配置并检验ACI中的主用/主用L1 PBR

目录

简介

本文档介绍如何在以应用为中心的基础设施(ACI)中配置和验证主用/主用L1服务图。

先决条件

要求

Cisco 建议您了解以下主题：

- 了解第3层服务图在ACI中如何工作
- 了解如何在ACI中配置终端策略组、桥接域和合同

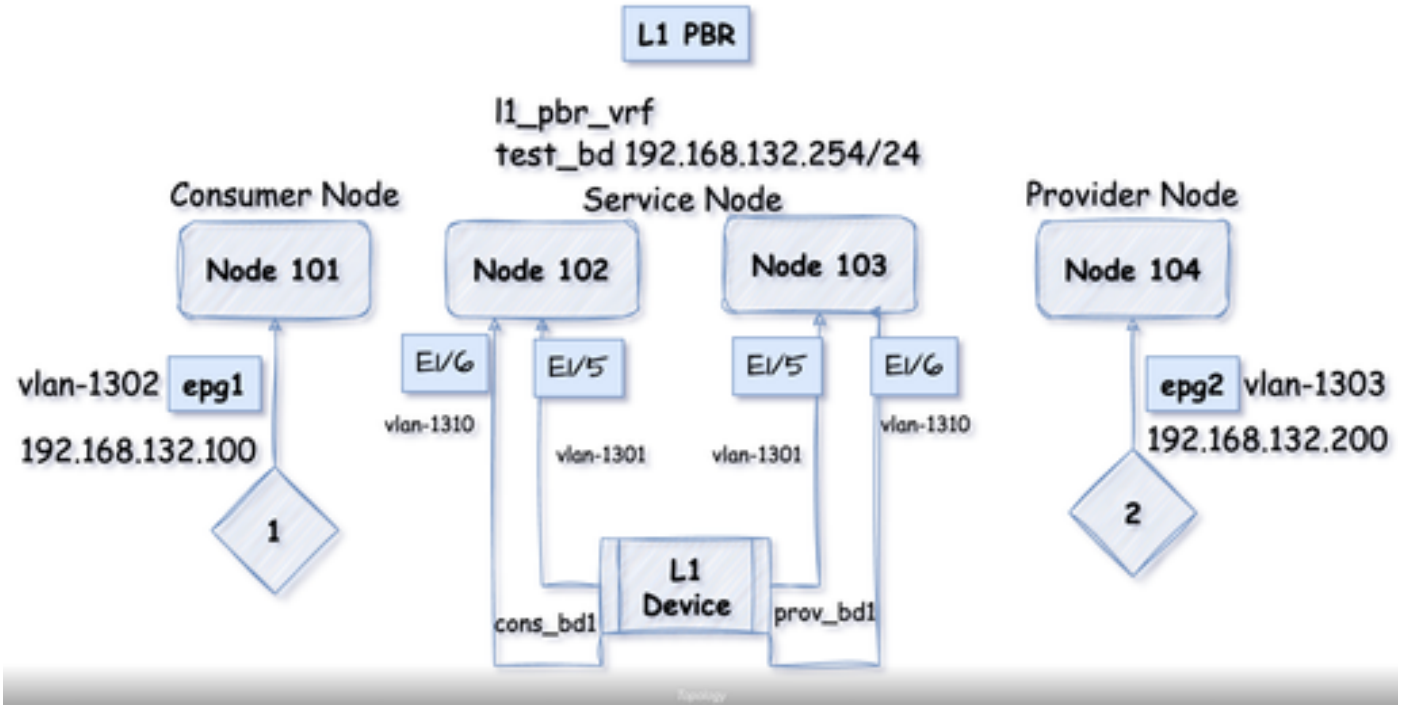
使用的组件

本文档中的信息基于以下软件和硬件版本：

- APIC版本：5.3(2a)
- 枝叶硬件：N9K-C93180YC-FX、N9K-C93180YC-EX
- 枝叶软件：n9000-15.3(2a)
- 枝叶节点101、102、103、104

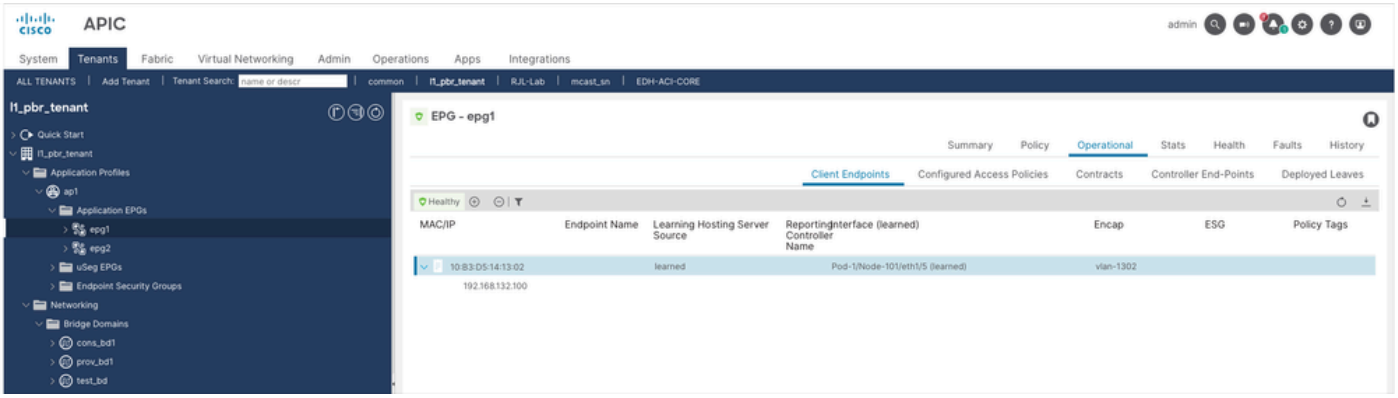
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解任何命令的潜在影响

拓扑

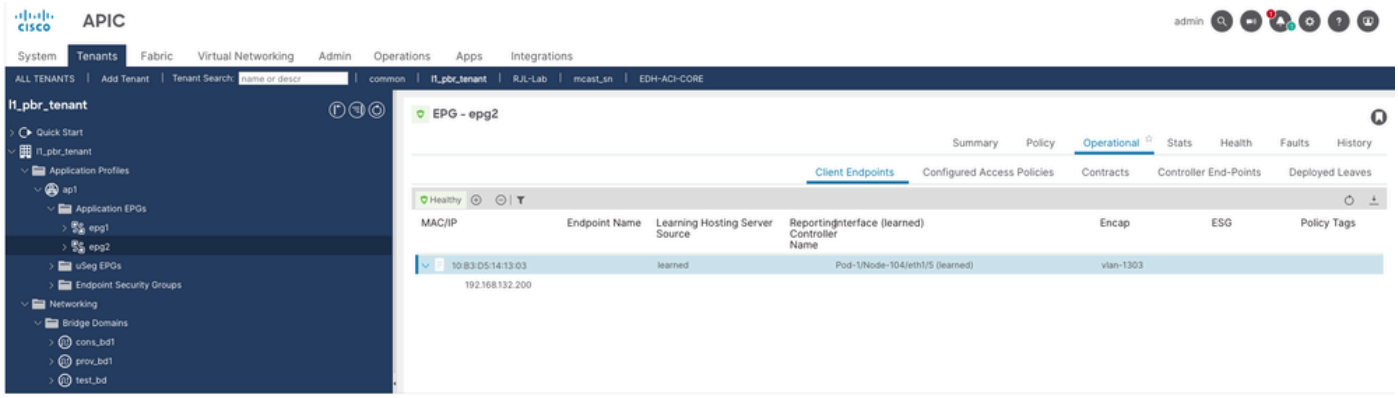


本文档中未显示EPG1和EPG2配置，必须在手前对其进行配置，且必须学习终端。

1.验证EPG1已获ș知的终端192.168.132.100（节点101）。



2.验证EPG2是否已获知终端192.168.132.200（节点104）。



为什么ACI中需要L1服务图？

在思科ACI中，您可以将L4-L7服务设备插入为L3/L2/L1。第3层表示外部设备能够执行路由决策来转发流量，而第2层表示仅根据MAC地址转发流量。在ACI中，您可以插入第2层设备，例如入侵防御系统(IPS)/透明防火墙。现在想象一下以下场景：您要重定向流量的设备无法做出任何转发决策，因此，在这些情况下，您可以部署L1策略型路由(PBR)。

流量转发对于L3和L2 PBR情况是相同的，唯一的区别是，L3 PBR流量被重定向到IP地址，而L1/L2 PBR流量被重定向到MAC地址。这些MAC地址被静态绑定到枝叶接口以用于转发。您会进一步看到这方面的更多内容。

有关主用/备用或主用/主用L1/L2 PBR使用案例的详细信息，请参阅链路；PBR白皮书。

关于L1设备

在此部署模式中，不会在服务设备上执行VLAN转换，并且其两个接口在同一个VLAN上运行。此方法通常称为内联模式或有线模式，通常用于防火墙和入侵防御系统(IPS)。 当期望服务设备在不参与第2层或第3层转发的情况下执行安全功能时，它非常理想。

主用/主用L1 PBR

从ACI版本5.0开始，支持在主用/主用模式下部署具有第4-7层设备的服务图。这可以通过为每个L4-L7设备接口（具体接口）分配唯一的封装并利用在隐藏服务EPG上自动配置“封装中泛洪”(Flood in encap)的ACI来实现。此隐藏服务EPG由ACI创建，以将L4-L7设备接口与服务网桥域相关联。

管理员无需手动配置隐藏的服务EPG，因为ACI会在服务图形呈现过程中自动启用“Flood in encap”。

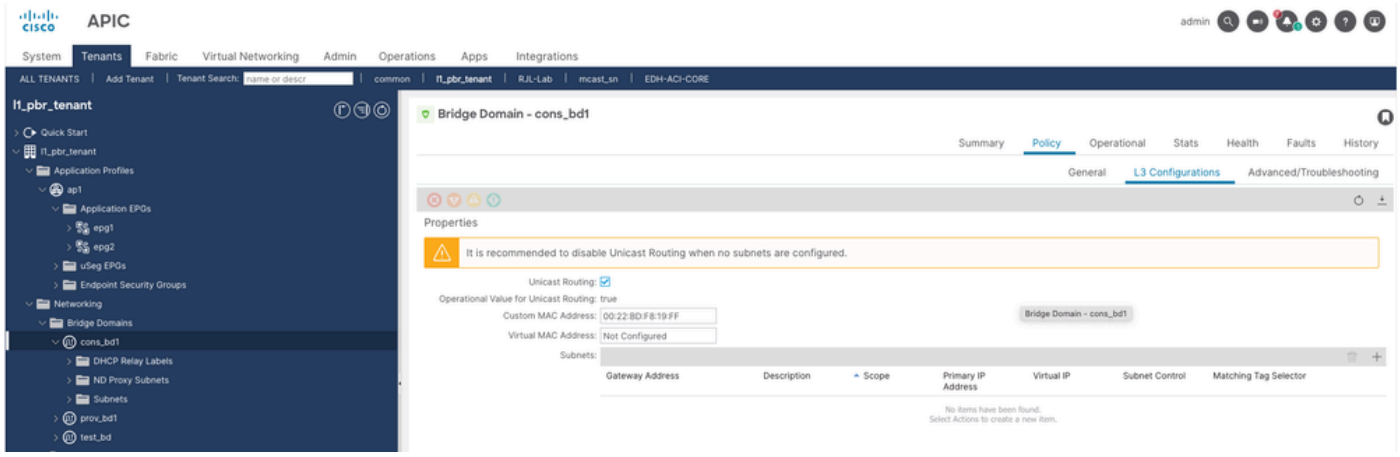
对于L1 PBR主用 — 主用部署，必须配置端口本地范围。这要求将L4-L7设备的消费者和提供商群集接口（连接器）置于单独的物理域中，每个域都有自己的VLAN池，同时在两个域中保持相同的VLAN范围。

参考：PBR白皮书。

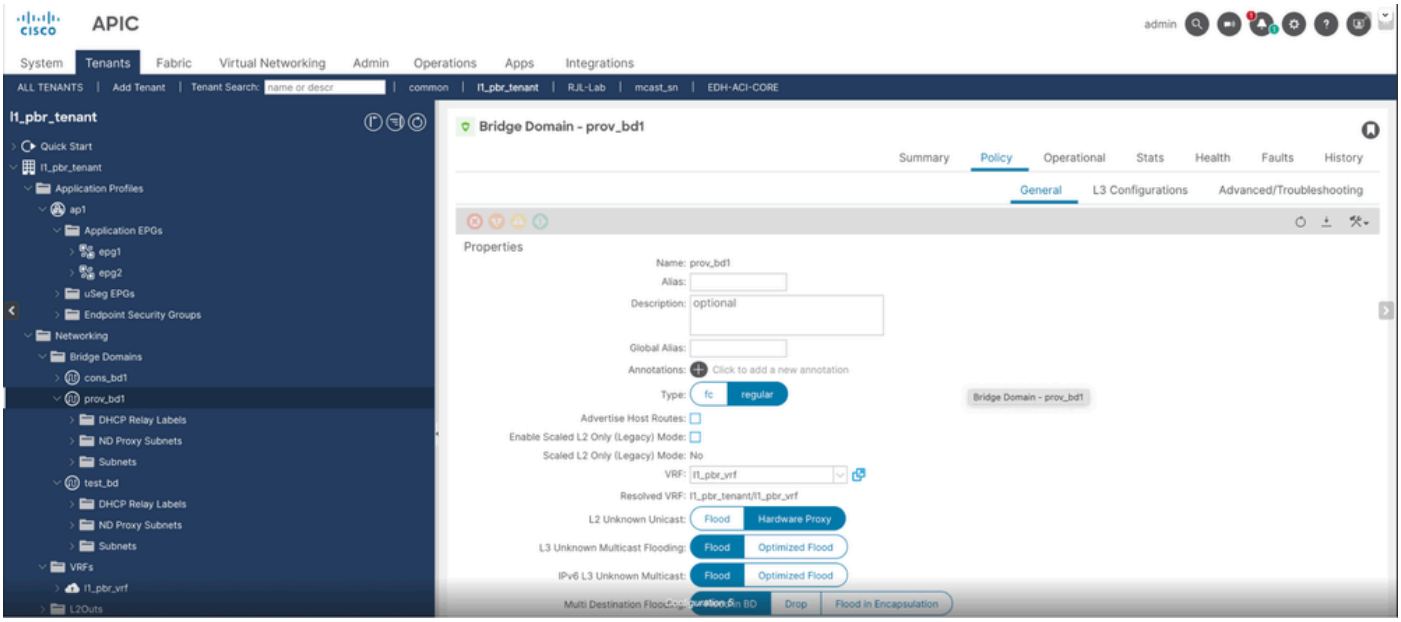
L1服务图的配置

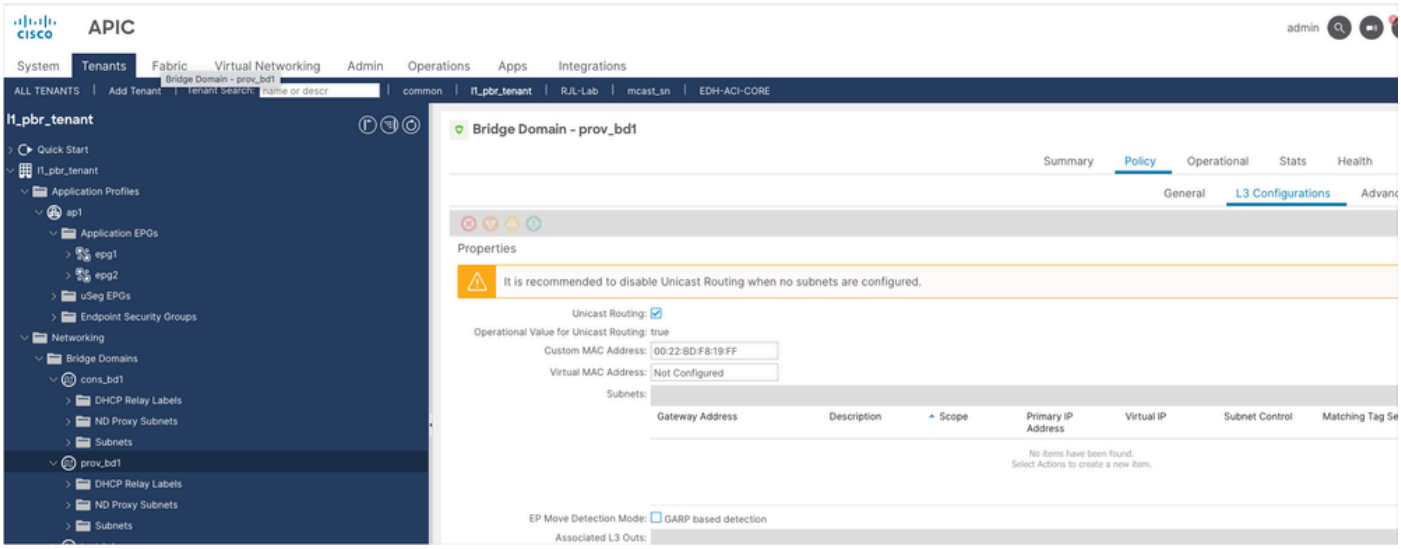
必须启用单播路由，L2未知单播必须设置为Hardware proxy，cons和prov网桥域不需要子网。

步骤1.配置名为cons_bd1的使用者网桥域。



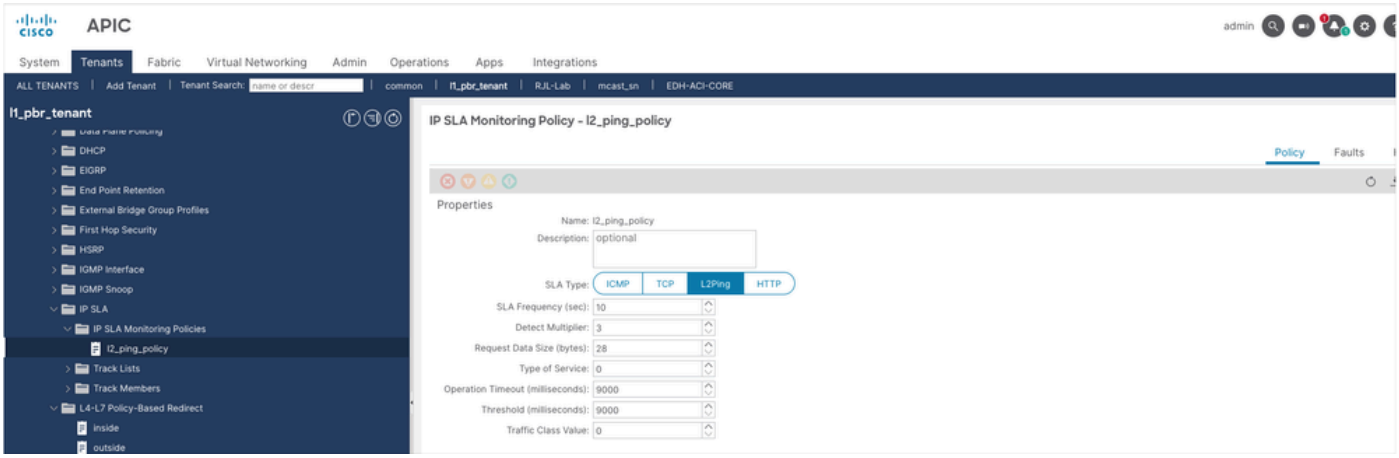
步骤2.配置名为prov-bd1的提供程序网桥域。





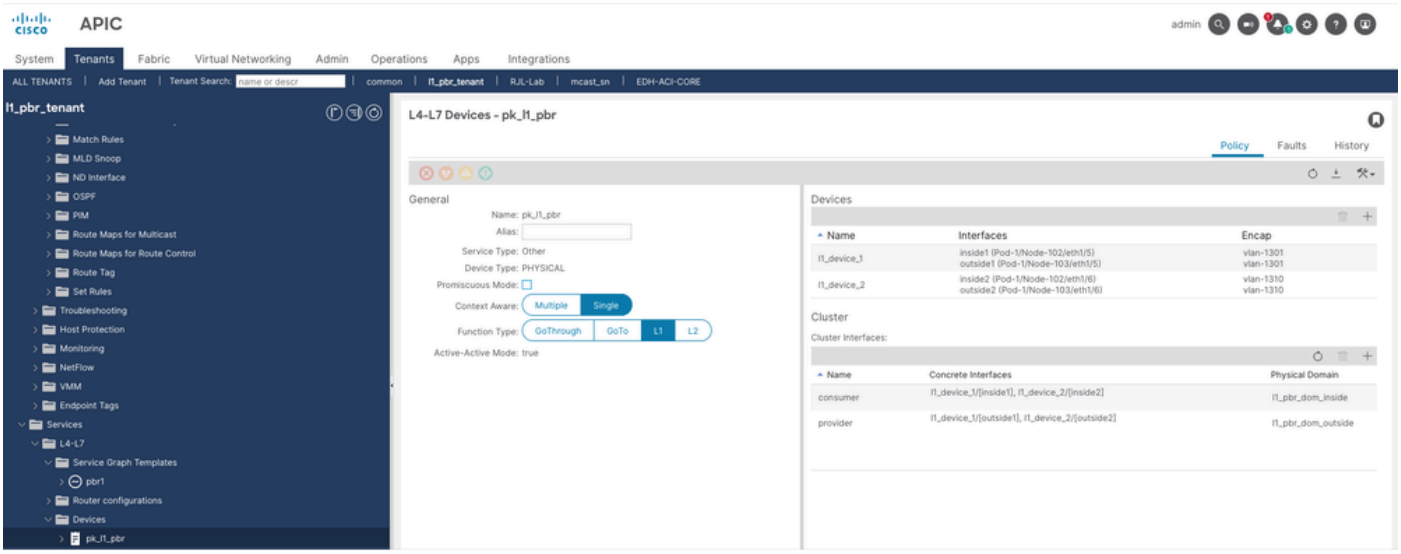
第3步：使用SLA类型L2Ping配置IP服务级别协议(SLA)策略。

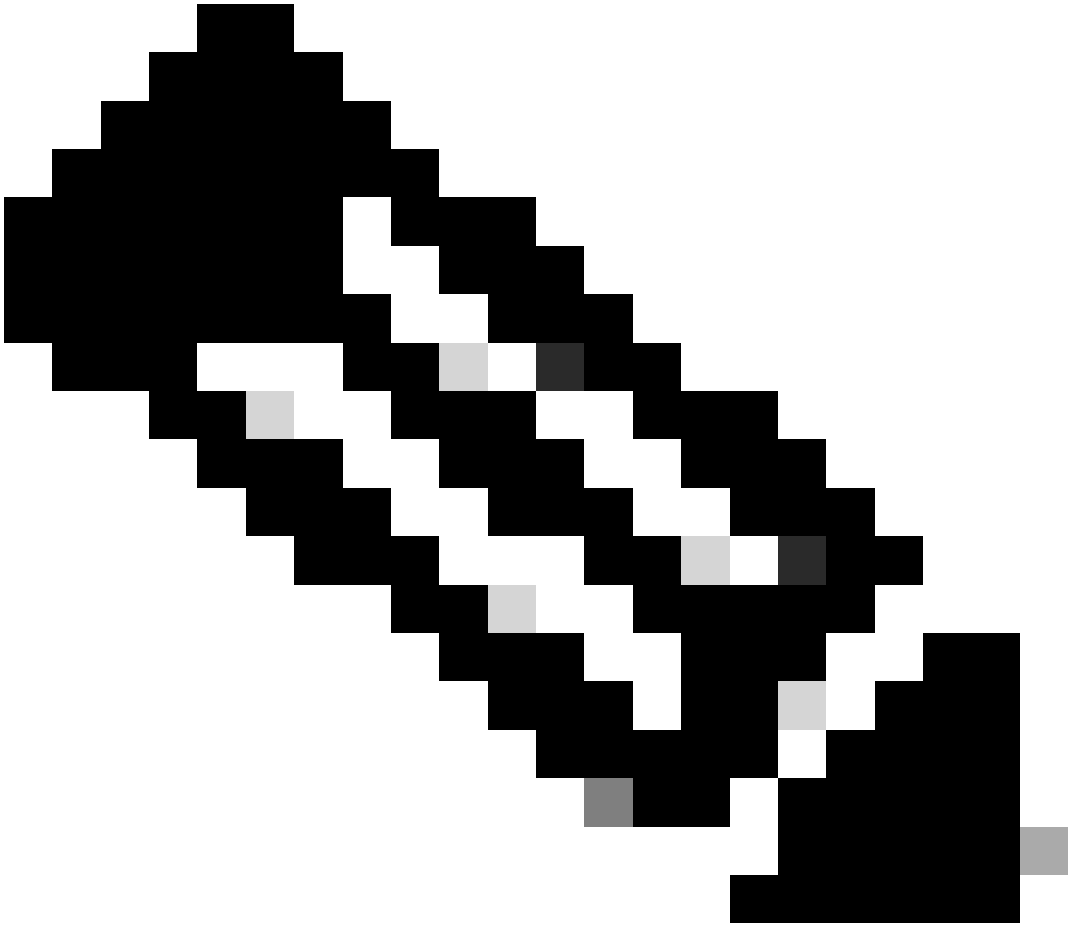
导航到Tenant > Policies > Protocol > IP SLA > IP SLA Monitoring Policies，然后右键点击并创建策略。



步骤4.配置第4/7层设备。

导航到租户>服务>设备，然后右键单击并创建L4-L7设备。



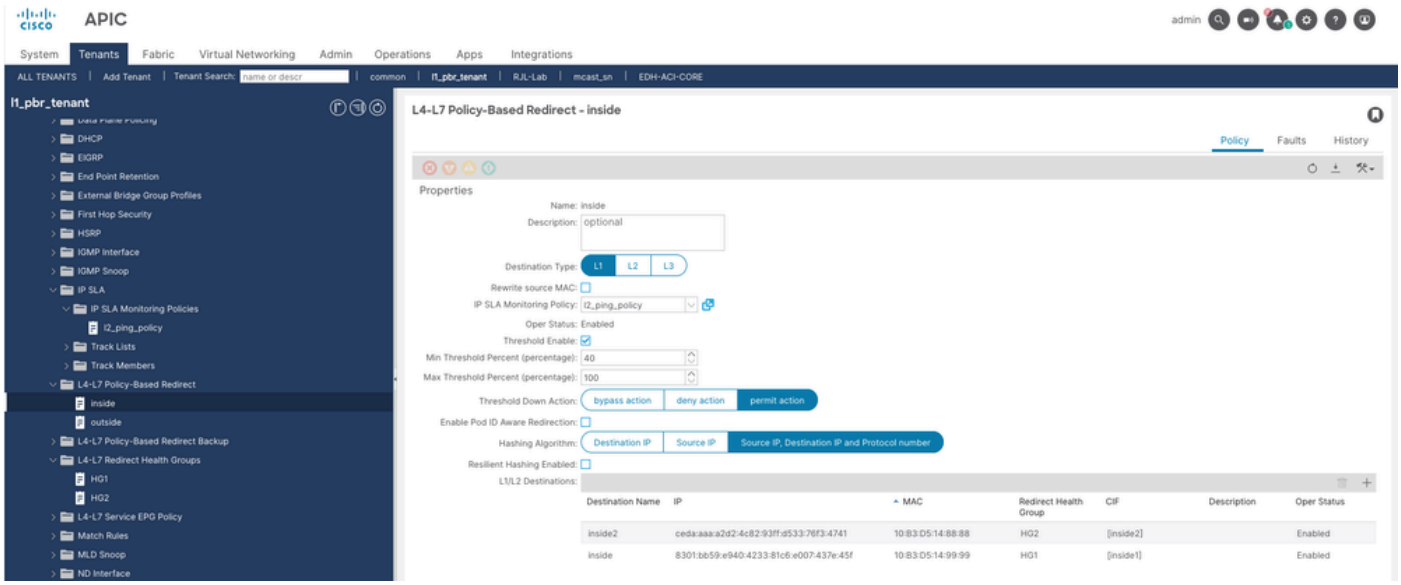


注意：对于L1设备，对于端口本地范围，每个集群接口必须位于不同的物理域中。

步骤5.为内部和外部接口配置基于L4-L7策略的重定向。

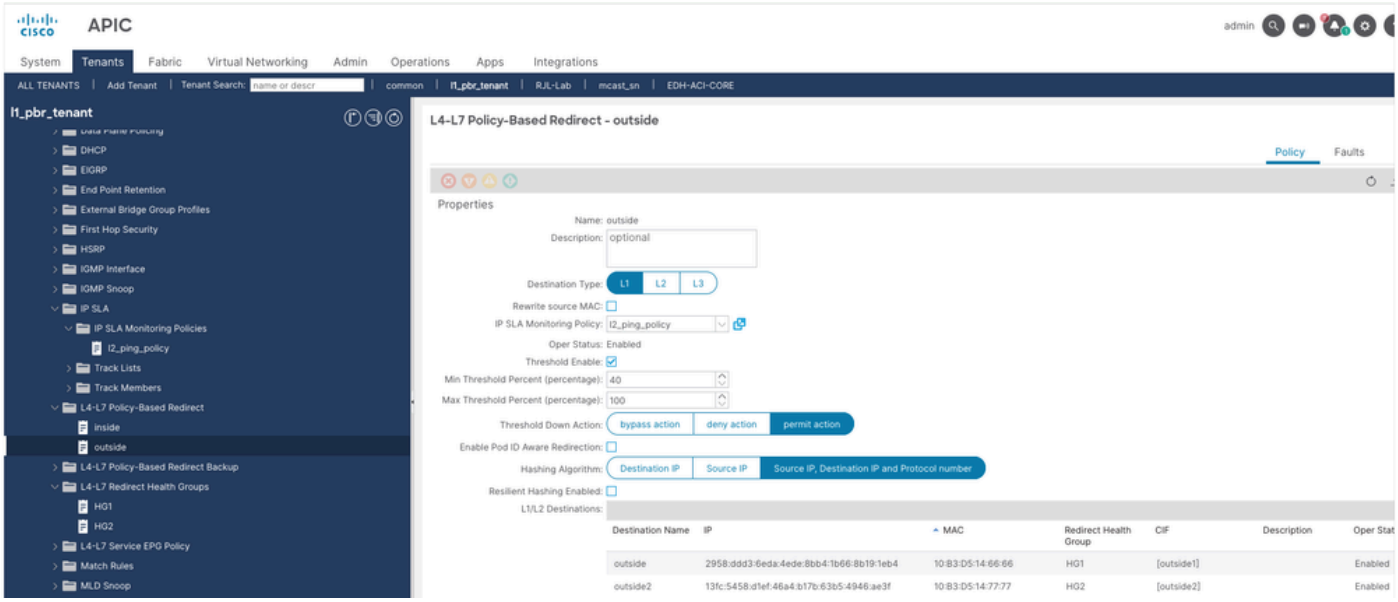
导航到Tenant > Policies > Protocol > L4-L7 Policy based redirect，然后右键单击并创建策略。

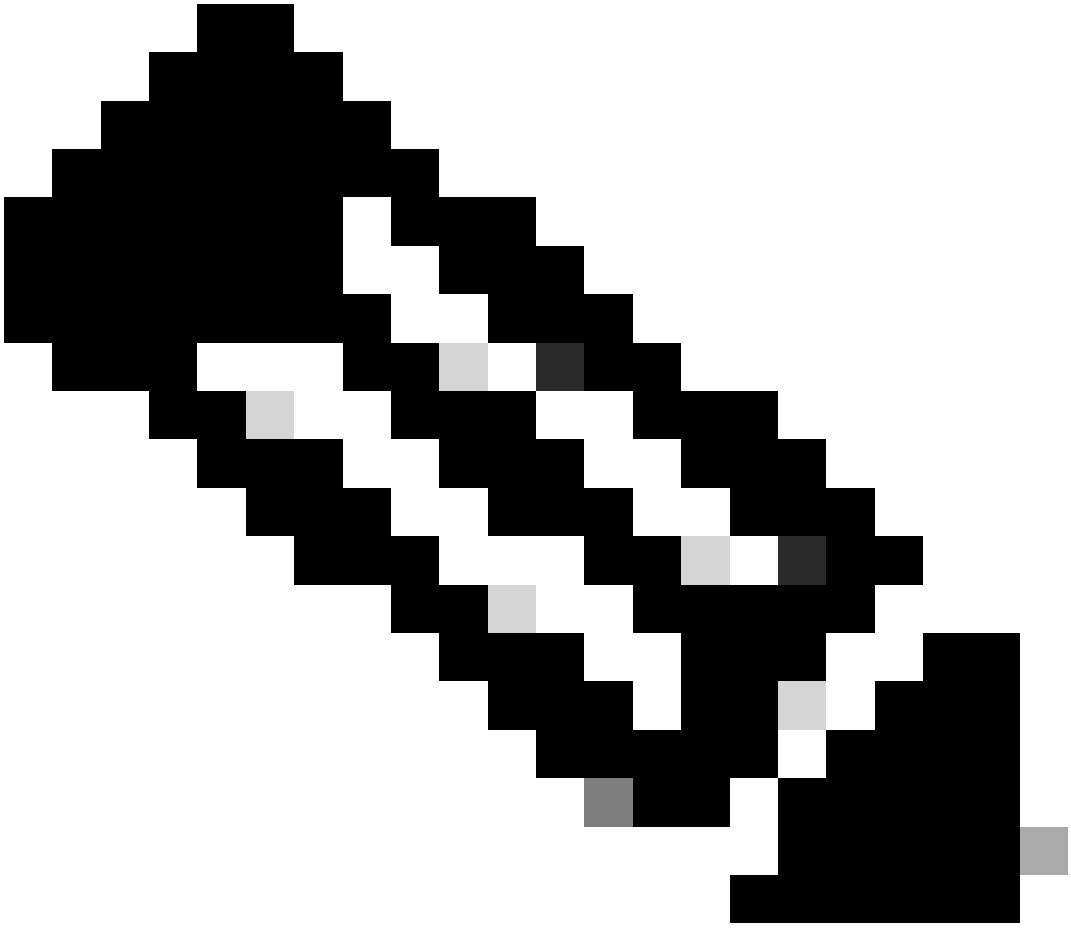
++策略名称在内部
++我们有两个L1目的地，每个L1设备对应一个



++策略名称外部

++我们有两个L1目的地，每个L1设备对应一个

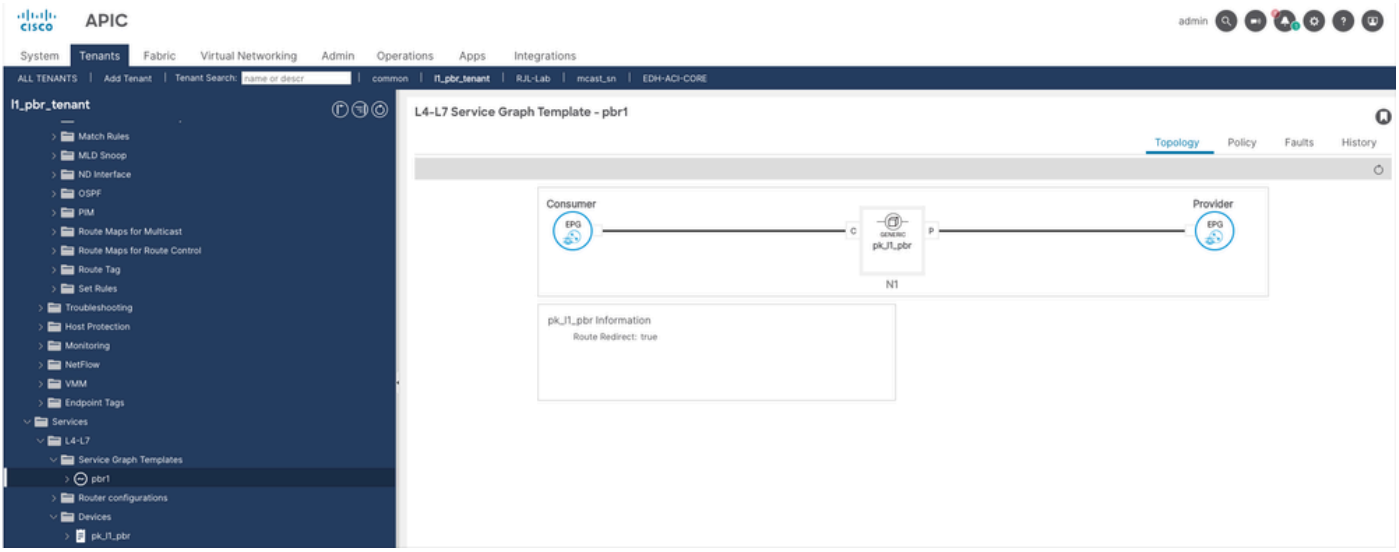




注意：两个L4-L7重定向策略的阈值关闭操作必须相同。

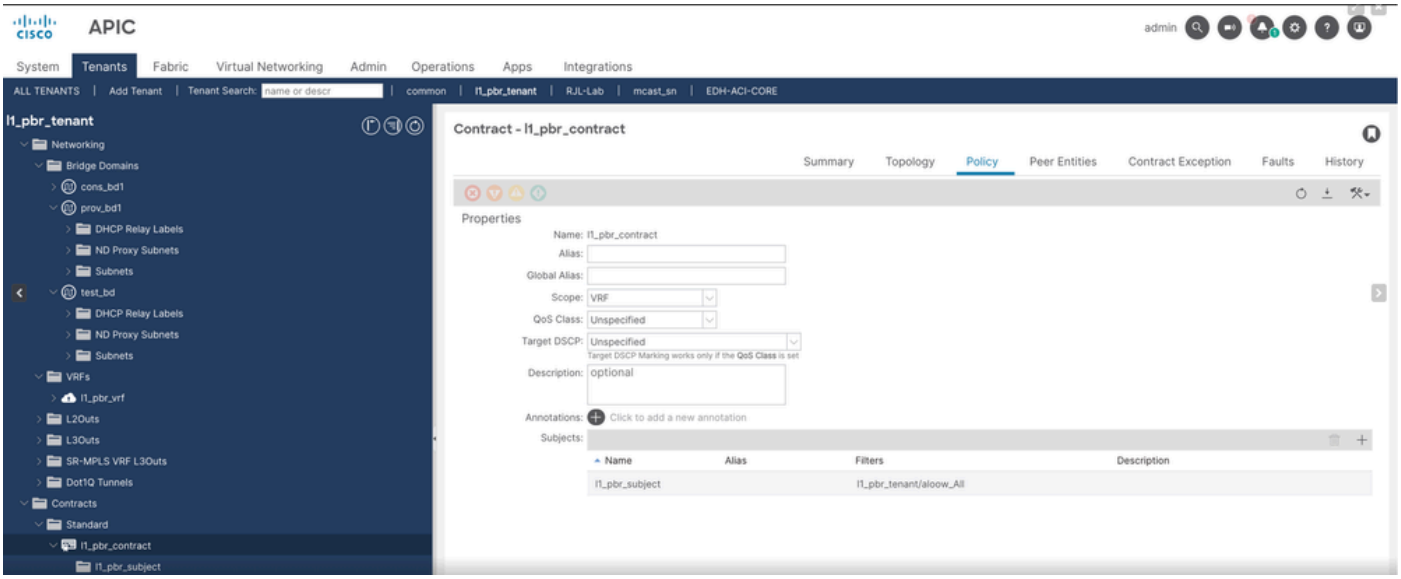
步骤6.配置Service graph模板。

导航到Tenant > Services > Service Graph Template，然后右键单击并创建L4-L7服务图模板。

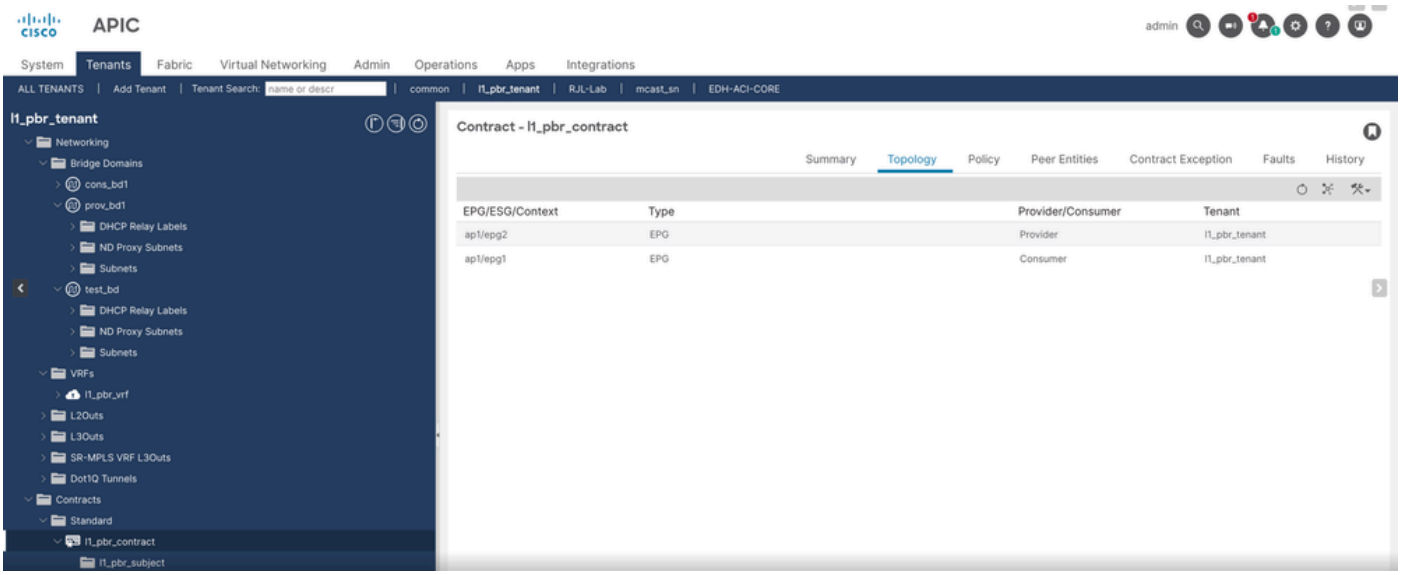


步骤7.创建合同。

导航到租户>合同>标准，然后右键单击并创建合同。

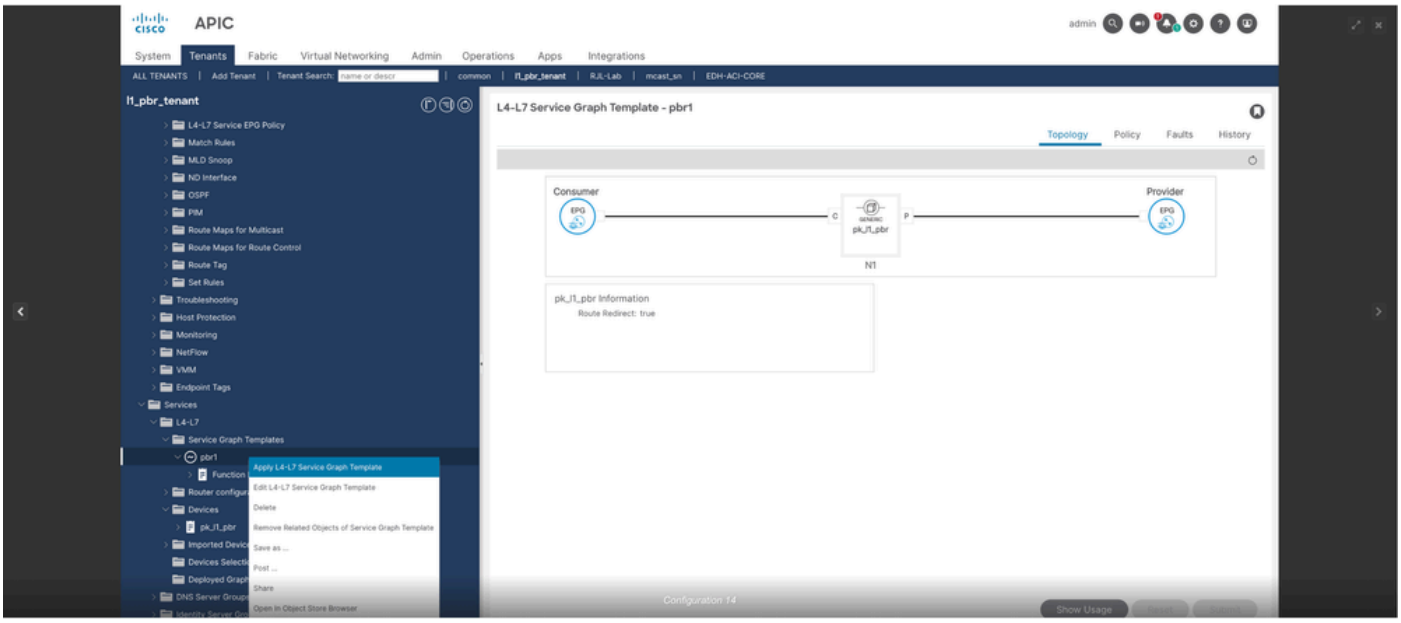


步骤8.将合同作为消费者和提供商分别应用于EPG1和EPG2。

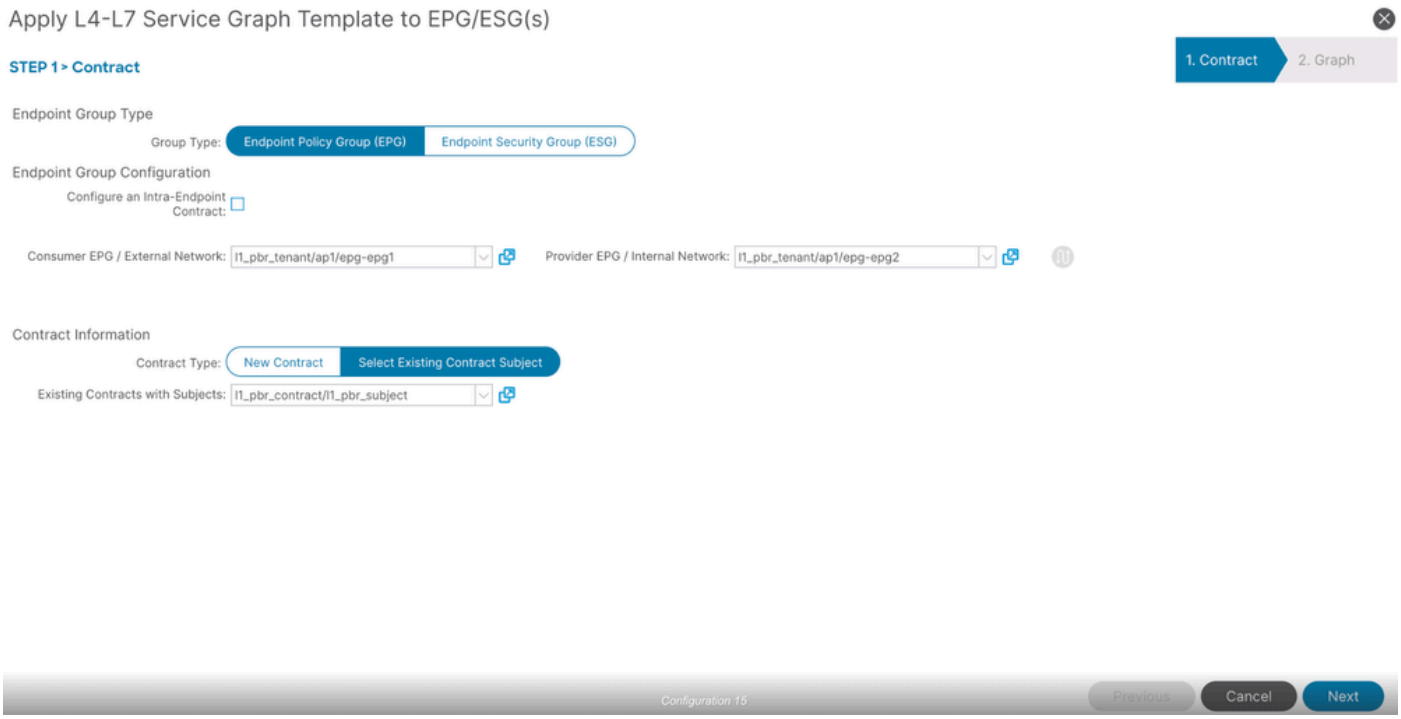


步骤9.应用L4-L7服务图模板。

导航到Tenant > Services > Service Graph Template，然后右键点击PBR1并应用L4-L7服务图模板。

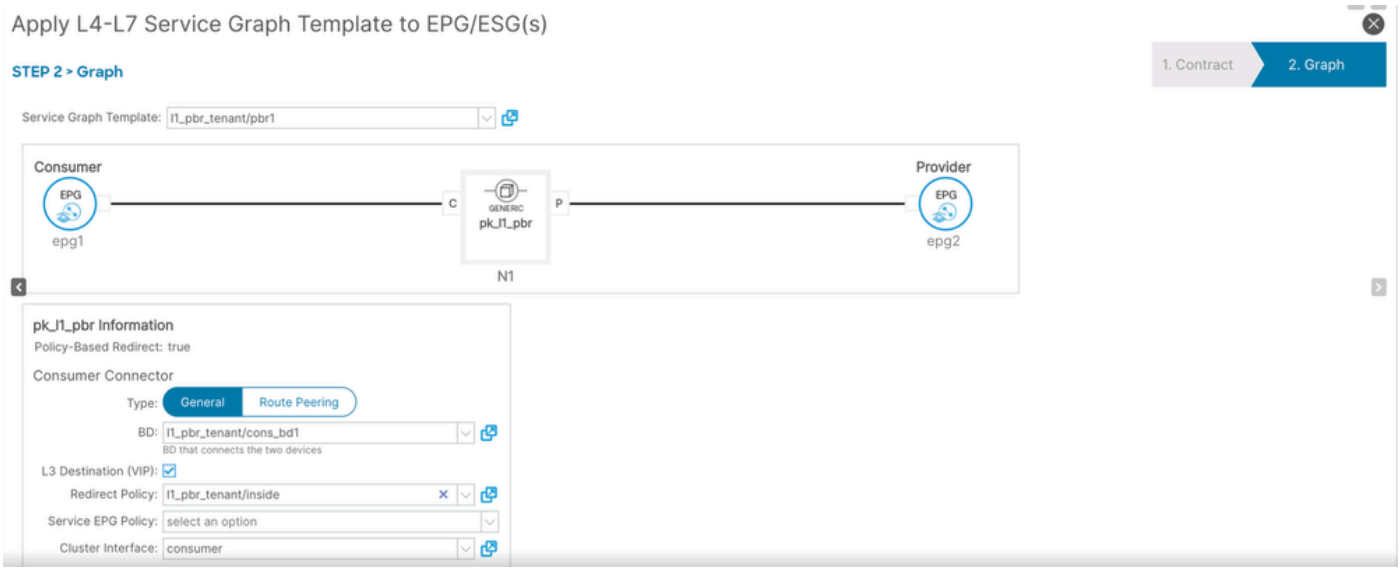


++添加消费者和提供商EPG
++指定合同

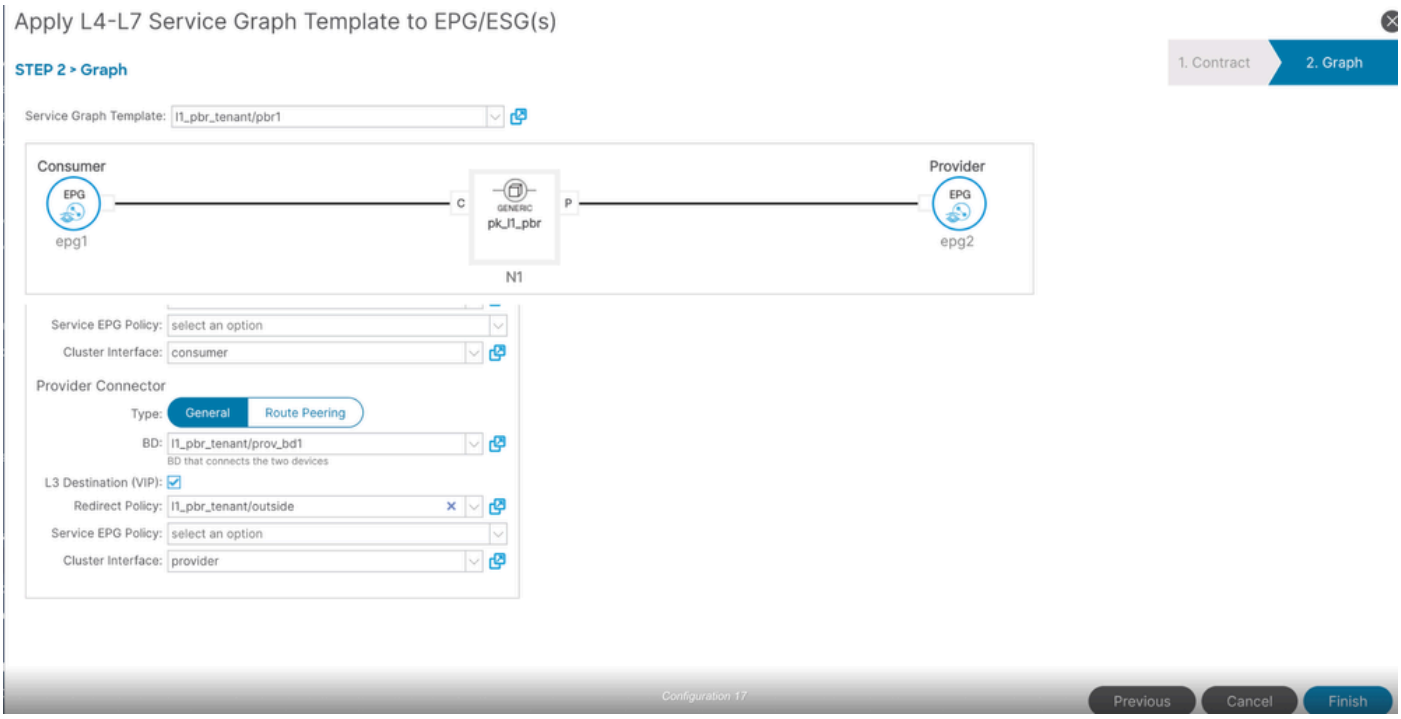


++击“下一步”

++指定使用者连接器详细信息



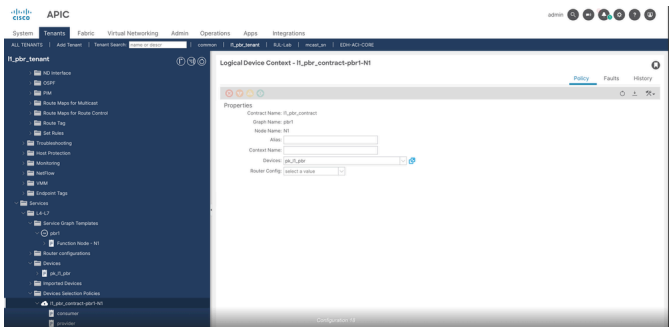
++指定提供程序连接器详细信息



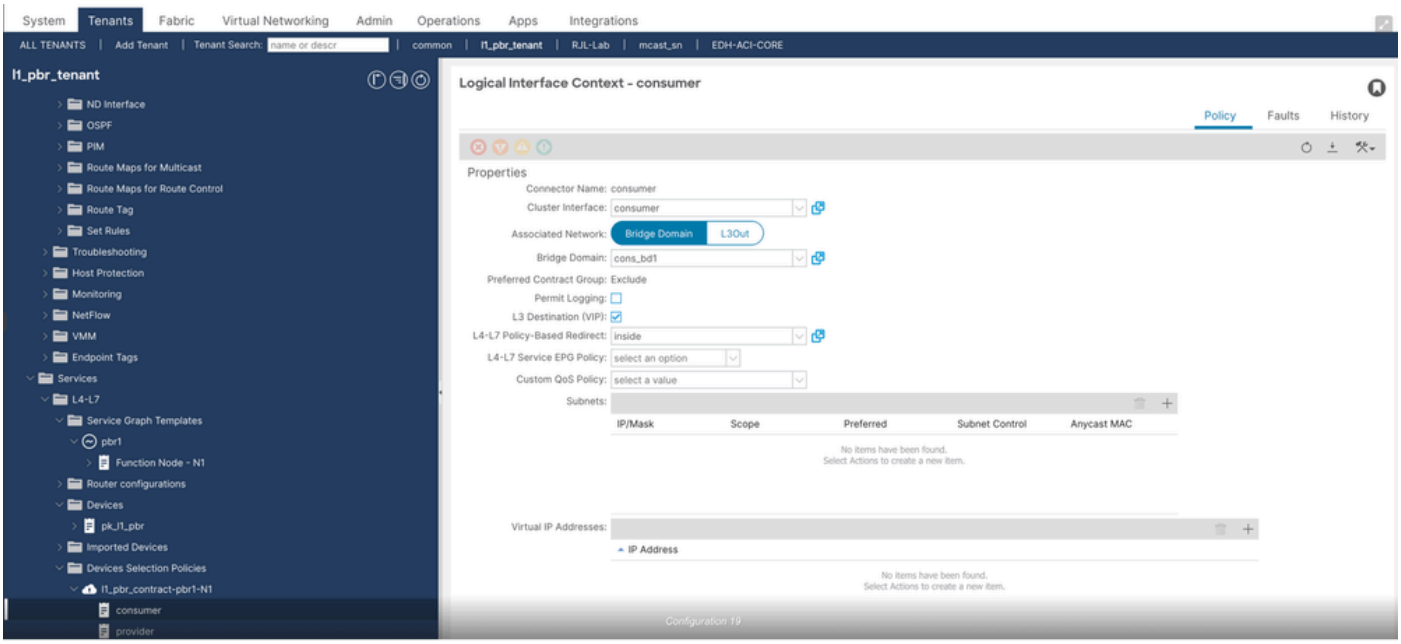
++单击“完成”

在APIC GUI上验证L1服务图

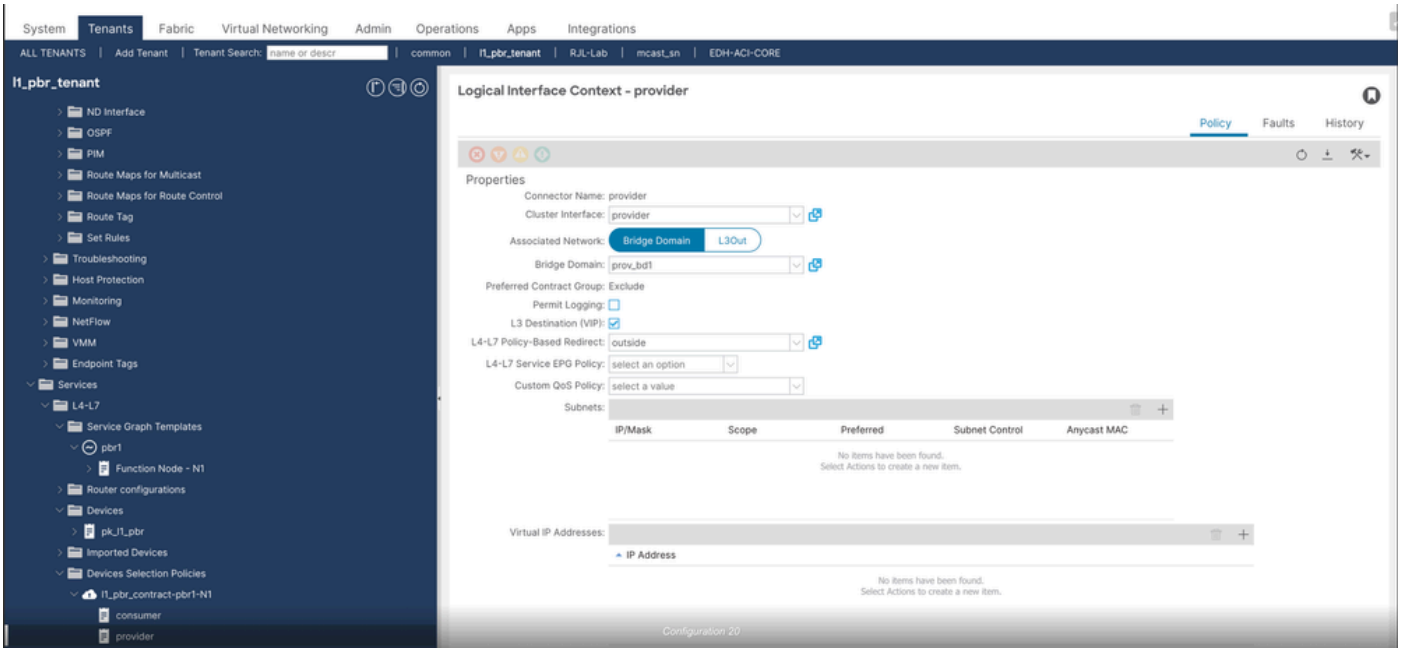
步骤1.验证应用服务图模板后创建的设备选择策略。



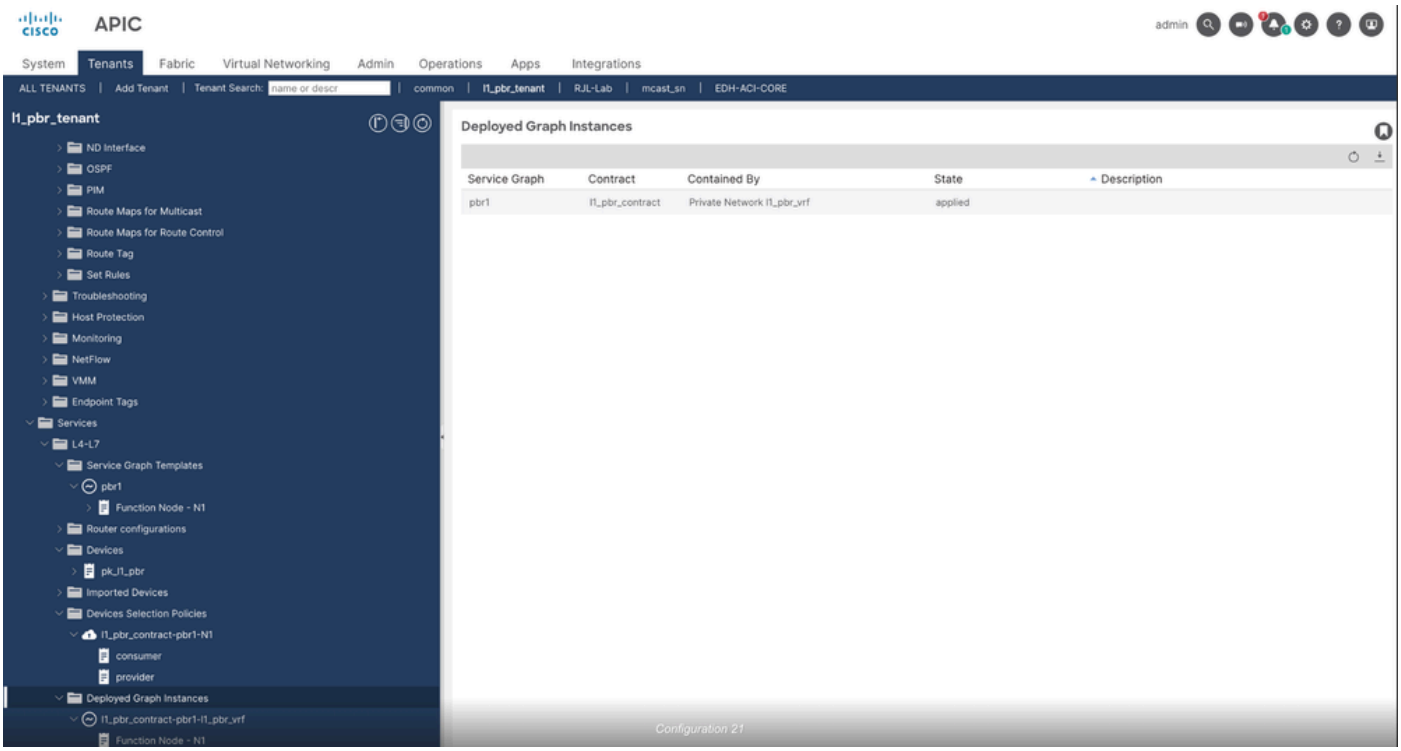
++验证消费者连接器



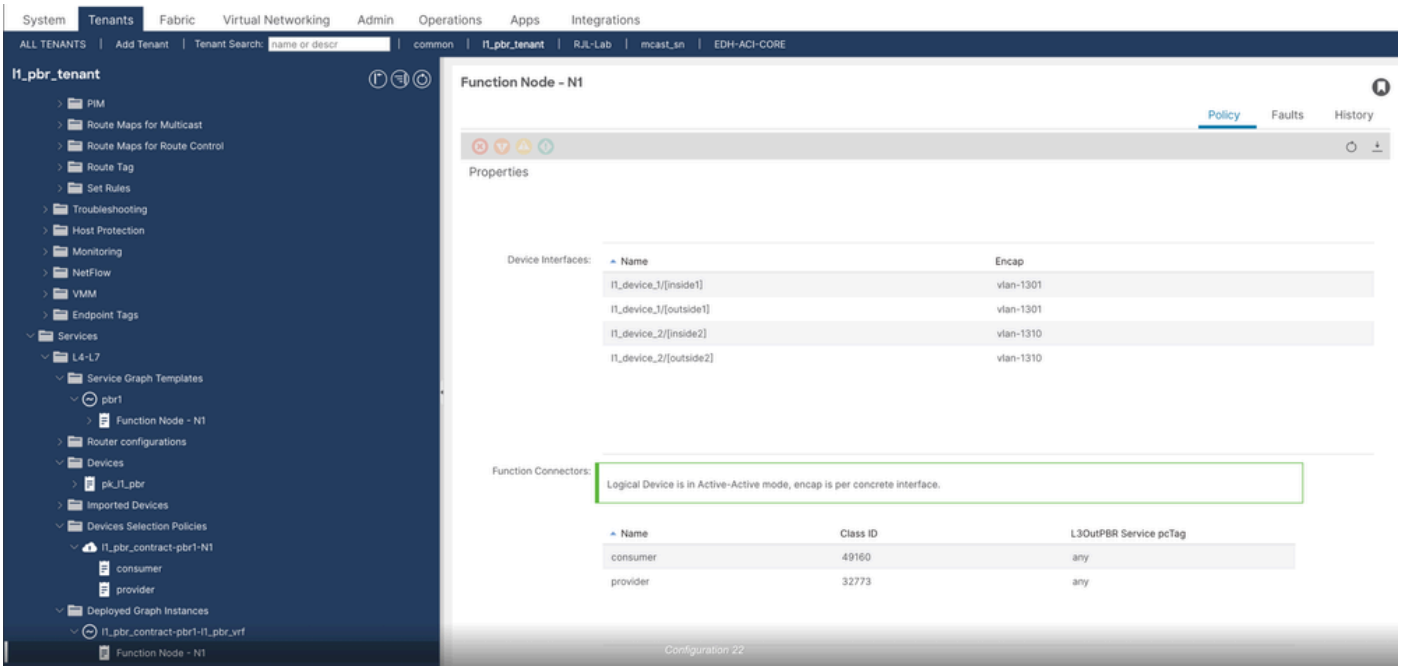
++配置提供商连接器



步骤2.验证部署的图形实例，您将在其中看到一个实例，该实例必须处于已应用状态。



++检查设备接口和功能连接器，您将在其中看到与服务EPG关联的PCTAG



在APIC CLI上验证L1服务图

步骤1.验证服务图是否与运行状况组状态一起应用于消费者和提供商节点。

<#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
```

步骤2.验证是否已在服务节点（102和103）上创建静态MAC绑定。

<#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
```

流量验证

1.正在从EP1到EP2生成2000 ICMP ping数据包，这些数据包将被重定向到L1设备。

```
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
```

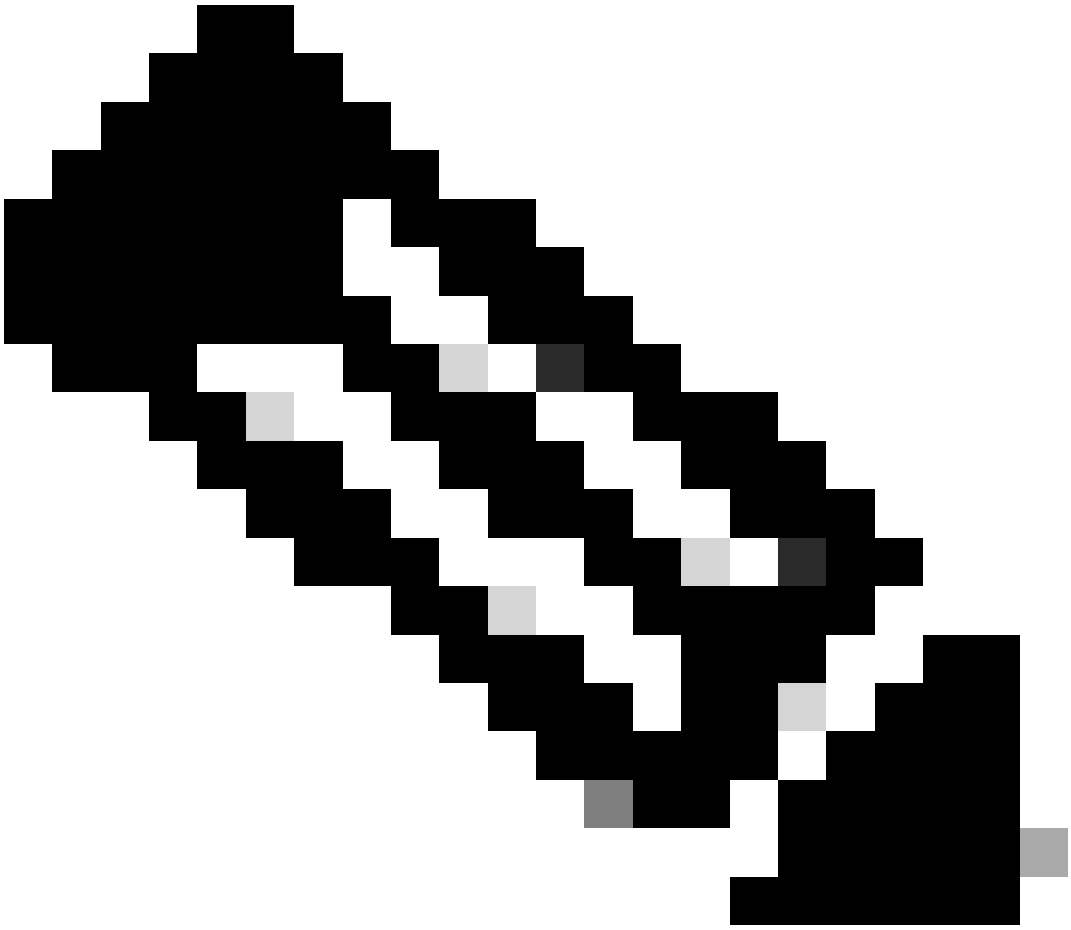
```
64 bytes from 192.168.132.200: icmp_seq=466 ttl=251 time=0.844 ms
64 bytes from 192.168.132.200: icmp_seq=467 ttl=251 time=0.821 ms
64 bytes from 192.168.132.200: icmp_seq=468 ttl=251 time=0.814 ms
64 bytes from 192.168.132.200: icmp_seq=469 ttl=251 time=0.846 ms
64 bytes from 192.168.132.200: icmp_seq=470 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.验证节点102和103上连接到L1设备的接口计数器。

```
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
```



注意：在测试流量之前，已清除节点102和103上的接口计数器。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。