# Solução de problemas do PBR na ACI

## Contents



## Introdução

Este documento descreve como solucionar problemas de ambientes da Application Centric Infrastructure (ACI) com Policy-Based Redirect (PBR) em uma única estrutura de pod.

## Pré-requisitos

### Requisitos

Para este artigo, é recomendável que você tenha conhecimento geral destes tópicos:

- Conceitos da ACI: Políticas de acesso, Aprendizado de endpoint, Contratos e L3out

### Componentes Utilizados

Este exercício de solução de problemas foi realizado na versão 6.0(8f) da ACI usando switches Nexus de segunda geração N9K-C93180YC-EX e N9K-C93240YC-FX2.

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.

### Abreviaturas

- BD: Domínio de bridge
- EPG: Grupo de endpoints
- ID da classe: Marca que identifica um EPG
- Nó PBR: Dispositivo L4-L7 usado para um destino PBR
- Conector do consumidor: Interface de nó PBR voltada para o lado do consumidor
- Conector do provedor: Interface de nó PBR voltada para o provedor

## Histórico de PBR

| Versão | Principais recursos |
|---|---|
| 2.0(1m) | • Os gráficos de serviço fornecem o recurso PBR. |
| 3.x e anterior | • Suporte a redirecionamento baseado em política (PBR - Policy-Based Redirect) de vários nós<br>• Hashing resiliente de PBR |
| 3.2(x) | • O Firewall PBR de um nó é suportado em ambientes de vários locais. |
| 4.0(x) | • O Firewall PBR de dois nós é compatível com ambientes de vários locais. |
| 4.2(1) | • Agora há suporte para uma política de backup para a criação de nós PBR em standby. |
| 4.2(3) | • A opção Filtrar a partir do contrato está disponível no modelo Gráfico de serviços usando a GUI. |
| 5.0(1) | • L3Outs são suportados em todos os lados do provedor dos nós de serviço.<br>• Os caminhos de implantação ativa-ativa/ECMP são compatíveis com dispositivos PBR de Camada 1/Camada 2. |
| 5.2(1) | • Um destino de PBR agora pode estar em uma L3Out.<br>• Você pode rastrear nós de serviço usando o URI HTTP.<br>• Não há mais suporte para os modos gerenciado e híbrido do gráfico de serviço.<br>• O endereço MAC do nó PBR dinâmico é suportado. |
| 6.0(1) | • Redirecionamento baseado em política simétrico (PBR - Policy-Based Redirect) baseado em peso |

### Considerações do projeto

- O PBR funciona com dispositivos físicos e virtuais
- O PBR pode ser usado entre EPGs L3Out e EPGs, entre EPGs e entre EPGs L3Out. PBR não é suportado se L2Out EPG faz parte do contrato
- O PBR é compatível com ambientes Cisco ACI Multi-Pod, Multi-Site e Remote Leaf.
- A estrutura da Cisco ACI deve ser o gateway para os servidores e para o nó PBR
- O dispositivo L4-L7 deve ser implantado no modo ir para (modo roteado)
- O nó PBR não é suportado em switches FEX
- Um domínio de Bridge dedicado é necessário para o nó PBR
- O endereço MAC dinâmico para o nó PBR agora é suportado usando grupos de funcionamento.
- Recomenda-se ativar a detecção baseada em GARP no domínio de ponte de nó PBR
- O filtro padrão comum que inclui ARP, tráfego ethernet e outro tráfego não IP não deve ser usado para PBR
- O nó de PBR pode estar entre instâncias de VRF ou dentro de uma das instâncias de VRF. Para essa topologia, o nó PBR não é suportado para estar em um terceiro VRF, deve ser configurado no VRF do consumidor ou do provedor

## Informações de Apoio

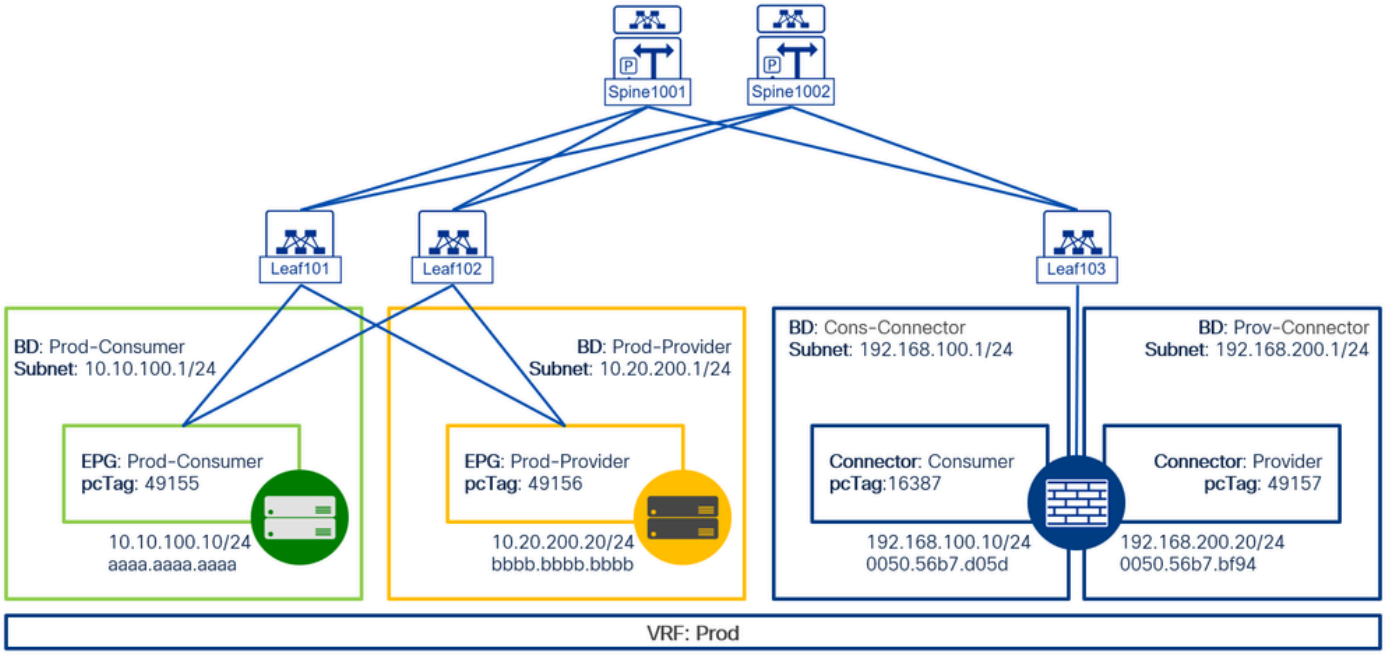
É possível encontrar explicações mais detalhadas sobre o ELAM e o Ftriage na biblioteca CiscoLive On-Demand na sessão BRKDCN-3900b.

Além disso, todas as diretrizes de configuração podem ser encontradas no white paper Cisco Application Centric Infrastructure Policy-Based Redirect Service Graph Design White Paper.

## Cenário: VRF único em uma única malha de pods

### Diagrama de Rede

Topologia física:




## Troubleshooting

Passo 1: Falhas

A ACI gera uma falha quando há um problema com a configuração ou com as interações de política. Falhas específicas foram identificadas para o processo de renderização de PBR em caso de falha:

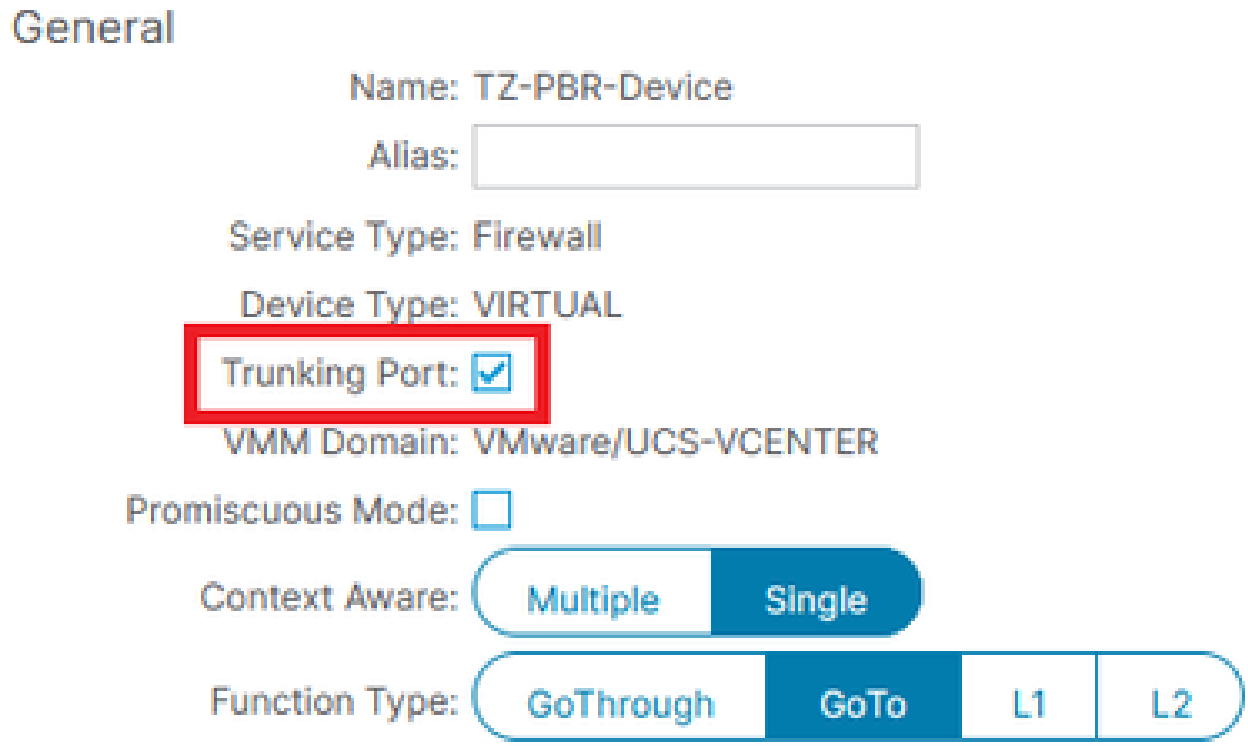
F1690: A configuração é inválida devido a:

- Falha na alocação de ID

  Essa falha significa que a VLAN encapsulada para o nó de serviço não está disponível. Por exemplo, não poderia haver VLAN dinâmica disponível no pool de VLANs associado ao domínio do Virtual Machine Manager (VMM) utilizado pelo dispositivo lógico.

  Resolução: Verifique o pool de VLANs dentro do domínio empregado pelo Dispositivo Lógico. Se a interface do Dispositivo Lógico estiver dentro de um domínio físico, inspecione também a configuração de VLAN encapsulada. Essas configurações podem ser encontradas em Locatário > Serviços > L4-L7 > Dispositivos e Malha > Políticas de acesso > Pools > VLAN.

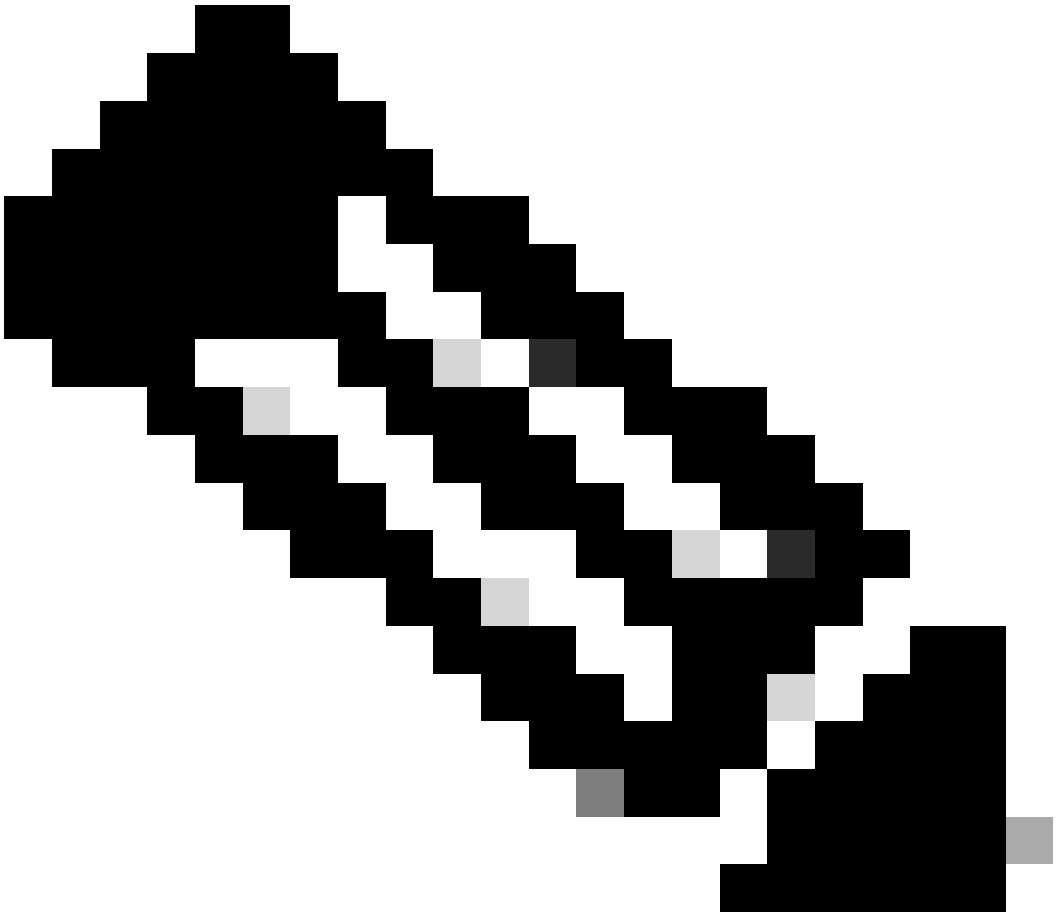
  Por outro lado, se a interface do dispositivo lógico residir em um domínio virtual e se conectar aos hosts ESXi por meio de uma interface de tronco, certifique-se de que a opção de porta de entroncamento esteja ativada.




- Nenhum contexto de dispositivo encontrado para LDev

Essa falha indica que o dispositivo lógico não pode ser localizado para a renderização do gráfico de serviço. Por exemplo, não poderia haver nenhuma política de seleção de dispositivo que corresponda ao contrato associado ao gráfico de serviço.

Resolução: Verifique se uma Política de Seleção de Dispositivo está definida. A Política de seleção de dispositivos especifica os critérios de seleção para um dispositivo de serviço e seus conectores, com base no nome do contrato, no nome do Gráfico de serviço e no nome do nó dentro do Gráfico de serviço. Isso pode ser encontrado em Locatário > Serviços > L4-L7 > Política de Seleção de Dispositivo.

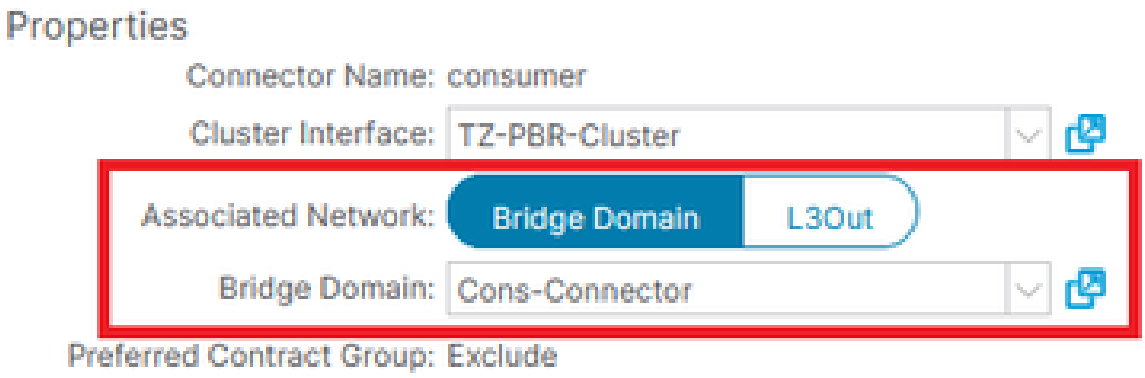


Note: Quando você implanta um modelo de gráfico de serviço, a ACI pré-seleciona o domínio de bridge para o EPG de origem. Você deve alterar esse domínio de ponte para o conector de consumidor PBR. O mesmo se aplica ao conector do provedor.

- Nenhum BD encontrado

  Essa falha indica que o domínio de ponte (BD) do nó de serviço não pode ser localizado. Por exemplo, o BD não é especificado na Política de Seleção de Dispositivo.

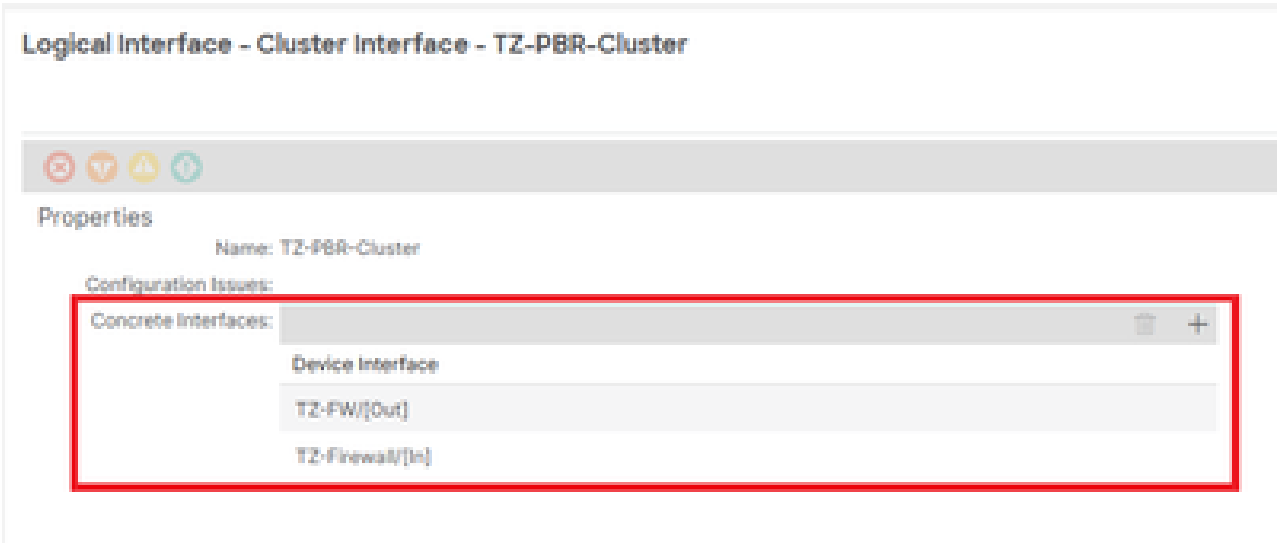
  Resolução: Verifique se o BD está especificado na Política de Seleção de Dispositivo e se o nome do conector está correto. Esta configuração está localizada em Locatário > Serviços > L4-L7 > Política de seleção de dispositivos > [ Contrato + SG ] > [ Consumidor | Provedor ].




- LIf não tem relação com CIf e LIf tem um CIf inválido
- Nenhuma interface de cluster encontrada

  Essas falhas indicam que o dispositivo não tem relação com as interfaces de cluster.

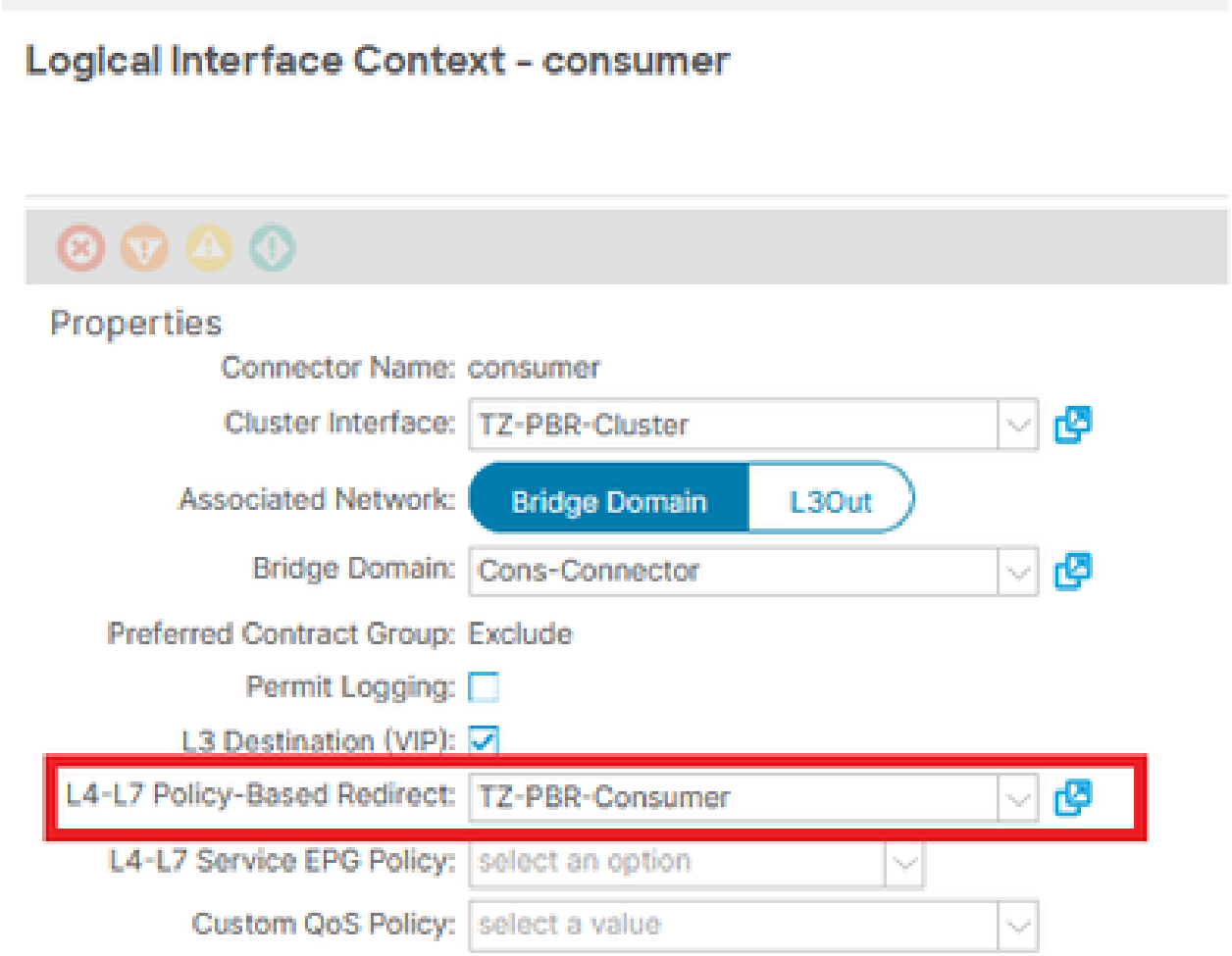
  Resolução: Certifique-se de que a configuração do dispositivo da Camada 4 para a Camada 7 (L4-L7) inclua um seletor de interface concreto especificado. Esta configuração está localizada em Locatário > Serviços > L4-L7 > Dispositivos > [ Dispositivo ] > Interfaces de cluster.




- Política de redirecionamento de serviço inválida

  Essa falha significa que a política de PBR não foi aplicada, apesar do redirecionamento ser ativado na função de serviço no Gráfico de serviço.

  Resolução: Certifique-se de que a política PBR esteja configurada dentro das configurações da Política de Seleção de Dispositivo. Esta configuração está localizada em Locatário > Serviços > L4-L7 > Política de seleção de dispositivos > [ Contrato + SG ] > [ Consumidor | Provedor ].




F0759 graph-rendering-failure - o "Service graph for tenant < tenant > não pôde ser instanciado. A configuração do nó de função < nó > é inválida."

Não foi possível criar uma instância do gráfico de serviço para o locatário especificado devido a uma configuração inválida do nome do nó de função.

Esse erro sugere que há problemas de configuração relacionados às condições acima mencionadas.

Além disso, durante as implantações iniciais, essa falha pode surgir temporariamente e ser resolvida imediatamente. Isso ocorre devido ao processo de renderização pelo qual a ACI passa para implantar todas as políticas.

Resolução: Investigue quaisquer falhas adicionais que tenham sido relatadas e resolva-as adequadamente.

F0764: falha de configuração - "A configuração de dispositivos L4-L7 < dispositivo > para o locatário < locatário > é inválida."

Não foi possível criar uma instância do gráfico de serviço para o locatário especificado devido a uma configuração inválida da política de Dispositivo PBR.

Esse erro sugere que há problemas de configuração relacionados às condições acima mencionadas.

Resolução: Investigue quaisquer falhas adicionais que tenham sido relatadas e resolva-as adequadamente.

F0772 falha de configuração - "A configuração de LIf < cluster > para dispositivos L4-L7 < dispositivo > para locatário < locatário > é inválida."

Não foi possível criar uma instância do gráfico de serviço para o locatário especificado devido a uma configuração inválida da seleção de interface do Cluster de Dispositivo PBR.

Esse erro sugere que há problemas de configuração relacionados às condições acima mencionadas.

Resolução: Investigue quaisquer falhas adicionais que tenham sido relatadas e resolva-as adequadamente.

Passo 2: Aprendizado de endpoint de origem e destino

Certifique-se de que os endpoints de origem e de destino sejam reconhecidos na malha, o que requer configuração básica:

- Um objeto Virtual Routing and Forwarding (VRF).
- Um objeto de domínio de ponte (BD) com roteamento unicast habilitado. Embora a habilitação do aprendizado do plano de dados IP seja considerada uma prática recomendada, ela não é obrigatória.
- Um objeto Endpoint Group (EPG), aplicável a domínios físicos e virtuais.
- Políticas de acesso: Verifique se a cadeia de configuração da política de acesso está completa e se nenhuma falha foi relatada no EPG.

Para confirmar o aprendizado do endpoint no EPG e na interface corretos, execute este comando na folha onde o endpoint é aprendido, também conhecido como folha de computação:

<#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#
```

Esse comando permite identificar o pcTag (class) associado ao EPG no qual o endpoint é classificado, bem como recuperar as informações de interface, escopo de VRF e endereço MAC.

Se você não souber o local do endpoint de origem ou de destino, sempre poderá se ajudar com esse comando no APIC:

<#root>

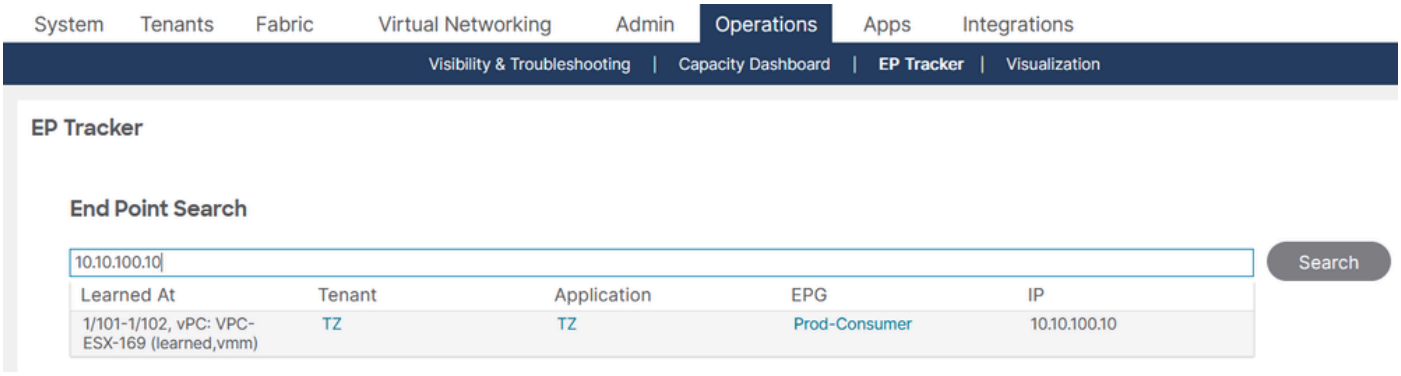
```
show endpoint [ ip | mac ] [ x.x.x.x | eeee.eeee.eeee ]
```

<#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#
```

Na GUI, o recurso EP Tracker pode ser acessado navegando para Operations > EP Tracker para monitoramento e gerenciamento de endpoint.




Com as informações coletadas de endpoints de origem e destino, você pode se concentrar na implantação da política de PBR.

Passo 3: Redirecionar contrato

O PBR está integrado à estrutura do Service Graph. Consequentemente, um modelo de Gráfico de serviço deve ser implantado e configurado nos switches de origem e destino de acordo com um contrato. Utilizando as informações de pcTags coletadas na etapa anterior, você pode determinar se um grupo de endpoint (EPG) está sendo redirecionado para um grupo de gráfico de serviço executando esse comando.

<#root>

```
show zoning-rule scope [ vrf_scope ]
```

Nas regras de zoneamento, essas regras devem ser consideradas:

1. EPG de origem para EPG de destino com um grupo de redirecionamento associado
2. EPG de sombra de nó PBR de origem para EPG de origem
3. EPG de destino para EPG de origem com um grupo de redirecionamento associado. Esse grupo pode ser idêntico ou diferente da configuração anterior.
4. EPG de sombra de nó PBR de destino para EPG de destino

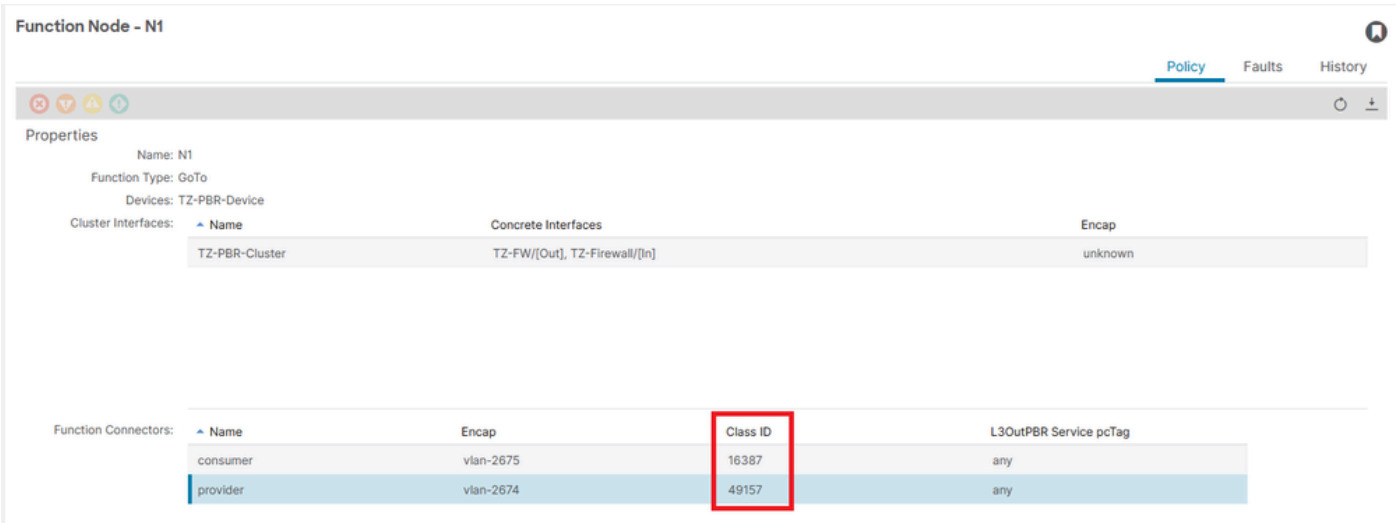
<#root>

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#
```

Para verificar o pcTag dos EPGs de sombra criados durante o processo de implantação do Roteamento baseado em política (PBR), navegue para Locatários > [ TENANT_NAME ] > Serviços > L4-L7 > Instância do gráfico implantado > [ SG_NAME ] > Nó de função - N1.




- Analisador de contrato

O script correlaciona regras de zoneamento, filtros, estatísticas e nomes de EPG. Você pode executar esse script com segurança diretamente em uma folha de ACI ou APIC. Quando executado no APIC, ele coleta objetos concretos em todos os switches leaf, o que pode levar vários minutos para grandes implantações de políticas.

Começando com a versão 3.2 do ACI, o contract_parser é incluído na imagem e está disponível no leaf. Basta digitar contract_parser.py a partir do shell iBash.

<#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#
```

Esse comando fornece detalhes como a ação do contrato, os EPGs de origem e destino, o nome do contrato em uso e a contagem de ocorrências.

Passo 4: Grupo de Redirecionamento

Após identificar o grupo de redirecionamento com base no contrato aplicado às regras de zoneamento, a próxima etapa é determinar os endereços IP e MAC dos dispositivos que serão direcionados para redirecionamento. Para ajudar com isso, execute o comando:

<#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: Tra
================================================================================================================
GrpID Name      destination                              HG-name        BAC W   operSt  operStQual   TL  TH
===== ====      ===========                              ============== === === ======= ============ === ===
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#
```

Esse comando nos permite determinar o status operacional (OperSt) de nosso grupo de redirecionamento, o endereço IP configurado na seção PBR de L4-L7 e o VNID do VRF associado aos domínios de bridge do nó PBR. Agora você precisa determinar o endereço MAC configurado:

<#root>

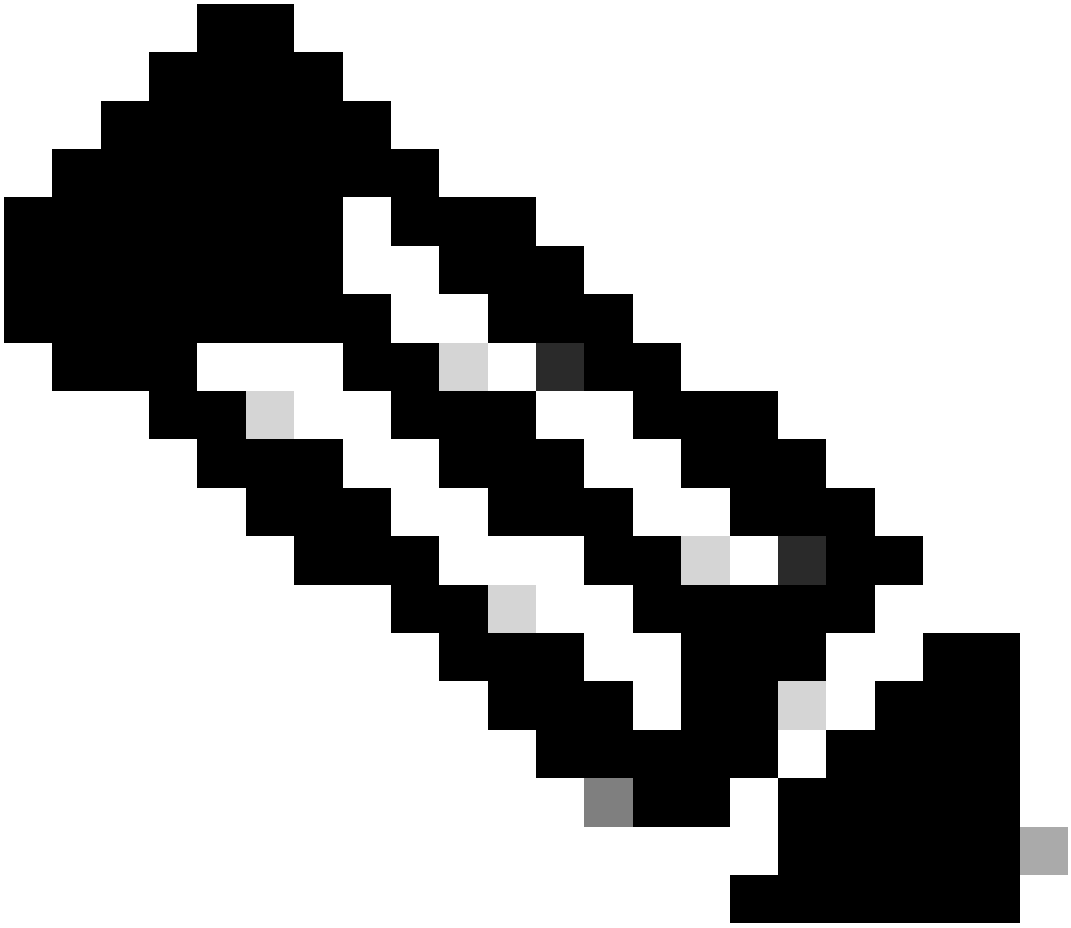
```
show service redir info destinations ip [ PBR-node IP ] vnid [ VRF_VNID ]
```

<#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-
====                                    ======         ====              ====    =====   =========    ====
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#
```

Além dos detalhes mencionados anteriormente, esse comando fornece informações valiosas, incluindo o nome VRF, BD VNID e o endereço MAC configurado do nó PBR.



Note: É importante observar que os endereços IP e MAC são configurados pelo usuário nesse estágio, o que significa que podem ocorrer erros tipográficos durante a definição de Roteamento Baseado em Políticas de L4-L7.

Passo 5: O nó PBR não está recebendo nenhum tráfego.

Um problema predominante encontrado com o encaminhamento PBR é a ausência de tráfego que chega ao nó PBR. Uma causa frequente desse problema é um endereço MAC especificado incorretamente na configuração de Roteamento Baseado em Políticas de L4-L7.

Para verificar a precisão do endereço MAC configurado no Roteamento Baseado em Políticas de L4-L7, execute o comando utilizado anteriormente da Etapa 2. Esse comando pode ser executado no switch leaf designado como o leaf de serviço, onde se espera que o nó seja aprendido.

<#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#
```

Verifique se o endereço MAC registrado na tabela EPM corresponde ao configurado no grupo de redirecionamento de serviço. Até mesmo erros tipográficos menores devem ser corrigidos para garantir o roteamento adequado do tráfego para o destino do nó PBR.

Passo 6: Fluxo de tráfego.

- FTRIAGEM

Uma ferramenta de CLI para o APIC projetada para automatizar a configuração e a interpretação de processos ELAM de ponta a ponta. A ferramenta permite que os usuários especifiquem um fluxo específico e o switch de folha onde o fluxo se origina. Executa sequencialmente ELAMs em cada nó para analisar o caminho de encaminhamento do fluxo. Essa ferramenta é especialmente útil em topologias complexas em que o caminho do pacote não é facilmente discernível.

<#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:

O Embedded Logic Analyzer Module (ELAM) é uma ferramenta de diagnóstico que permite aos usuários estabelecer condições específicas no hardware para capturar o pacote ou quadro inicial

que atende a esses critérios. Quando uma captura é bem-sucedida, o status do ELAM é indicado como acionado. Após o acionamento, o ELAM é desativado, permitindo que um despejo de dados seja coletado, o que facilita a análise das numerosas decisões de encaminhamento executadas pelo ASIC do switch para esse pacote ou quadro. O ELAM opera no nível ASIC, garantindo que não afete a CPU ou outros recursos do switch.

Estrutura da sintaxe do comando. Essa estrutura foi coletada do livro Troubleshoot ACI IntraFabric Forwarding Tools (Solucionar problemas das ferramentas de encaminhamento de estrutura da ACI)

```
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]
```

Definir condições para disparar

```
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]
```

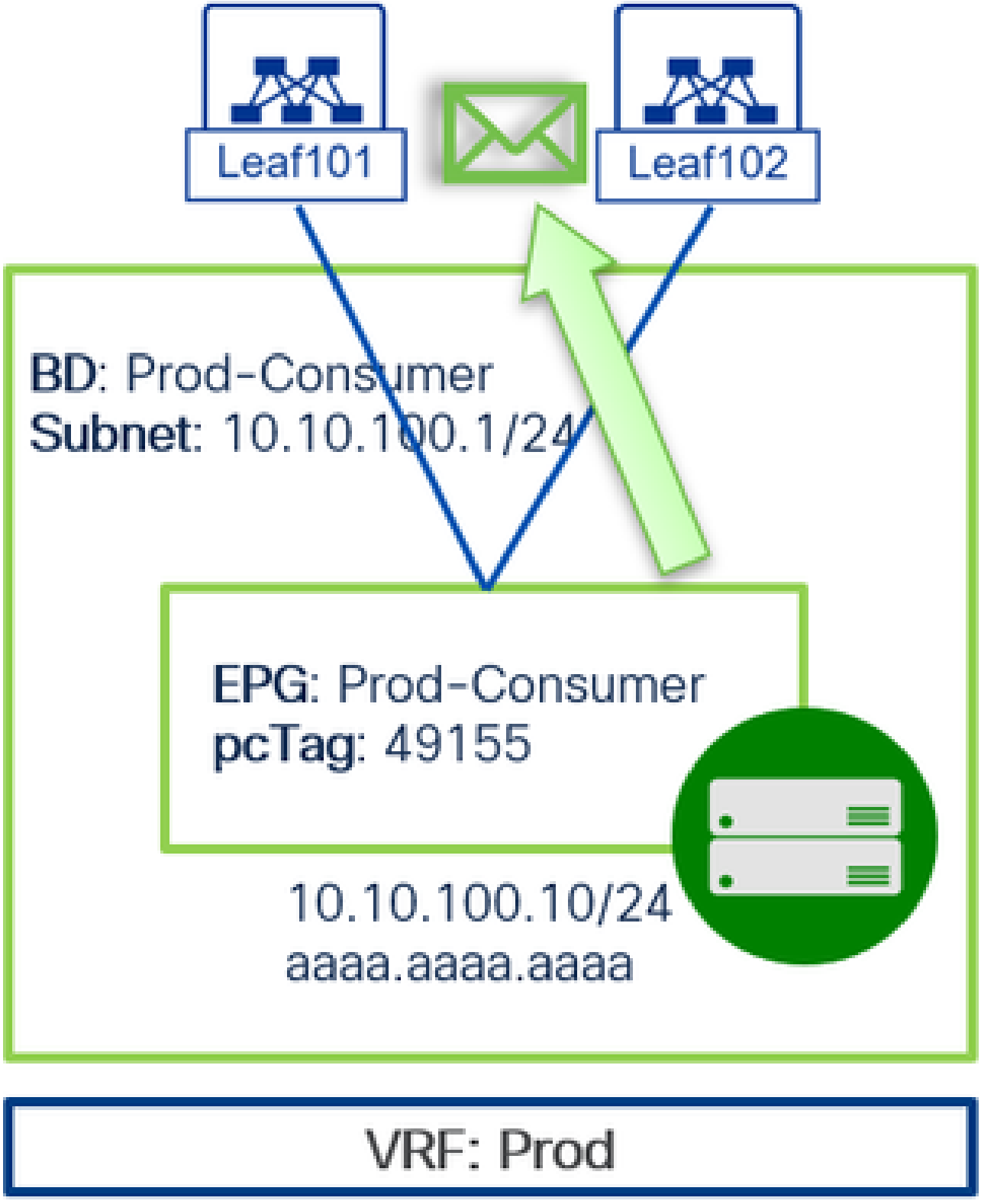
Gere o despejo que contém a análise do pacote.

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

- Fluxo de tráfico

É crucial compreender o fluxo de tráfego em todos os dispositivos em questão. A ferramenta Ftriagem fornece um excelente resumo desse fluxo. No entanto, para obter uma validação detalhada passo a passo e obter insights mais profundos sobre o processo de recepção de pacotes, você pode executar o ELAM (Embedded Logic Analyzer Module) em cada ponto da topologia de rede.

1. O tráfego de entrada ocorre na folha de computação onde o servidor de origem é aprendido. Neste cenário específico, como a origem é posicionada atrás de uma interface vPC, o ELAM deve ser configurado nos peers do vPC. Isso é necessário porque a interface física selecionada pelo algoritmo de hash é indeterminada.




<#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


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

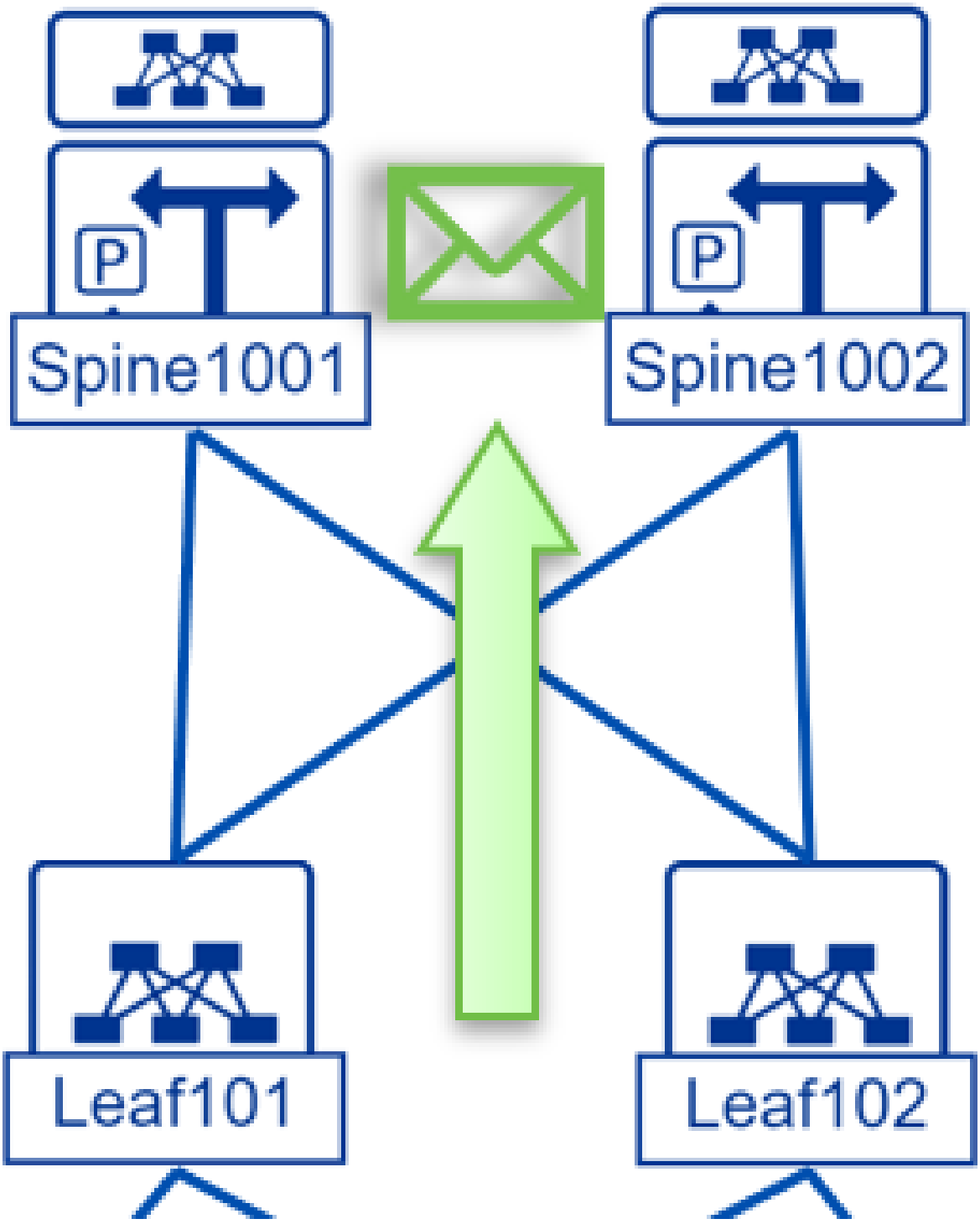
Com base nas informações fornecidas, é evidente que o pacote está sendo redirecionado através do Roteamento Baseado em Políticas (PBR - Policy-Based Routing), pois a opção service_redir está habilitada. Além disso, você recupera os valores class e dclass. Neste cenário específico, o switch reconhece a classe. No entanto, se o ponto final de destino não estiver presente na tabela EPM, o valor de dclass assumirá 1 como padrão.

Além disso, a interface de entrada é determinada pelo SRCID e a interface de saída é identificada pelos valores vetoriais. Esses valores podem ser convertidos em uma porta frontal executando-se este comando no nível vsh_lc:

<#root>

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

2. A etapa subsequente no fluxo envolve acessar o switch spine para mapear o endereço MAC de destino para o nó PBR. Como o tráfego é encapsulado em cabeçalhos VXLAN, a execução do ELAM em uma lombada ou folha remota requer o uso da seleção interna 14 para decodificar corretamente o encapsulamento.




<#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**

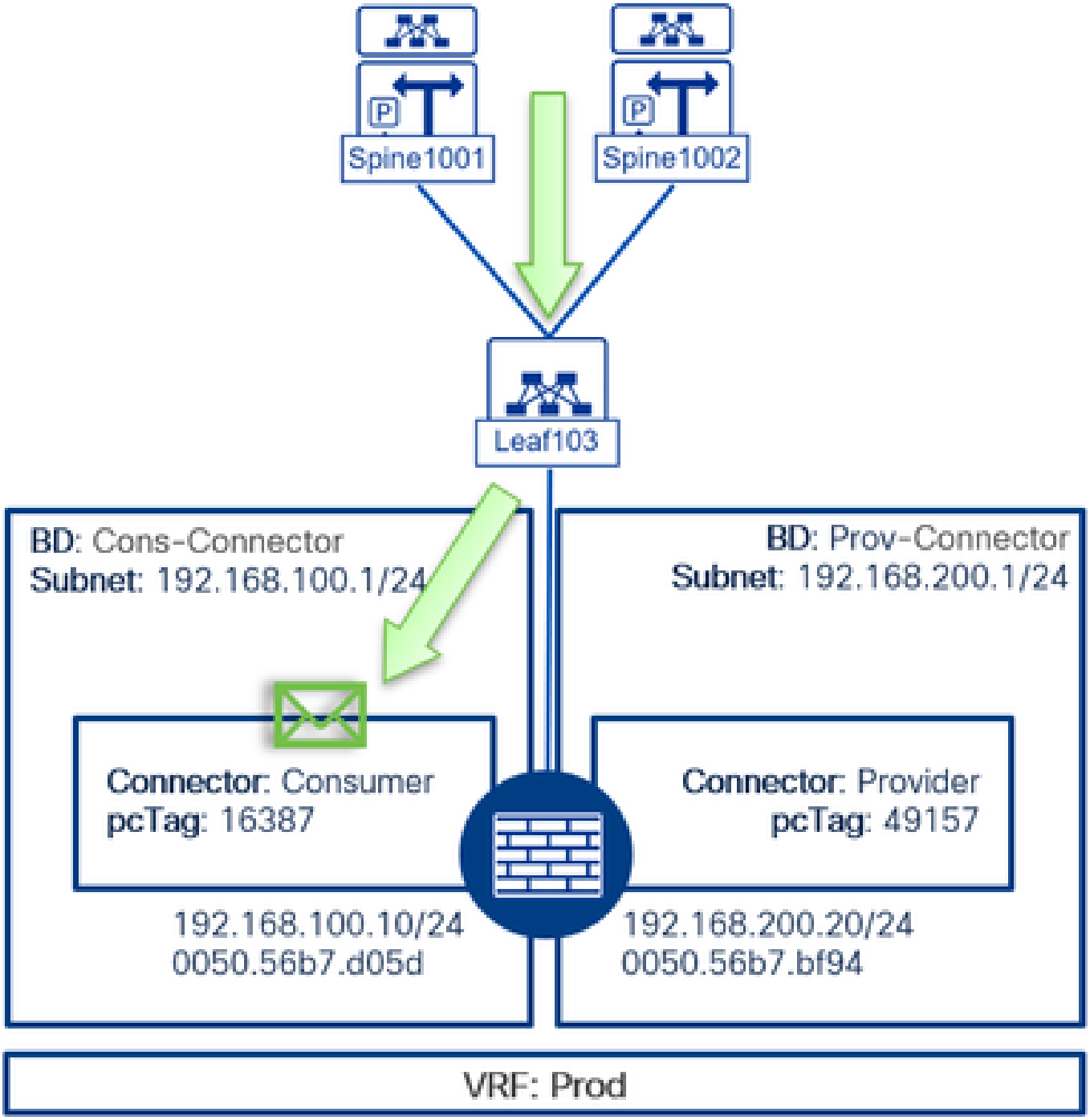
---

A partir da saída anterior, é evidente que o endereço MAC destino é regravado no endereço MAC do firewall. Subsequentemente, uma pesquisa de COOP é executada para identificar o editor de destino do MAC, e o pacote é encaminhado para a interface correspondente do switch.

Você pode simular essa pesquisa no spine executando esse comando, utilizando o VNID de domínio de bridge e o endereço MAC do firewall:

```
<#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. O tráfego alcança o leaf de serviço onde o endereço MAC do firewall é reconhecido e subsequentemente encaminhado ao nó PBR.




<#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 )
```

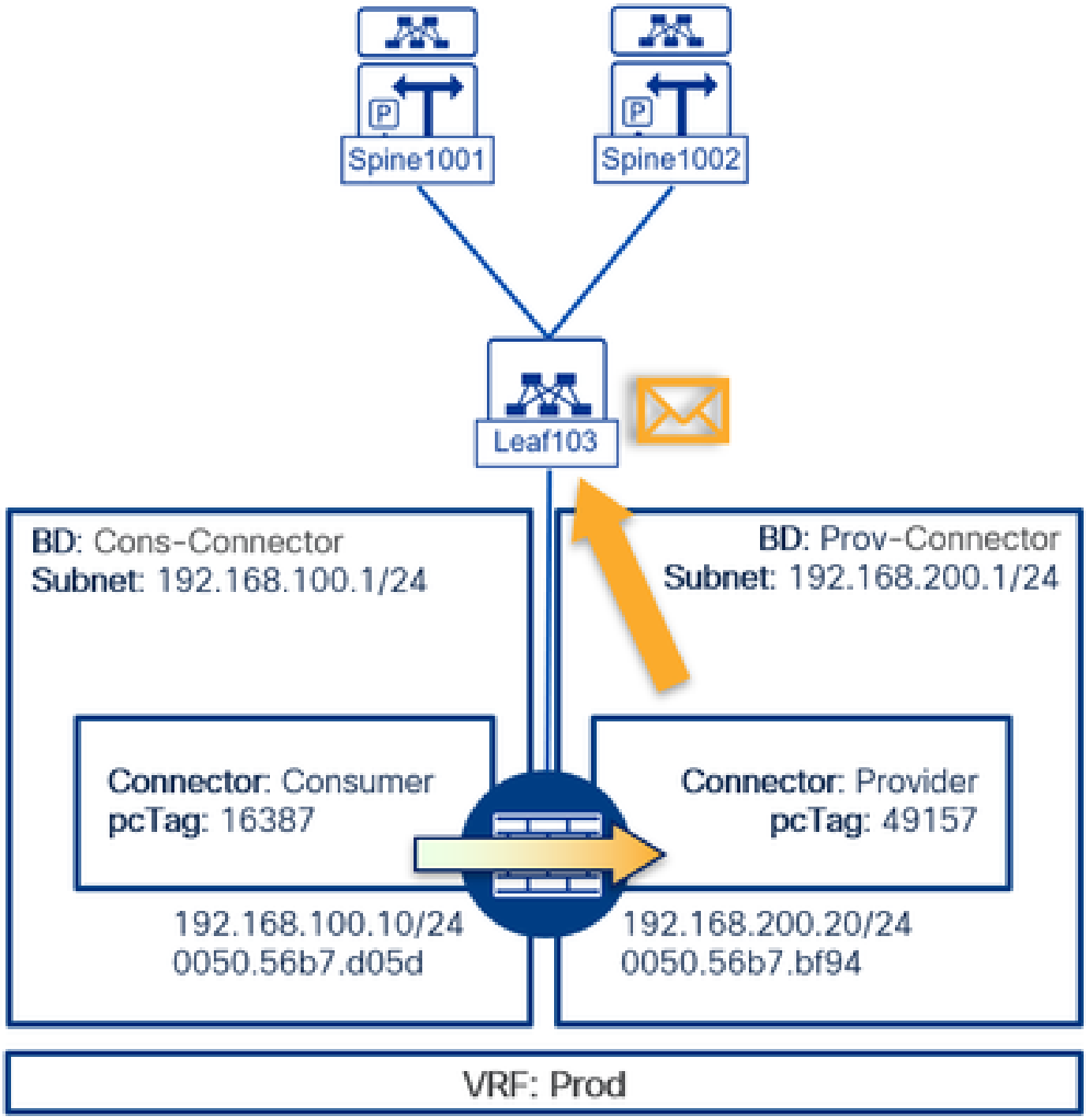
**sclass (src pcTag) : 49155( 0xC003 ) >>> Prod-Consumer EPG**

**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. Para o empacotador que está sendo retornado pelo nó PBR, primeiro, este precisa fazer sua própria diligência e ter o VRF, a interface ou a VLAN alterados. O pacote será encaminhado de volta para a ACI no conector do provedor:




<#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**

---

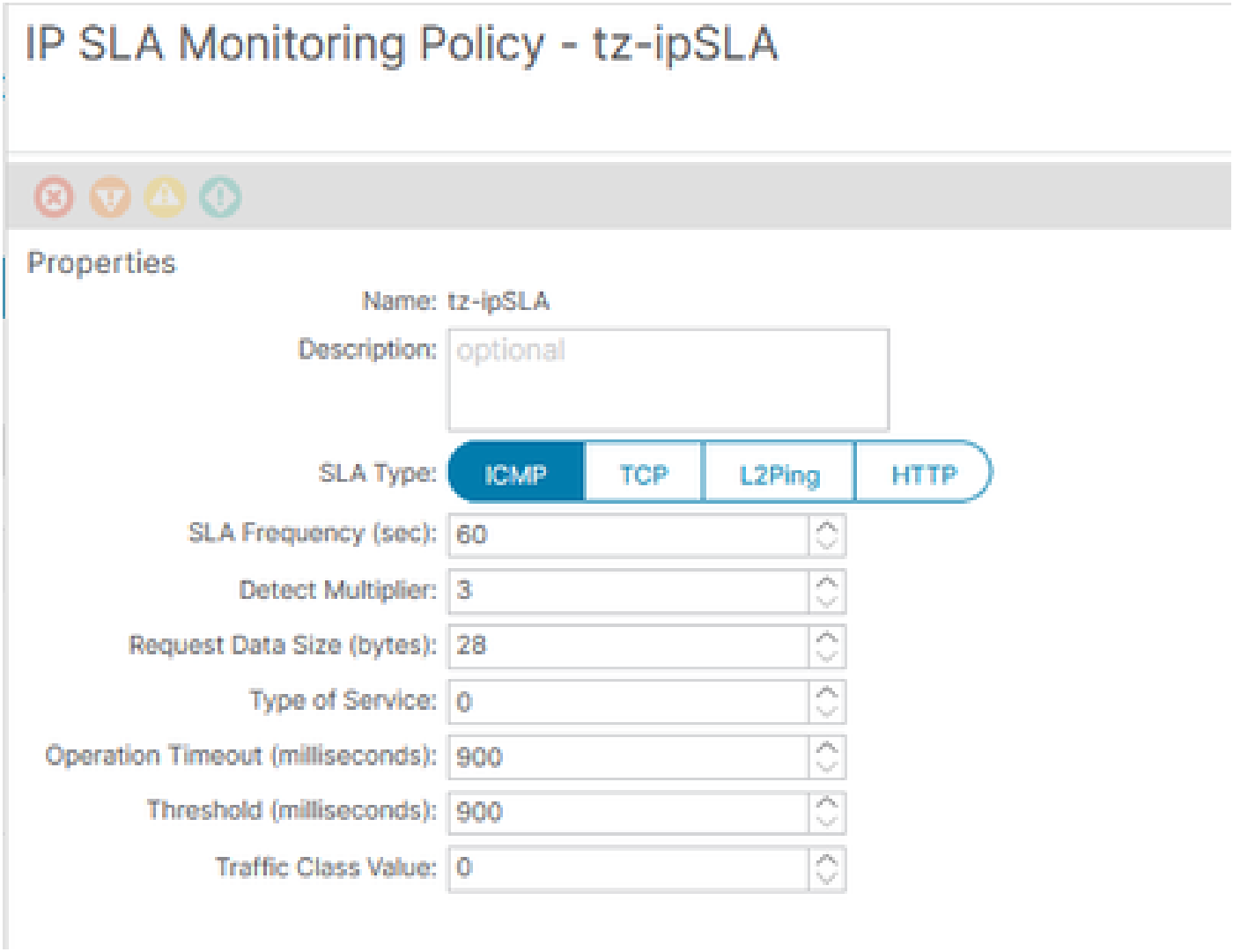
5. O tráfego de rede restante segue as etapas estabelecidas mencionadas até agora, nas quais os pacotes retornam aos switches spine para determinar o destino final do servidor, com base na pesquisa de cooperação. Subsequentemente, os pacotes são direcionados para o switch leaf de computação que tem o flag de aprendizagem local e disseminam essas informações para a tabela COOP nos spines. A execução do ELAM para as etapas 2 e 3 é consistente para a distribuição do pacote para seu destino final. É essencial validá-los como o EPG pcTag de destino e a interface de saída para garantir uma entrega precisa.

# SLA IP

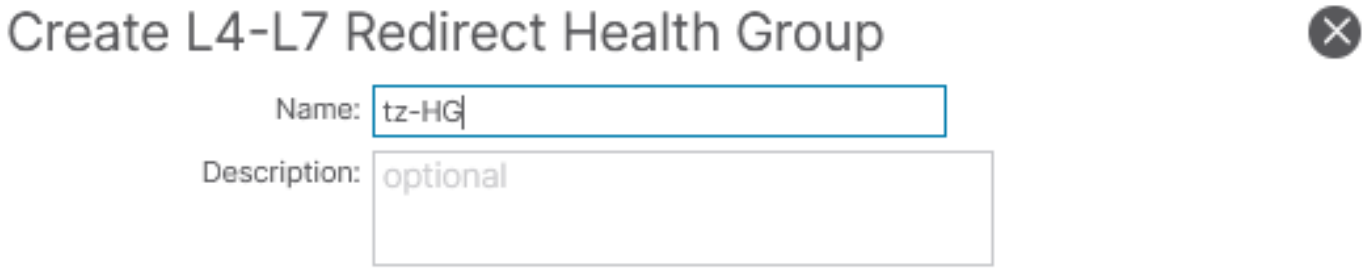
O SLA IP é utilizado para avaliar o status operacional e o desempenho dos caminhos de rede. Ela ajuda a garantir que o tráfego seja roteado de forma eficiente, de acordo com as políticas definidas, com base nas condições da rede em tempo real. Na ACI, o PBR aproveita o SLA IP para tomar decisões de roteamento bem fundamentadas. Se as métricas de SLA IP indicarem que um caminho está com baixo desempenho, o PBR poderá rotear novamente o tráfego através de caminhos alternativos que atendam aos critérios de desempenho exigidos.

Começando na versão 5.2(1), você pode habilitar o rastreamento dinâmico de MAC para SLA IP. Isso é útil para cenários em que um nó PBR faz failover e altera o endereço MAC para o mesmo endereço IP, em implantações estáticas, uma alteração na política de redirecionamento baseado em política precisa ser feita toda vez que o nó PBR altera seu endereço MAC para continuar a enviar tráfego. Com o IP SLA, o endereço MAC usado nessa política retransmite para a resposta da sonda. Testes diferentes podem ser usados para determinar se o nó PBR está ou não íntegro. No momento da redação deste texto, eles incluem: ICMP, TCP, L2Ping e HTTP.

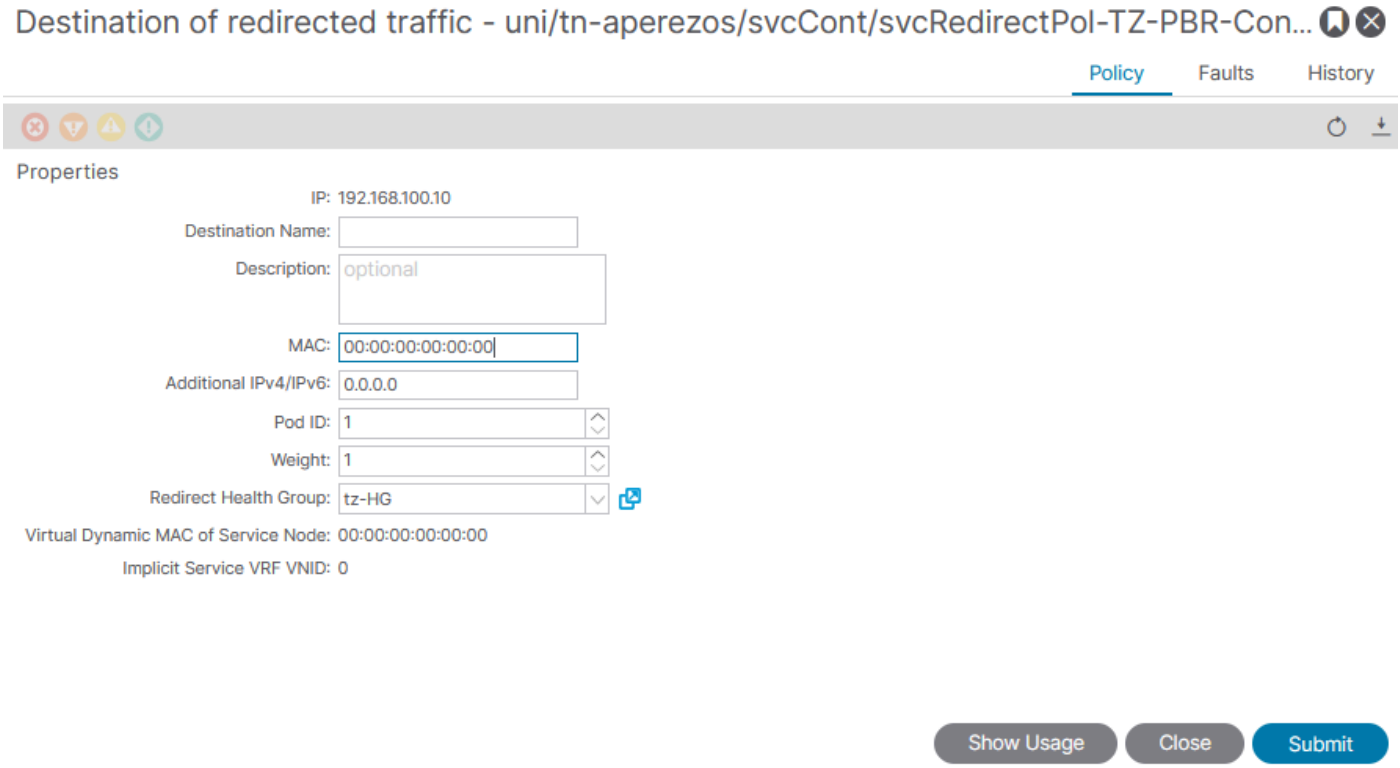
A configuração geral de uma política IP SLA deve ser semelhante a:



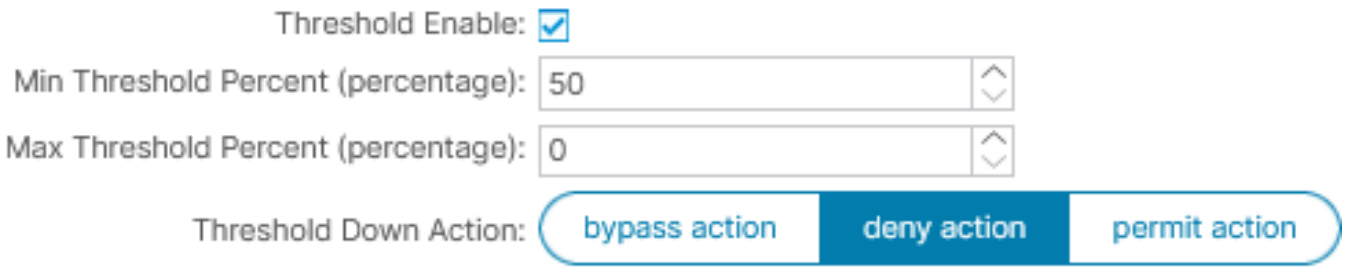

A política IP SLA precisa ser mapeada para o IP do nó PBR por meio de um grupo de integridade.




Se o SLA IP para descobrir dinamicamente o endereço MAC for usado, esse campo não poderá ficar vazio, mas definido para todos os 0s:




Quando um Grupo de Integridade estiver associado ao IP do nó PBR por meio do Destino L3 na política de Redirecionamento Baseado em Política L4-L7, defina limites para definir o comportamento do SLA IP em caso de inacessibilidade. Especifique um número mínimo de Destinos L3 ativos necessários para manter o redirecionamento. Se a contagem de nós PBR ativos cair ou exceder o percentual de limite, o grupo inteiro será afetado pela Ação de Limite Inativo selecionada, interrompendo a redistribuição. Essa abordagem suporta o desvio do nó PBR durante a solução de problemas sem afetar o fluxo de tráfego.




Os Grupos de Integridade vinculam todos os IPs definidos nos Destinos L3 de uma única política de Redirecionamento de Base de Política L4-L7 ou várias políticas de Redirecionamento de Base de Política L4-L7, desde que a mesma política de Grupo de Integridade seja usada.

```
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#
```

## Informações Relacionadas

- White paper de design do gráfico de serviço de redirecionamento baseado em políticas da Cisco Application Centric Infrastructure
- Mergulho profundo no redirecionamento baseado em políticas (PBR - Policy-Based Redirect) das camadas 4 a 7 da ACI (Apresentação ao vivo da Cisco)
- Solucionar problemas de SLA IP em PBR de vários pods

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.