Configurar e verificar o PBR L1 ativo/ativo na ACI

Contents

Introdução

Este documento descreve como configurar e verificar o gráfico de serviço L1 ativo/ativo na Application Centric Infrastructure (ACI).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Compreensão de como o gráfico de serviço de camada 3 funciona na ACI
- Compreensão de como configurar o grupo de políticas de endpoint, domínios de ponte e contrato na ACI

Componentes Utilizados

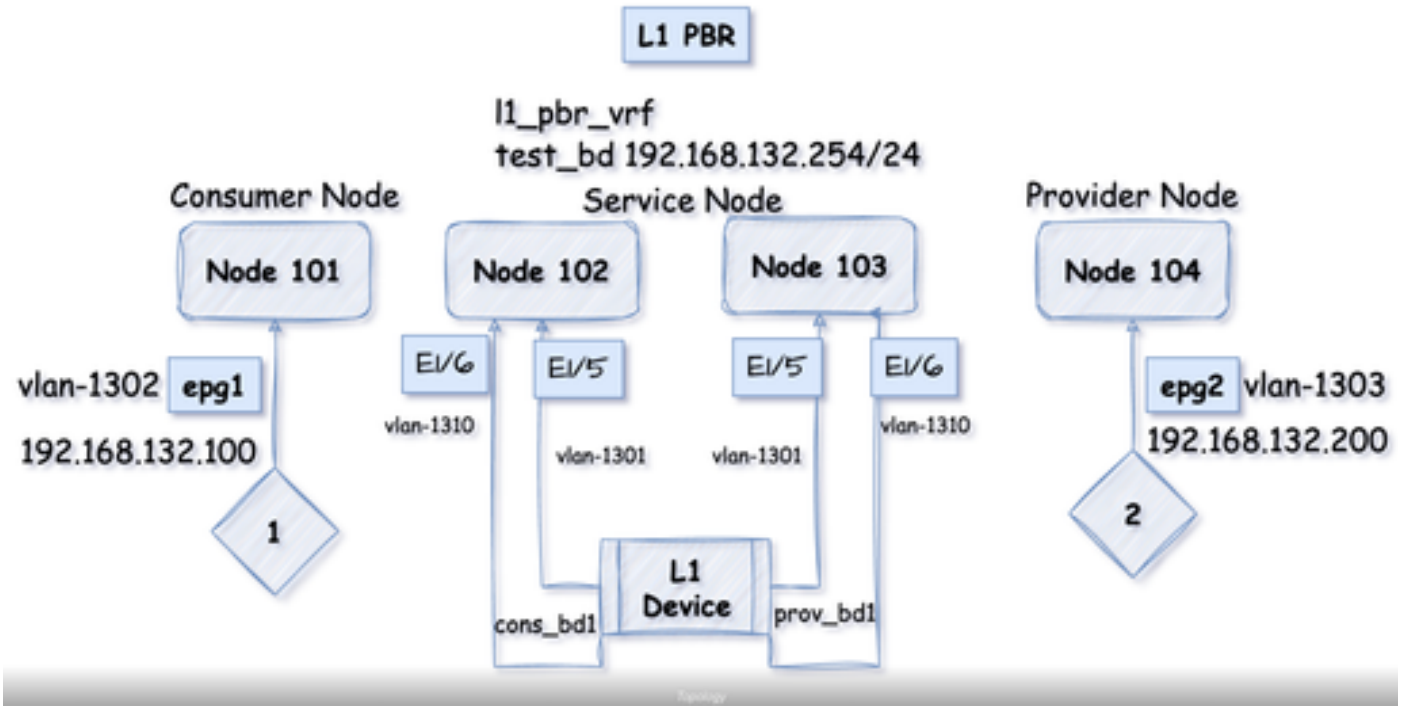
As informações neste documento são baseadas nestas versões de software e hardware:

- Versão do APIC: 5.3(2a)
- Folha H/W: N9K-C93180YC-FX , N9K-C93180YC-EX
- Folha S/W: n9000-15.3(2a)
- Nó Folha 101, 102 , 103 ,104

As informações neste documento foram criadas a partir de dispositivos em um ambiente de

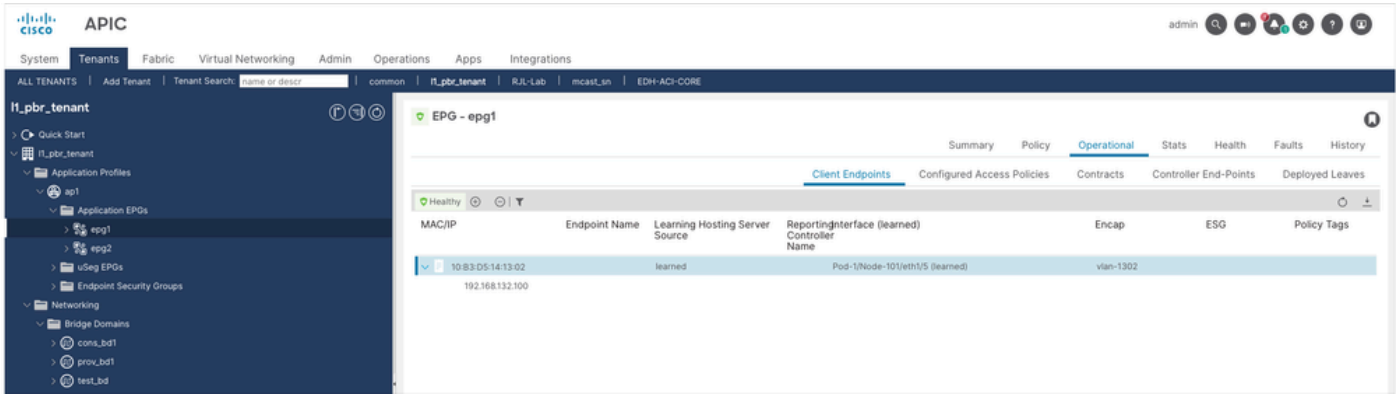
laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando

Topologia

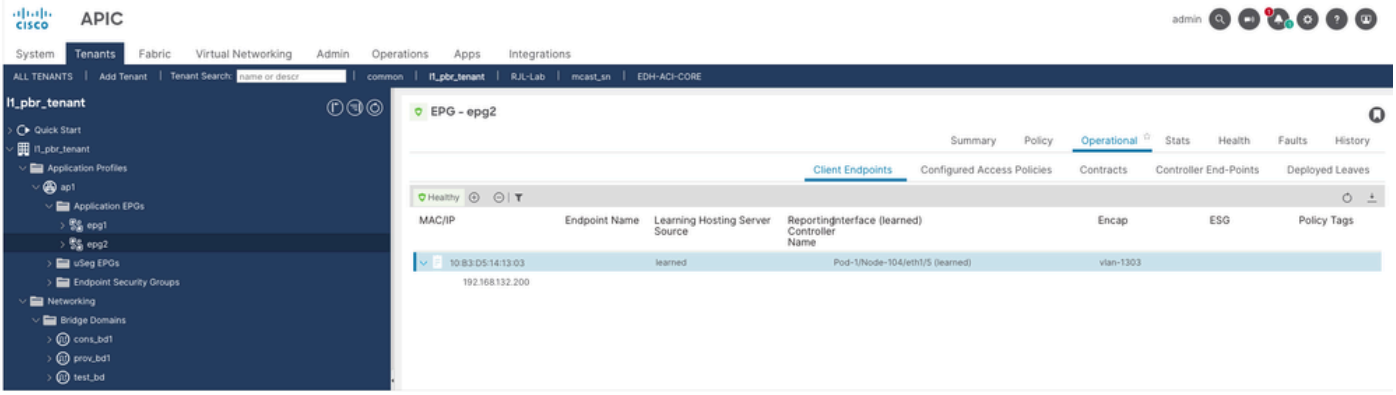


A configuração de EPG1 e EPG2 não é mostrada neste documento, ela deve ser configurada antes de ser usada e o endpoint deve ser aprendido.

1. Validar o ponto final 192.168.132.100 aprendido do EPG1 haș (Nó 101).



2. Validar que o EPG2 tem o ponto de extremidade 192.168.132.200 aprendido (Nó 104).



Por que o L1 Service Graph é necessário na ACI?

Na Cisco ACI, você pode inserir o dispositivo de serviço L4-L7 como L3/L2/L1. A camada 3 significa que o dispositivo externo é capaz de executar a decisão de roteamento para encaminhar tráfego, enquanto a camada 2 significa que o tráfego será encaminhado exclusivamente com base no endereço MAC. Na ACI, você pode inserir um dispositivo L2, como o Sistema de prevenção de intrusão (IPS)/Firewall transparente. Agora pense em um cenário onde o dispositivo que você vai redirecionar o tráfego não é capaz de tomar qualquer decisão de encaminhamento, então, nesses casos, você pode implantar o Roteamento Baseado em Políticas (PBR - Policy-Based Routing) de L1.

O encaminhamento de tráfego é o mesmo para os casos PBR de L3 e L2, a única diferença é que no caso do tráfego PBR de L3 é redirecionado para um endereço IP, quando o tráfego PBR de L1/L2 é redirecionado para o endereço MAC. Esses endereços MAC são vinculados estaticamente à interface de folha para fins de encaminhamento. Você verá mais sobre isso, indo além.

Para obter mais informações sobre casos de uso Ativos/Em espera ou Ativos/Ativos de PBR L1/L2, consulte o link; White Paper sobre PBR.

Sobre o dispositivo L1

Nesse modelo de implantação, nenhuma conversão de VLAN é executada no dispositivo de serviço e ambas as interfaces operam na mesma VLAN. Essa abordagem é comumente conhecida como modo em linha ou modo de fio e é normalmente usada para firewalls e sistemas de prevenção de intrusão (IPS). É ideal quando se espera que o dispositivo de serviço execute funções de segurança sem participar do encaminhamento de Camada 2 ou Camada 3.

PBR L1 ativo/ativo

A partir da versão 5.0 da ACI, é suportada a implantação de um gráfico de serviço com dispositivos L4-L7 em modo ativo/ativo. Isso é obtido atribuindo-se um encapsulamento exclusivo a cada interface de dispositivo L4-L7 (interface concreta) e aproveitando-se a configuração automática da ACI de 'Flood in encapsulamento' no EPG de serviço oculto. Esse EPG de serviço oculto é criado pela ACI para associar a interface do dispositivo L4-L7 ao domínio da ponte de

serviço.

Os administradores não precisam configurar manualmente o EPG de serviço oculto, pois a ACI habilita automaticamente 'Flood in encap' durante o processo de processamento do gráfico de serviço.

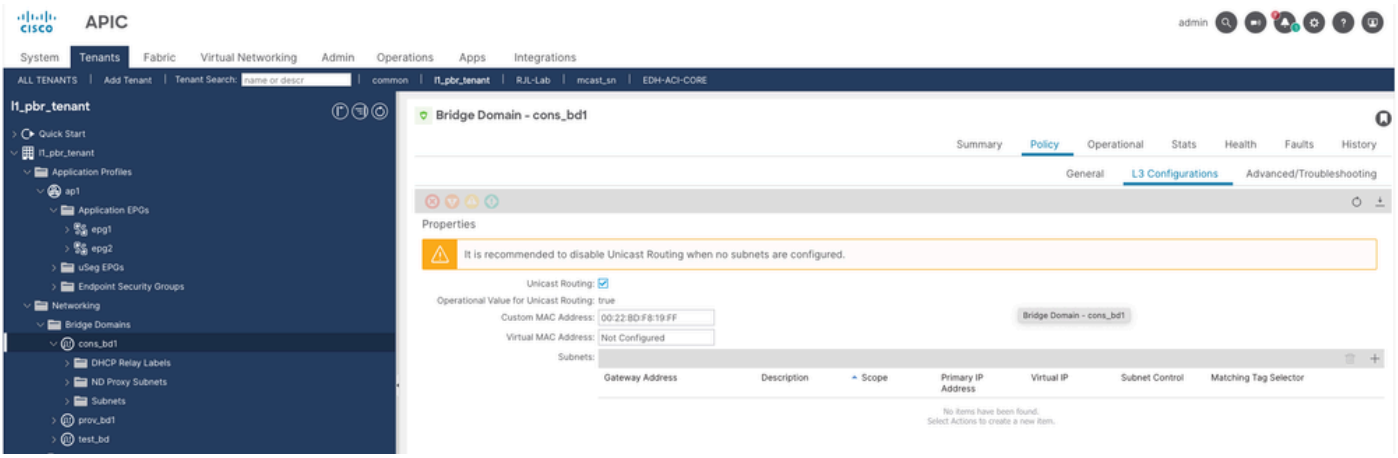
Para implantações ativas-ativas de PBR L1, o escopo de porta local deve ser configurado. Isso requer a colocação das interfaces de cluster do consumidor e do provedor (conectores) do dispositivo L4-L7 em domínios físicos separados, cada um com seu próprio pool de VLAN, enquanto mantém o mesmo intervalo de VLAN em ambos os domínios.

Referência: White paper do PBR.

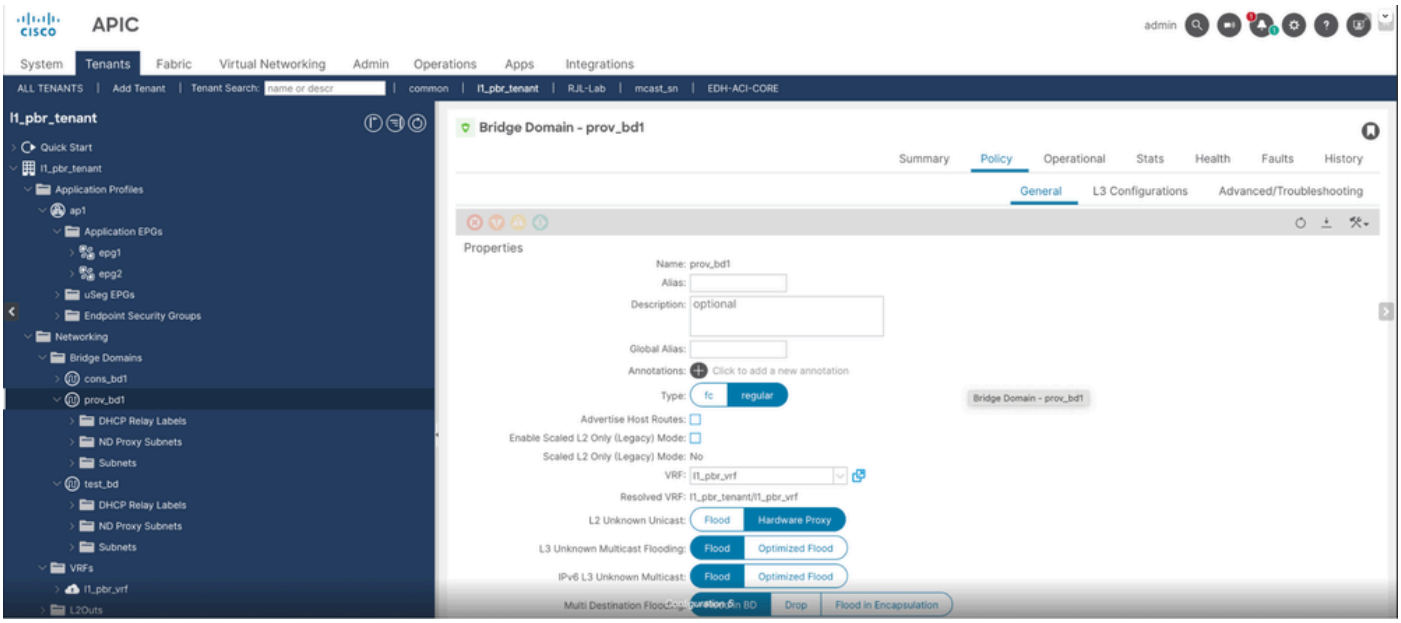
Configuração do gráfico de serviço L1

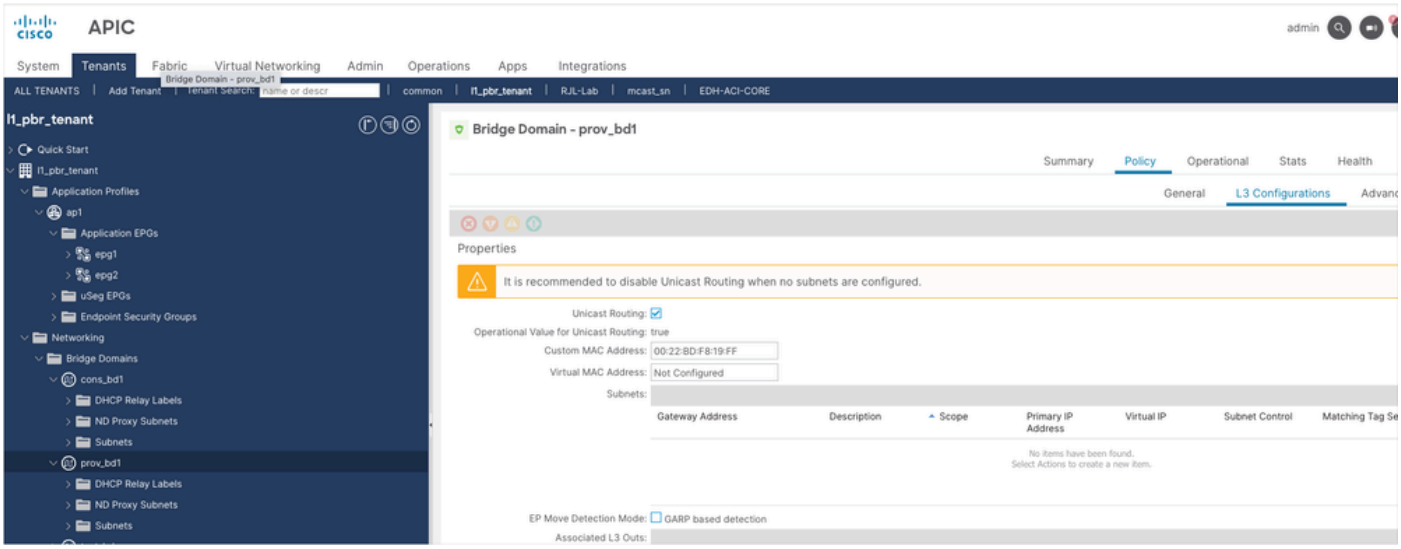
O roteamento unicast deve ser ativado, o unicast L2 desconhecido deve ser definido como proxy de Hardware e nenhuma sub-rede é necessária para domínios de ponte cons e prov.

Etapa 1. Configure o domínio da ponte do consumidor nomeado como cons_bd1.



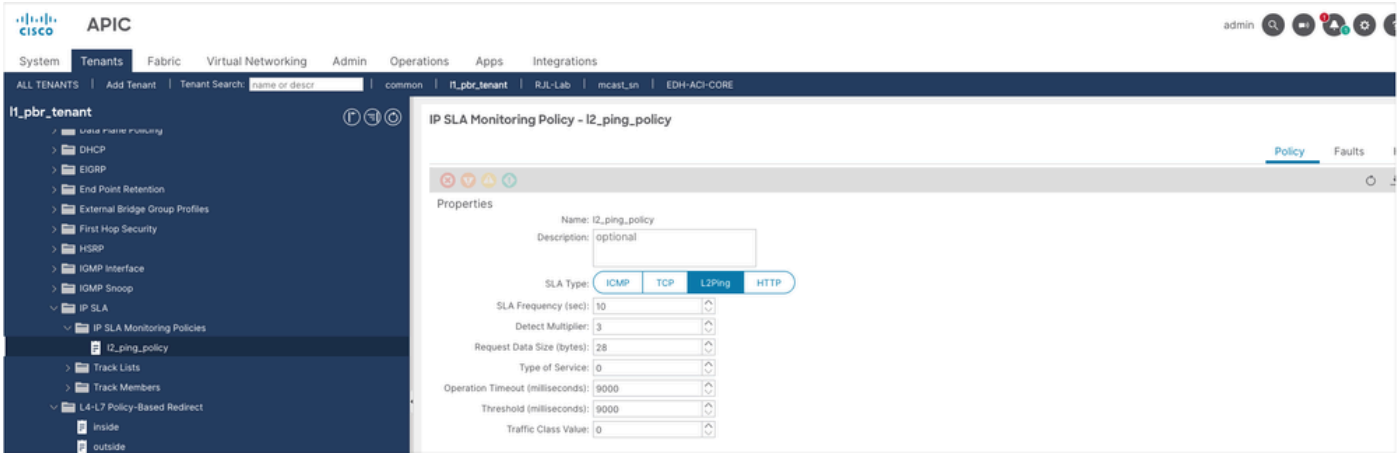
Etapa 2. Configure o domínio da ponte do provedor nomeado como prov-bd1.





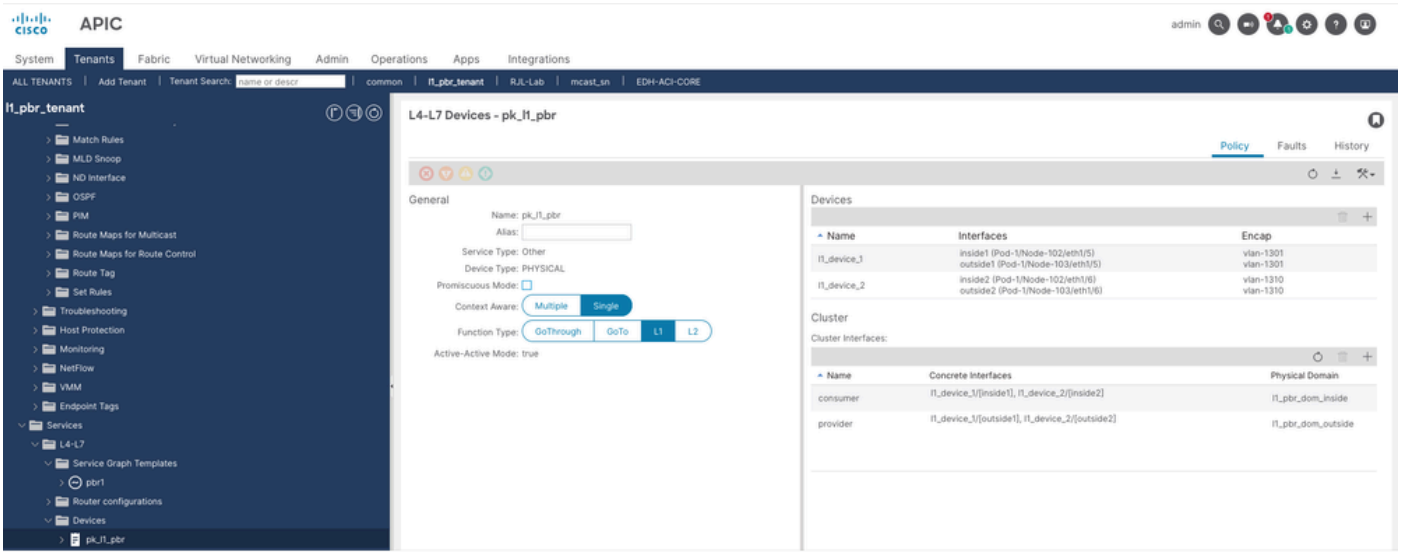
Etapa 3. Configurar a política do contrato de nível de serviço (SLA) IP com o tipo de SLA L2Ping.

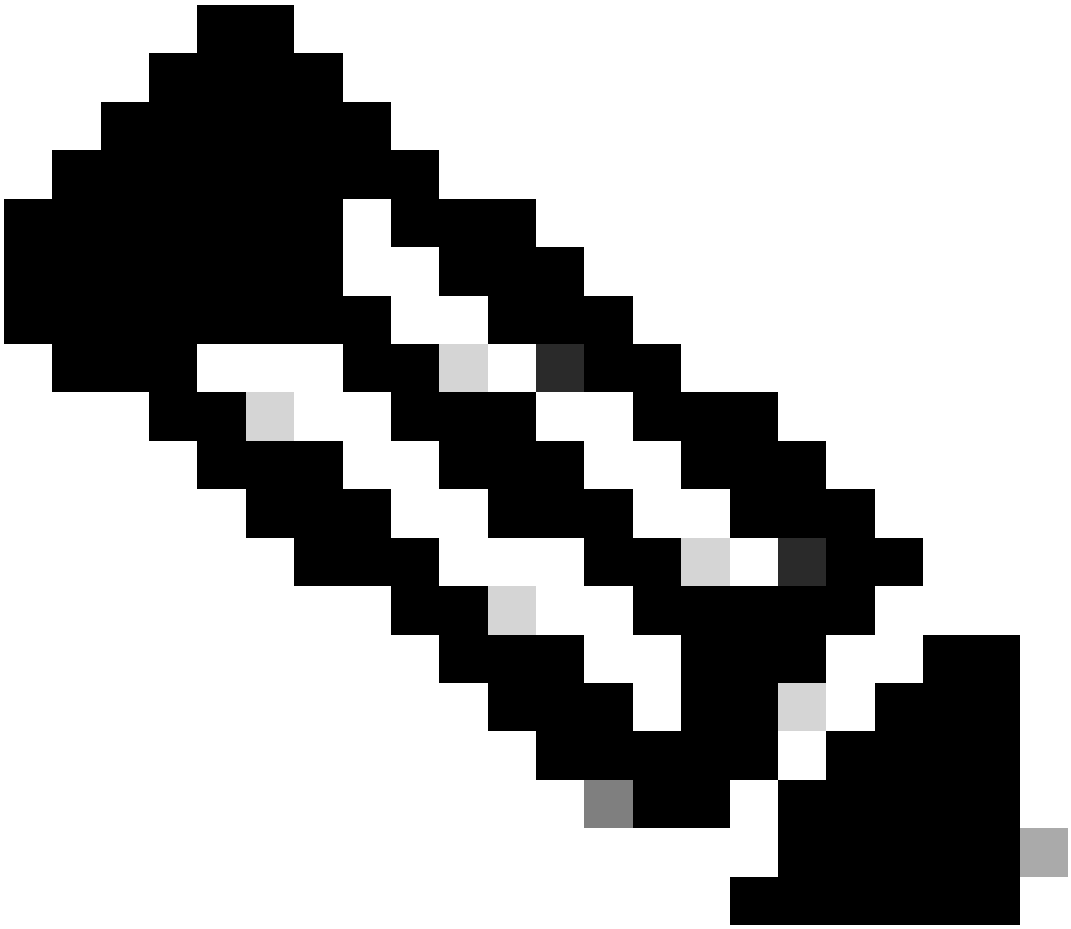
Navegue até Tenant > Policies > Protocol > IP SLA > IP SLA Monitoring Policies e clique com o botão direito do mouse em create policy.



Etapa 4. Configurar o dispositivo L4/L7.

Navegue para Locatário > Serviços > Dispositivos, clique com o botão direito do mouse e crie o dispositivo L4-L7.



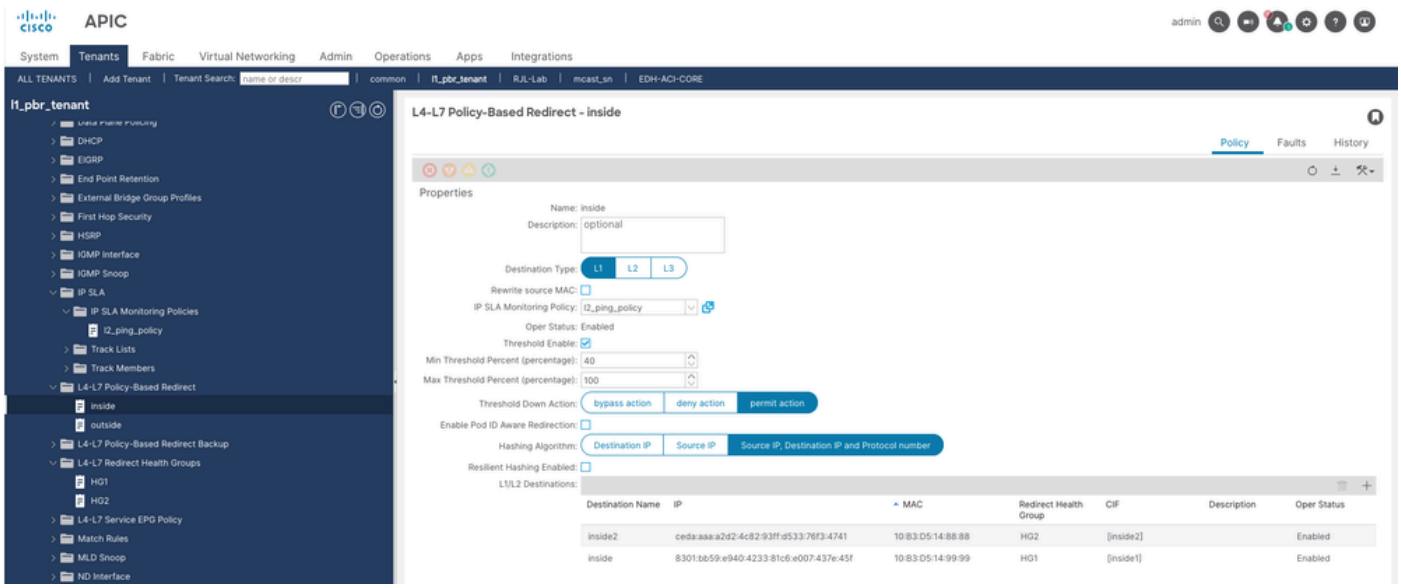


Note: Para o dispositivo L1, cada interface de cluster deve estar em domínios físicos diferentes para o escopo de porta local.

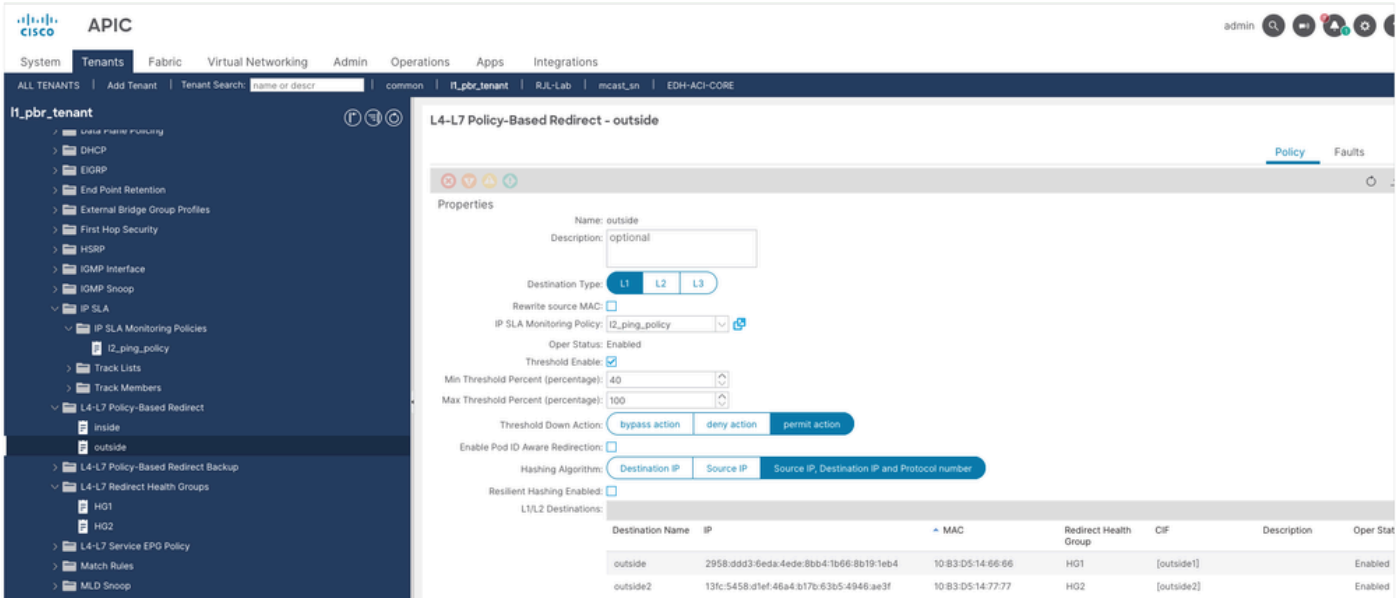
Etapa 5. Configure o redirecionamento baseado em política de L4-L7 para a interface interna e externa.

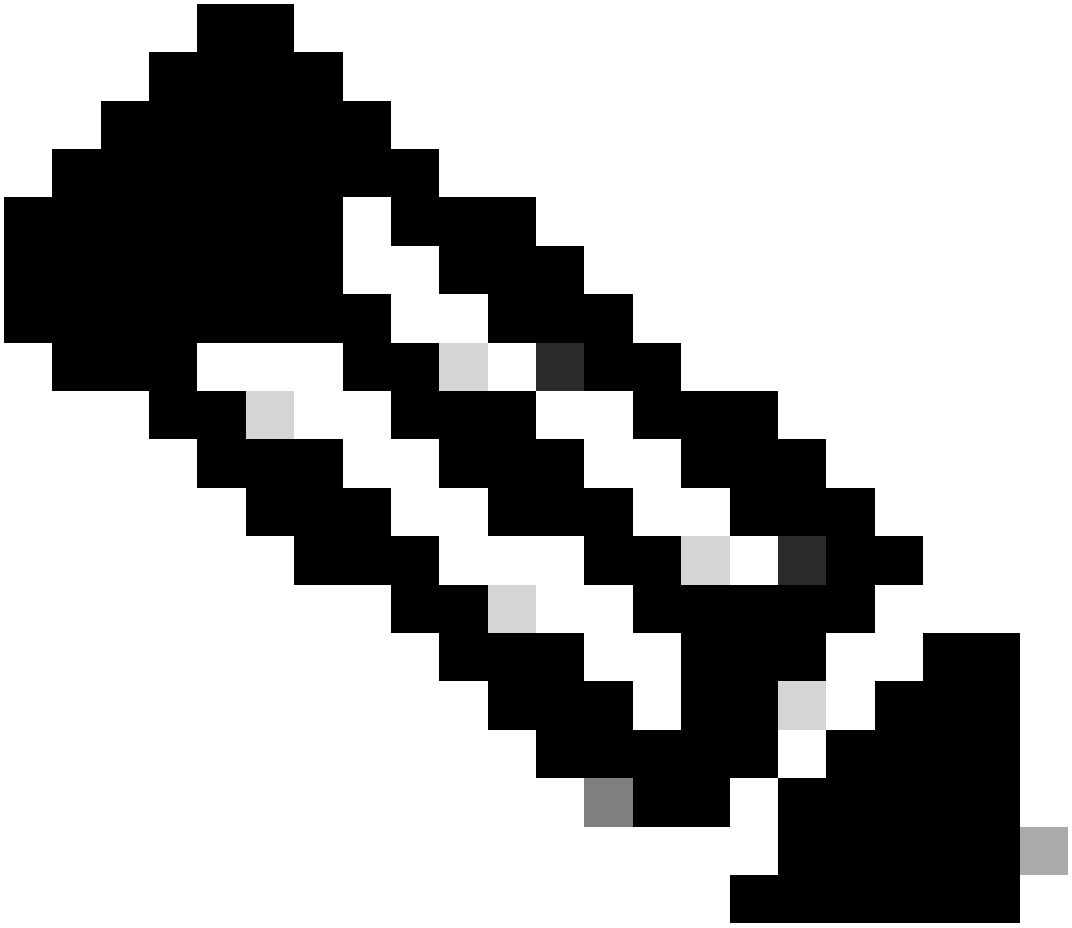
Navegue até Tenant > Policies > Protocol > L4-L7 Policy based redirect e clique com o botão direito do mouse e crie a política.

O nome da Política de ++ está dentro
++ Temos dois destinos L1, um para cada dispositivo L1



O nome da Política de ++ está fora
++ Temos dois destinos L1, um para cada dispositivo L1

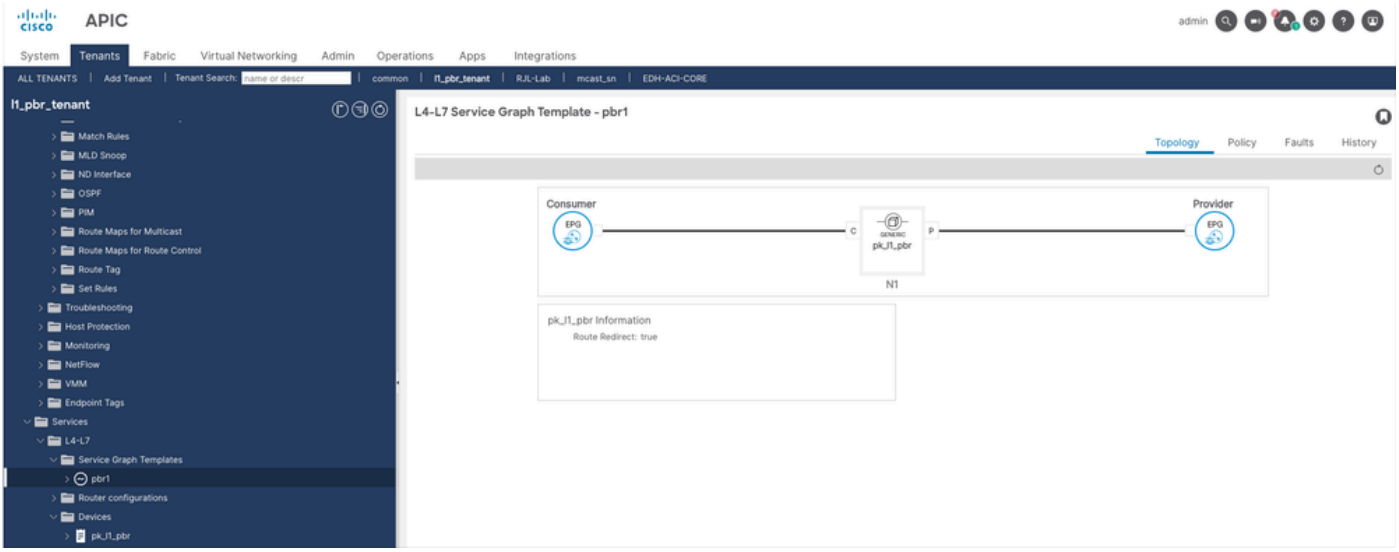




Note: A ação de limite deve ser a mesma para as políticas de redirecionamento L4-L7.

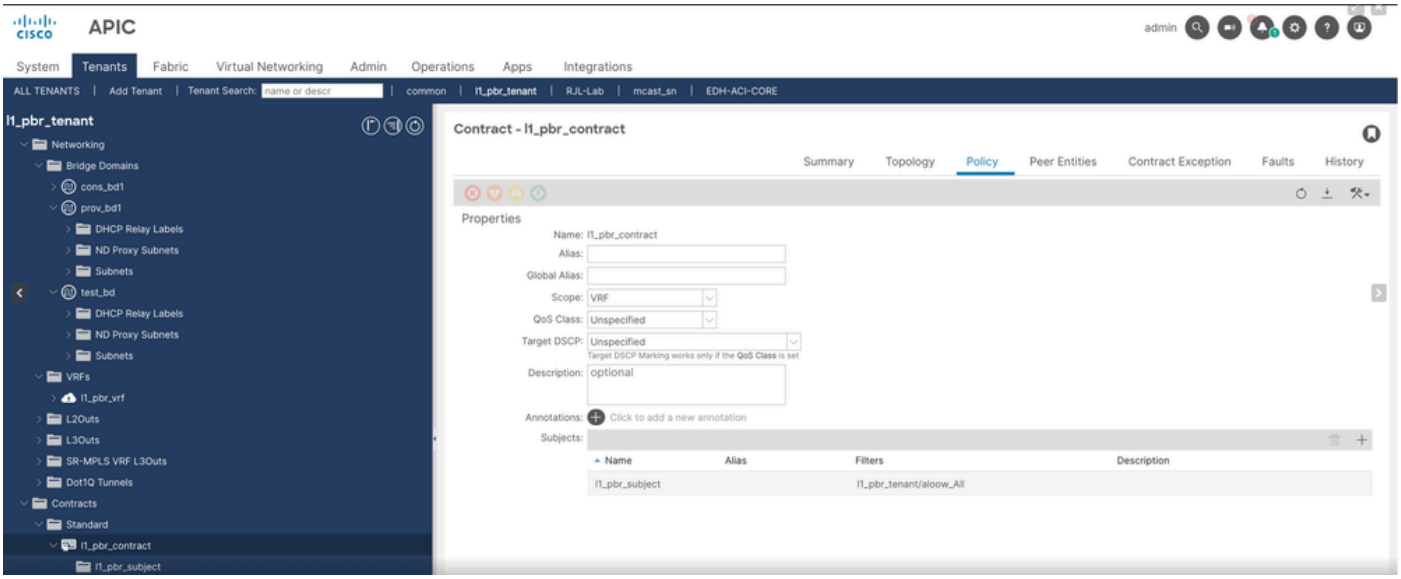
Etapa 6. Configurar o modelo de gráfico de Serviço.

Navegue para Locatário > Serviços > Modelo de gráfico de serviço, clique com o botão direito do mouse e crie o modelo de gráfico de serviço L4-L7.

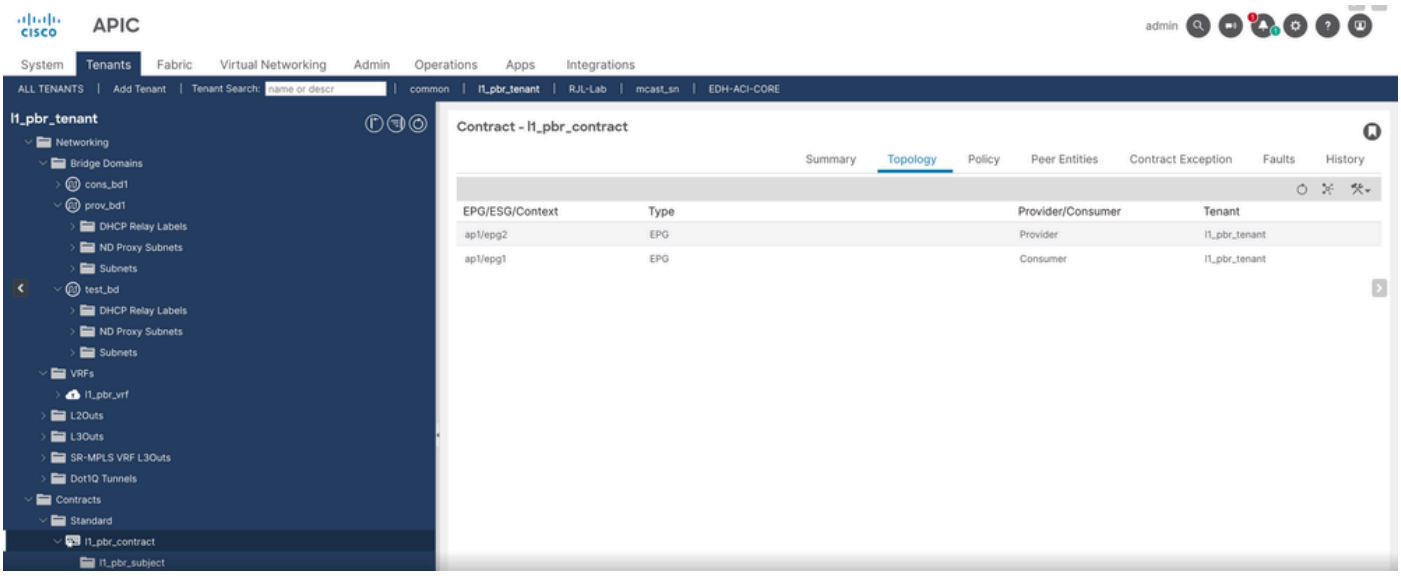


Etapa 7. Criar um contrato.

Navegue para Locatário > Contrato > Padrão, clique com o botão direito do mouse e crie o contrato.

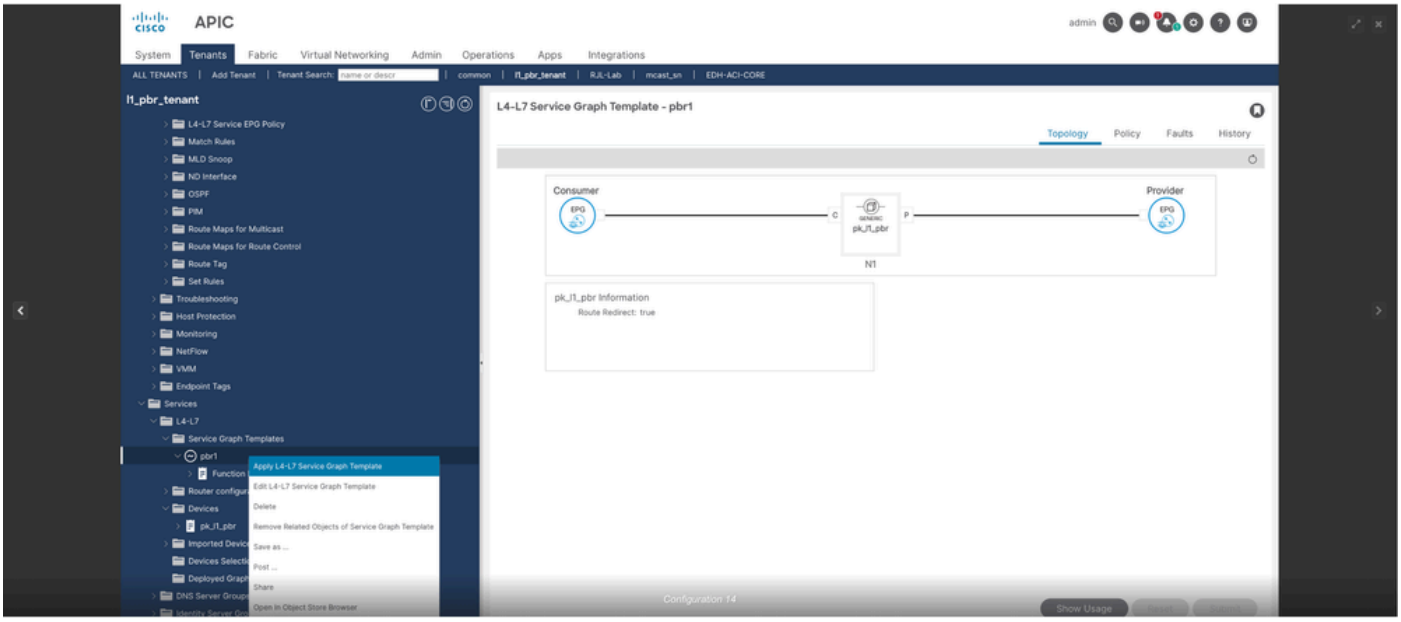


Etapa 8. Aplique o contrato como consumidor e provedor para EPG1 e EPG2, respectivamente.

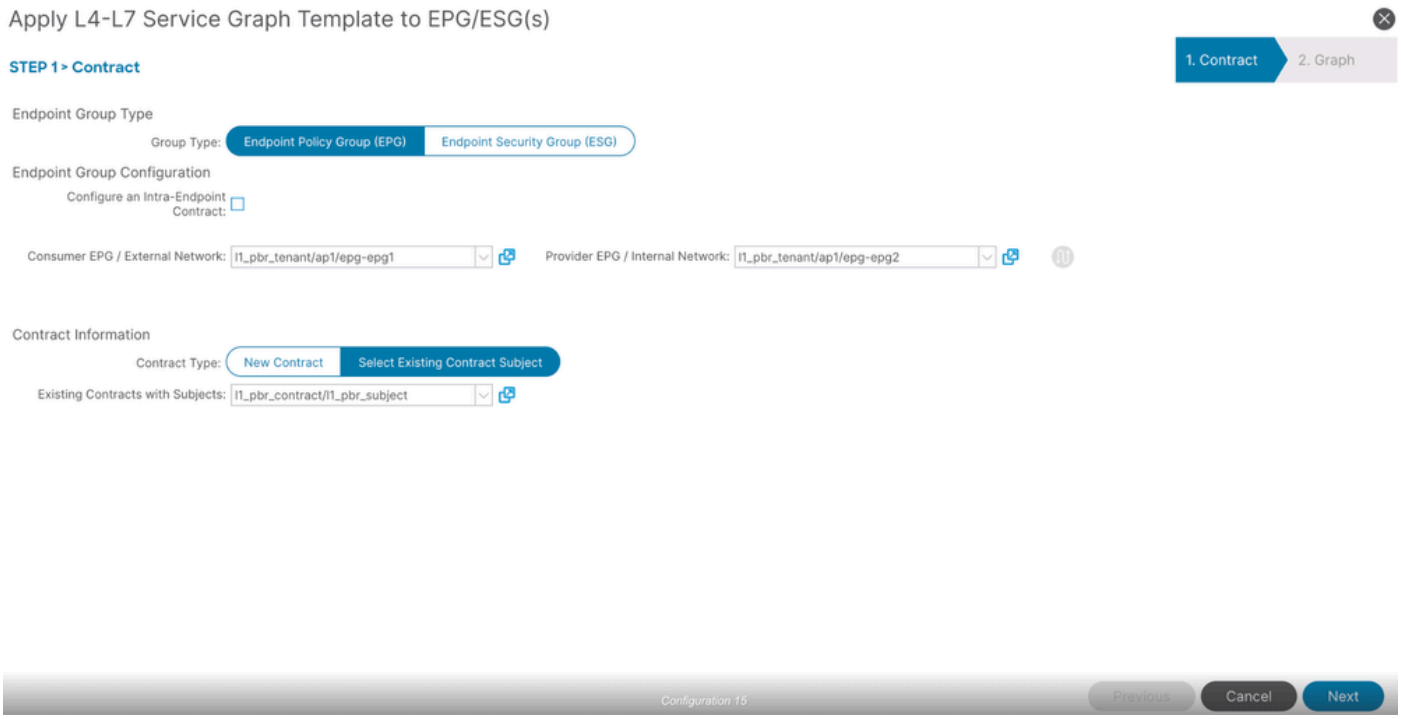


Etapa 9. Aplicar o modelo de gráfico de serviço L4-L7.

Navegue para Locatário > Serviços > Modelo de gráfico de serviço, clique com o botão direito do mouse em PBR1 e aplique o modelo de gráfico de serviço L4-L7.

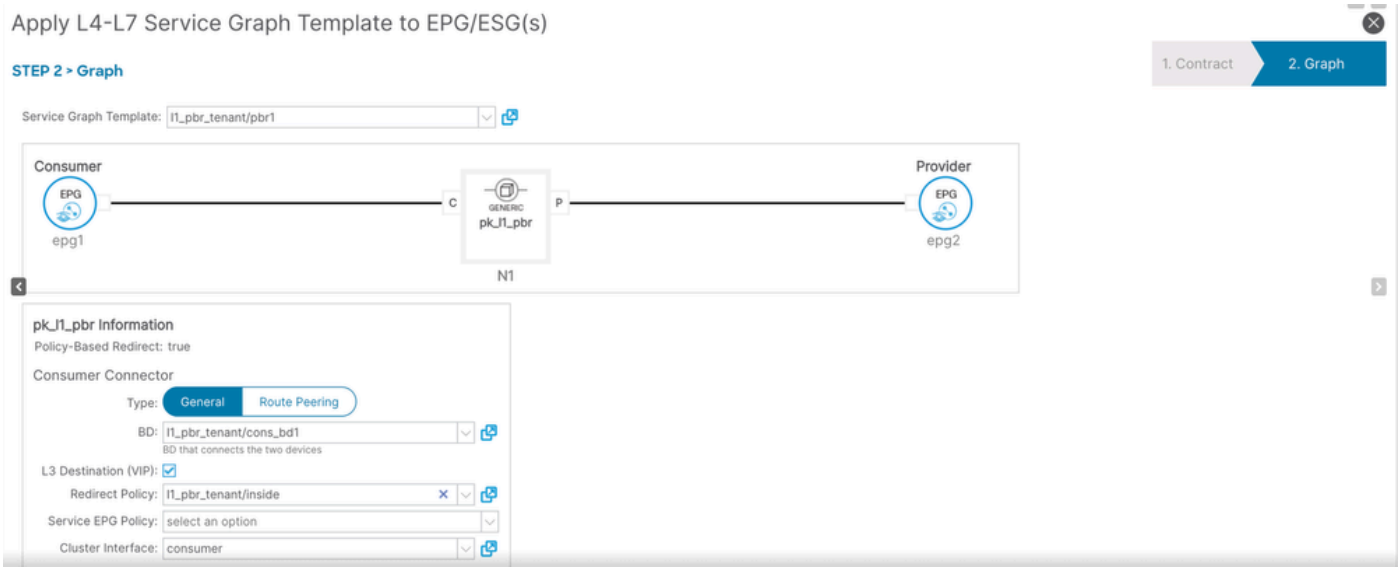


++ Adicionar EPG de consumidor e provedor
++ Especificar contrato

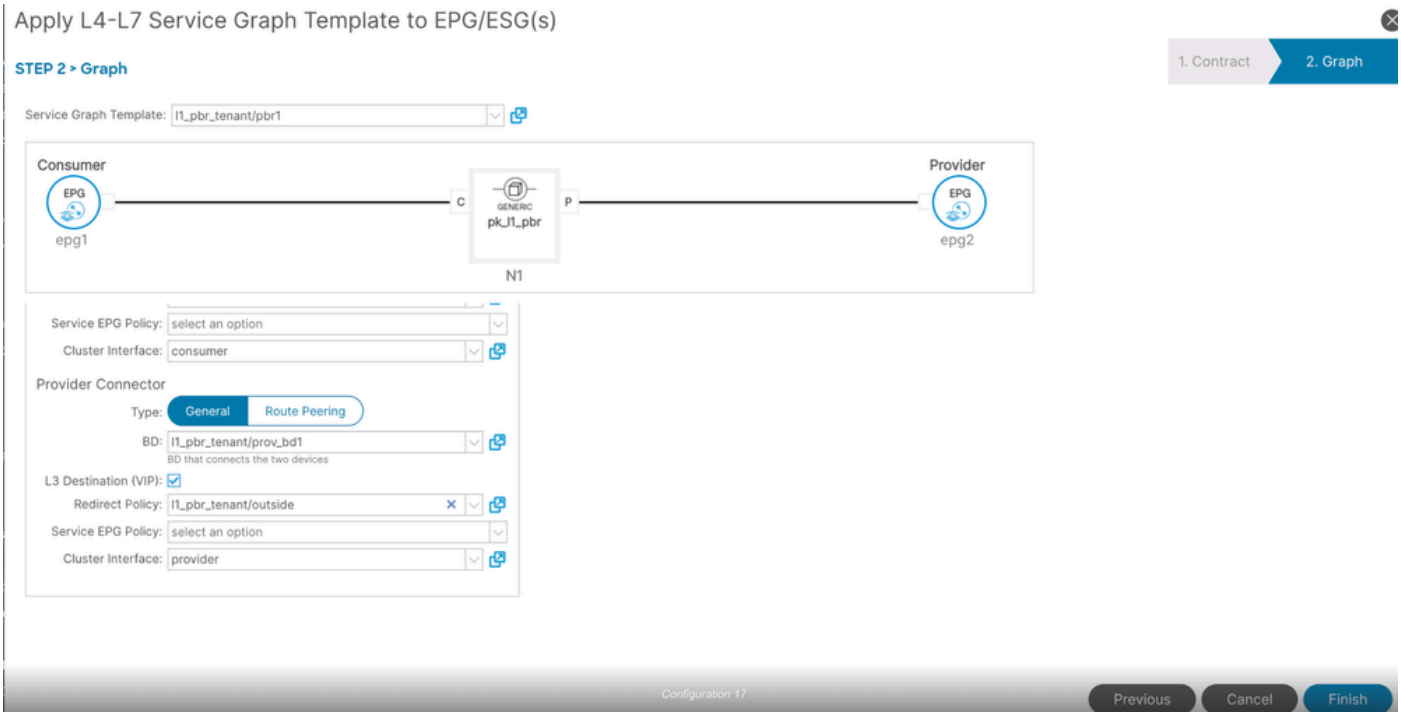


++ em Avançar

++ Especificar detalhes do conector do consumidor



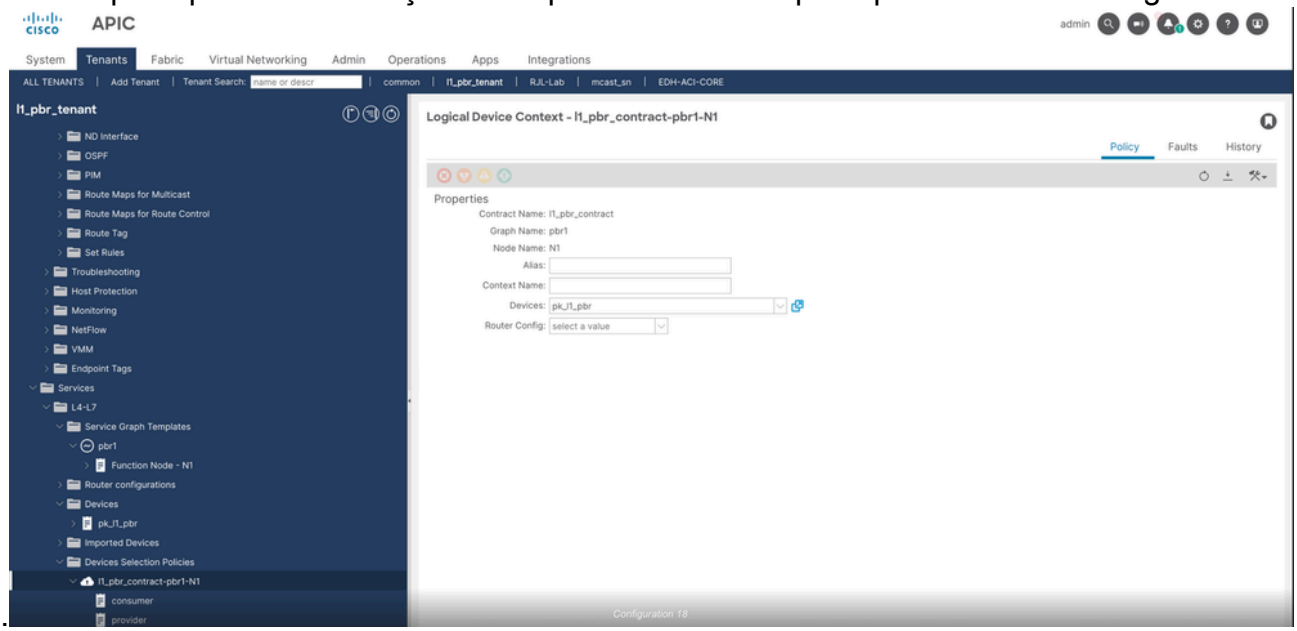
++ Especificar detalhes do conector do provedor



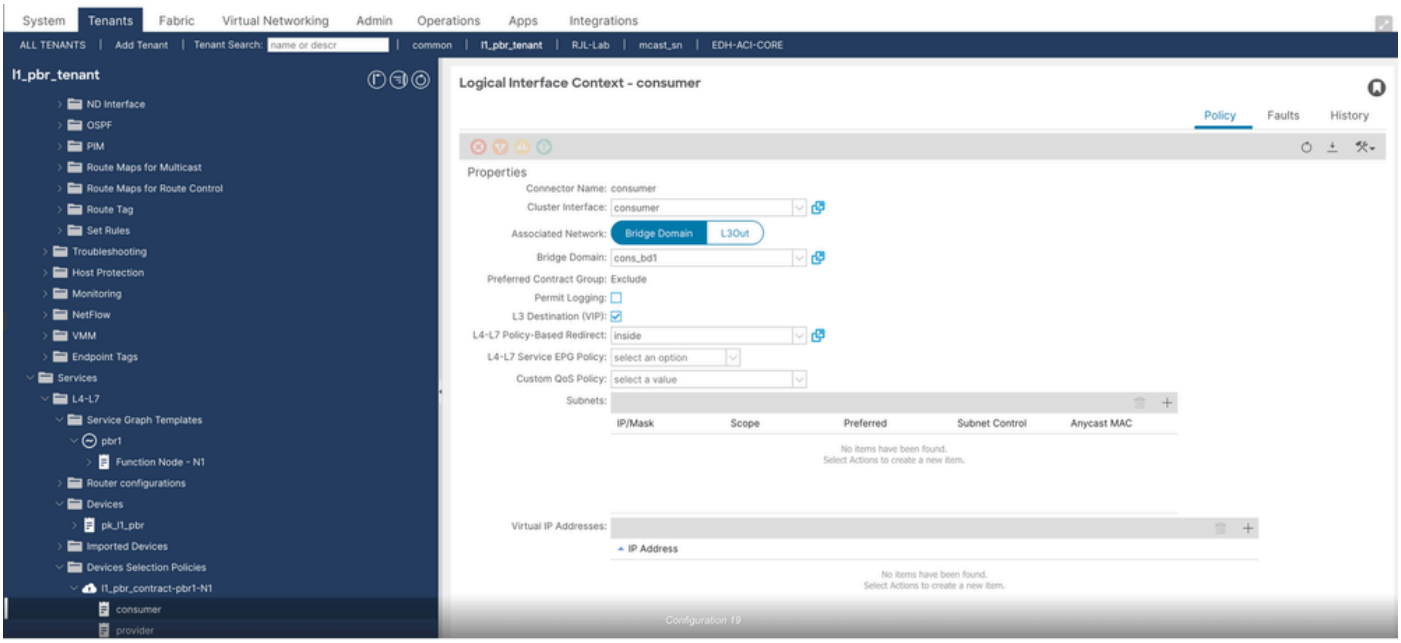
++ Clique em Concluir

Verificação do gráfico de serviço L1 na GUI do APIC

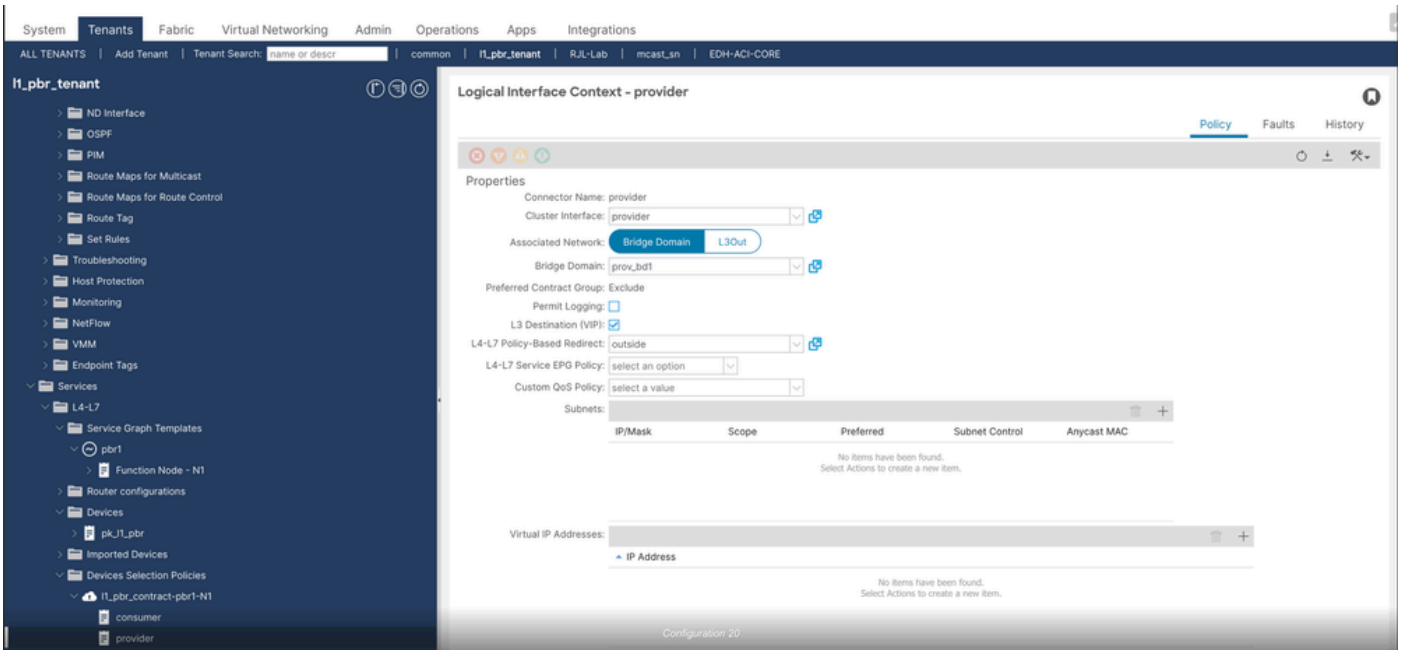
Etapa 1. Verifique a política de seleção de dispositivos criada após aplicar o modelo de gráfico de serviço.



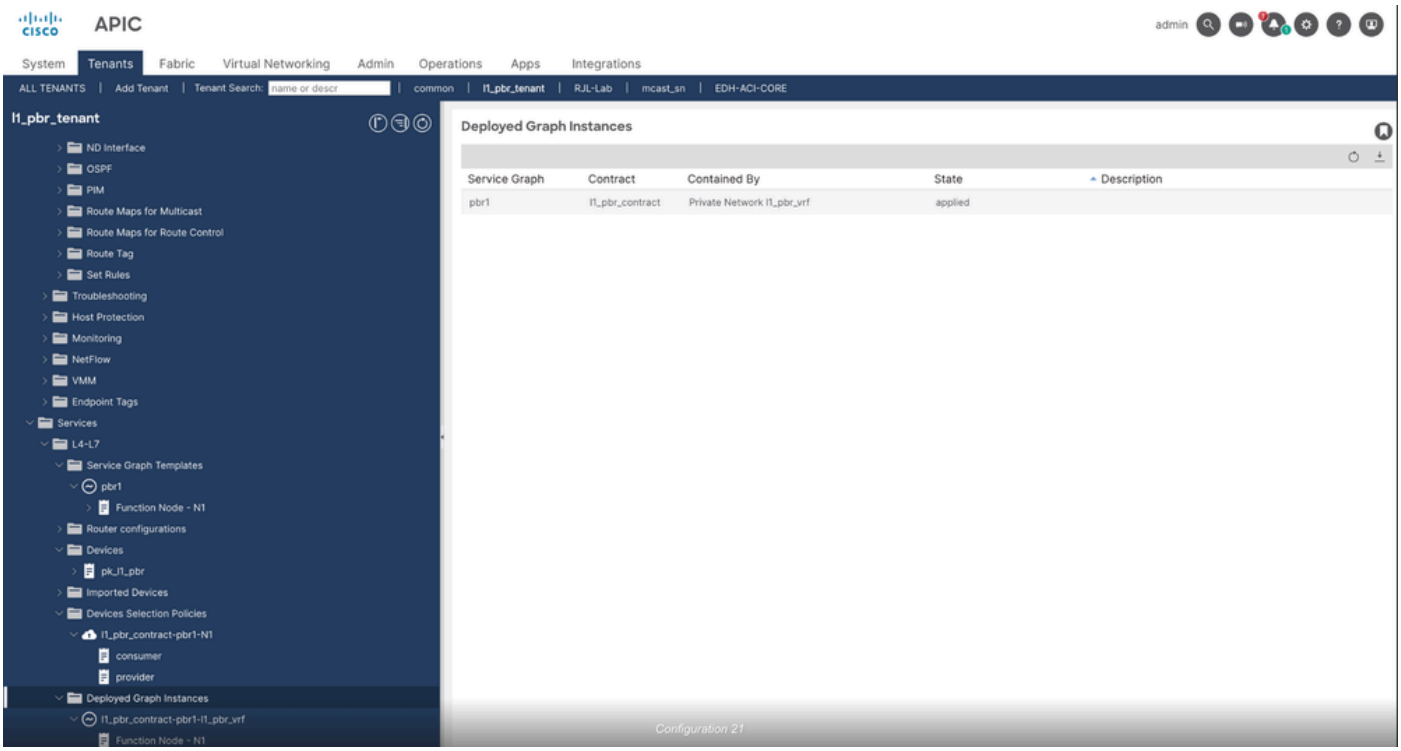
++ Verificar o conector do consumidor



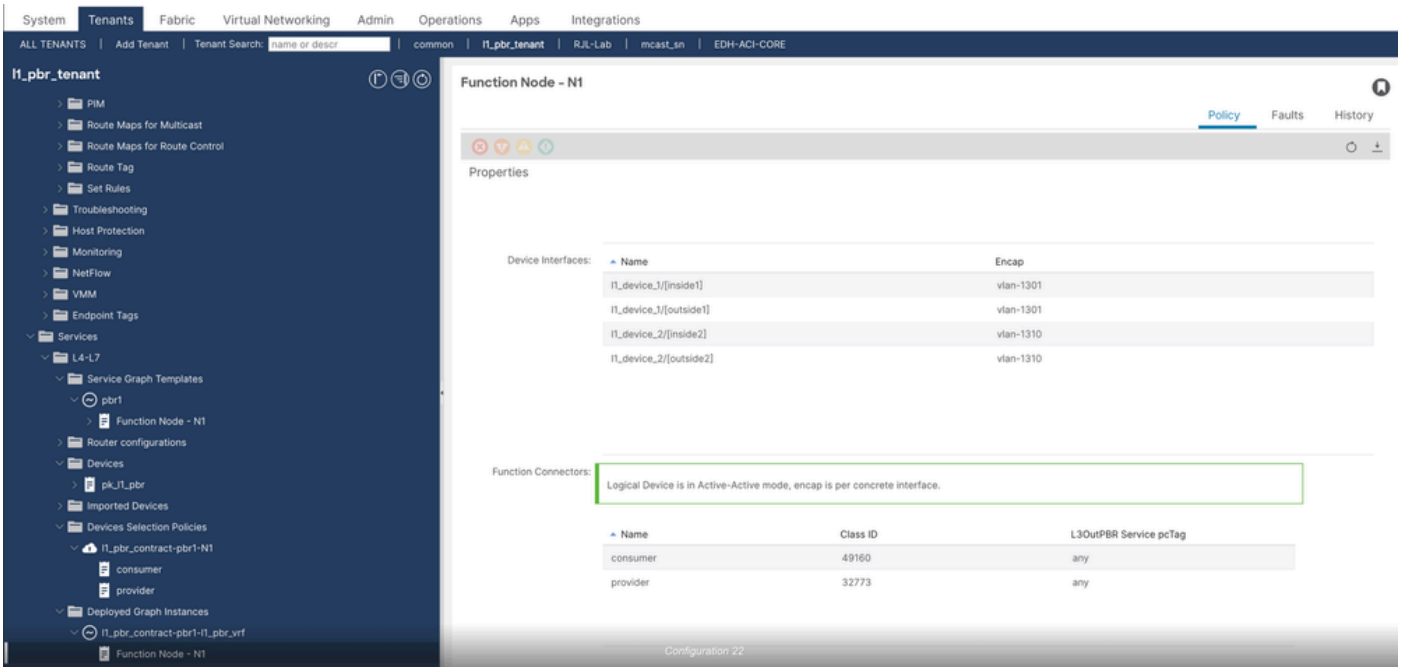
++ Configurar conector do provedor



Etapa 2. Verifique as instâncias do gráfico implantado. Lá você verá uma instância, ela deve estar no estado aplicado.



++ Verifique as interfaces do dispositivo e os conectores de função onde você verá o PCTAG associado aos EPGs de serviço



Verificação do gráfico de serviço L1 no APIC CLI

Etapa 1. Verificar se o gráfico de serviço é aplicado no nó do consumidor e provedor juntamente com o status do grupo de funcionamento.

<#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
```

Etapa 2. Verificar se a associação MAC estática foi criada nos nós de serviço (102 e 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
```

Validação de tráfego

1. 2000 pacotes de ping ICMP estão sendo gerados de EP1 para EP2 que serão redirecionados para o dispositivo L1.

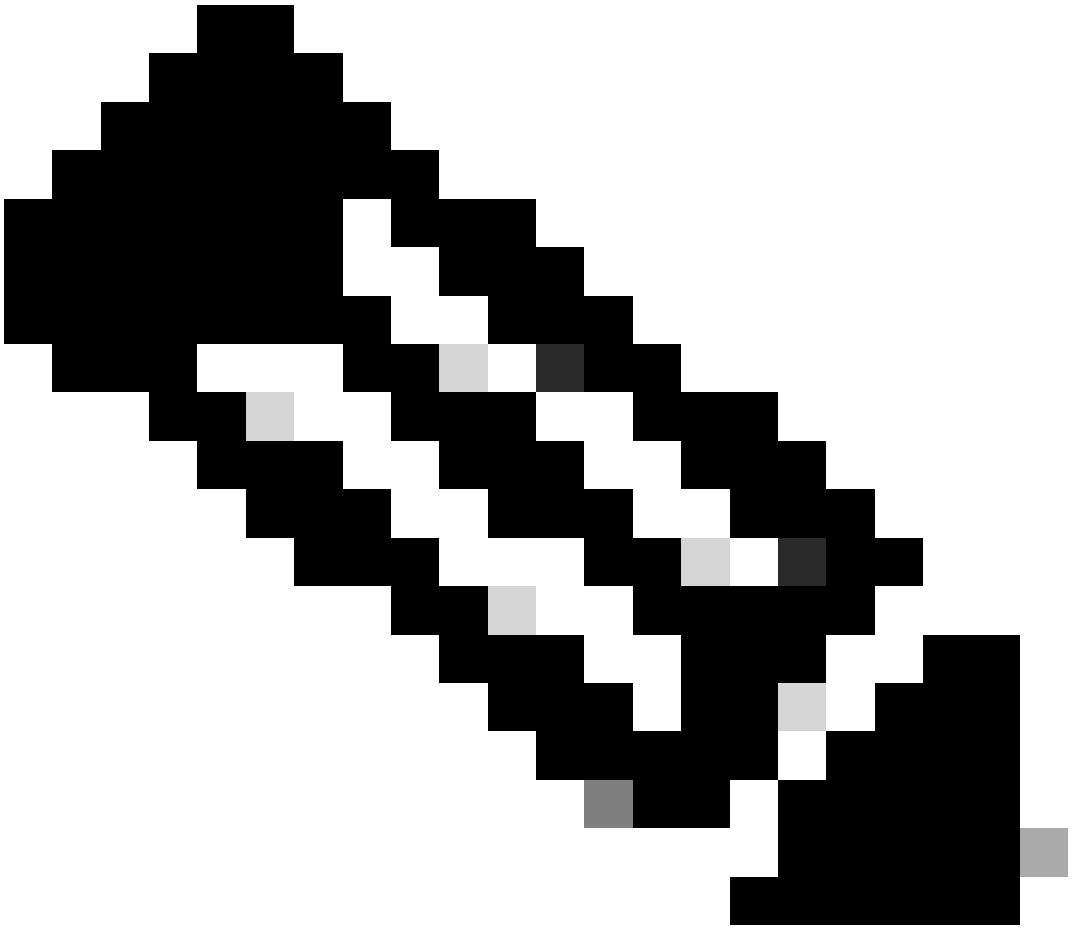
```
switch1# ping 192.168.132.200 vrf l1_pbr1 count 2000 >>>>> sending 2000 packets
64 bytes from 192.168.132.200: icmp_seq=464 ttl=251 time=0.859 ms
64 bytes from 192.168.132.200: icmp_seq=465 ttl=251 time=0.872 ms
64 bytes from 192.168.132.200: icmp_seq=466 ttl=251 time=0.844 ms
64 bytes from 192.168.132.200: 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 os contadores de interfaces nos nós 102 e 103 que estão conectados ao 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
```



Note: Os contadores de interface foram apagados nos nós 102 e 103 antes que o tráfego fosse testado.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.