ACIでのアクティブ/アクティブL1 PBRの設定と確認

内容

はじめに

このドキュメントでは、アプリケーションセントリックインフラストラクチャ(ACI)でアクティブ/アクティブL1サービスグラフを設定および確認する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ACIでのレイヤ3サービスグラフの動作の仕組みについて
- ACIでのエンドポイントポリシーグループ、ブリッジドメイン、およびコントラクトの設定方法に関する理解

使用するコンポーネント

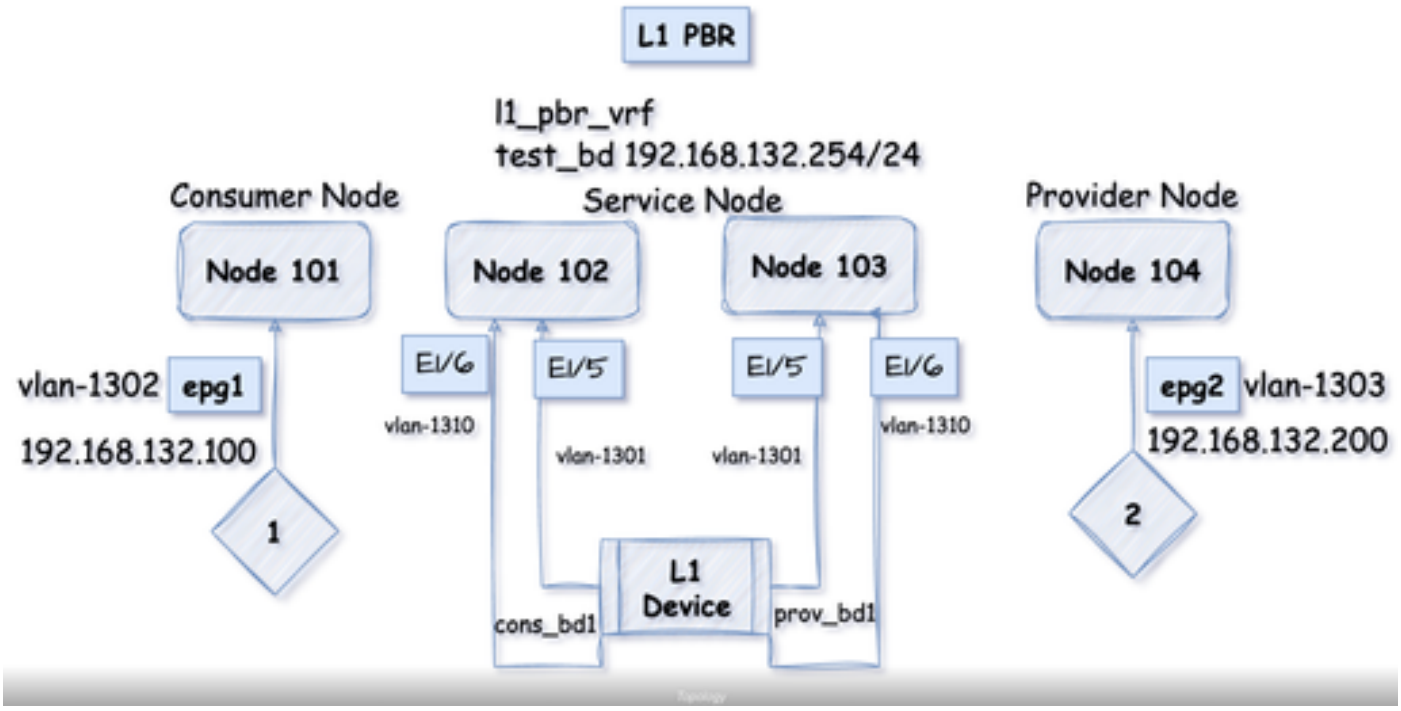
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- APICバージョン：5.3(2a)
- リーフH/W:N9K-C93180YC-FX、N9K-C93180YC-EX
- リーフS/W:n9000-15.3(2a)
- リーフノード101、102、103、104

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

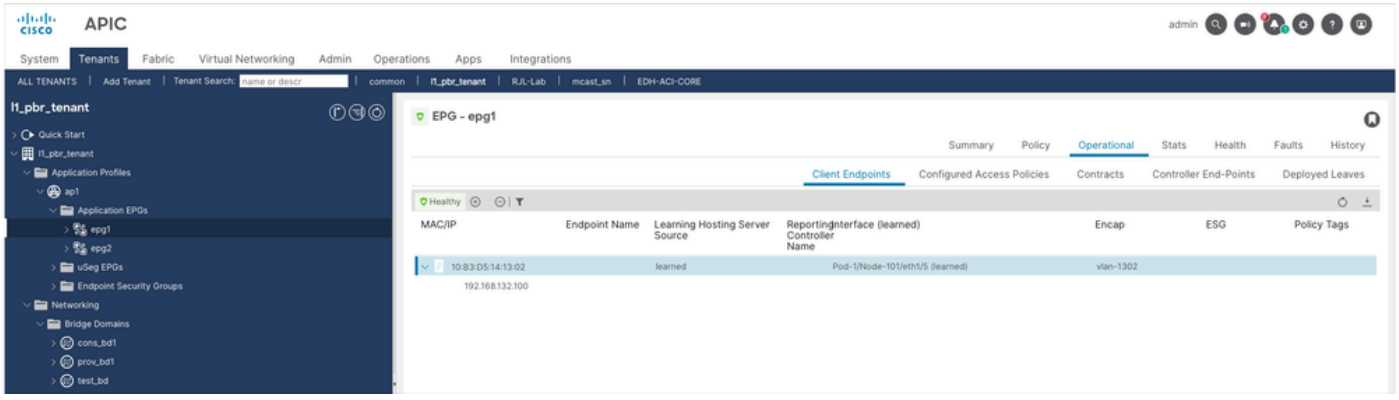
キュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください

トポロジ

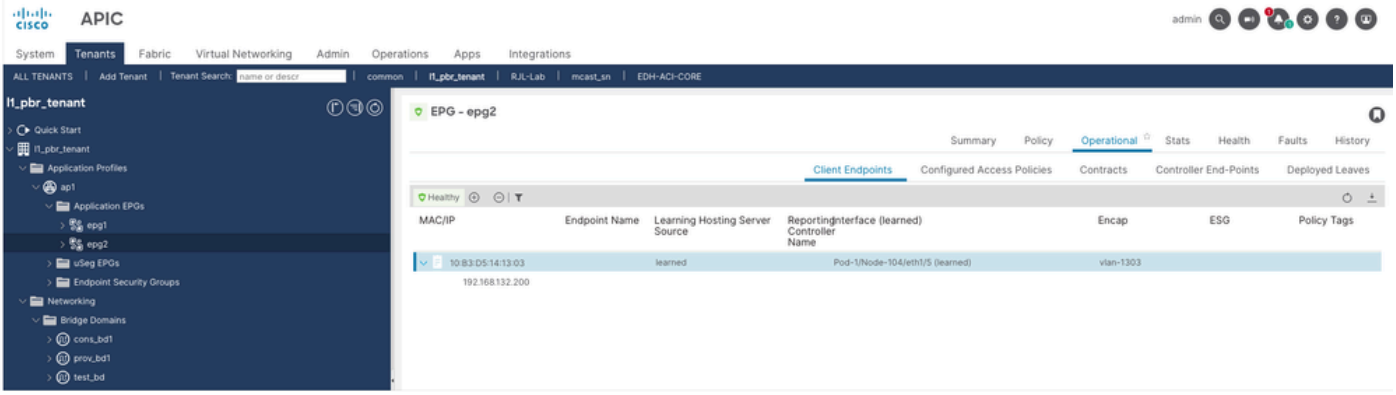


EPG1とEPG2の設定はこのドキュメントに示されていません。手およびエンドポイントを学習する前に設定する必要があります。

1. EPG1 haṣエンドポイント192.168.132.100 learned（ノード101）を検証します。



2. EPG2にエンドポイント192.168.132.200が学習されたことを検証します（ノード104）。



ACIでL1サービスグラフが必要な理由

Cisco ACIでは、L4-L7サービスデバイスをL3/L2/L1として挿入できます。レイヤ3は外部デバイスがトラフィックを転送するルーティング決定を実行できることを意味し、レイヤ2はトラフィックがMACアドレスに基づいてのみ転送されることを意味します。ACIでは、侵入防御システム(IPS)/トランスペアレントファイアウォールなどのL2デバイスを挿入できます。ここで、トラフィックをリダイレクトしようとしているデバイスが転送に関する決定を行うことができないというシナリオを考えます。このような場合は、L1ポリシーベースルーティング(PBR)を導入できます。

トラフィック転送は、L3とL2 PBRの場合で同じです。唯一の違いは、L3 PBRトラフィックがIPアドレスにリダイレクトされる場合と、L1/L2 PBRトラフィックがMACアドレスにリダイレクトされる場合です。これらのMACアドレスは、転送用にリーフインターフェイスに静的にバインドされます。この件に関する詳細は、今後も引き続き表示されます。

アクティブ/スタンバイまたはアクティブ/アクティブL1/L2 PBRの使用例の詳細については、『PBRホワイトペーパー』を参照してください。

L1デバイスについて

この導入モデルでは、サービスデバイスでVLAN変換が実行されず、両方のインターフェイスが同じVLANで動作します。この方法は、一般にインラインモードまたはワイヤモードと呼ばれ、ファイアウォールおよび侵入防御システム(IPS)で一般的に使用されます。 サービスデバイスがレイヤ2またはレイヤ3フォワーディングに参加せずにセキュリティ機能を実行することが期待される場合に最適です。

アクティブ/アクティブL1 PBR

ACIリリース5.0以降では、アクティブ/アクティブモードのL4-L7デバイスを使用したサービスグラフの導入がサポートされています。これは、各L4-L7デバイスインターフェイス（具象インターフェイス）に固有のencapを割り当て、隠しサービスEPGで「Flood in encap」のACIの自動設定を活用することで実現されます。この隠しサービスEPGは、L4-L7デバイスインターフェイスをサービスブリッジドメインに関連付けるためにACIによって作成されます。

サービスグラフのレンダリングプロセス中にACIが自動的に「Flood in encap」を有効にするので

、管理者は非表示のサービスEPGを手動で設定する必要はありません。

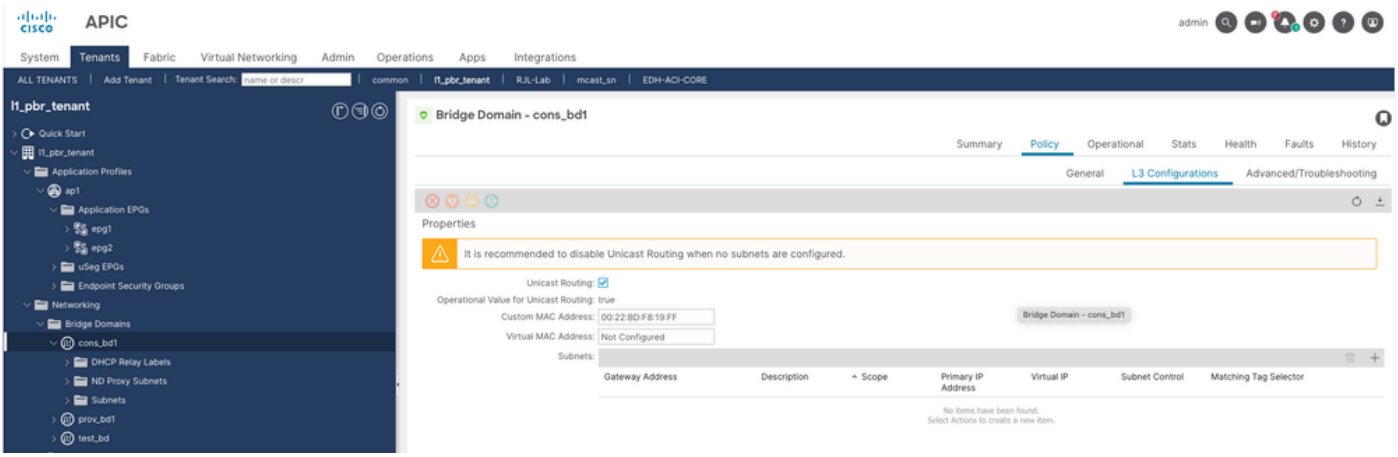
L1 PBRのアクティブ – アクティブ展開では、ポートローカルスコープを設定する必要があります。このためには、L4-L7デバイスのコンシューマクラスタインターフェイス（コネクタ）とプロバイダークラスタインターフェイス（コネクタ）を、それぞれ独自のVLANプールを持つ別々の物理ドメインに配置し、両方のドメインで同じVLAN範囲を維持する必要があります。

参考：PBRホワイトペーパー。

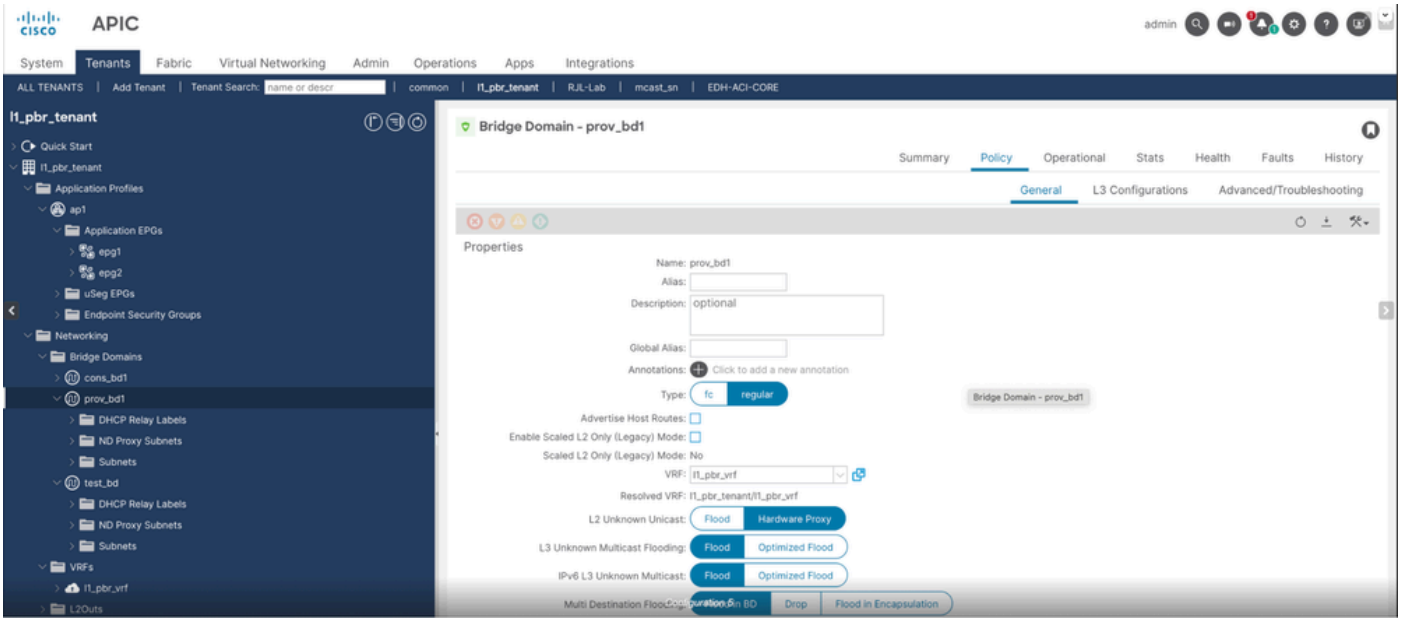
L1サービスグラフの設定

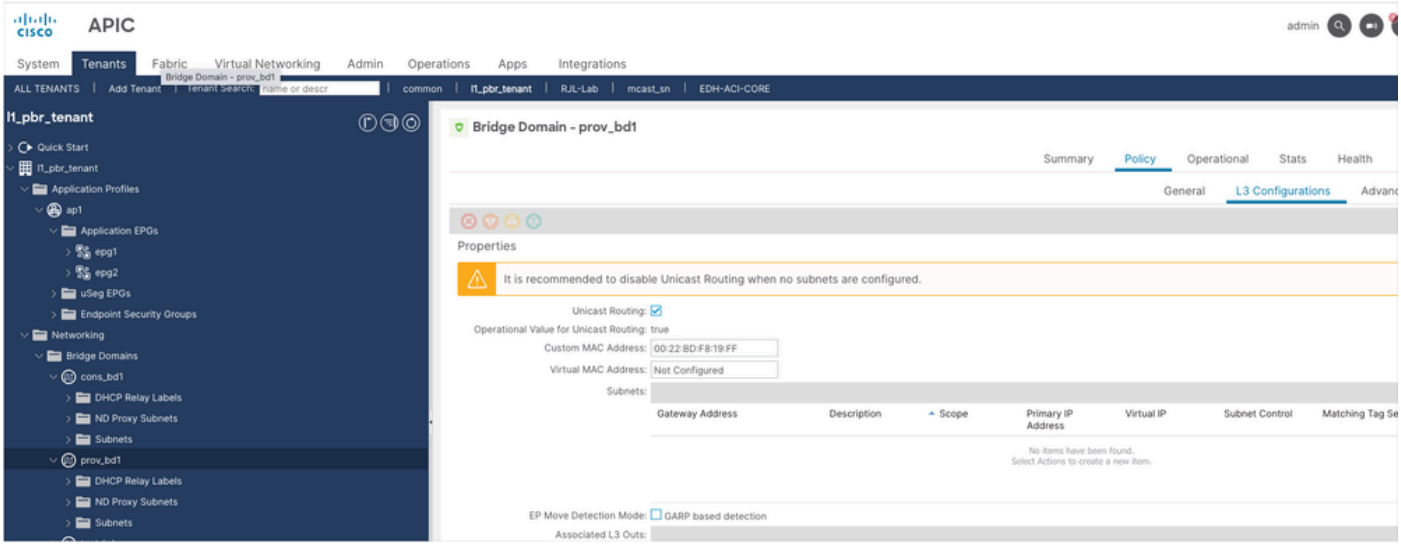
ユニキャストルーティングを有効にし、L2不明なユニキャストをハードウェアプロキシに設定する必要があります。consおよびprovブリッジドメインにはサブネットは必要ありません。

ステップ 1： consumer bridge(CONS)ドメインをcons_bd1という名前で設定します。



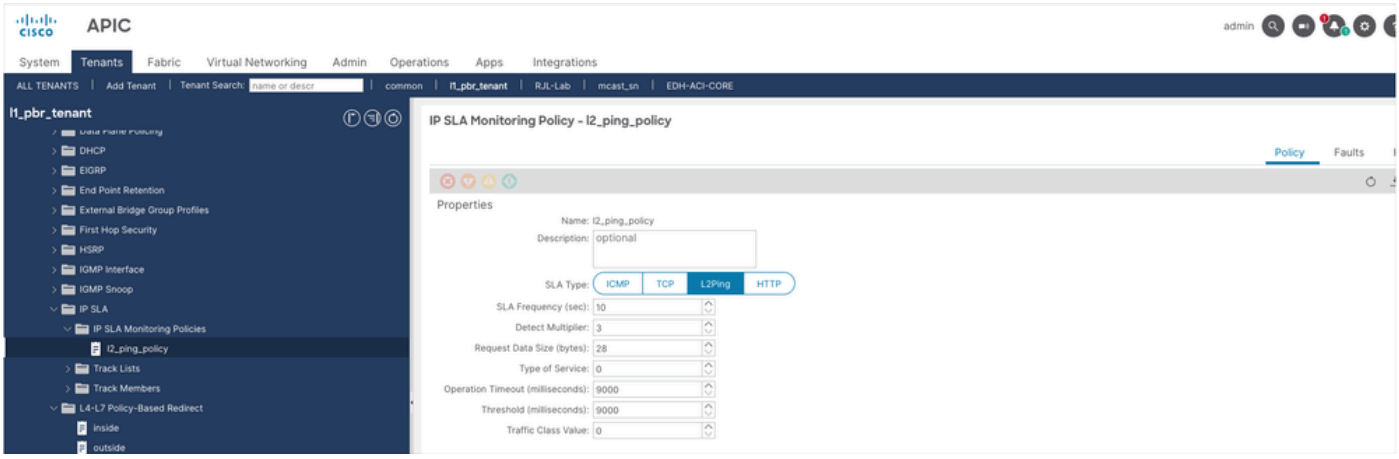
ステップ 2： prov-bd1という名前のプロバイダーブリッジドメインを設定します。





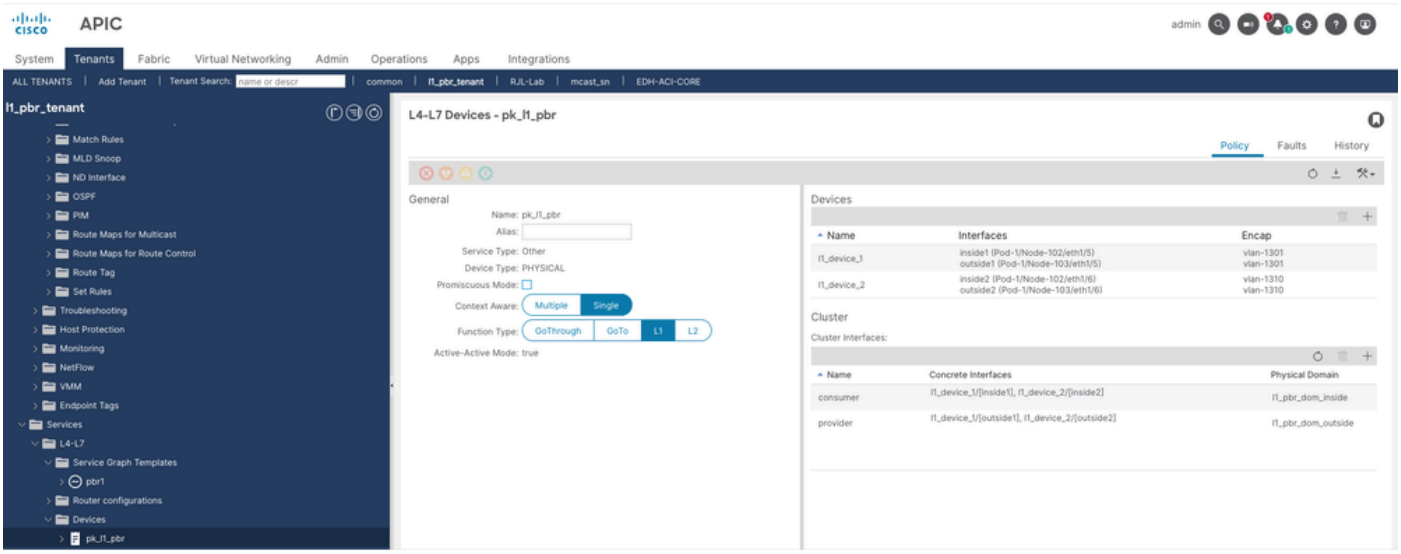
ステップ 3： SLAタイプL2PingでIPサービスレベル契約(SLA)ポリシーを設定します。

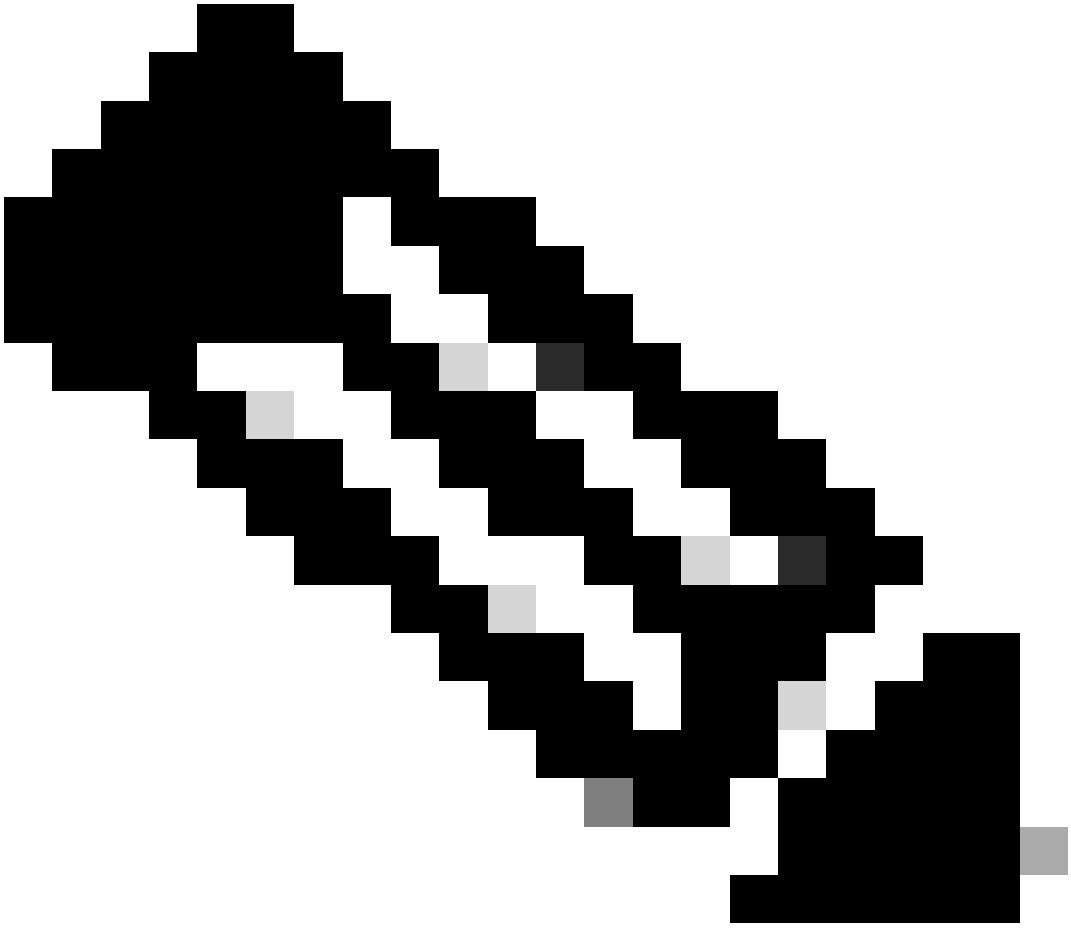
テナント>ポリシー>プロトコル> IP SLA > IP SLAモニタリングポリシーに移動し、右クリックしてポリシーを作成します。



ステップ 4： L4/L7デバイスを設定します。

テナント>サービス>デバイスに移動し、右クリックしてL4-L7デバイスを作成します。



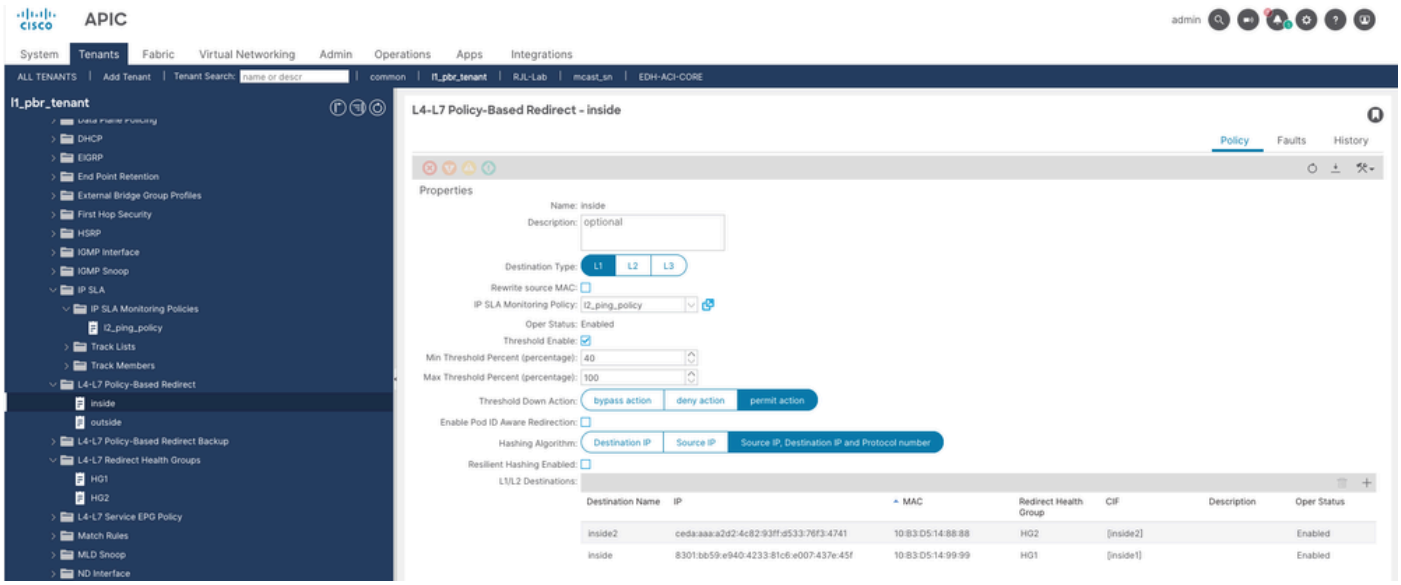


注:L1デバイスの場合、各クラスタインターフェイスは、ポートローカルスコープのために異なる物理ドメインに存在する必要があります。

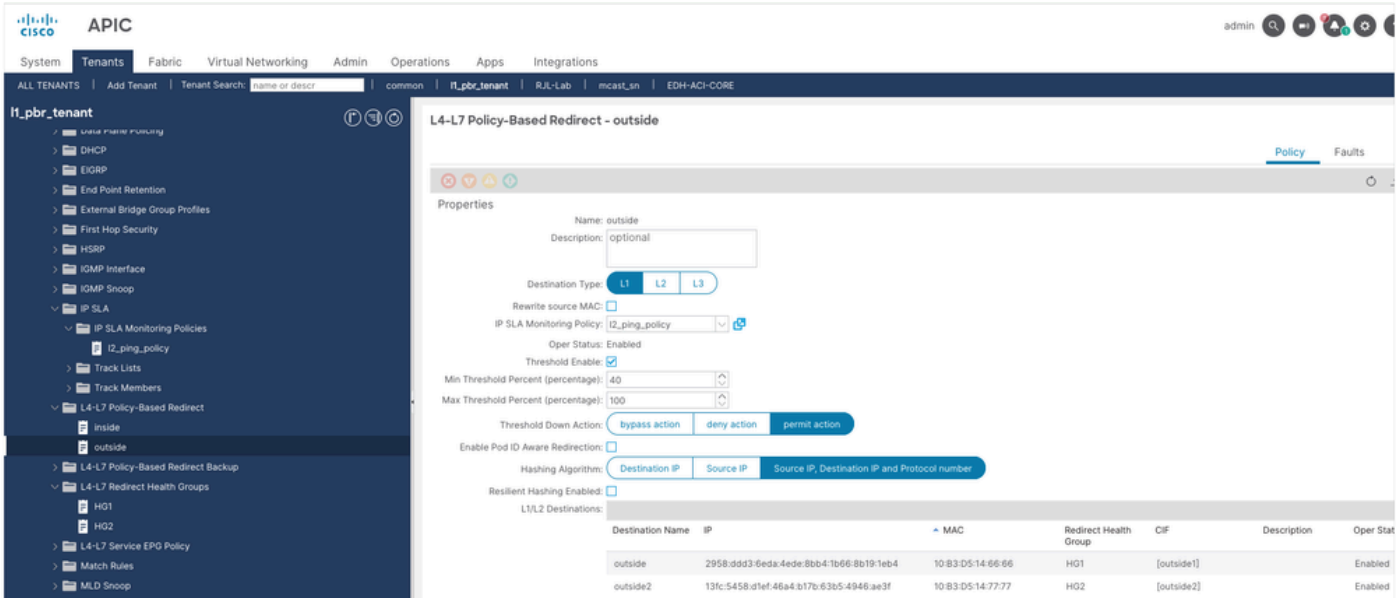
ステップ 5： InsideおよびOutsideインターフェイスに対してL4-L7ポリシーベースのリダイレクトを設定します。

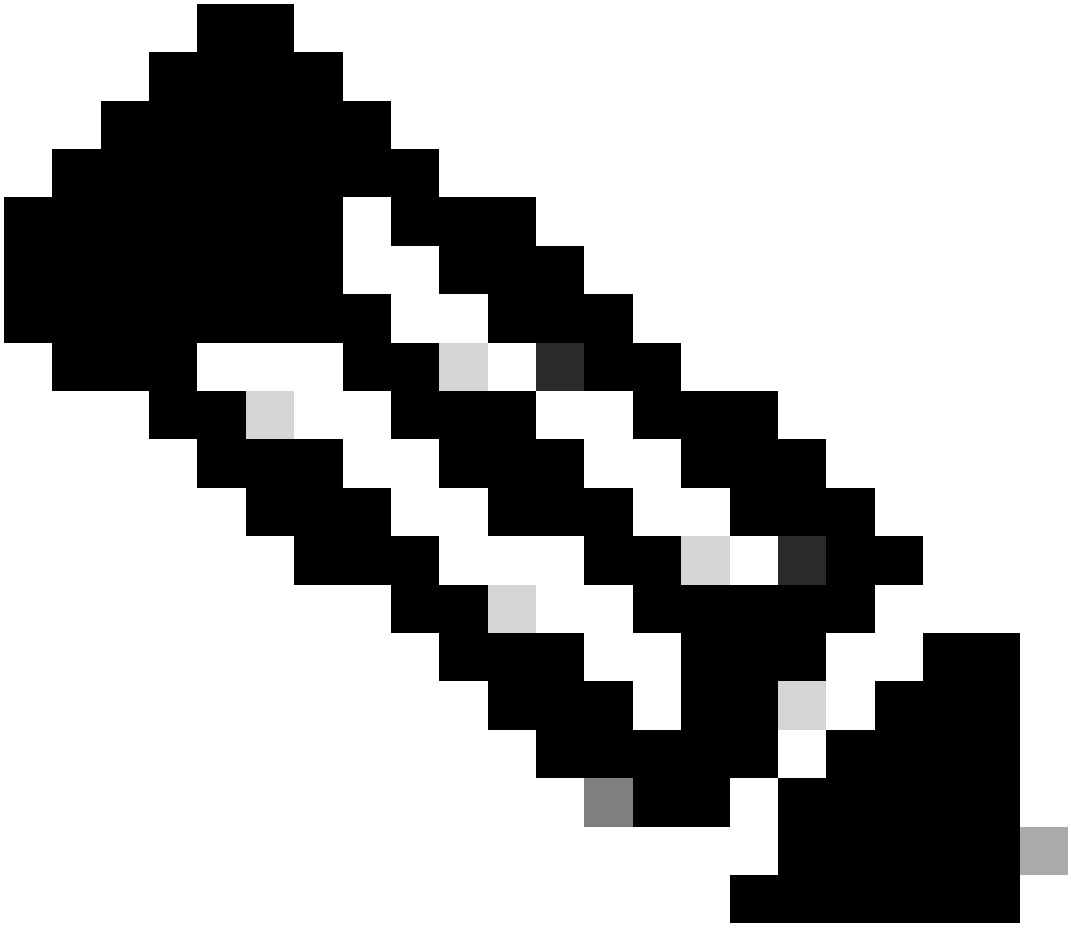
テナント>ポリシー>プロトコル> L4-L7ポリシーベースのリダイレクトに移動し、右クリックしてポリシーを作成します。

++ポリシー名は内部です
++各L1デバイスに1つずつ、合計2つのL1宛先があります



++ポリシー名は外部です
++各L1デバイスに1つずつ、合計2つのL1宛先があります

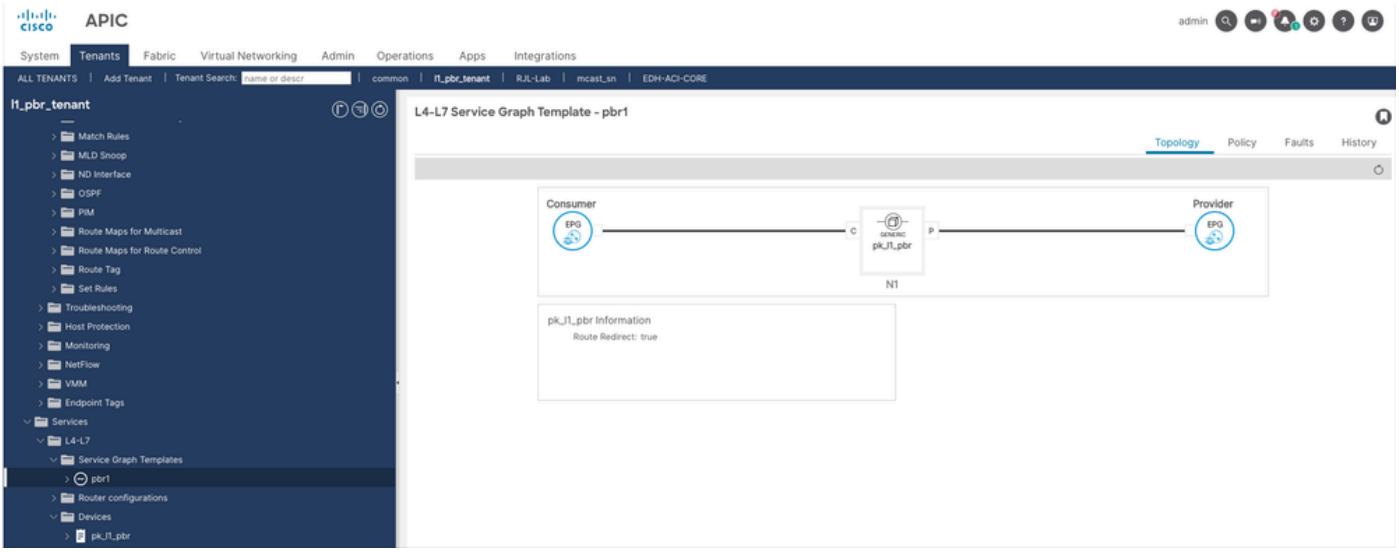




注：しきい値ダウンアクションは、両方のL4-L7リダイレクトポリシーで同じである必要があります。

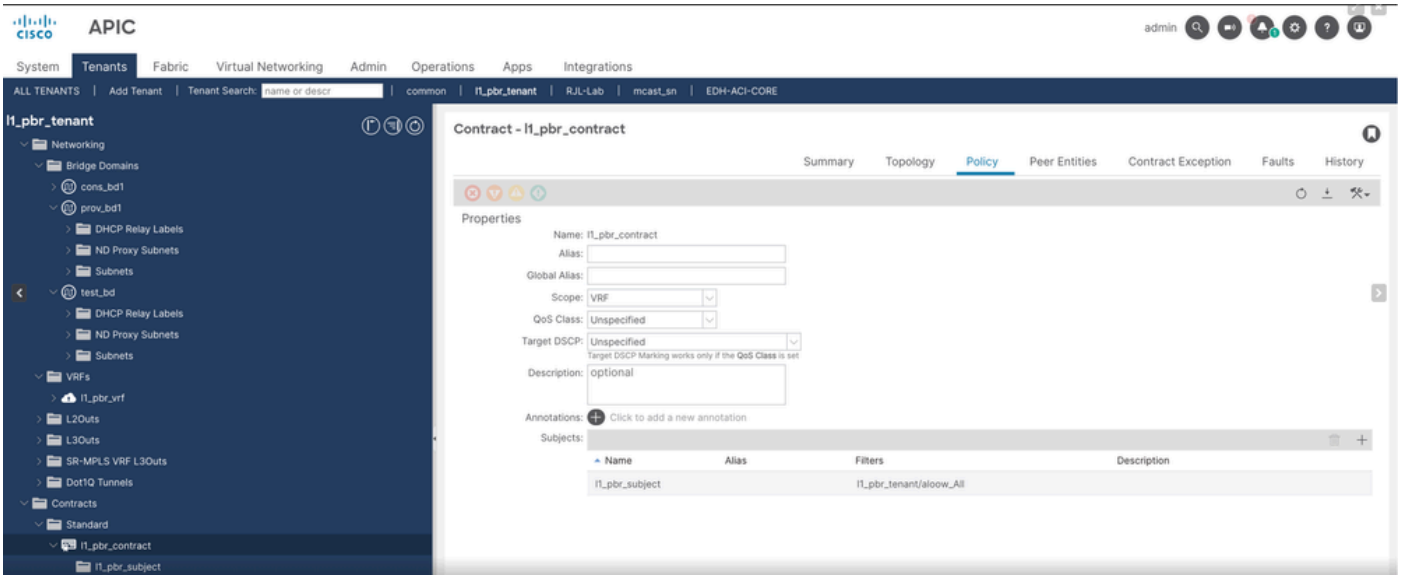
手順 6：サービスグラフテンプレートを設定します。

テナント>サービス>サービスグラフテンプレートに移動し、右クリックしてL4-L7サービスグラフテンプレートを作成します。

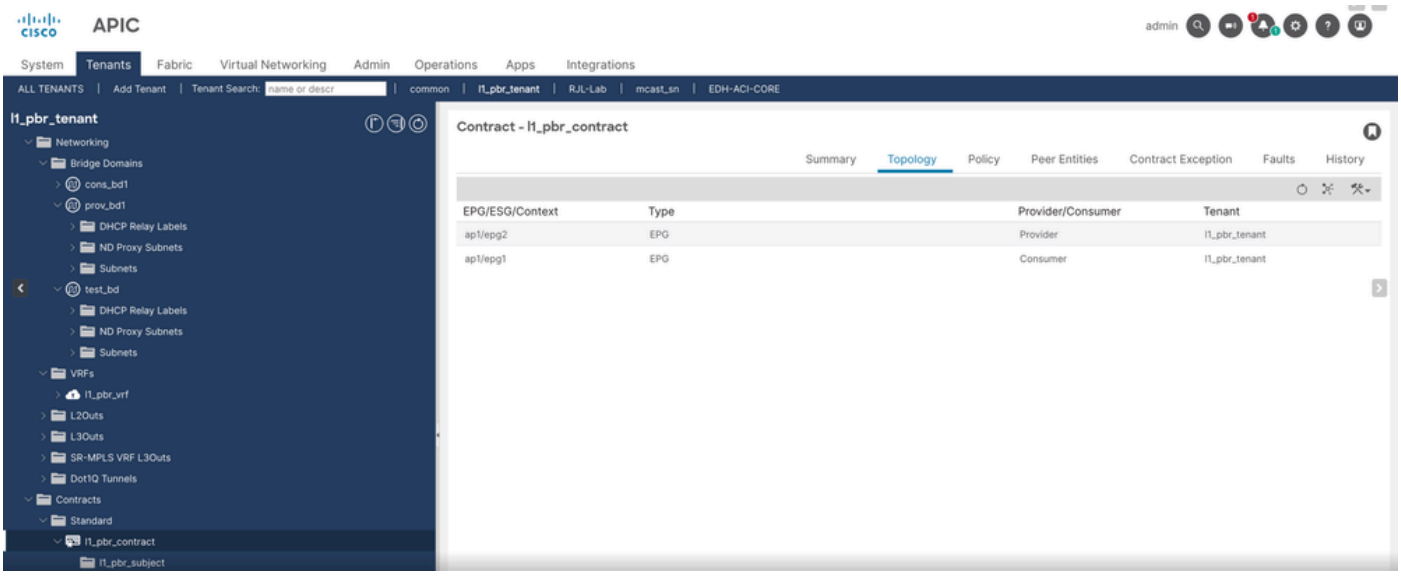


手順 7：コントラクトを作成します。

テナント>契約> Standardに移動し、右クリックして契約を作成します。

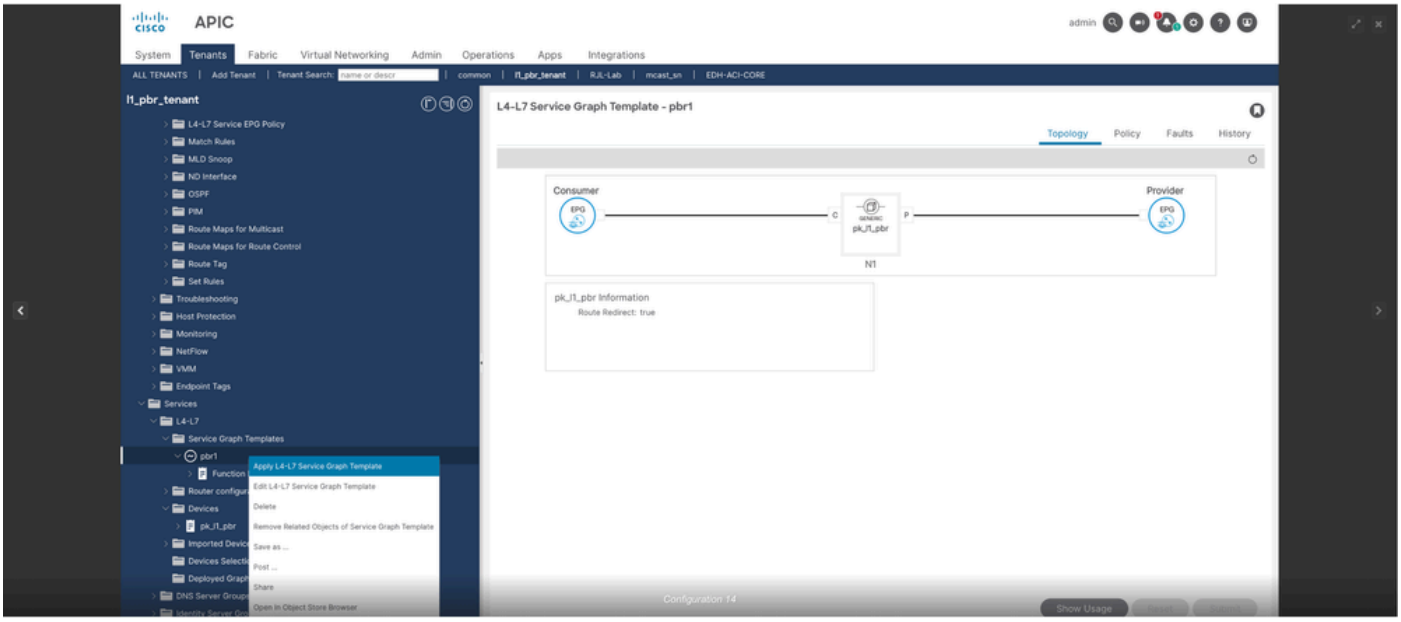


ステップ 8：コントラクトをコンシューマおよびプロバイダーとしてEPG1およびEPG2にそれぞれ適用します。

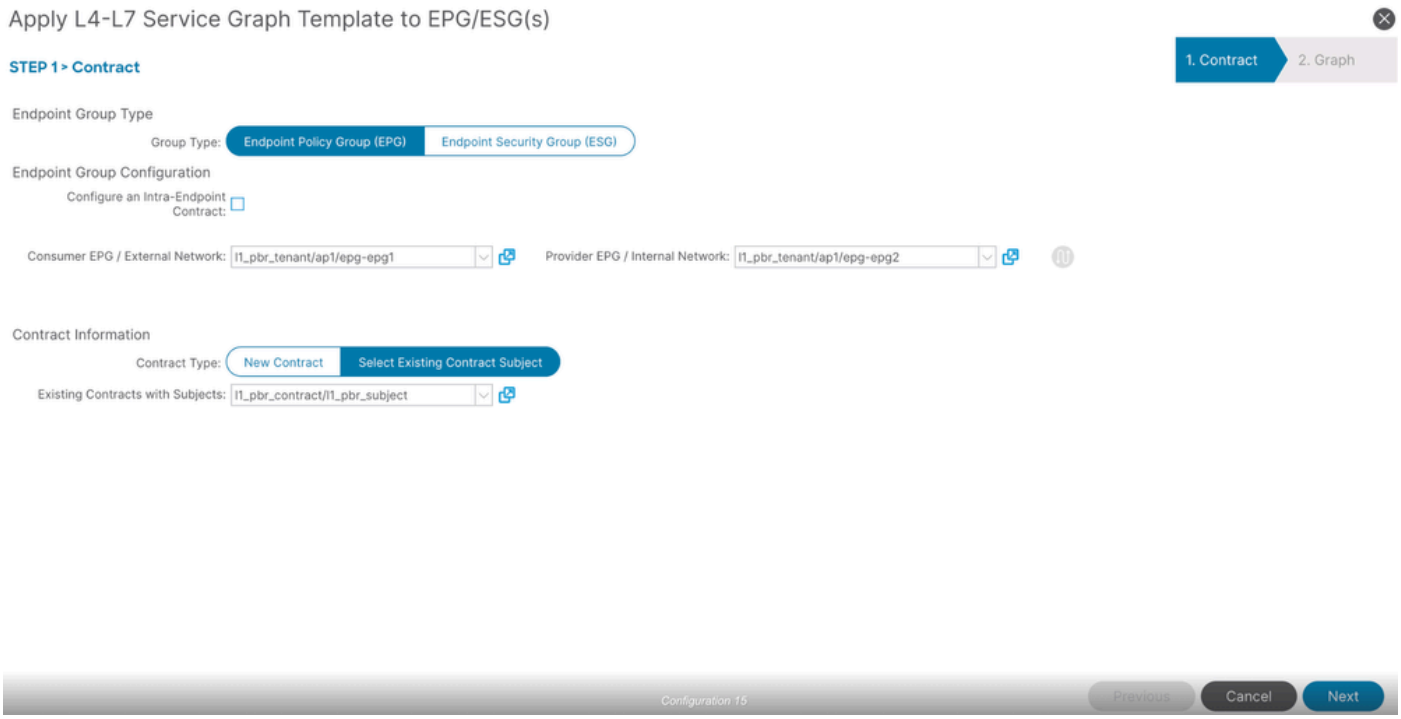


ステップ 9：L4-L7サービスグラフテンプレートを適用します。

Tenant > Services > Service Graph Templateの順に移動し、PBR1を右クリックしてL4-L7サービスグラフテンプレートを適用します。

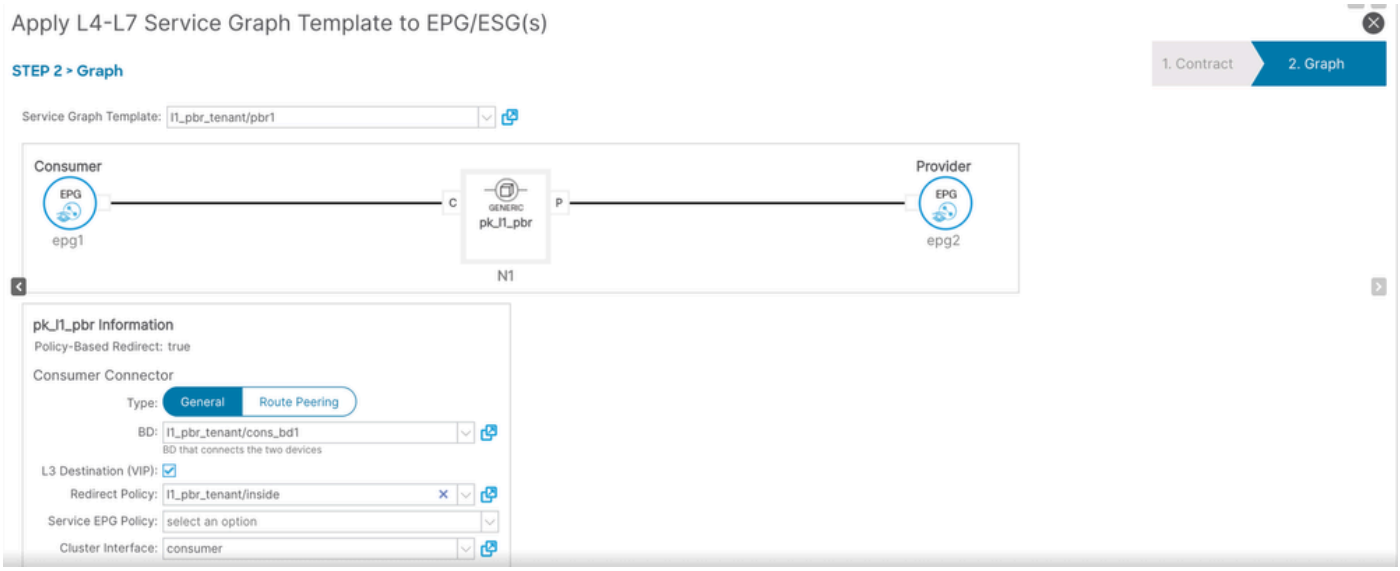


++コンシューマおよびプロバイダーEPGの追加
++契約の指定

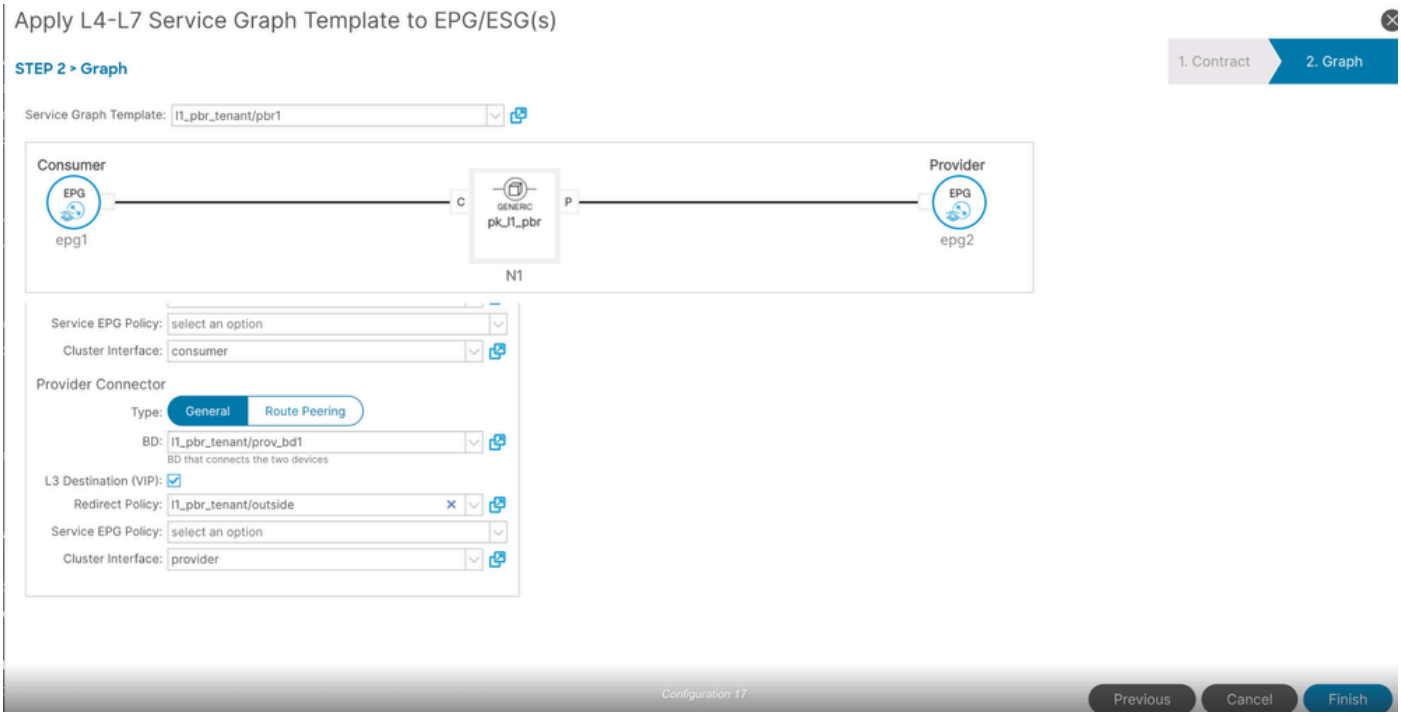


++ Nextをクリックします。

++コンシューマコネクタの詳細の指定



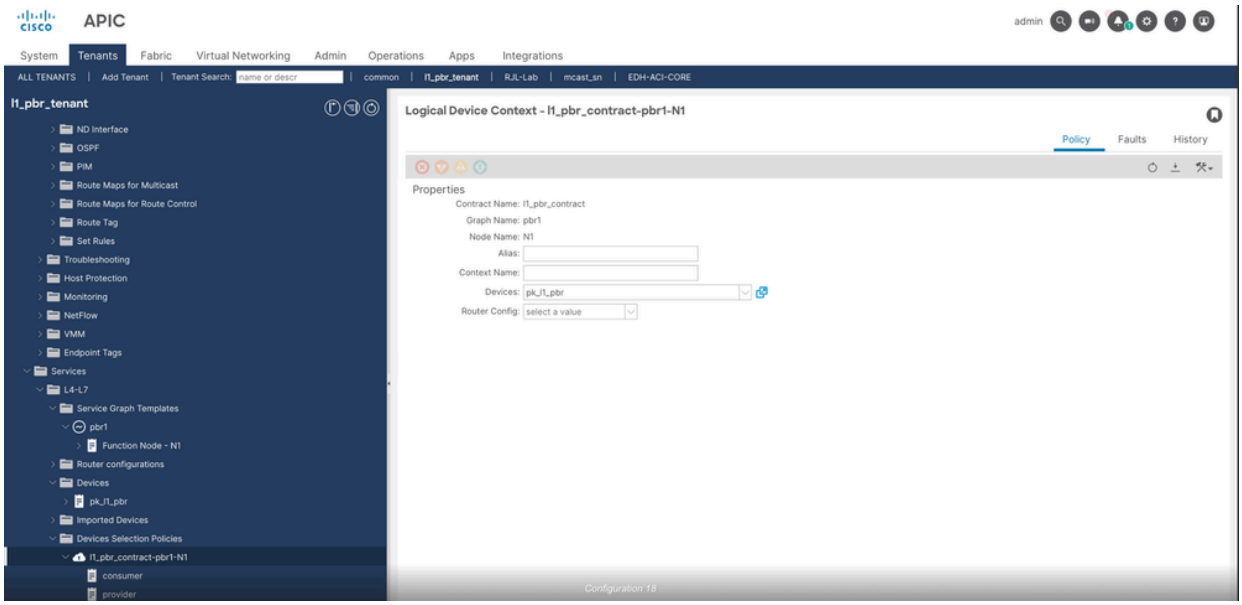
++プロバイダーコネクタの詳細の指定



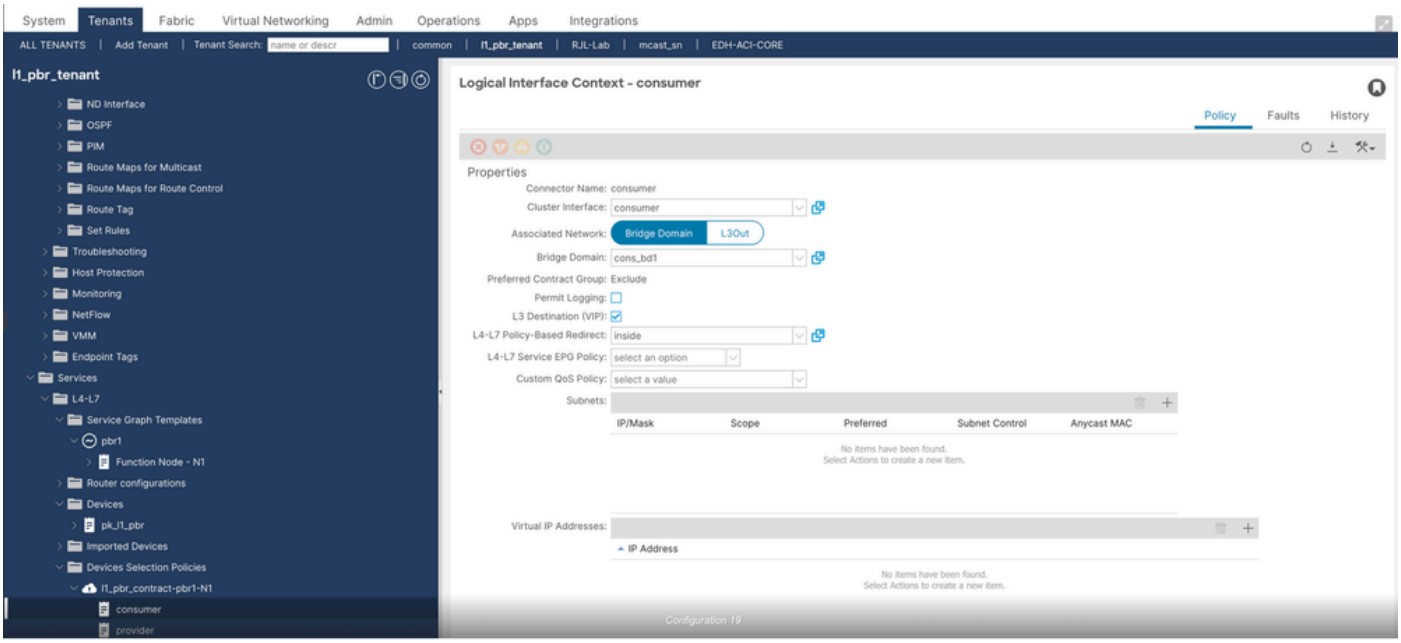
++ [完了]をクリックします。

APIC GUIでのL1サービスグラフの検証

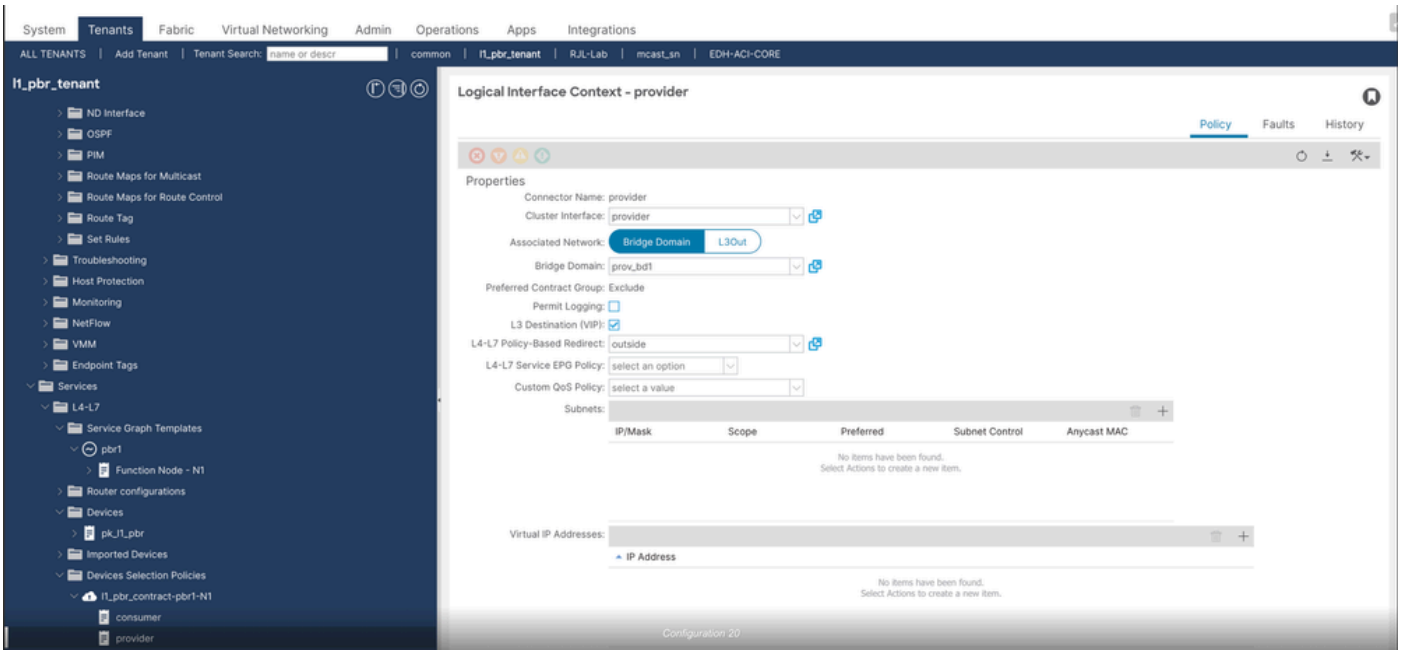
ステップ 1：サービスグラフテンプレートを適用した後に作成されたデバイス選択ポリシーを確認します。



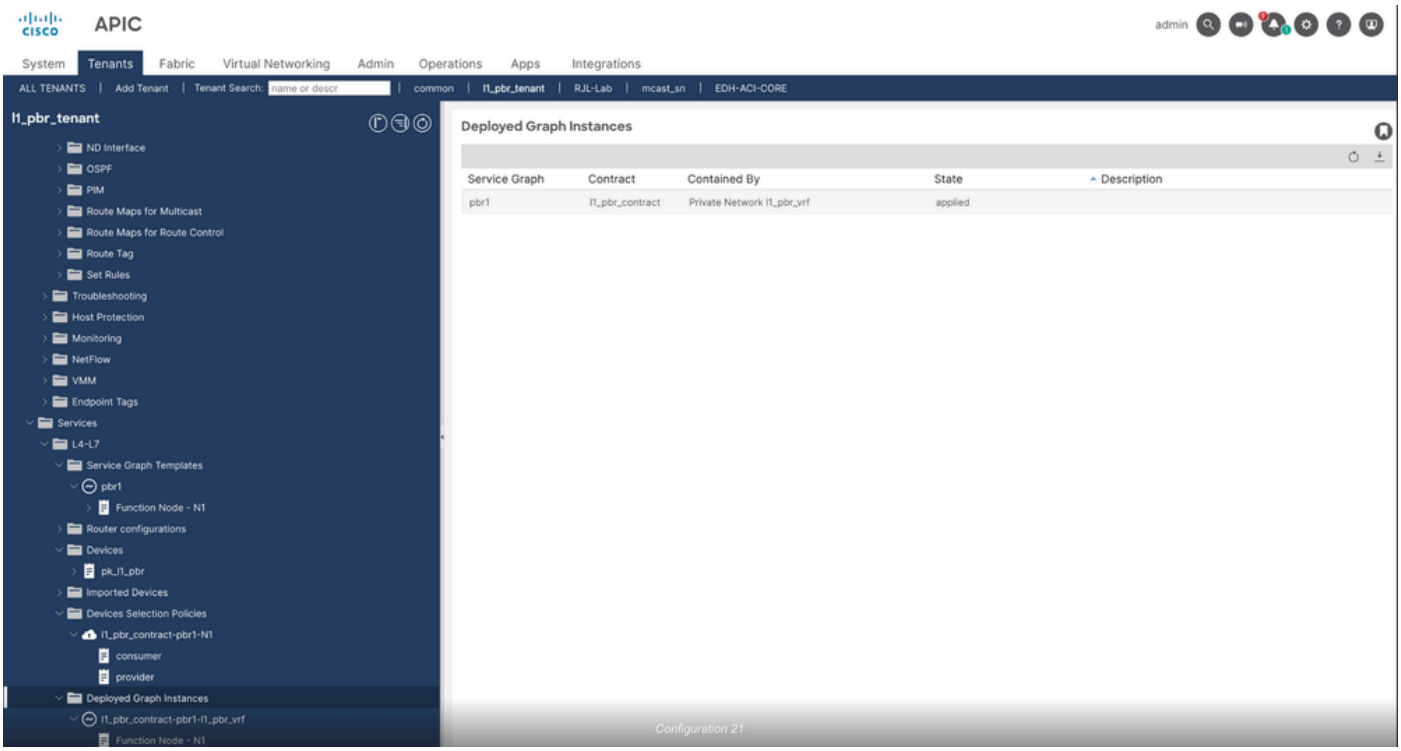
++コンシューマコネクタの確認



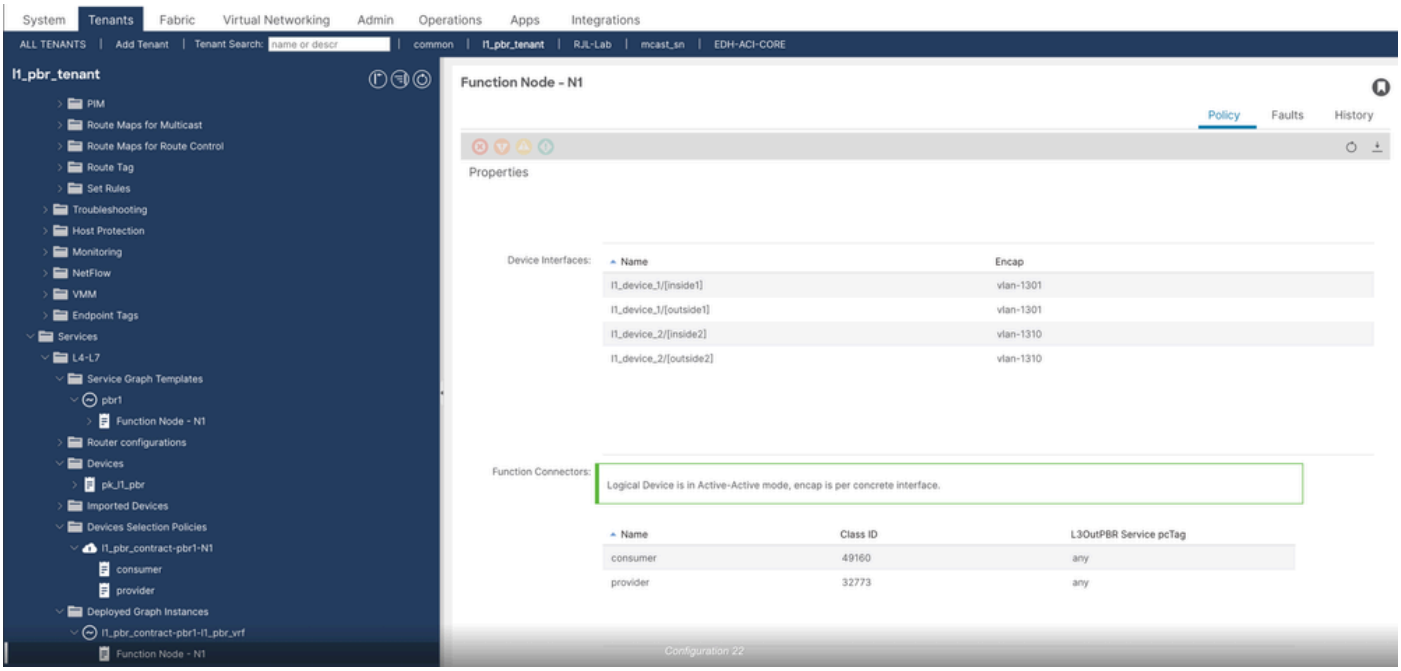
++プロバイダーコネクタの構成



ステップ 2：導入済みグラフインスタンスを確認します。インスタンスが表示されます。インスタンスは適用済み状態である必要があります。



++サービスEPGに関連付けられたPCTAGが表示される予定のデバイスインターフェイスと機能コネクタを確認します。



APIC CLIでのL1サービスグラフの検証

ステップ 1：サービスグラフがコンシューマノードとプロバイダーノードに適用され、さらにヘルスグループステータスも適用されているかどうかを確認します。

<#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
```

ステップ 2：サービスノード（102および103）でスタティックMACバインディングが作成されているかどうかを確認します。

<#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
```

トラフィックの検証

1. EP1からEP2に2000個のICMP pingパケットが生成され、これらはL1デバイスにリダイレクトされます。

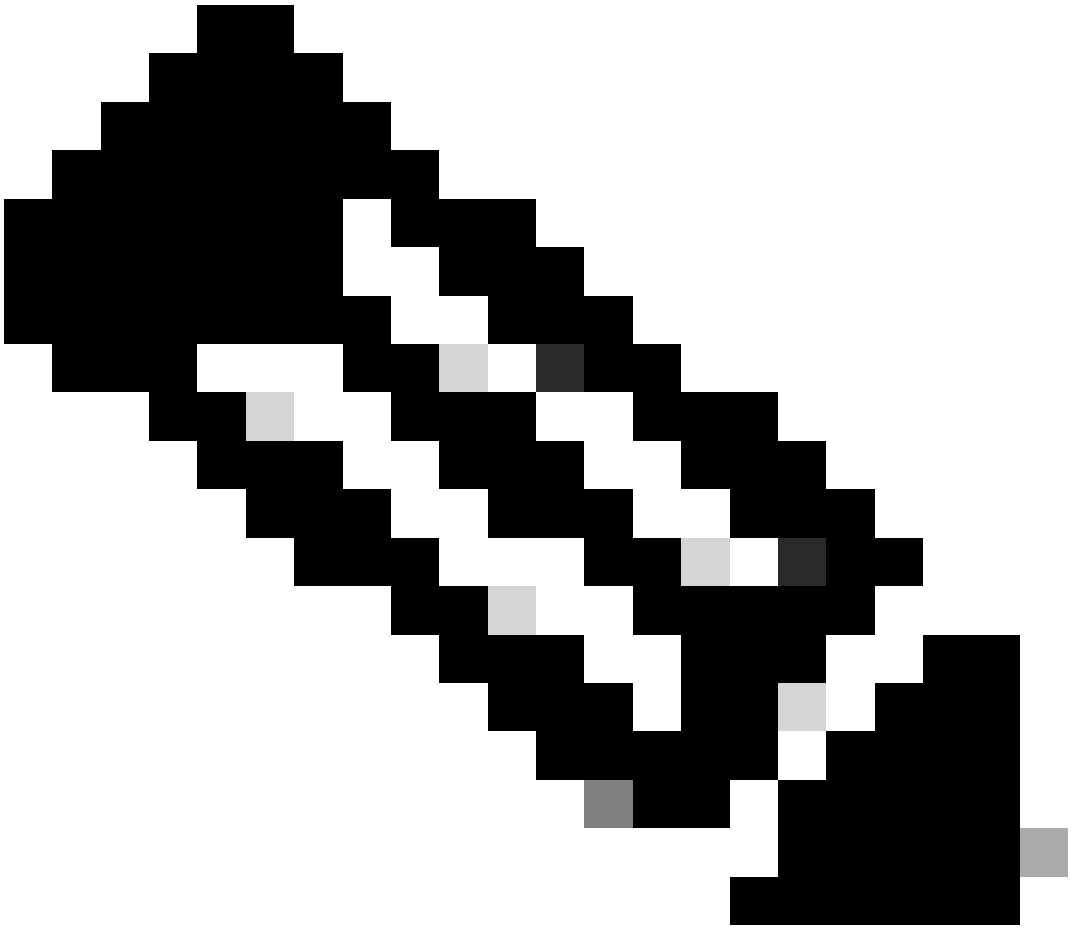
```
switch1# ping 192.168.132.200 vrf l1_pbr1 count 2000 >>>>> sending 2000 packets
64 bytes from 192.168.132.200: icmp_seq=464 ttl=251 time=0.859 ms
64 bytes from 192.168.132.200: icmp_seq=465 ttl=251 time=0.872 ms
64 bytes from 192.168.132.200: icmp_seq=466 ttl=251 time=0.844 ms
64 bytes from 192.168.132.200: 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. L1デバイスに接続されているノード102および103のインターフェイスカウンタを確認します。

```
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：インターフェイスカウンタは、トラフィックがテストされる前にノード102および103でクリアされています。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。