99:99    l1_
```

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

Paso 2. Verifique si el enlace MAC estático se crea en los nodos de servicio (102 y 103).

<#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-rl 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-rl 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
```

Validación de tráfico

1. Se están generando 2000 paquetes ping ICMP de EP1 a EP2 que se redirigirán al dispositivo L1.

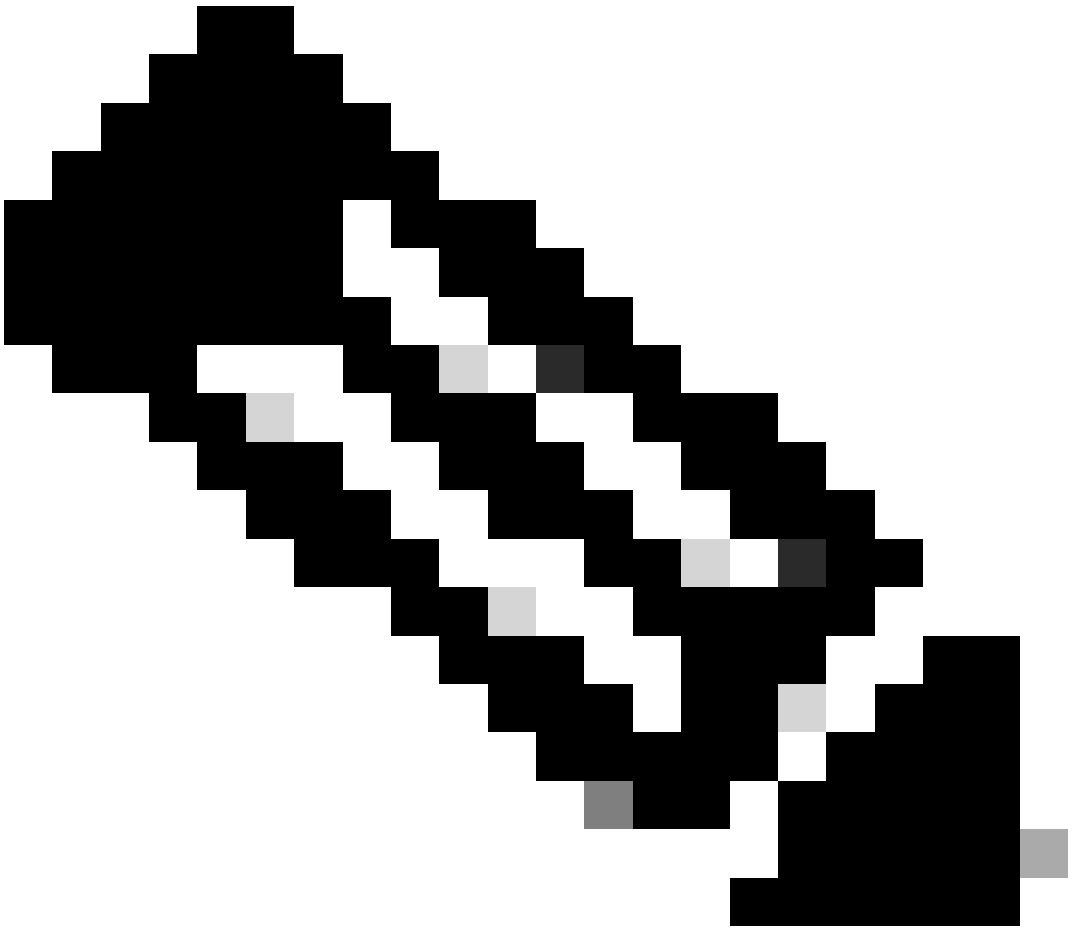
```
switch1# ping 192.168.132.200 vrf l1_pbr1 count 2000 >>>>> sending 2000 packets
64 bytes from 192.168.132.200: icmp_seq=464 ttl=251 time=0.859 ms
64 bytes from 192.168.132.200: icmp_seq=465 ttl=251 time=0.872 ms
64 bytes from 192.168.132.200: icmp_seq=466 ttl=251 time=0.844 ms
64 bytes from 192.168.132.200: 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. Valide los contadores de interfaces en los nodos 102 y 103 que están conectados al dispositivo L1.

```
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
```



Nota: Los contadores de interfaz se borraron en los nodos 102 y 103 antes de que se probara el tráfico.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).