ACIのPBRのトラブルシューティング

内容

はじめに

このドキュメントでは、単一のポッドファブリックでポリシーベースのリダイレクト(PBR)を使用して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)環境をトラブルシューティングする方法について説明します。

前提条件

要件

この記事では、次の項目に関する一般的な知識を持っていることが推奨されます。

- ACIの概念：アクセスポリシー、エンドポイントラーニング、契約、およびL3out

使用するコンポーネント

このトラブルシューティングの演習は、第2世代のNexusスイッチN9K-C93180YC-EXおよびN9K-C93240YC-FX2を使用するACIバージョン6.0(8f)で行われました。

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。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

略語

- BD：ブリッジドメイン
- EPG：エンドポイントグループ
- クラスID:EPGを識別するタグ
- PBRノード：PBR宛先に使用されるL4-L7デバイス
- コンシューマコネクタ：コンシューマ側に面したPBRノードインターフェイス
- プロバイダーコネクタ：プロバイダー側に面したPBRノードインターフェイス

PBR履歴

バージョン	主な機能
2.0(1m)	• サービスグラフはPBR機能を提供します。
3.x以前	• マルチノードポリシーベースリダイレクト(PBR)のサポート • PBR復元ハッシュ
3.2(x)	• 1ノードファイアウォールPBRは、マルチサイト環境でサポートされます。
4.0(x)	• 2ノードファイアウォールPBRは、マルチサイト環境でサポートされます。
4.2(1)	• スタンバイPBRノードを作成するためのバックアップポリシーがサポートされるようになりました。
4.2(3)	• Filter-from-contractオプションは、GUIを使用してサービスグラフテンプレートで使用できます。
5.0(1)	• L3Outは、サービスノードのすべてのプロバイダー側でサポートされています。 • アクティブ – アクティブ展開/ECMPパスは、レイヤ1/レイヤ2 PBRデバイスでサポートされます。
5.2(1)	• これで、PBRの宛先はL3Outになります。 • サービスノードは、HTTP URIを使用して追跡できます。 • サービスグラフマネージドモードとハイブリッドモードはサポートされなくなりました。 • ダイナミックPBRノードのMACアドレスがサポートされています。

6.0(1)	• ウェイトベースの対称ポリシーベースリダイレクト(PBR)

設計上の考慮事項

- PBRは、物理アプライアンスと仮想アプライアンスの両方と連携します
- PBRは、L3Out EPGとEPGの間、EPG間、およびL3Out EPG間で使用できます。L2Out EPGが契約の一部である場合、PBRはサポートされません
- PBRは、Cisco ACIマルチポッド、マルチサイト、およびリモートリーフ環境でサポートされます。
- Cisco ACIファブリックは、サーバおよびPBRノードのゲートウェイである必要があります
- L4-L7デバイスは、go-toモード（ルーテッドモード）で導入する必要があります
- PBRノードはFEXスイッチではサポートされません
- PBRノードには専用ブリッジドメインが必要です
- PBRノードのダイナミックMACアドレスは、現在、ヘルスグループを使用してサポートされています。
- PBRノードブリッジドメインでGARPベースの検出を有効にすることをお勧めします
- ARP、イーサネットトラフィック、およびその他の非IPトラフィックを含む一般的なデフォルトフィルタをPBRに使用しないでください
- PBRノードは、VRFインスタンス間またはVRFインスタンス内のいずれかになります。このトポロジでは、3番目のVRFでのPBRノードのサポートは行われず、コンシューマまたはプロバイダーVRFのいずれかでPBRノードを設定する必要があります

背景説明

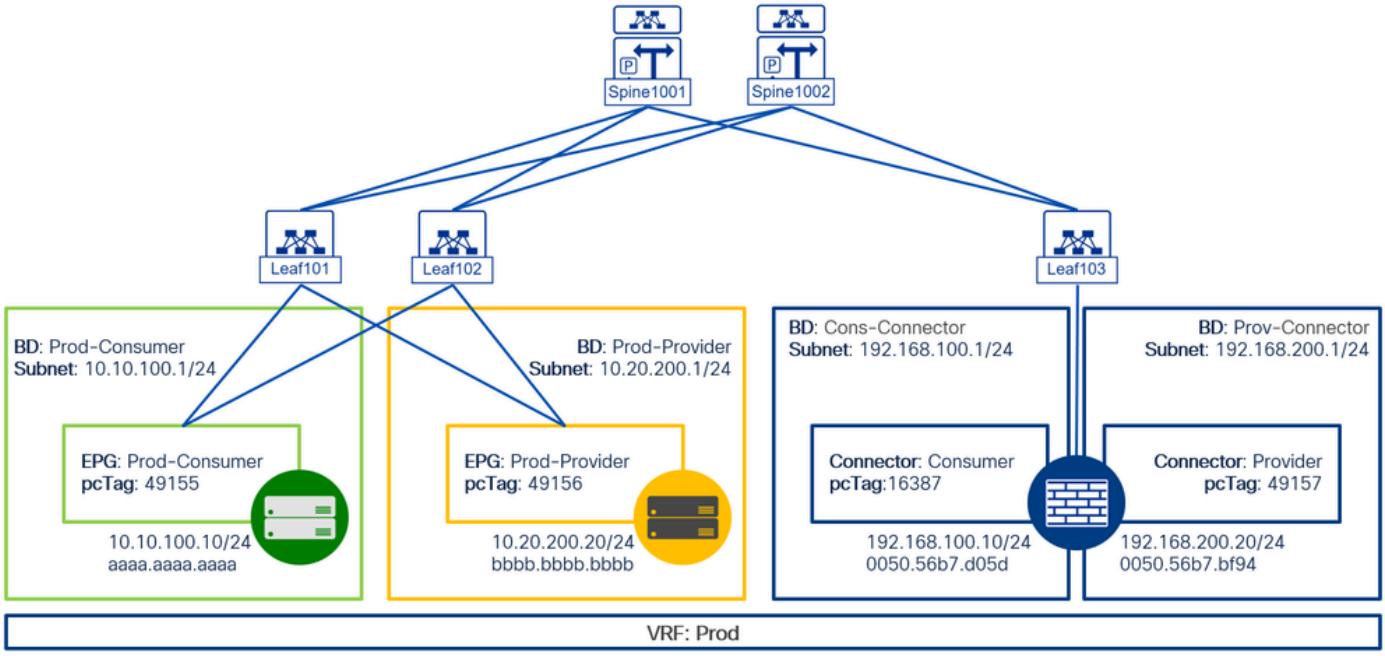
ELAMとFtriageの詳細な説明は、セッションBRKDCN-3900bのCiscoLiveオンデマンドライブラリにあります。

また、すべての設定ガイドラインは、ホワイトペーパー『Cisco Application Centric Infrastructure Policy-Based Redirect Service Graph Design White Paper』に記載されています。

シナリオ：単一ポッドファブリックでの単一VRF

ネットワーク図

物理トポロジ：



トラブルシューティング

ステップ1：障害

設定またはポリシーのインタラクションに問題がある場合、ACIは障害を生成します。障害が発生した場合のPBRレンダリングプロセスに関する特定の障害が特定されています。

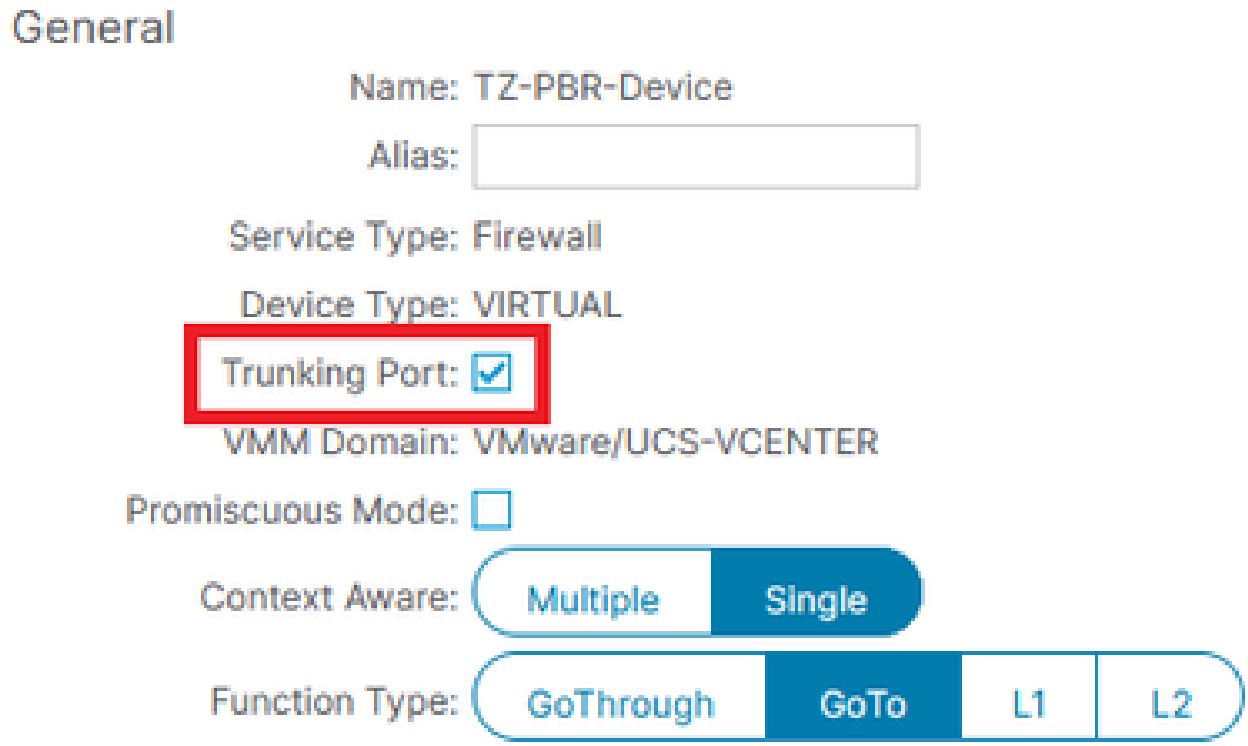
F1690：構成は次の理由により無効です：

- ID割り当てエラー

  このエラーは、サービスノードのカプセル化されたVLANが使用できないことを示します。たとえば、論理デバイスで使用されるVirtual Machine Manager (VMM)ドメインに関連付けられたVLANプールで使用可能なダイナミックVLANがない可能性があります。

  解決策：論理デバイスで使用されているドメイン内のVLANプールを確認します。 論理デバイスインターフェイスが物理ドメイン内にある場合は、カプセル化されたVLAN設定も検査します。これらの設定は、テナント>サービス> L4-L7 >デバイスおよびファブリック>アクセスポリシー>プール> VLANにあります。

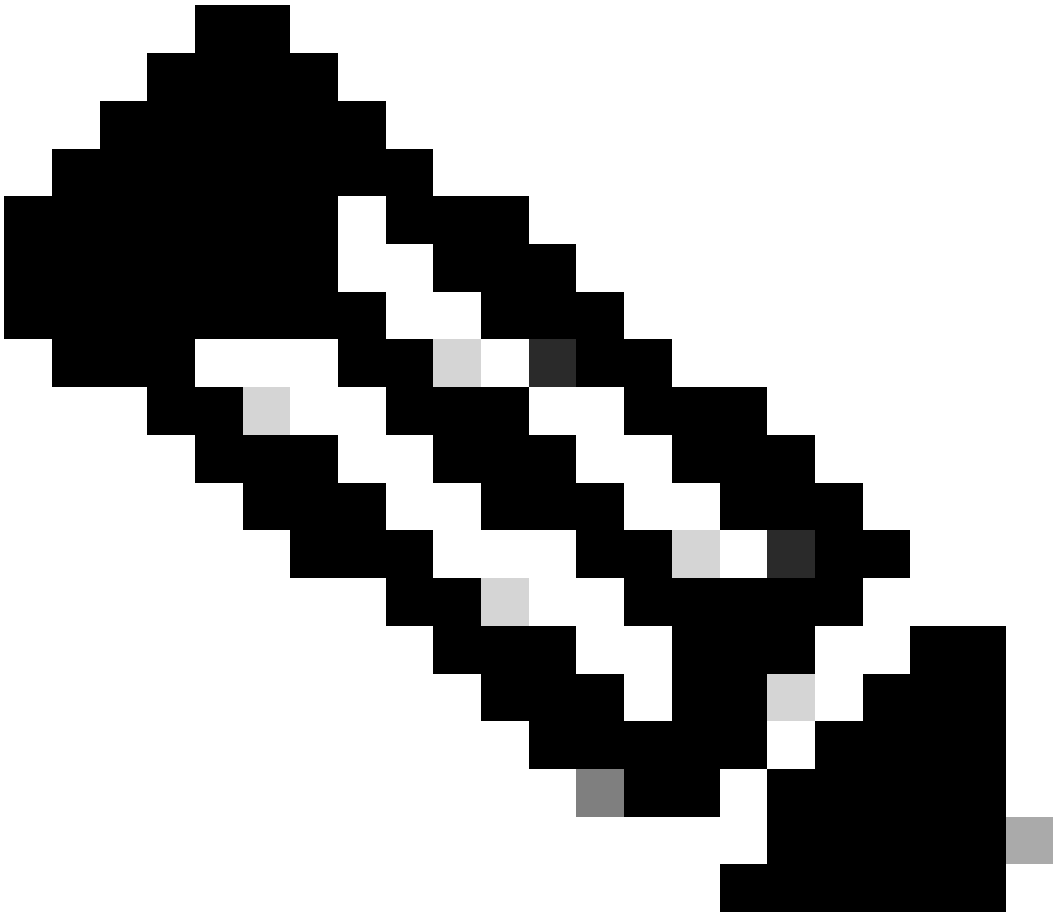
  逆に、論理デバイスインターフェイス(LODI)が仮想ドメイン内にあり、トランクインターフェイス経由でESXiホストに接続する場合は、trunking portオプションが有効になっていることを確認します。



- LDevのデバイスコンテキストが見つかりません

このエラーは、論理デバイスがサービスグラフのレンダリングに配置できないことを示します。たとえば、サービスグラフに関連付けられた契約に一致するデバイス選択ポリシーがない可能性があります。

解決策：デバイス選択ポリシーが定義されていることを確認します。デバイス選択ポリシーは、契約名、サービスグラフ名、およびサービスグラフ内のノード名に基づいて、サービスデバイスとそのコネクタの選択基準を指定します。これは、テナント>サービス> L4-L7 > Device Selection Policyの下にあります。

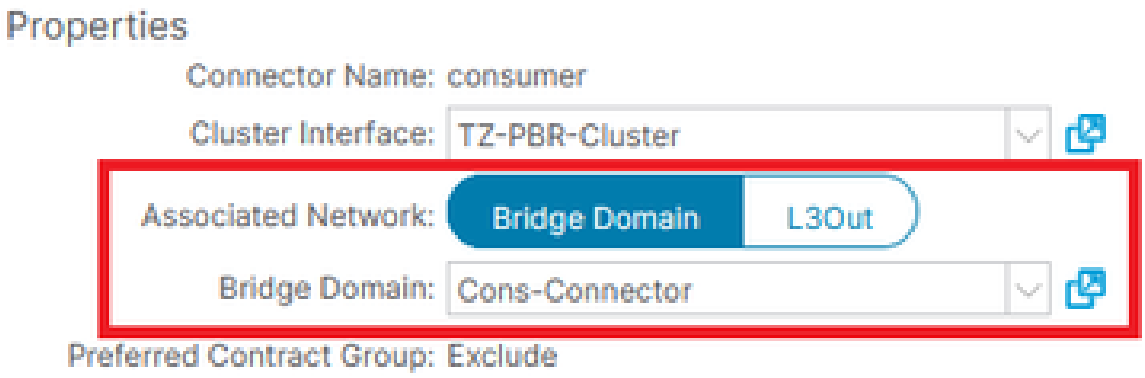


注：サービスグラフテンプレートを導入すると、ACIはソースEPGのブリッジドメインを事前に選択します。PBRコンシューマコネクタのブリッジドメインを変更する必要があります。同じことが、プロバイダーコネクタにも当てはまります。

- BDが見つかりません

  このエラーは、サービスノードのブリッジドメイン(BD)が見つからないことを示します。たとえば、BDはデバイス選択ポリシーでは指定されません。

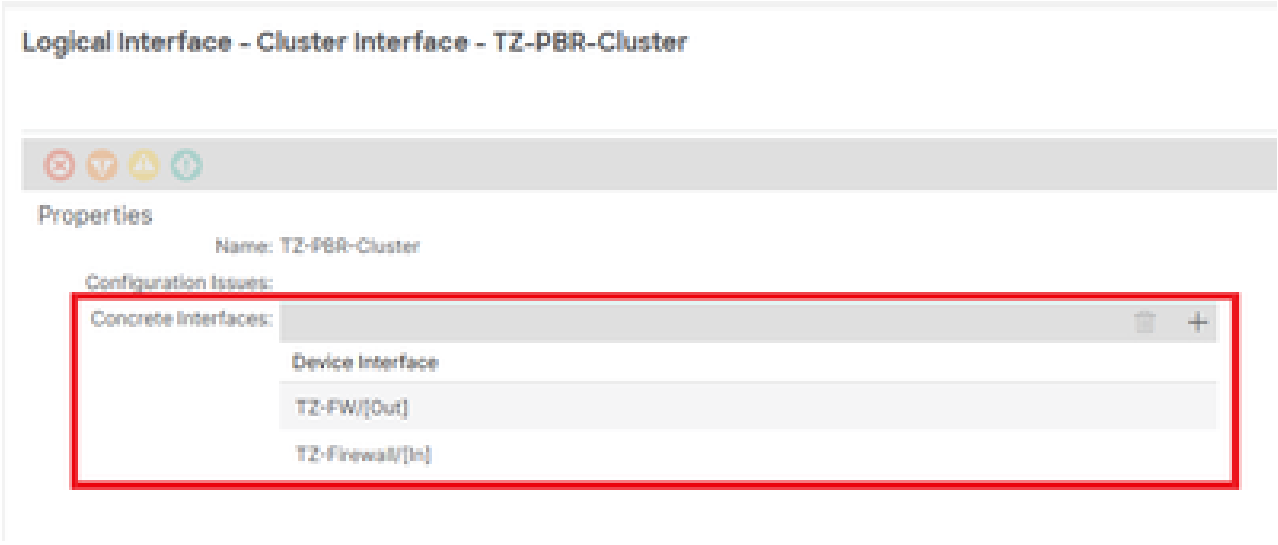
  解決策：デバイス選択ポリシーでBDが指定されていることと、コネクタ名が正しいことを確認します。この設定は、テナント>サービス> L4-L7 > Devices Selection Policy > [Contract + SG] > [Consumer | Provider]の下にあります。



- LIfはCIfと関係がなく、LIfには無効なCIfがあります
- クラスタインターフェイスが見つかりません

これらの障害は、デバイスがクラスタインターフェイスと関係がないことを示しています。

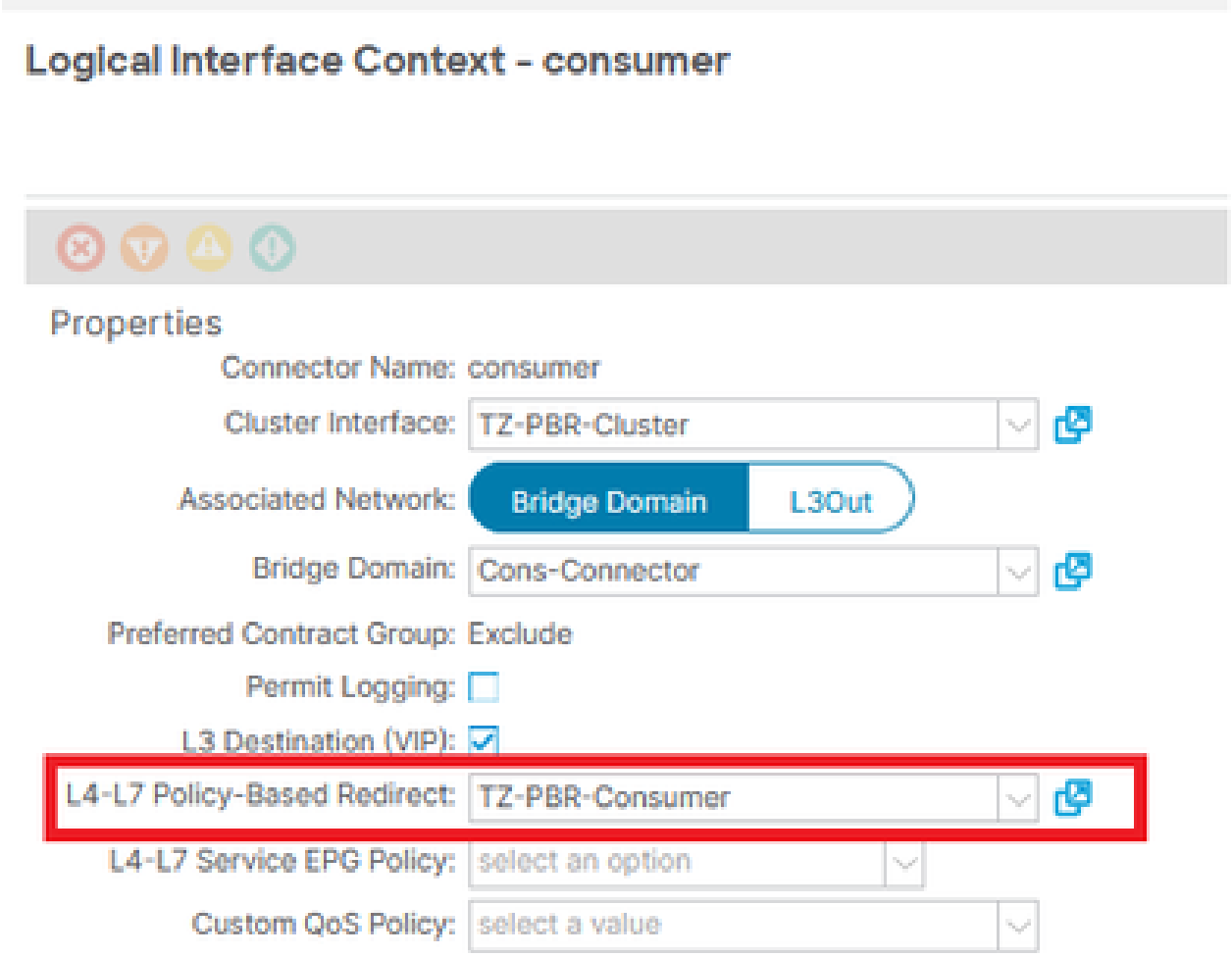
解決策：レイヤ4 ~ レイヤ7(L4-L7)デバイス設定に、特定の具体的なインターフェイスセレクタが含まれていることを確認します。この設定は、テナント>サービス> L4-L7 >デバイス> [Device] >クラスタインターフェイスにあります。



- 無効なサービスリダイレクトポリシー

このエラーは、サービスグラフ内のサービス機能でリダイレクションがアクティブ化されているにもかかわらず、PBRポリシーが適用されていないことを示します。

解決策：PBRポリシーがDevice Selection Policy設定内で設定されていることを確認します。この設定は、テナント>サービス> L4-L7 > Devices Selection Policy > [Contract + SG] > [Consumer | Provider]の下にあります。



F0759: graph-rendering-failure - "Service graph for tenant < tenant > could not be instantiated.関数ノード<ノード>構成が無効です。

関数ノード名の構成が無効なため、指定されたテナントのサービスグラフをインスタンス化できませんでした。

このエラーは、前述の状態に関連する設定の問題があることを示唆しています。

さらに、初期導入時に、この障害が一時的に発生し、すぐに解決される可能性があります。これは、すべてのポリシーを導入するためにACIで実行されるレンダリングプロセスが原因で発生します。

解決：報告された他の障害を調査し、状況に応じて解決します。

F0764: configuration-failed - "L4-L7 Devices configuration < device > for tenant < tenant > is invalid."

PBRデバイスポリシーの構成が無効なため、指定されたテナントのサービスグラフをインスタンス化できませんでした。

このエラーは、前述の状態に関連する設定の問題があることを示唆しています。

解決：報告された他の障害を調査し、状況に応じて解決します。

F0772: configuration-failed - "LIf configuration < cluster > for L4-L7 Devices < device > for tenant < tenant >は無効です。"

PBRデバイスクラスタインターフェイス選択の構成が無効なため、指定されたテナントのサービスグラフをインスタンス化できませんでした。

このエラーは、前述の状態に関連する設定の問題があることを示唆しています。

解決：報告された他の障害を調査し、状況に応じて解決します。

ステップ2：送信元および宛先エンドポイントのラーニング

ファブリック内で送信元エンドポイントと宛先エンドポイントが認識されていることを確認します。これには基本設定が必要です。

- Virtual Routing and Forwarding(VRF)オブジェクト
- ユニキャストルーティングが有効になっているブリッジドメイン(BD)オブジェクト。IPデータプレーンのラーニングを有効にすることはベストプラクティスと見なされますが、必須ではありません。
- 仮想ドメインと物理ドメインの両方に適用できるエンドポイントグループ(EPG)オブジェクト。
- アクセスポリシー：アクセスポリシー設定チェーンが完了していること、およびEPGで障害が報告されていないことを確認します。

正しいEPGとインターフェイスでエンドポイント学習を確認するには、エンドポイントが学習されたリーフ（コンピュートリーフとも呼ばれる）で次のコマンドを実行します。

<#root>

show system internal epm endpoint [ip | mac] [x.x.x.x | eeee.eeee.eeee]

<#root>

Leaf101#

show system internal epm endpoint ip 10.10.100.10

MAC :

aaaa.aaaa.aaaa

::: Num IPs : 1

IP# 0 : 10.10.100.10

::: IP# 0 flags : ::: l3-sw-hit: No
Vlan id : 57 ::: Vlan vnid : 10865 :::

VRF name : TZ:Prod

```
BD vnid : 16056291 ::: VRF vnid : 2162692
Phy If : 0x16000008 ::: Tunnel If : 0
Interface :
```

port-channel9

```
Flags : 0x80004c05 :::
```

sclass : 49155

```
 ::: Ref count : 5
EP Create Timestamp : 02/18/2025 15:00:18.767228
EP Update Timestamp : 02/18/2025 15:04:57.908343
EP Flags : local|VPC|IP|MAC|sclass|timer|

::::


Leaf101#
```

このコマンドでは、エンドポイントが分類されているEPGに関連付けられているpcTag(sclass)を識別し、インターフェイス、VRFスコープ、およびMACアドレス情報を取得できます。

送信元または宛先エンドポイントの場所がわからない場合は、APICで次のコマンドを使用できます。

<#root>

show endpoint [ip | mac] [x.x.x.x | eeee.eeee.eeee]

<#root>

```
APIC#
```

show endpoint ip 10.10.100.10

```
Legends:
(P):Primary VLAN
(S):Secondary VLAN


Dynamic Endpoints:
Tenant : TZ
Application : TZ
AEPg : Prod-Consumer

End Point MAC     IP Address                                Source       Node       Interface
----------------- ----------------------------------------- ------------ ---------- --------------------
```

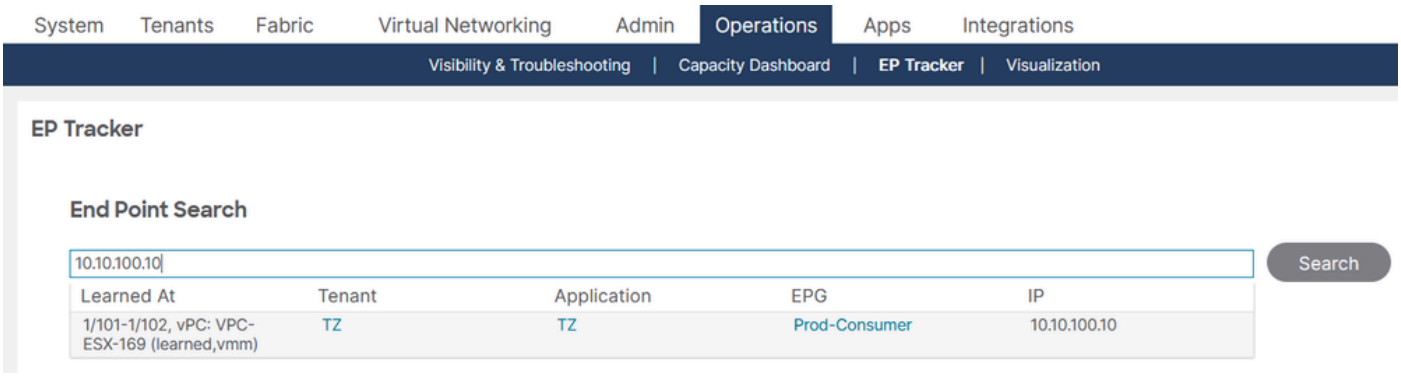
AA:AA:AA:AA:AA:AA 10.10.100.10

```
                              learned,vmm
```

101 102   vpc VPC-ESX-169

```
                vlan-2673       not-applicable    2025-02-18T15:16:40.

Total Dynamic Endpoints: 1
Total Static Endpoints: 0
APIC#
```

GUIでは、エンドポイントの監視と管理のために、Operations > EP Trackerの順に選択することで、EP Tracker機能にアクセスできます。



送信元と宛先のエンドポイントから収集した情報を使用して、PBRポリシーの導入に集中できます。

ステップ3：契約のリダイレクト

PBRはサービスグラフフレームワークに統合されています。そのため、サービスグラフテンプレートは、契約に従って送信元スイッチと宛先スイッチの両方に導入し、設定する必要があります。前の手順で収集したpcTags情報を利用して、次のコマンドを実行すると、エンドポイントグループ(EPG)がサービスグラフグループにリダイレクトされているかどうかを確認できます。

<#root>

show zoning-rule scope [vrf_scope]

ゾーン分割ルールでは、次のルールを考慮する必要があります。

1. 関連付けられたリダイレクトグループを持つ宛先EPGへの送信元EPG
2. ソースPBRノードシャドウEPGからソースEPG
3. 関連付けられたリダイレクトグループを持つ送信元EPGへの宛先EPG。このグループは、以前の設定と同じであることも、異なることもあります。
4. 宛先PBRノードシャドウEPGから宛先EPG

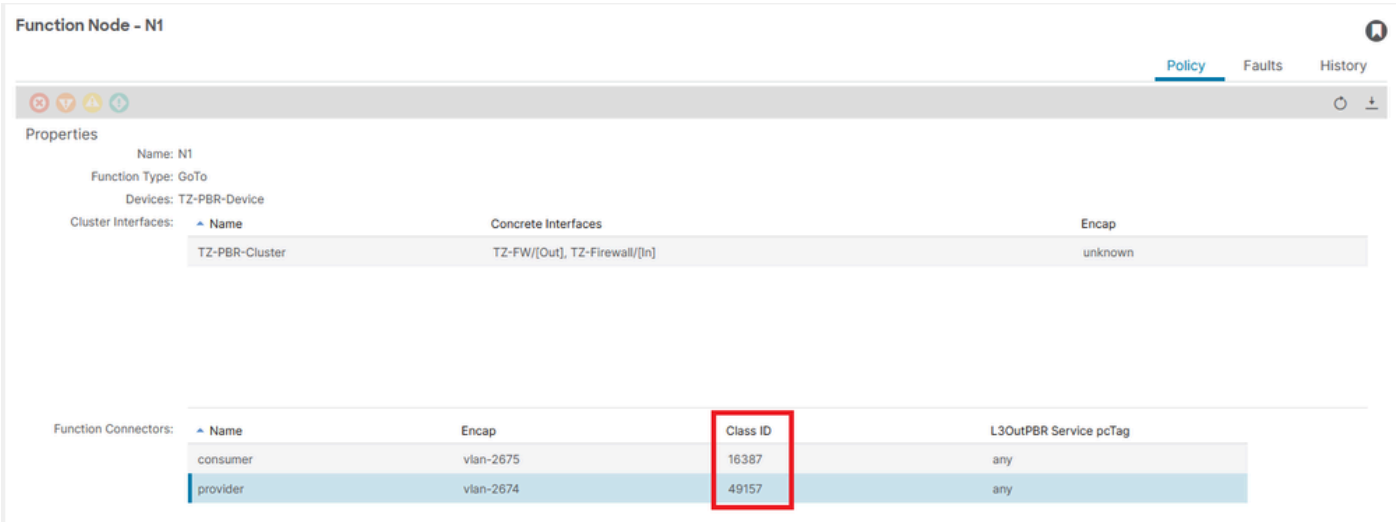
<#root>

```
Leaf101#
```

show zoning-rule scope 2162692

```
+---------+--------+--------+----------+----------------+---------+---------+------+------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |       Dir      |  operSt |  Scope  | Name |      Action      |
+---------+--------+--------+----------+----------------+---------+---------+------+------------------+
|   4565  |  49155 |  49156 |  default |     bi-dir     | enabled | 2162692 |      | redir(destgrp-8) |
|   4565  |  49156 |  49155 |  default | uni-dir-ignore | enabled | 2162692 |      | redir(destgrp-9) |
|   4973  |  16387 |  49155 |  default |     uni-dir    | enabled | 2162692 |      |      permit      |
|   4564  |  49157 |  49156 |  default |     uni-dir    | enabled | 2162692 |      |      permit      |
+---------+--------+--------+----------+----------------+---------+---------+------+------------------+
Leaf101#
```

ポリシーベースルーティング(PBR)の導入プロセス中に作成されたシャドウEPGのpcTagを確認するには、Tenants > [TENANT_NAME] > Services > L4-L7 > Deployed Graph Instance > [SG_NAME] > Function Node - N1に移動します。



- コントラクトパーサー

このスクリプトは、ゾーン分割ルール、フィルタ、統計情報、およびEPG名を関連付けます。このスクリプトは、ACIリーフまたはAPIC上で直接安全に実行できます。APIC上で実行すると、すべてのリーフスイッチで具体的なオブジェクトが収集されます。大規模なポリシー展開では数分かかる場合があります。

ACIバージョン3.2以降では、contract_parserはイメージ内にバンドルされており、リーフで使用できます。iBashシェルからcontract_parser.pyと入力するだけです。

<#root>

```
Leaf101#
```

contract_parser.py --sepg 49155

```
Key:
[prio:RuleId] [vrf:{str}] action protocol src-epg [src-l4] dst-epg [dst-l4] [flags][contract:{str}] [hi

[7:4999] [vrf:TZ:Prod] log,
```

redir

```
 ip tn-TZ/ap-TZ/epg-
```

Prod-Consumer(49155)

tn-TZ/ap-TZ/epg-

Prod-Provideer(49156)

[contract:uni/tn-TZ/brc-

TZ-PBR-Contract

] [

hit=81

]

destgrp-8

vrf:TZ:Prod ip:

192.168.100.10

mac:

00:50:56:B7:D0:5D

bd:uni/tn-TZ/

BD-Cons-Connector

Leaf101#

このコマンドは、コントラクトアクション、送信元および宛先EPG、使用中のコントラクト名、ヒットカウントなどの詳細を提供します。

ステップ4：リダイレクトグループ

ゾーン分割ルールに適用されたコントラクトに基づいてリダイレクトグループを特定した後、次のステップとして、リダイレクト対象のデバイスのIPアドレスとMACアドレスを特定します。これを行うには、次のコマンドを実行します。

<#root>

show service redir info group [destgrp_ID]

<#root>

Leaf101#

show service redir info group 8

```
========================================================================================================
LEGEND
TL: Threshold(Low) | TH: Threshold(High) | HP: HashProfile | HG: HealthGrp | BAC: Backup-Dest | TRA: Tr
========================================================================================================
GrpID Name      destination                                HG-name        BAC W   operSt  operStQual   TL  T
```

```
===== ====      ===========                              ============== === === ======= ============ === ==
8     destgrp-8 dest-[

192.168.100.10

]-[vxlan-

2162692

] Not attached   N   1

enabled

 no-oper-grp  0   0   sym no  no
Leaf101#
Leaf101# show service redir info group 9
================================================================================================================
LEGEND
TL: Threshold(Low) | TH: Threshold(High) | HP: HashProfile | HG: HealthGrp | BAC: Backup-Dest | TRA: Tra
================================================================================================================
GrpID Name      destination                              HG-name        BAC W   operSt  operStQual   TL  TH
===== ====      ===========                              ============== === === ======= ============ === ==
9     destgrp-9 dest-[

192.168.200.20

]-[vxlan-

2162692

] Not attached   N   1

enabled

 no-oper-grp  0   0   sym no  no
Leaf101#
```

このコマンドを使用すると、リダイレクトグループの動作ステータス(OperSt)、L4-L7 PBRセクションで設定されたIPアドレス、およびPBRノードブリッジドメインに関連付けられたVRFのVNIDを確認できます。次に、設定されているMACアドレスを判別する必要があります。

<#root>

show service redir info destinations ip [PBR-node IP] vnid [VRF_VNID]

<#root>

```
Leaf101#

show service redir info destination ip 192.168.100.10 vnid 2162692


================================================================================================================
LEGEND
TL: Threshold(Low) | TH: Threshold(High) | HP: HashProfile | HG: HealthGrp | BAC: Backup-Dest | TRA: Tra
================================================================================================================
Name                                  bdVnid         vMac              vrf     operSt  operStQual   HG-n
====                                  ======         ====              ====    =====   ==========   ====
dest-[
```

192.168.100.10

]-[vxlan-

2162692

] vxlan-

15826939

00:50:56:B7:D0:5D

TZ:Prod

enabled

no-oper-dest Not attached
Leaf101#
Leaf101# show service redir info destination ip 192.168.200.20 vnid 2162692
==========
LEGEND
TL: Threshold(Low) | TH: Threshold(High) | HP: HashProfile | HG: HealthGrp | BAC: Backup-Dest | TRA: Tra
==========
Name bdVnid vMac vrf operSt operStQual HG-
==== ====== ==== ==== ===== ========= ===
dest-[

192.168.200.20

]-[vxlan-

2162692

] vxlan-

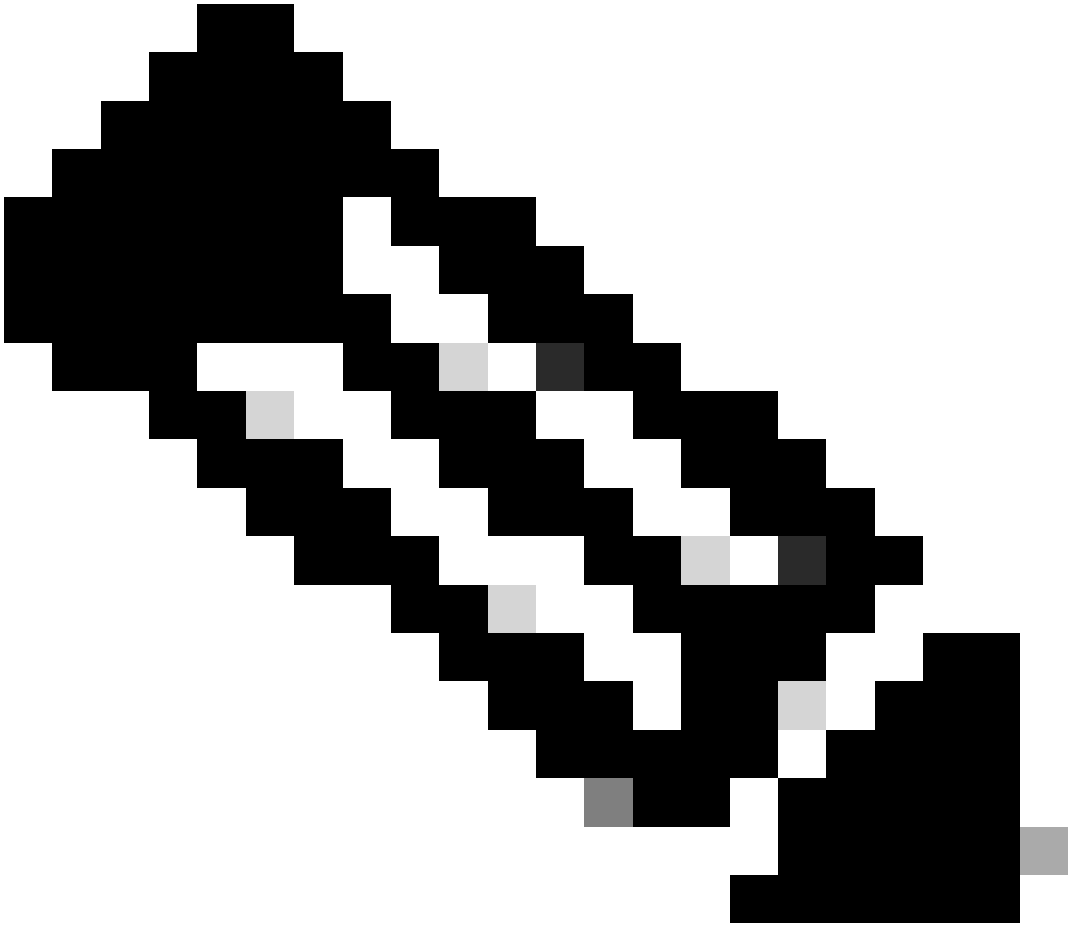
16646036 00:50:56:B7:BF:94

TZ:Prod

enabled

no-oper-dest Not attached
Leaf101#

前述の詳細に加えて、このコマンドは、VRF名、BD VNID、およびPBRノードの設定済みMACアドレスなどの有益な情報を提供します。



注：この段階では、IPアドレスとMACアドレスの両方がユーザ設定になっていることに注意してください。つまり、L4-L7ポリシーベースルーティング(PBR)定義中に入力エラーが発生する可能性があります。

ステップ5:PBRノードがトラフィックを受信していません。

PBRフォワーディングで発生する一般的な問題は、PBRノードに到達するトラフィックがないことです。この問題の一般的な原因は、L4-L7ポリシーベースルーティング(PBR)設定内のMACアドレスの指定が誤っていることです。

L4-L7ポリシーベースルーティングで設定されたMACアドレスの精度を検証するには、ステップ2で以前使用したコマンドを実行します。このコマンドは、サービスリーフとして指定されたリーフスイッチ上で実行できます。このリーフスイッチでノードが学習されます。

<#root>

```
show system internal epm endpoint [ ip | mac ] [ x.x.x.x | eeee.eeee.eeee ]
```

<#root>

Leaf103#

show system internal epm endpoint ip 192.168.100.10

MAC :

0050.56b7.d05d

::: Num IPs : 1
IP# 0 :

192.168.100.10

::: IP# 0 flags : ::: l3-sw-hit: Yes ::: flags2 :

dp-lrn-dis

Vlan id : 71 ::: Vlan vnid : 10867 ::: VRF name : TZ:Prod
BD vnid : 15826939 ::: VRF vnid :

2162692

Phy If : 0x16000008 ::: Tunnel If : 0
Interface : port-channel19
Flags : 0x80004c25 ::: sclass : 16387 ::: Ref count : 5
EP Create Timestamp : 02/19/2025 12:07:44.065032
EP Update Timestamp : 02/19/2025 15:27:03.400086
EP Flags : local|vPC|peer-aged|IP|MAC|sclass|timer|

::::

Leaf103#

.....

Leaf103#

show system internal epm endpoint ip 192.168.200.20

MAC :

0050.56b7.bf94

::: Num IPs : 1
IP# 0 :

192.168.200.20

::: IP# 0 flags : ::: l3-sw-hit: Yes ::: flags2 :

dp-lrn-dis

Vlan id : 60 ::: Vlan vnid : 10866 ::: VRF name : TZ:Prod
BD vnid : 16646036 ::: VRF vnid :

2162692

```
Phy If : 0x16000008 ::: Tunnel If : 0
Interface : port-channel19
Flags : 0x80004c25 ::: sclass : 49157 ::: Ref count : 5
EP Create Timestamp : 02/19/2025 13:51:03.377942
EP Update Timestamp : 02/19/2025 15:28:34.151877
EP Flags : local|vPC|peer-aged|IP|MAC|sclass|timer|

::::


Leaf103#
```

EPMテーブルに記録されたMACアドレスが、サービスリダイレクトグループで設定されたアドレスと一致することを確認します。PBRノードの宛先への適切なトラフィックルーティングを確保するには、わずかな入力エラーでも修正する必要があります。

ステップ6：トラフィックフロー。

- ファトリアージ

ELAMプロセスの設定と解釈をエンドツーエンドで自動化するように設計されたAPIC用のCLIツール。このツールを使用すると、特定のフローと、そのフローの起点となるリーフスイッチを指定できます。各ノードでELAMを順次実行して、フローの転送パスを分析します。このツールは、パケットパスを容易に認識できない複雑なトポロジで特に役立ちます。

<#root>

APIC #

ftriage -user admin route -sip 10.10.100.10 -dip 10.20.200.20 -ii LEAF:101,102

```
Starting ftriage

Log file name for the current run is: ftlog_2025-02-25-10-26-05-108.txt


2025-02-25 10:26:05,116 INFO /controller/bin/ftriage -user admin route -sip 10.10.100.10 -dip 10.20.200
Request password info for username: admin
Password:
2025-02-25 10:26:31,759 INFO ftriage: main:2505 Invoking ftriage with username: admin
2025-02-25 10:26:34,188 INFO ftriage: main:1546 Enable Async parellel ELAM with 2 nodes
2025-02-25 10:26:57,927 INFO ftriage: fcls:2510

LEAF101

: Valid ELAM for asic:0 slice:0 srcid:64 pktid:1913
2025-02-25 10:26:59,120 INFO ftriage: fcls:2863

LEAF101

: Signal ELAM found for Async lookup
2025-02-25 10:27:00,620 INFO ftriage: main:1317 L3 packet

Seen on LEAF101
```

Ingress:

Eth1/45 (Po9)

Egress: Eth1/52 Vnid: 2673
2025-02-25 10:27:00,632 INFO ftriage: main:1372 LEAF101: Incoming Packet captured with [

SIP:10.10.100.10, DIP:10.20.200.20

]
...
2025-02-25 10:27:08,665 INFO ftriage: main:480 Ingress

BD(s) TZ:Prod-Consumer

2025-02-25 10:27:08,666 INFO ftriage: main:491 Ingress

Ctx: TZ:Prod Vnid: 2162692

...
2025-02-25 10:27:45,337 INFO ftriage: pktrec:367 LEAF101:

traffic is redirected

...
2025-02-25 10:28:10,701 INFO ftriage: unicast:1550 LEAF101:

traffic is redirected

to vnid:15826939

mac:00:50:56:B7:D0:5D

via tenant:TZ

graph:TZ-PBR-SG

contract:

TZ-PBR-Contract

...
2025-02-25 10:28:20,339 INFO ftriage: main:975

Found peer-node SPINE1001

and IF: Eth1/1 in candidate list
...
2025-02-25 10:28:39,471 INFO ftriage: main:1366

SPINE1001

: Incoming Packet captured with Outer [SIP:10.2.200.64, DIP:10.2.64.97] .... Inner [

SIP:10.10.100.10, DIP:10.20.200.20

]
2025-02-25 10:28:39,472 INFO ftriage: main:1408

SPINE1001

: Outgoing packet's Vnid:

15826939

```
2025-02-25 10:28:58,469 INFO ftriage: fib:524
SPINE1001: Proxy in spine

...
2025-02-25 10:29:07,898 INFO ftriage: main:975
Found peer-node LEAF103
. and IF: Eth1/50 in candidate list
...
2025-02-25 10:29:35,331 INFO ftriage: main:1366
LEAF103
: Incoming Packet captured with Outer [SIP:10.2.200.64, DIP:10.2.200.64] .... Inner [
SIP:10.10.100.10, DIP:10.20.200.20
]
...
2025-02-25 10:29:50,277 INFO ftriage: ep:128 LEAF103: pbr traffic with dmac:
00:50:56:B7:D0:5D

2025-02-25 10:30:07,374 INFO ftriage: main:800 Computed egress encap string
vlan-2676

2025-02-25 10:30:13,326 INFO ftriage: main:535 Egress
Ctx TZ:Prod

2025-02-25 10:30:13,326 INFO ftriage: main:536 Egress BD(s):
TZ:Cons-Connector

...
2025-02-25 10:30:18,812 INFO ftriage: misc:908 LEAF103: caller unicast:581
EP if(Po19)
 same as egr if(Po19)
2025-02-25 10:30:18,812 INFO ftriage: misc:910 LEAF103: L3 packet caller unicast:668 getting
bridged
 in SUG
2025-02-25 10:30:18,813 INFO ftriage: main:1822 dbg_sub_nexthop function returned values on node LEAF10
2025-02-25 10:30:19,378 INFO ftriage: acigraph:794 : Ftriage Completed with hunch: matching service dev
APIC #
```

- ELAM:

Embedded Logic Analyzer Module(ELAM)は、ユーザがハードウェアで特定の条件を確立し、それらの条件を満たす最初のパケットまたはフレームをキャプチャできるようにする診断ツールです。キャプチャが成功すると、ELAMステータスはtriggeredと表示されます。トリガー時に

ELAMが無効になり、データダンプの収集が可能になるため、そのパケットまたはフレームに対してスイッチのASICで実行される多数の転送決定の分析が容易になります。ELAMはASICレベルで動作し、スイッチのCPUや他のリソースに影響を与えないようにします。

コマンド構文の構造。この構造は、『ACI Intra-Fabric Forwarding Toolsのトラブルシューティング』のドキュメントから収集されたものです

```
vsh_lc                                          [This command enters the line card shell where ELAMs are r
debug platform internal <asic> elam asic 0      [refer to the ASICs table]
```

トリガーする条件の設定

```
trigger reset                                                   [ensures no existing triggers are running]
trigger init in-select <number> out-select <number>             [determines what information about a packet is
set outer/inner                                                 [sets conditions]
start                                                           [starts the trigger]
status                                                          [checks if a packet is captured]
```

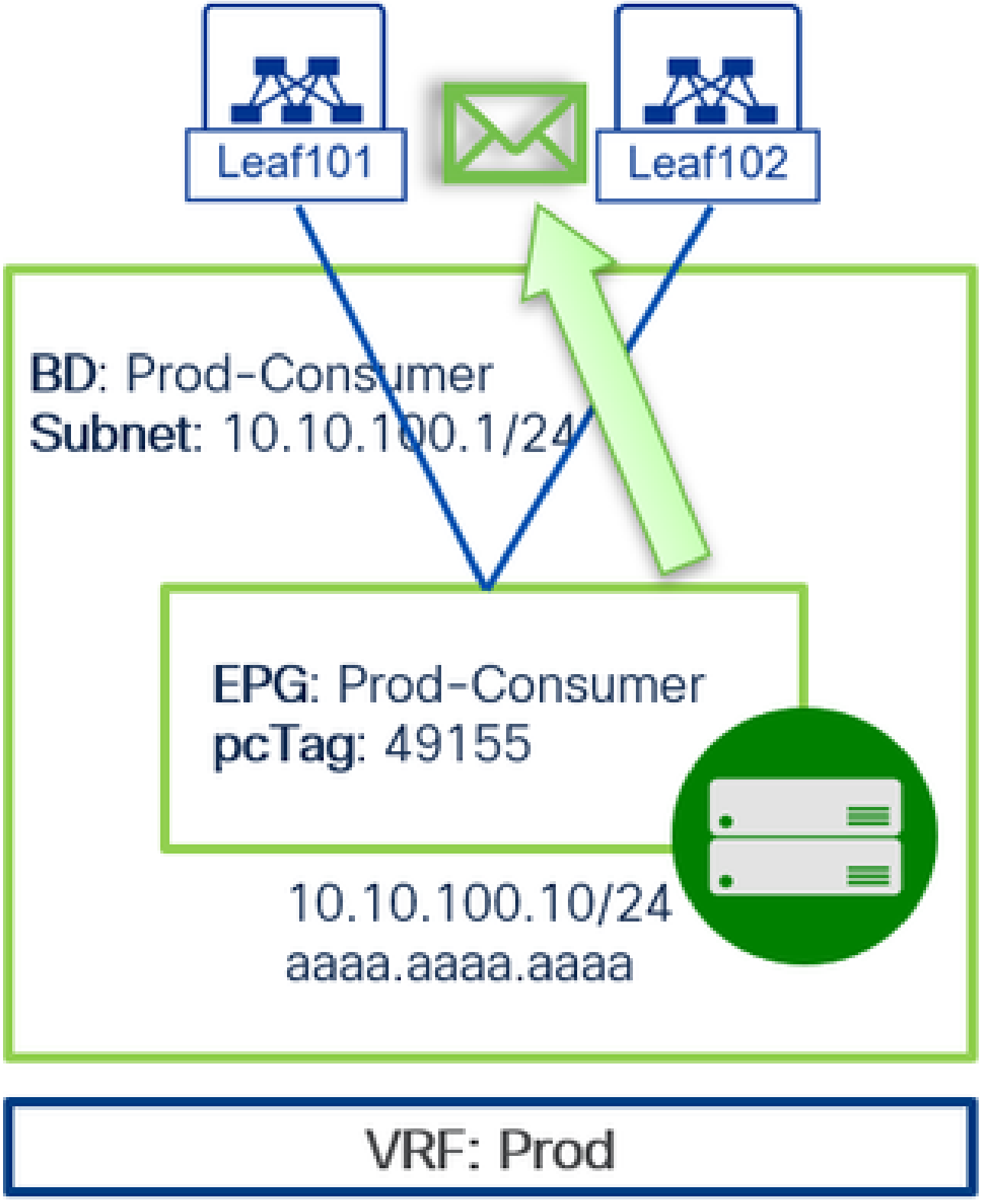
パケット分析を含むダンプを生成します。

```
ereport             [display detailed forwarding decision for the packet]
```

- Traffic flow

対象となるすべてのデバイス間のトラフィックフローを把握することが重要です。Ftriageツールは、このフローの優れた要約を提供します。ただし、詳細な段階的検証と、パケット受信プロセスのより深い洞察を得るために、ネットワークトポロジ内の各点でEmbedded Logic Analyzer Module(ELAM)を実行できます。

1. 入力トラフィックは、送信元サーバが学習されたコンピューティングリーフで発生します。この特定のシナリオでは、送信元がvPCインターフェイスの背後に配置されているため、vPCピアでELAMを設定する必要があります。これは、ハッシュアルゴリズムによって選択された物理インターフェイスが不確定であるために必要です。



<#root>

LEAF101#

vsh_lc

module-1#

debug platform internal tah elam asic 0

```
module-1(DBG-elam)#
trigger reset

module-1(DBG-elam)#
trigger init in-select 6 out-select 1

module-1(DBG-elam-insel6)#
reset

module-1(DBG-elam-insel6)#
set outer ipv4 src_ip 10.10.100.10 dst_ip 10.20.200.20

module-1(DBG-elam-insel6)#
start

module-1(DBG-elam-insel6)#
status

ELAM STATUS
===========
Asic 0 Slice 0 Status
Triggered

Asic 0 Slice 1 Status Armed

module-1(DBG-elam-insel6)#
 ereport

================================================================================================================
Trigger/Basic Information
================================================================================================================
...
Incoming Interface : 0x40( 0x40 )


>>> Eth1/45


...

----------------------------------------------------------------------------------------------------------------
Outer L2 Header
----------------------------------------------------------------------------------------------------------------
Destination MAC : 0022.BDF8.19FF >>> Bridge-domain MAC address


Source MAC : AAAA.AAAA.AAAA
```

802.1Q tag is valid : yes(0x1)
CoS : 0(0x0)

Access Encap VLAN : 2673

(0xA71)

Outer L3 Header

L3 Type : IPv4
IP Version : 4
DSCP : 0
IP Packet Length : 84 (= IP header(28 bytes) + IP payload)
Don't Fragment Bit : set
TTL : 64
IP Protocol Number : ICMP
IP CheckSum : 6465(0x1941)

Destination IP : 10.20.200.20

Source IP : 10.10.100.10

Contract Lookup Key

IP Protocol : ICMP(0x1)
L4 Src Port : 2048(0x800)
L4 Dst Port : 7345(0x1CB1)

sclass (src pcTag) : 49155(0xC003) >>> Prod-Consumer

EPG

dclass (dst pcTag) : 49156(0xC004)

>>> Prod-Provider EPG

src pcTag is from local table : yes

>>> EPGs are known locally

derived from a local table on this node by the lookup of src IP or MAC
Unknown Unicast / Flood Packet : no
If yes, Contract is not applied here because it is flooded

Sideband Information

---

ovector : 176(0xB0) >>> Eth1/52

```
Ovec in "show plat int hal l2 port gpd"

Opcode : OPCODE_UC


------------------------------------------------------------------------------------------------------------------------
sug_luc_latch_results_vec.luc3_0.

service_redir: 0x1 >>> Service Redir 0x1 = PBR was applied


------------------------------------------------------------------------------------------------------------------------
```

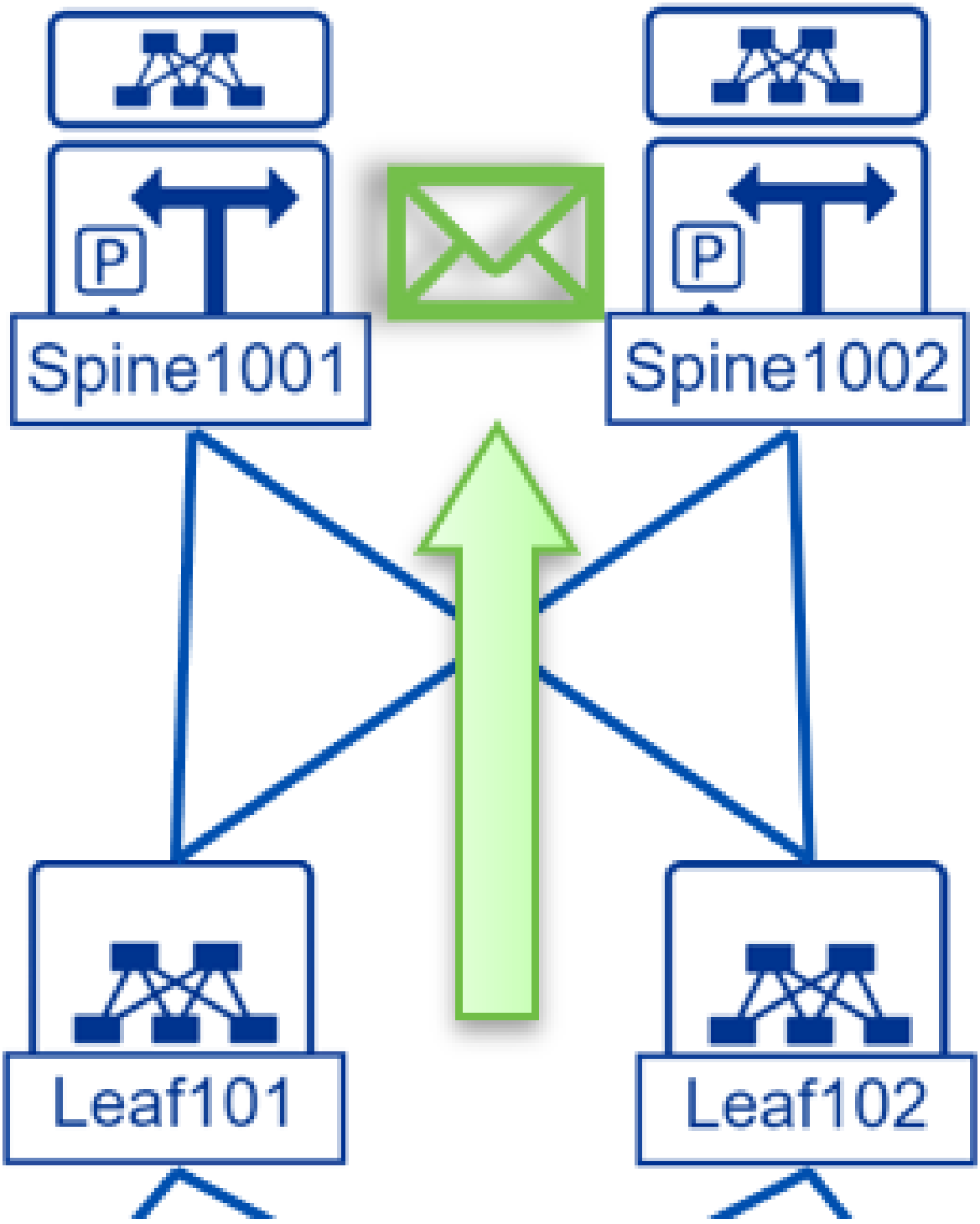
提供された情報から、service_redirオプションが有効なため、パケットがポリシーベースルーティング(PBR)経由でリダイレクトされていることが明らかです。また、sclassとdclassの値を取得します。この特定のシナリオでは、スイッチはdclassを認識します。ただし、宛先エンドポイントがEPMテーブルに存在しない場合、dclass値はデフォルトで1になります。

さらに、入力インターフェイスはSRCIDによって決定され、出力インターフェイスはベクトル値によって識別されます。次の値は、vsh_lcレベルで次のコマンドを実行することによって、前面ポートに変換できます。

<#root>

```
show platform internal hal l2 port gpd
```

2. フローの後続のステップでは、スパインスイッチに到達して宛先MACアドレスをPBRノードにマッピングします。トラフィックはVXLANヘッダーでカプセル化されるため、スパインまたはリモートリーフでELAMを実行するには、in-select 14を使用してカプセル化を正しくデコードする必要があります。



<#root>

SPINE1001#

vsh_lc

module-1#

debug platform internal roc elam asic 0

```
module-1(DBG-elam)#
trigger reset

module-1(DBG-elam)#
trigger init in-select 14 out-selec 0

module-1(DBG-elam-insel14)#
reset

module-1(DBG-elam-insel14)#
set inner ipv4 src_ip 10.10.100.10 dst_ip 10.20.200.20

module-1(DBG-elam-insel14)#
start

module-1(DBG-elam-insel14)#
status

ELAM STATUS
===========
Asic 0 Slice 0 Status Armed
Asic 0 Slice 1 Status Armed
Asic 0 Slice 2 Status Triggered

Asic 0 Slice 3 Status Armed

module-1(DBG-elam-insel14)#
ereport



================================================================================================================
Trigger/Basic Information
================================================================================================================
Incoming Interface :
0x48( 0x48 )  >>> Eth1/1

( Slice Source ID(Ss) in "show plat int hal l2 port gpd" )
Packet from vPC peer LEAF : yes
Packet from tunnel (remote leaf/avs) : yes

----------------------------------------------------------------------------------------------------------------
Outer L2 Header
----------------------------------------------------------------------------------------------------------------
Destination MAC : 000D.0D0D.0D0D
Source MAC : 000C.0C0C.0C0C

----------------------------------------------------------------------------------------------------------------
Inner L2 Header
```

Inner Destination MAC : 0050.56B7.D05D >>> Firewall MAC

Source MAC : AAAA.AAAA.AAAA

Outer L3 Header

L3 Type : IPv4
DSCP : 0
Don't Fragment Bit : 0x0
TTL : 32
IP Protocol Number : UDP
Destination IP : 10.2.64.97
Source IP : 10.2.200.64

Inner L3 Header

L3 Type : IPv4
DSCP : 0
Don't Fragment Bit : 0x1
TTL : 63
IP Protocol Number : ICMP

Destination IP : 10.20.200.20

Source IP : 10.10.100.10

Outer L4 Header

L4 Type : iVxLAN
Don't Learn Bit : 1
Src Policy Applied Bit : 1
Dst Policy Applied Bit : 1

sclass (src pcTag) : 0xc003 >>> pcTag 49155 (Prod-Consumer)

VRF or BD VNID : 15826939(0xF17FFB) >>> BD: Prod-Consumer

Sideband Information

Opcode : OPCODE_UC

---

bky_elam_out_sidebnd_no_spare_vec.

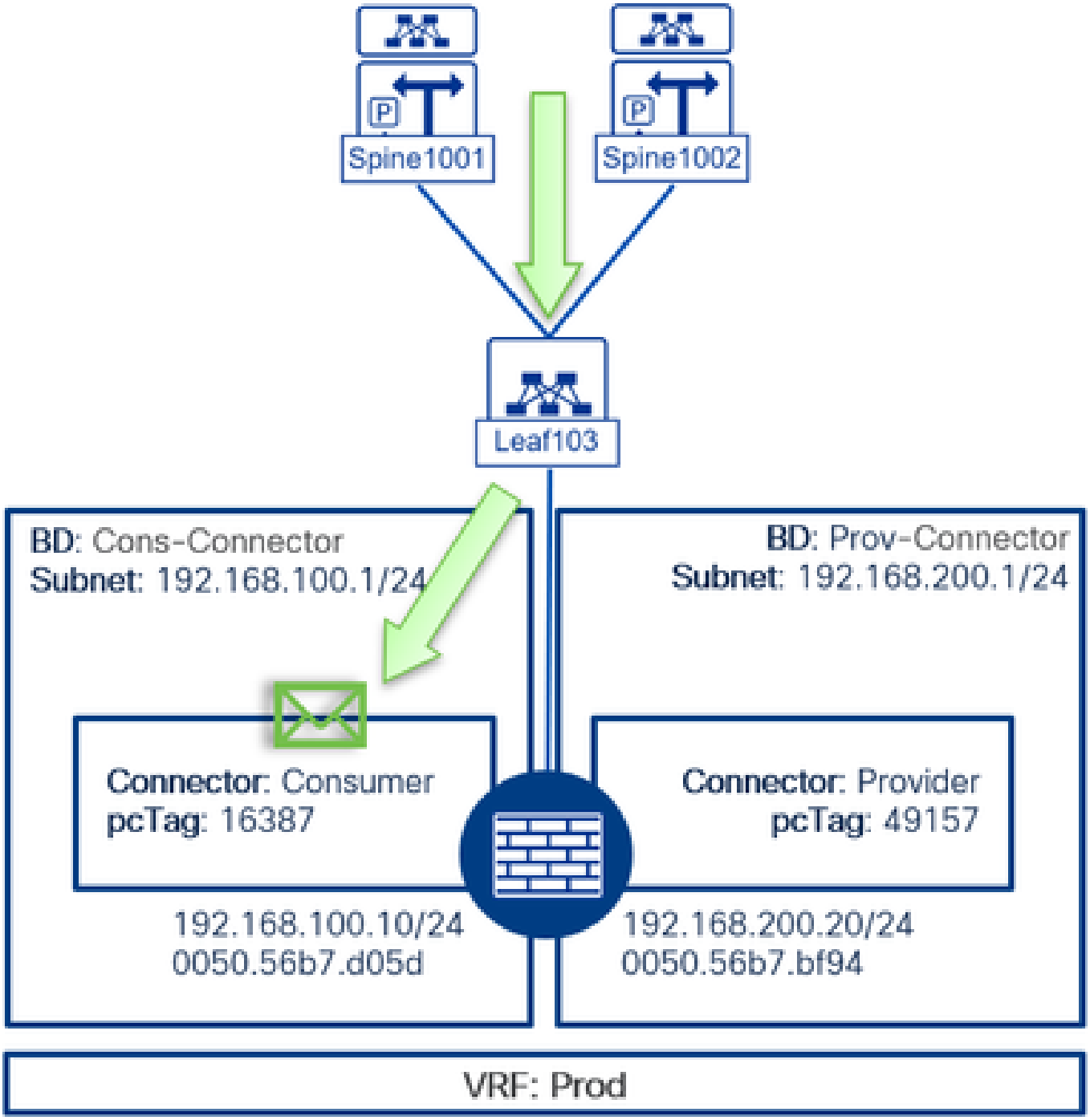
ovector_idx: 0x1F0 >>> Eth1/10

上記の出力から、宛先MACアドレスがファイアウォールのMACアドレスに書き換えられていることがわかります。その後、COOPルックアップが実行されて、MACの宛先パブリッシャが識別され、パケットはスイッチの対応するインターフェイスに転送されます。

ブリッジドメインVNIDとファイアウォールのMACアドレスを使用して次のコマンドを実行すると、このルックアップをスパインでシミュレートできます。

```
<#root>

SPINE1001#

show coop internal info repo ep key 15826939 0050.56B7.D05D | egrep "Tunnel|EP" | head -n 3


EP bd vnid : 15826939
EP mac : 00:50:56:B7:D0:5D

Tunnel nh : 10.2.200.66


SPINE1001#
```

3. トラフィックは、ファイアウォールのMACアドレスが認識されたサービスリーフに到達し、PBRノードに転送されます。



<#root>

MXS2-LF101#

vsh_lc

module-1#

debug platform internal tah elam asic 0

module-1(DBG-elam)#

trigger reset

```
module-1(DBG-elam)#
trigger init in-select 14 out-select 1

module-1(DBG-elam-insel14)#
reset

module-1(DBG-elam-insel14)#
set inner ipv4 src_ip 10.10.100.10 dst_ip 10.20.200.20

module-1(DBG-elam-insel14)#
start

module-1(DBG-elam-insel14)#
status


ELAM STATUS
===========
Asic 0 Slice 0 Status Armed
Asic 0 Slice 1 Status Triggered


module-1(DBG-elam-insel14)#
ereport


================================================================================================================
Trigger/Basic Information
================================================================================================================
Incoming Interface : 0x0( 0x0 ) >>> Eth1/17

( Slice Source ID(Ss) in "show plat int hal l2 port gpd" )
Packet from vPC peer LEAF : yes
Packet from tunnel (remote leaf/avs) : yes

----------------------------------------------------------------------------------------------------------------
Outer L2 Header
----------------------------------------------------------------------------------------------------------------
Destination MAC : 000D.0D0D.0D0D
Source MAC : 000C.0C0C.0C0C

----------------------------------------------------------------------------------------------------------------
Inner L2 Header
----------------------------------------------------------------------------------------------------------------
Inner
Destination MAC : 0050.56B7.D05D >>> Firewall MAC

Source MAC : AAAA.AAAA.AAAA
```

```
------------------------------------------------------------------------------------------------------------
Outer L3 Header
------------------------------------------------------------------------------------------------------------
L3 Type : IPv4
DSCP : 0
Don't Fragment Bit : 0x0
TTL : 32
IP Protocol Number : UDP
Destination IP : 10.2.200.66
Source IP : 10.2.200.64

------------------------------------------------------------------------------------------------------------
Inner L3 Header
------------------------------------------------------------------------------------------------------------
L3 Type : IPv4
DSCP : 0
Don't Fragment Bit : 0x1
TTL : 63
IP Protocol Number : ICMP
```

Destination IP : 10.20.200.20

Source IP : 10.10.100.10

```
------------------------------------------------------------------------------------------------------------
Outer L4 Header
------------------------------------------------------------------------------------------------------------
L4 Type : iVxLAN
Don't Learn Bit : 1
Src Policy Applied Bit : 1
Dst Policy Applied Bit : 1
```

sclass (src pcTag) : 0xc003 >>> pcTag 49155 (Prod-Consumer)

VRF or BD VNID : 15826939(0xF17FFB) >>> BD: Prod-Consumer

```
------------------------------------------------------------------------------------------------------------
Contract Lookup Key
------------------------------------------------------------------------------------------------------------
IP Protocol : ICMP( 0x1 )
L4 Src Port : 2048( 0x800 )
L4 Dst Port : 50664( 0xC5E8 )
```

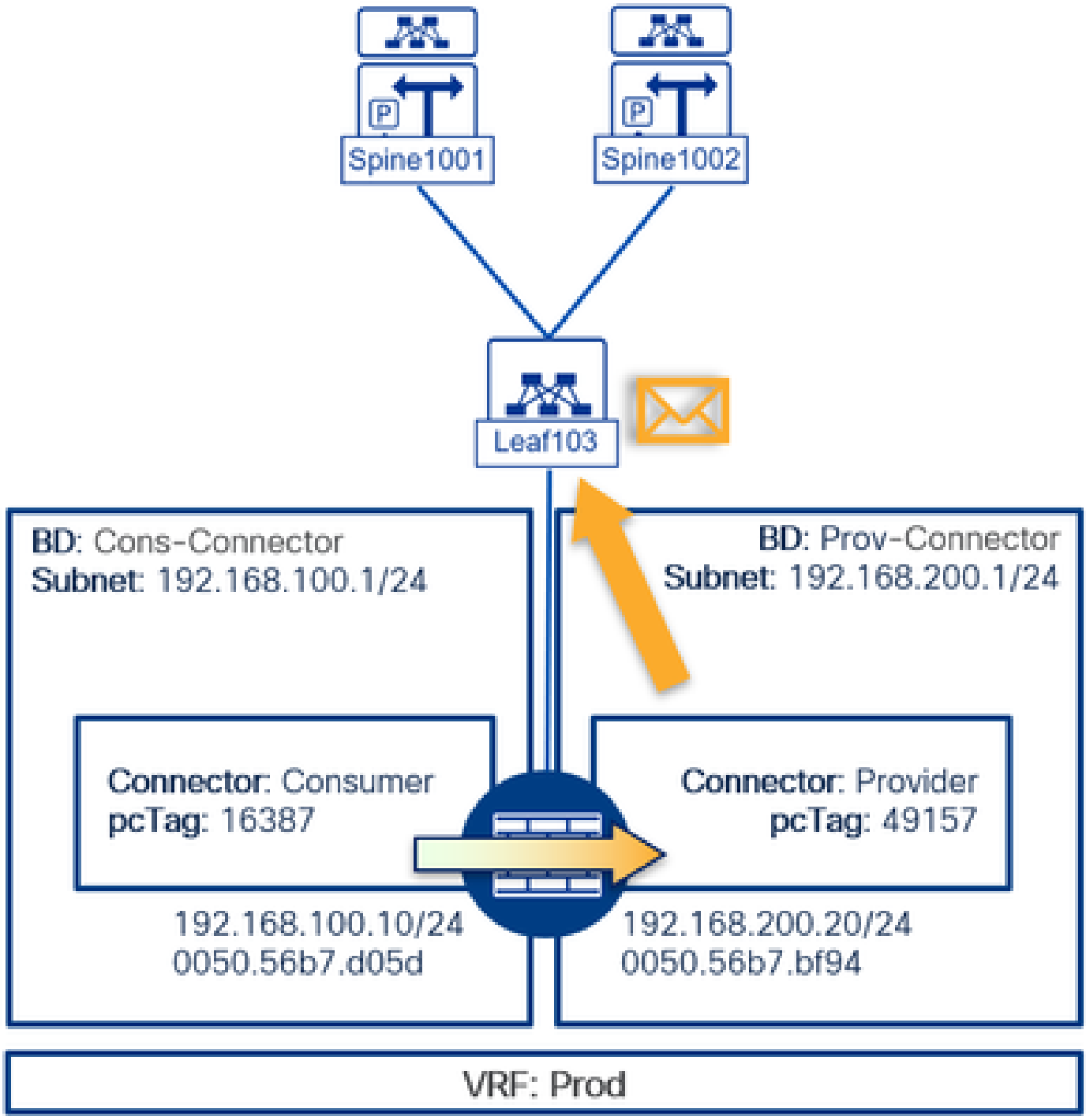
sclass (src pcTag) : 49155(0xC003) >>> Prod-Consumer EPG

dclass (dst pcTag) : 16387(0x4003) >>> Consumer connector EPG

```
src pcTag is from local table : no
derived from group-id in iVxLAN header of incoming packet
Unknown Unicast / Flood Packet : no
If yes, Contract is not applied here because it is flooded

------------------------------------------------------------------------------------------------------------
Sideband Information
```

```
-------------------------------------------------------------------------------------------------------------------
ovector

 :

64( 0x40 ) >>> Eth1/45


Ovec in "show plat int hal l2 port gpd"
Opcode : OPCODE_UC
```

4. PBRノードから返されるパッカーの場合、まず、このノードが自身のディリジェンスを行い、VRF、インターフェイス、またはVLANを変更する必要があります。次に、パケットはプロバイダーコネクタのACIに転送されます。



<#root>

LEAF103#

vsh_lc

module-1#

debug platform internal tah elam asic 0

module-1(DBG-elam)#

trigger reset

```
module-1(DBG-elam)#
trigger init in-select 6 out-select 1

module-1(DBG-elam-insel6)#
reset

module-1(DBG-elam-insel6)#
set outer ipv4 src_ip 10.10.100.10 dst_ip 10.20.200.20

module-1(DBG-elam-insel6)#
 set outer l2 src_mac 0050.56b7.bf94

module-1(DBG-elam-insel6)#
start

module-1(DBG-elam-insel6)#
stat

ELAM STATUS
===========
Asic 0 Slice 0 Status Triggered

Asic 0 Slice 1 Status Armed
module-1(DBG-elam-insel6)#
ereport


================================================================================================================
Trigger/Basic Information
================================================================================================================
...
Incoming Interface : 0x40( 0x40 )


>>> Eth1/45


...

----------------------------------------------------------------------------------------------------------------
Outer L2 Header
----------------------------------------------------------------------------------------------------------------
Destination MAC : 0022.BDF8.19FF
Source MAC : 0050.56B7.BF94

802.1Q tag is valid : yes( 0x1 )
```

CoS : 0(0x0)

Access Encap VLAN : 2006(0x7D6)

Outer L3 Header

L3 Type : IPv4
IP Version : 4
DSCP : 0
IP Packet Length : 84 (= IP header(28 bytes) + IP payload)
Don't Fragment Bit : set
TTL : 62
IP Protocol Number : ICMP
IP CheckSum : 46178(0xB462)

Destination IP : 10.20.200.20

Source IP : 10.10.100.10

Contract Lookup Key

IP Protocol : ICMP(0x1)
L4 Src Port : 2048(0x800)
L4 Dst Port : 37489(0x9271)

sclass (src pcTag) : 49157(0xC005) >>> Provider connector EPG

dclass (dst pcTag) : 49156(0xC004)

>>> Prod-Provider EPG

src pcTag is from local table : yes
derived from a local table on this node by the lookup of src IP or MAC
Unknown Unicast / Flood Packet : no
If yes, Contract is not applied here because it is flooded

Sideband Information

---

ovector : 176(0xB0) >>> Eth1/52

Ovec in "show plat int hal l2 port gpd"
Opcode : OPCODE_UC

---

sug_luc_latch_results_vec.luc3_0.

service_redir: 0x0

---

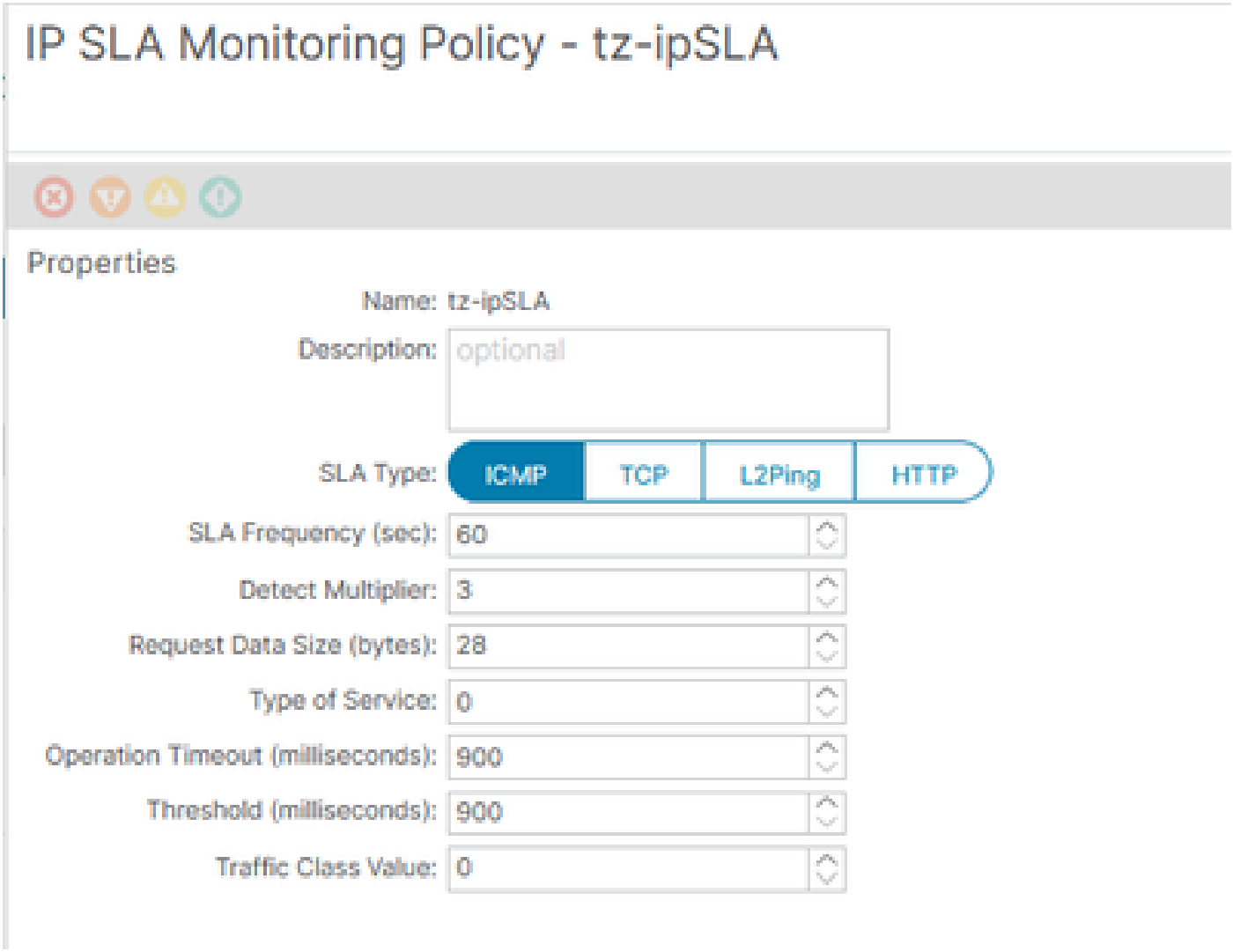
5. 残りのネットワークトラフィックは、これまでに説明した手順（パケットがスパインスイッチに戻り、coopルックアップに基づいて最終的なサーバ宛先が決定される）に従います。その後、パケットはローカル学習フラグを持つコンピューティングリーフスイッチに送信され、スパインのCOOPテーブルにこの情報を伝達します。ステップ2とステップ3のELAMの実行は、最終的な宛先へのパケットの配布に関して一貫しています。正確な配信を保証するには、これらを宛先EPGのpcTagと出力インターフェイスで検証することが不可欠です。

IP SLA

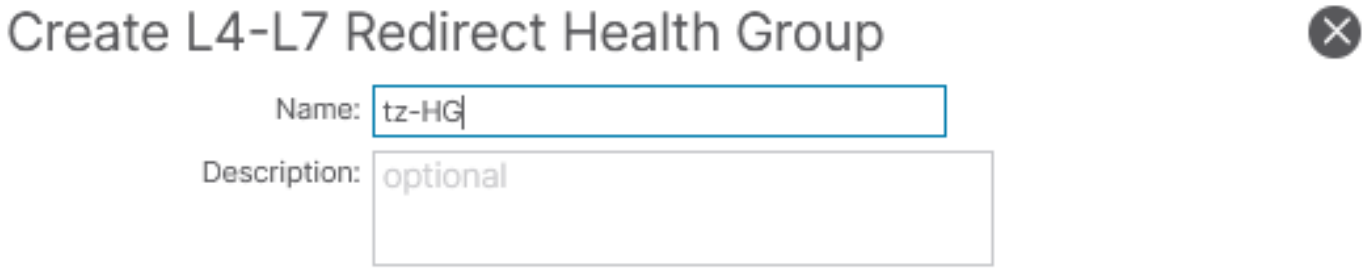
IP SLAは、ネットワークパスの動作ステータスとパフォーマンスを評価するために使用されます。リアルタイムネットワークの状態に基づいて、定義されたポリシーに従ってトラフィックが効率的にルーティングされるようにします。ACIでは、PBRはIP SLAを活用して、情報に基づいたルーティングの決定を行います。IP SLAメトリックにパスのパフォーマンスが低下していることが示されている場合、PBRは必要なパフォーマンス基準を満たす代替パスを介してトラフィックを再ルーティングできます。

バージョン5.2(1)以降では、IP SLAのダイナミックMACトラッキングを有効にできます。これは、PBRノードがフェールオーバーし、同じIPアドレスのMACアドレスを変更するシナリオに役立ちます。スタティックな導入では、トラフィックの送信を続行するためにPBRノードがMACアドレスを変更するたびに、ポリシーベースのリダイレクトポリシーの変更を行う必要があります。IP SLAでは、このポリシーで使用されるMACアドレスがプローブ応答にリレーされます。このドキュメントの執筆時点で、PBRノードが正常であるかどうかを判断するために、ICMP、TCP、L2Ping、HTTPなどの各種プローブを使用できます。

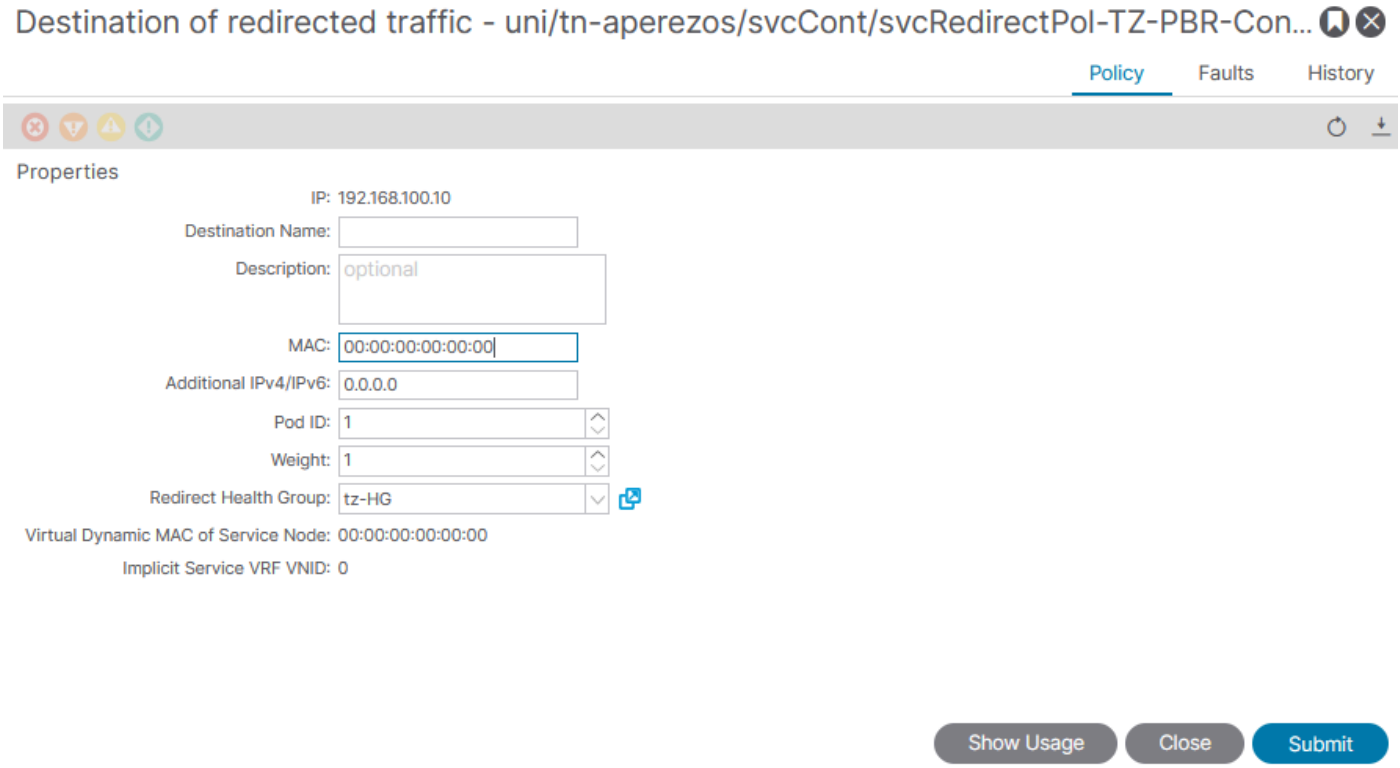
IP SLAポリシーの一般的な設定は次のようになります。



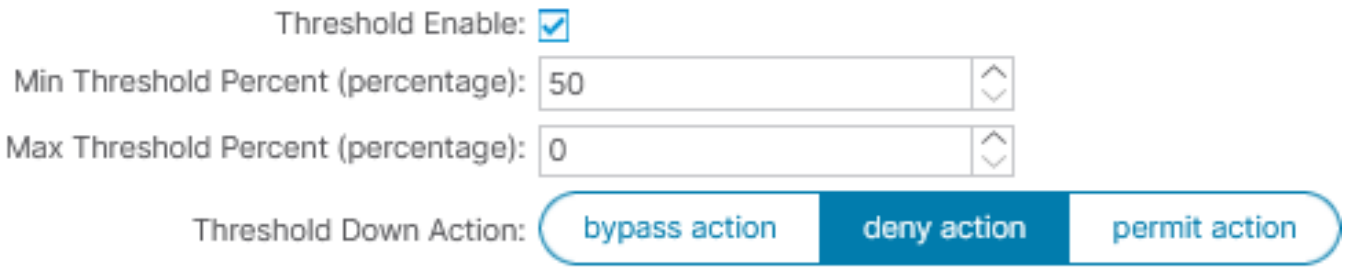
IP SLAポリシーは、ヘルスグループを使用してPBRノードIPにマッピングする必要があります。



MACアドレスを動的に検出するIP SLAが使用される場合、このフィールドは空ではなく、すべて0に設定されます。



L4-L7ポリシーベースのリダイレクトポリシーで、L3宛先を介してHealth GroupがPBRノードIPと関連付けられると、到達不能時のIP SLA動作を定義するためのしきい値を設定します。リダイレクションを維持するために必要なアクティブL3宛先の最小数を指定します。ライブPBRノードの数がしきい値のパーセンテージを下回るか、超える場合、選択されたしきい値ダウンアクションによってグループ全体が影響を受け、再配布が停止されます。このアプローチは、トラフィックフローに影響を与えずに、トラブルシューティング中のPBRノードのバイパスをサポートします。



同一のHealth Groupポリシーが使用される限り、1つのL4-L7ポリシーベースリダイレクトポリシーまたは複数のL4-L7ポリシーベースリダイレクトポリシーのL3宛先で定義されたすべてのIPは、Health Groupによってバインドされます。

```
Leaf101# show service redir info health-group aperezos::tz-HG
==========================================================================================================
LEGEND
TL: Threshold(Low) | TH: Threshold(High) | HP: HashProfile | HG: HealthGrp | BAC: Backup-Dest | TRA: Tr
==========================================================================================================
HG-Name HG-OperSt HG-Dest HG-Dest-OperSt
======= ========== ======= ==============
aperezos::tz-HG enabled dest-[192.168.100.10]-[vxlan-2162692]] up
                        dest-[192.168.200.20]-[vxlan-2162692]] up
```

```
Leaf1011#
```

関連情報

- Cisco Application Centric Infrastructure Policy-Based Redirect Service Graph Designホワイトペーパー
- ACIレイヤ4-7ポリシーベースリダイレクト(PBR)の詳細とヒント（Cisco Liveプレゼンテーション）
- マルチポッドPBRでのIP SLAのトラブルシューティング

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。