Solucionar problemas de PBR en ACI

Contenido

Introducción

Este documento describe cómo resolver problemas de entornos de Infraestructura centrada en aplicaciones (ACI) con Redirección basada en políticas (PBR) en un único fabric de grupo de dispositivos.

Prerequisites

Requirements

Para este artículo, se recomienda que tenga un conocimiento general de estos temas:

- Conceptos de ACI: Políticas de acceso, aprendizaje de terminales, contratos y L3out

Componentes Utilizados

Este ejercicio de resolución de problemas se realizó en la versión 6.0(8f) de ACI con los switches Nexus de segunda generación N9K-C93180YC-EX y N9K-C93240YC-FX2.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Abreviaturas

- BD: Dominio de Bridge
- EPG: Grupo de terminales
- ID de clase: Etiqueta que identifica un EPG
- Nodo PBR: Dispositivo L4-L7 que se utiliza para un destino PBR
- Conector de consumidor: Interfaz de nodo PBR orientada al consumidor
- Conector del proveedor: Interfaz de nodo PBR orientada al proveedor

Historial PBR

Versión	Características principales
2.0(1 m)	• Los gráficos de servicio proporcionan la función PBR.
3.x y anteriores	• Compatibilidad con redirección basada en políticas (PBR) de varios nodos • Hashing resistente PBR
3.2.x)	• La PBR de firewall de un nodo es compatible con entornos multisitio.
4.0(x)	• Firewall PBR de dos nodos es compatible con entornos multisitio.
4.2(1)	• Ahora se soporta una política de respaldo para crear nodos PBR en espera.
4.2(3)	• La opción Filtrar desde contrato está disponible en la plantilla de Service Graph mediante la GUI.
5.0(1)	• Las L3Outs son compatibles en todos los lados del proveedor de los nodos de servicio. • Las rutas de ECMP/implementación activa-activa son compatibles con los dispositivos PBR de capa 1/capa 2.
5.2(1)	• Un destino PBR ahora puede estar en una salida L3. • Puede realizar un seguimiento de los nodos de servicio mediante el URI HTTP. • Ya no se admiten los modos gestionados e híbridos del gráfico de servicios. • Se admite la dirección MAC de nodo PBR dinámico.

6.0(1)	• Redirección basada en políticas simétrica basada en peso (PBR)

Aspectos del diseño

- PBR funciona con dispositivos físicos y virtuales
- PBR se puede utilizar entre EPG L3Out y EPG, entre EPG y entre EPG L3Out. PBR no es compatible si el EPG L2Out forma parte del contrato
- PBR es compatible con los entornos Cisco ACI Multi-Pod, Multi-Site y Remote Leaf.
- El fabric de Cisco ACI debe ser el gateway para los servidores y para el nodo PBR
- El dispositivo L4-L7 debe implementarse en el modo de acceso (modo enrutado)
- El nodo PBR no es compatible con los switches FEX
- Se necesita un dominio de puente dedicado para el nodo PBR
- La dirección MAC dinámica para el nodo PBR se admite ahora mediante grupos de mantenimiento.
- Se recomienda habilitar la detección basada en GARP en el dominio de puente de nodo PBR
- El filtro predeterminado común que incluye ARP, tráfico Ethernet y otro tráfico no IP no se debe utilizar para PBR
- El nodo PBR puede estar entre instancias VRF o dentro de una de las instancias VRF. Para esta topología, el nodo PBR no se soporta para estar en un tercer VRF, debe configurarse en el VRF del consumidor o del proveedor

Antecedentes

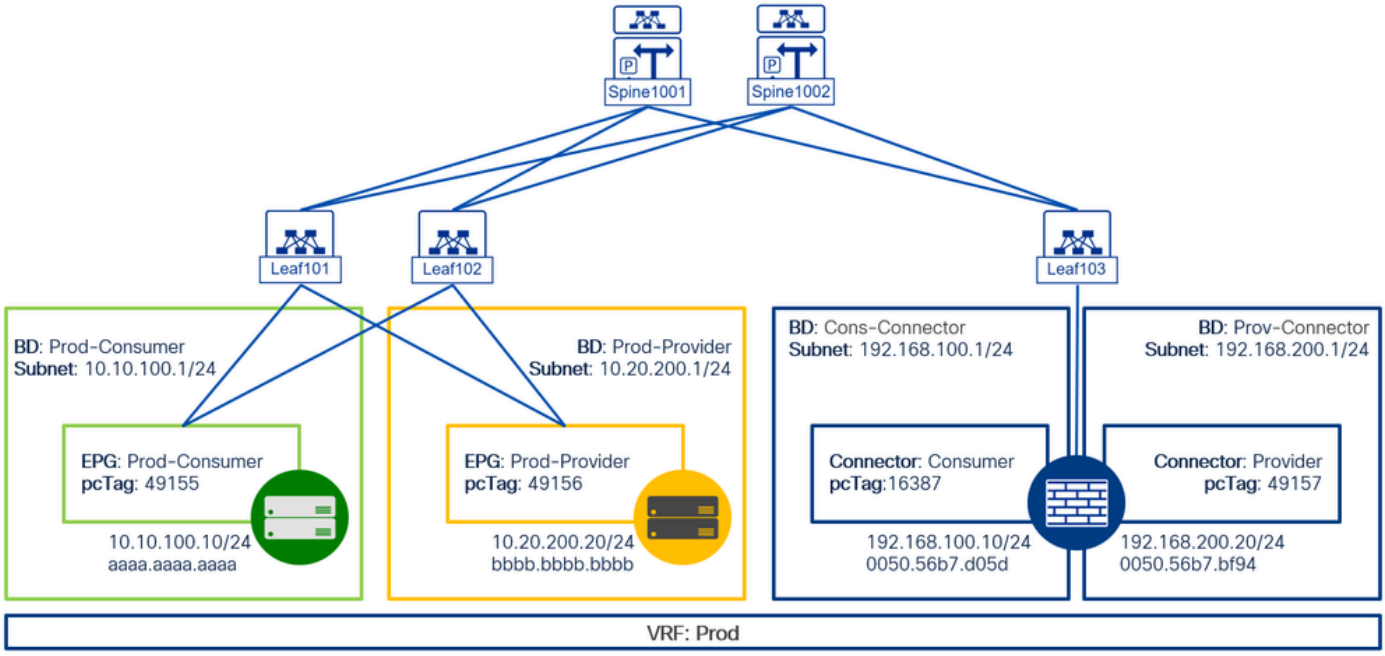
Encontrará explicaciones más detalladas de ELAM y Ftriage en la biblioteca Cisco Live On-Demand en la sesión BRKDCN-3900b.

Además, todas las directrices de configuración se pueden encontrar en el informe técnico Diseño gráfico de servicios de redirección basados en políticas de Cisco Application Centric Infrastructure (IPA).

Situación: VRF único en un único fabric de grupo de dispositivos

Diagrama de la red

Topología física:



Resolución de problemas

Paso 1: Fallos

ACI genera un fallo cuando existe un problema con la configuración o las interacciones de políticas. Se han identificado fallas específicas para el proceso de representación PBR en caso de falla:

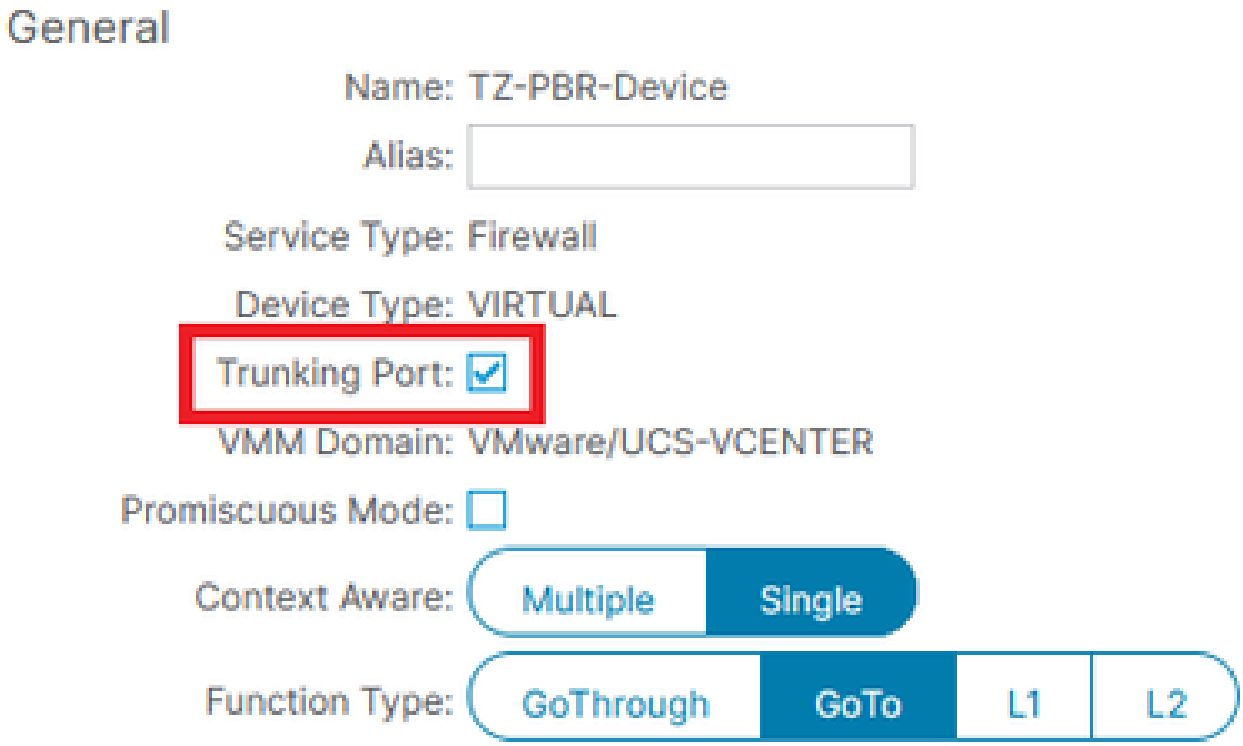
F1690: La configuración no es válida debido a:

- Error de asignación de ID

  Este fallo significa que la VLAN encapsulada para el nodo de servicio no está disponible. Por ejemplo, no podría haber ninguna VLAN dinámica disponible en el grupo de VLAN asociado al dominio Virtual Machine Manager (VMM) utilizado por el dispositivo lógico.

  Resolución: Verifique el conjunto de VLAN dentro del dominio empleado por el dispositivo lógico. Si la interfaz del dispositivo lógico está dentro de un dominio físico, también inspeccione la configuración de VLAN encapsulada. Esta configuración se puede encontrar en Arrendatario > Servicios > L4-L7 > Dispositivos y entramado > Políticas de acceso > Conjuntos > VLAN.

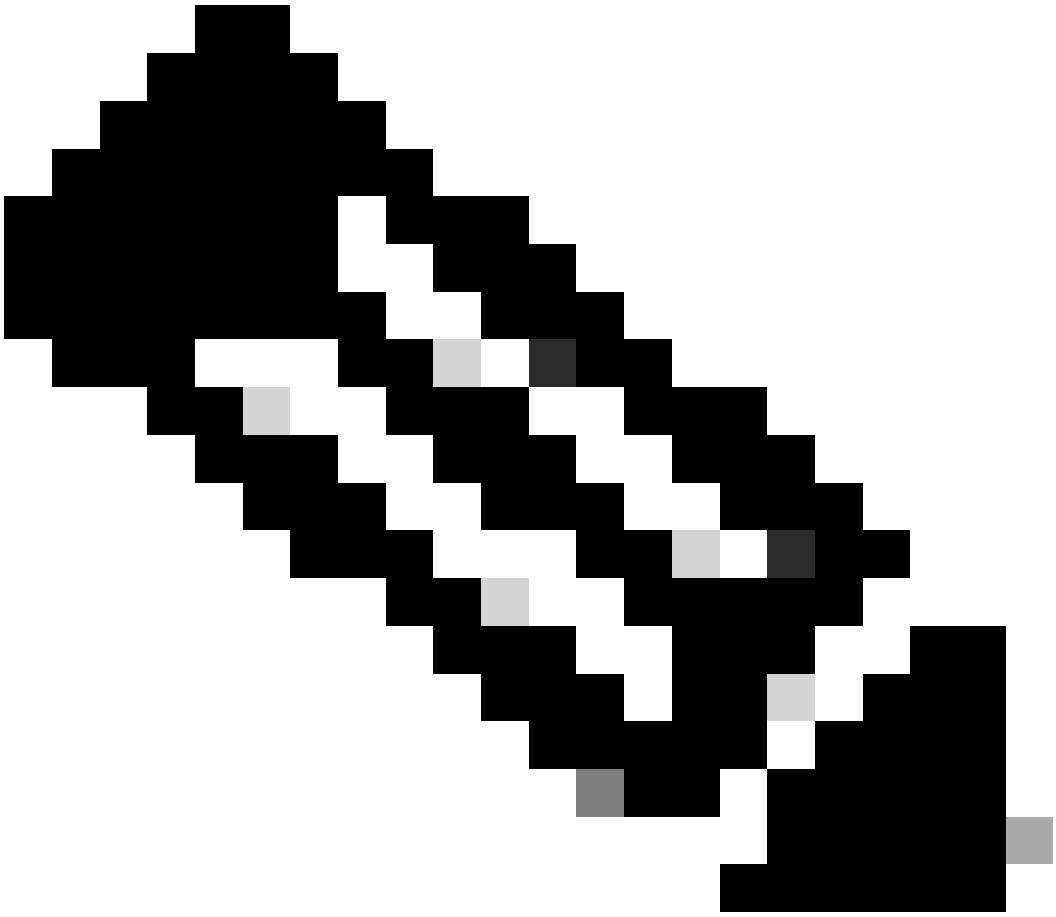
  Por el contrario, si la interfaz de dispositivo lógico reside en un dominio virtual y se conecta a los hosts de ESXi a través de una interfaz troncal, asegúrese de que la opción de puerto troncal está activada.



- No se encontró contexto de dispositivo para LDev

Este error indica que el dispositivo lógico no se puede localizar para la representación del gráfico de servicios. Por ejemplo, no puede haber ninguna política de selección de dispositivos que coincida con el contrato asociado con Service Graph.

Resolución: Verifique que se haya definido una política de selección de dispositivos. La directiva de selección de dispositivos especifica los criterios de selección para un dispositivo de servicio y sus conectores, basándose en el nombre del contrato, el nombre del gráfico de servicios y el nombre del nodo dentro del gráfico de servicios. Esto se puede encontrar en Arrendatario > Servicios > L4-L7 > Política de selección de dispositivos.

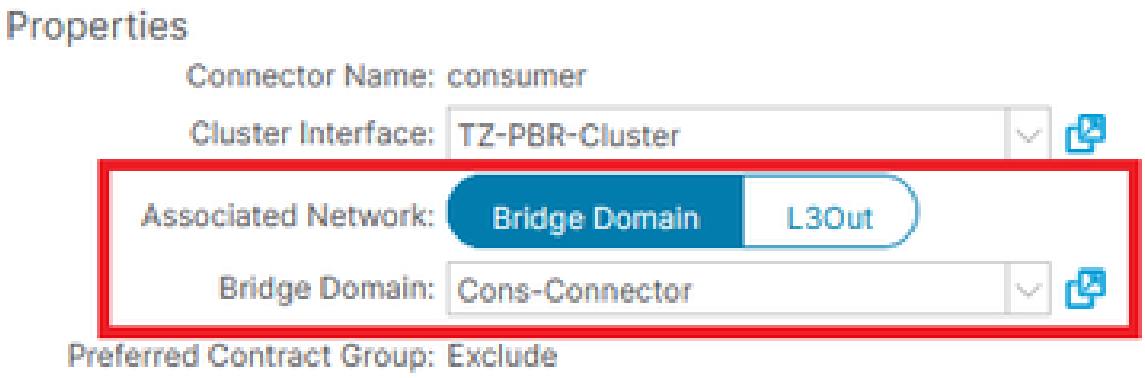


Nota: Al implementar una plantilla de Service Graph, ACI preselecciona el dominio de puente para el EPG de origen. Debe cambiar este dominio de bridge para el conector de consumidor PBR. Lo mismo se aplica para el conector de proveedor.

- No se ha encontrado BD

  Este error indica que no se puede encontrar el dominio de puente (BD) para el nodo de servicio. Por ejemplo, el BD no se especifica en la política de selección de dispositivos.

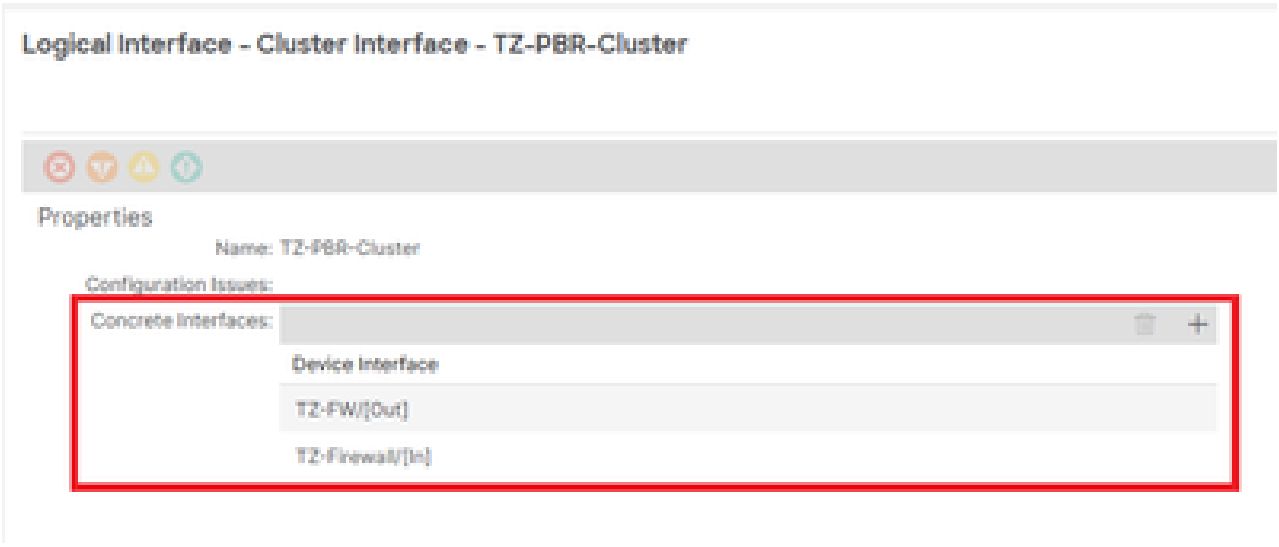
  Resolución: Asegúrese de que el BD esté especificado en la política de selección de dispositivos y que el nombre del conector sea correcto. Esta configuración se encuentra en Arrendatario > Servicios > L4-L7 > Política de selección de dispositivos > [Contrato + SG] > [Consumidor | Proveedor].



- LIf no tiene relación con CIf y LIf tiene un CIf inválido
- No se encontró ninguna interfaz de clúster

  Estos fallos indican que el dispositivo no tiene relación con las interfaces del clúster.

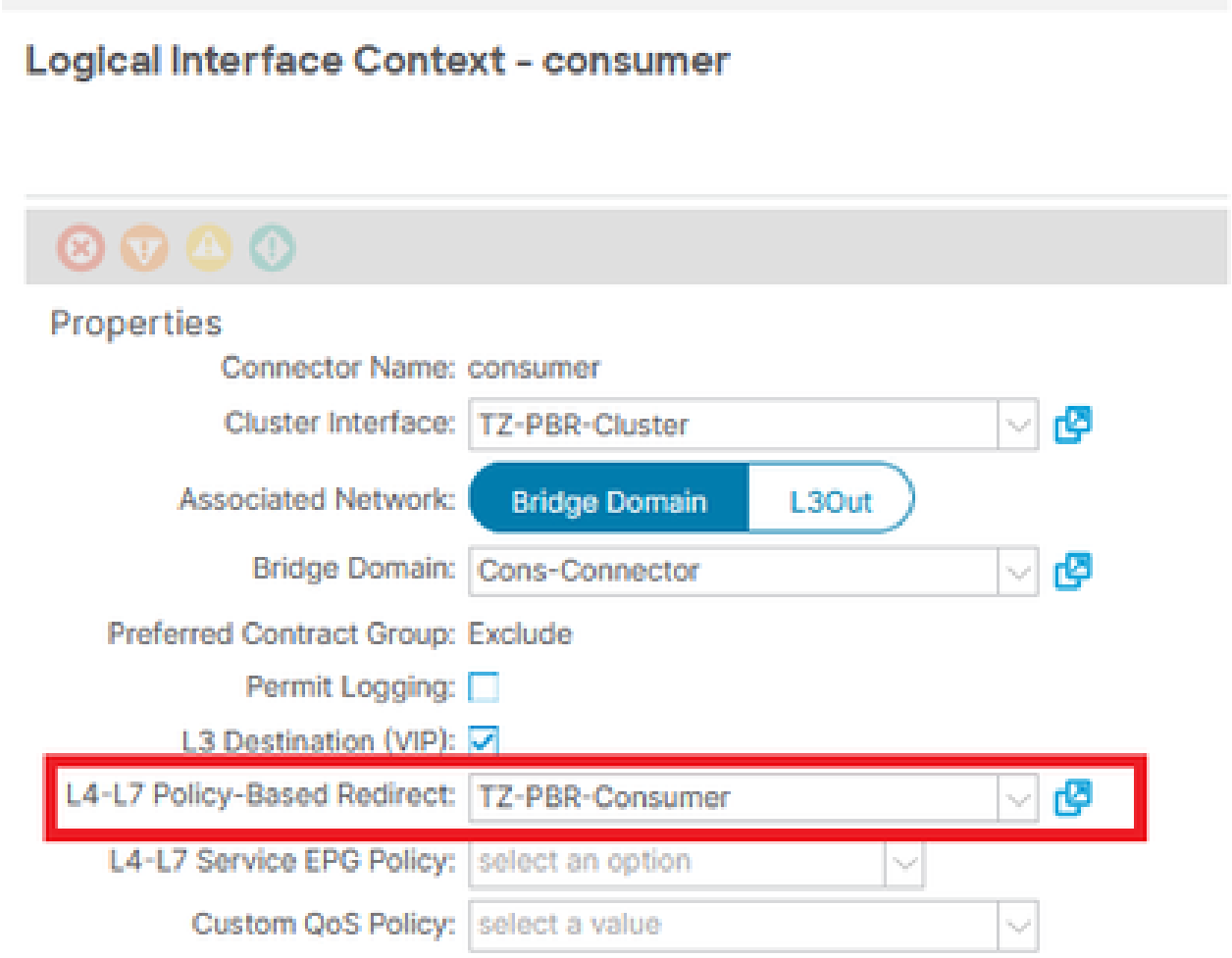
  Resolución: Asegúrese de que la configuración del dispositivo de la capa 4 a la capa 7 (L4-L7) incluya un selector de interfaz concreto especificado. Esta configuración se encuentra en Arrendatario > Servicios > L4-L7 > Dispositivos > [Dispositivo] > Interfaces de clúster.



- Política de redireccionamiento de servicio no válida

  Este fallo significa que la política PBR no se ha aplicado a pesar de que la redirección se haya activado en la función de servicio dentro del Gráfico de servicios.

  Resolución: Asegúrese de que la política PBR esté configurada dentro de la configuración de la Política de selección de dispositivos. Esta configuración se encuentra en Arrendatario > Servicios > L4-L7 > Política de selección de dispositivos > [Contrato + SG] > [Consumidor | Proveedor].



F0759 graph-render-failure - "No se pudo crear una instancia del gráfico de servicios para el arrendatario < arrendatario >. La configuración del nodo de función < nodo > no es válida."

No se pudo crear una instancia del gráfico de servicios para el arrendatario especificado debido a una configuración no válida del nombre del nodo de función.

Este error sugiere que hay problemas de configuración relacionados con las condiciones antes mencionadas.

Además, durante las implementaciones iniciales, este fallo puede surgir temporalmente y resolverse rápidamente. Esto ocurre debido al proceso de representación que la ACI experimenta para implementar todas las políticas.

Resolución: Investigue cualquier fallo adicional del que se haya informado y resuelva el problema en consecuencia.

F0764 configuration-failed - "La configuración de dispositivos L4-L7 < dispositivo > para el arrendatario < arrendatario > no es válida."

No se pudo crear una instancia del gráfico de servicios para el arrendatario especificado debido a una configuración no válida de la directiva de dispositivo PBR.

Este error sugiere que hay problemas de configuración relacionados con las condiciones antes mencionadas.

Resolución: Investigue cualquier fallo adicional del que se haya informado y resuelva el problema en consecuencia.

F0772 configuration-failed - "La configuración de línea < cluster > para dispositivos L4-L7 < device > para arrendatario < tenant > no es válida."

No se pudo crear una instancia del gráfico de servicios para el arrendatario especificado debido a una configuración no válida de la selección de la interfaz de clúster de dispositivos PBR.

Este error sugiere que hay problemas de configuración relacionados con las condiciones antes mencionadas.

Resolución: Investigue cualquier fallo adicional del que se haya informado y resuelva el problema en consecuencia.

Paso 2: Aprendizaje de terminales de origen y destino

Asegúrese de que los terminales de origen y destino se reconocen dentro del fabric, lo que requiere una configuración básica:

- Objeto de reenvío y routing virtuales (VRF).
- Objeto de dominio de puente (BD) con el enrutamiento de unidifusión habilitado. Aunque habilitar el aprendizaje del plano de datos IP se considera una práctica recomendada, no es obligatorio.
- Objeto de grupo de terminales (EPG), aplicable tanto a dominios virtuales como físicos.
- Políticas de acceso: Verifique que la cadena de configuración de la política de acceso esté completa y que no se informe de ningún fallo en el EPG.

Para confirmar el aprendizaje del terminal en el EPG y la interfaz correctos, ejecute este comando en la hoja donde se aprende el terminal, también conocido como hoja de cálculo:

<#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#
```

Este comando le permite identificar la pcTag (clase) asociada con el EPG donde se clasifica el terminal, así como recuperar la interfaz, el alcance VRF y la información de dirección MAC.

Si no conoce la ubicación del terminal de origen o de destino, siempre puede utilizar este comando en el APIC:

<#root>

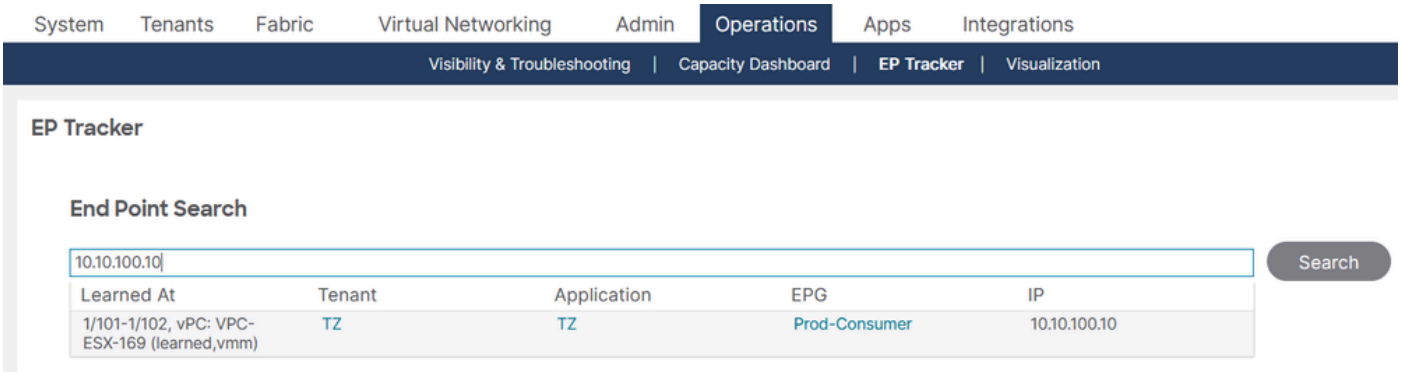
```
show endpoint [ ip | mac ] [ x.x.x.x | eeee.eeee.eeee ]
```

<#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#
```

En la GUI, se puede acceder a la función EP Tracker navegando hasta Operations > EP Tracker para la supervisión y gestión de terminales.



Con la información recopilada de los terminales de origen y destino, ahora puede centrarse en la implementación de políticas PBR.

Paso 3: Redirigir contrato

PBR está integrado en el marco de Service Graph. Por consiguiente, se debe implementar y configurar una plantilla de Service Graph en los switches de origen y de destino de acuerdo con un contrato. Mediante la utilización de la información de pcTags recopilada en el paso anterior, puede determinar si un grupo de terminales (EPG) se está redirigiendo a un grupo de Service Graph ejecutando este comando.

<#root>

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

En las reglas de zonificación, estas reglas deben considerarse:

1. EPG de origen a EPG de destino con un grupo de redirección asociado
2. EPG de sombra de nodo PBR de origen a EPG de origen
3. EPG de destino a EPG de origen con un grupo de redirección asociado. Este grupo puede ser idéntico o diferente a la configuración anterior.

4. EPG de sombra de nodo PBR de destino a EPG de destino

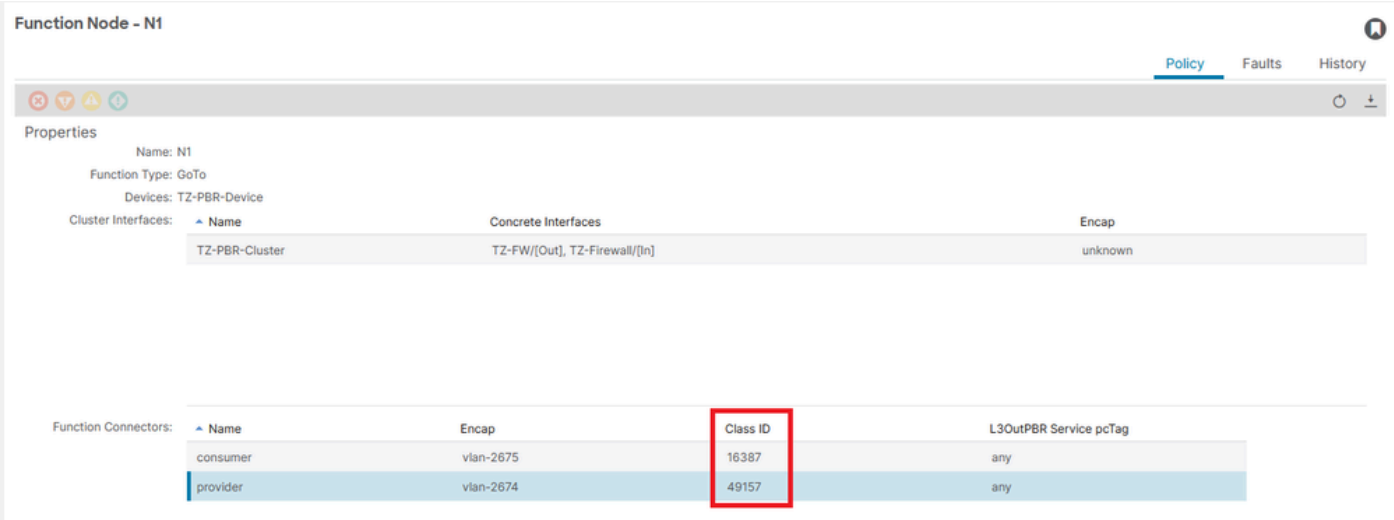
<#root>

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 la pcTag de los Shadow EPG creados durante el proceso de implementación de Policy-Based Routing (PBR), vaya a Arrendatarios > [TENANT_NAME] > Servicios > L4-L7 > Instancia de gráfico implementada > [SG_NAME] > Nodo de función - N1.



- Analizador de contratos

El script correlaciona reglas de zonificación, filtros, estadísticas y nombres de EPG. Puede ejecutar este script de forma segura directamente en una hoja de ACI o APIC. Cuando se ejecuta en el APIC, recopila objetos concretos en todos los switches de hoja, lo que puede tardar varios minutos en implementaciones de políticas de gran tamaño.

A partir de la versión 3.2 de ACI, contract_parser se incluye en la imagen y está disponible en la hoja. Simplemente ingrese contract_parser.py desde el shell de 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#
```

Este comando proporciona detalles como la acción del contrato, los EPG de origen y destino, el nombre del contrato en uso y el número de visitas.

Paso 4: Grupo de redirección

Una vez identificado el grupo de redirección según el contrato aplicado a las reglas de zonificación, el siguiente paso es determinar las direcciones IP y MAC de los dispositivos objetivo para la redirección. Para ayudar con esto, ejecute el 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#
```

Este comando nos permite determinar el estado operativo (OperSt) de nuestro grupo de redirección, la dirección IP configurada en la sección PBR L4-L7 y el VNID del VRF asociado con los dominios de puente de nodo PBR. Ahora debe determinar la dirección MAC configurada:

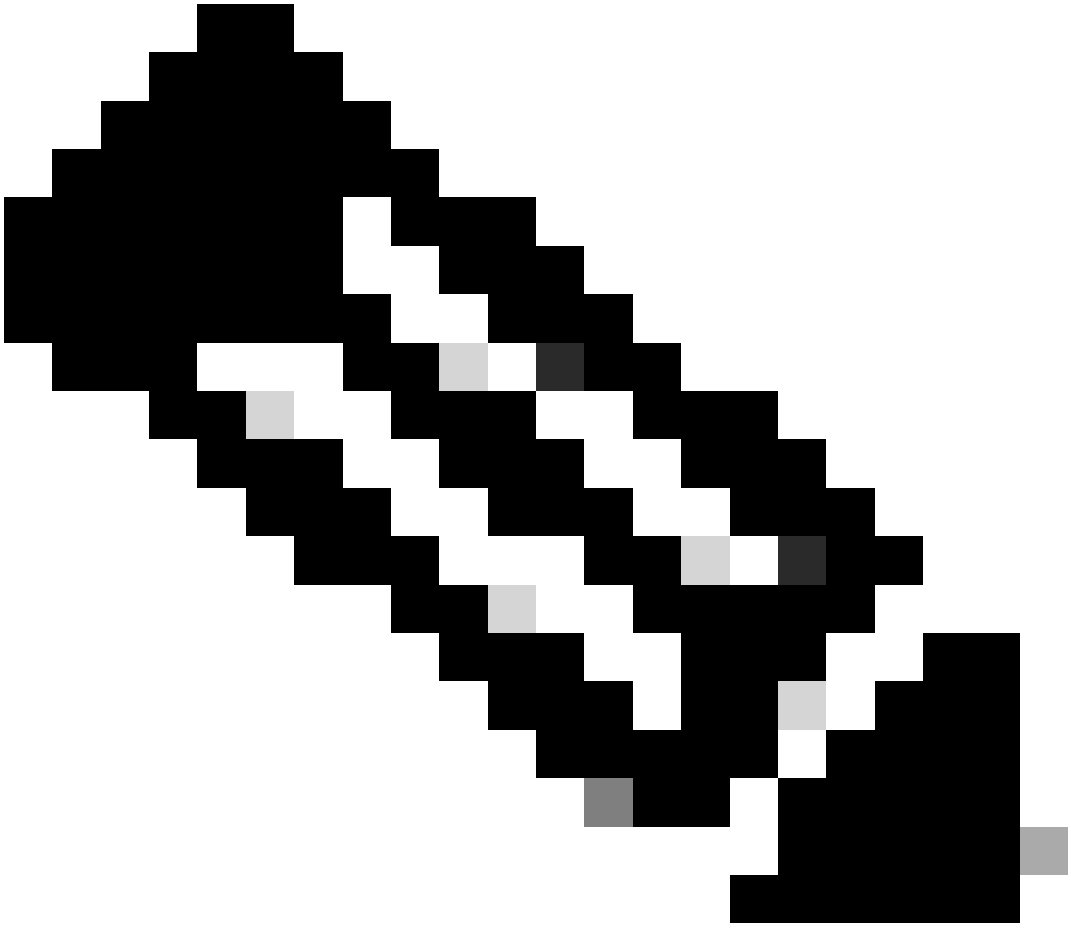
<#root>

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#
```

Además de los detalles mencionados anteriormente, este comando proporciona información valiosa, incluyendo el nombre VRF, BD VNID y la dirección MAC configurada del nodo PBR.



Nota: Es importante tener en cuenta que tanto la dirección IP como la dirección MAC están configuradas por el usuario en esta etapa, lo que significa que pueden producirse errores tipográficos durante la definición de routing basado en políticas L4-L7.

Paso 5: El nodo PBR no recibe tráfico.

Un problema frecuente con el reenvío PBR es la ausencia de tráfico que llega al nodo PBR. Una causa frecuente de este problema es una dirección MAC especificada incorrectamente dentro de la configuración de ruteo basado en políticas L4-L7.

Para verificar la precisión de la dirección MAC configurada en el routing basado en políticas L4-L7, ejecute el comando utilizado anteriormente del paso 2. Este comando se puede ejecutar en el switch de hoja designado como hoja de servicio, donde se espera que se aprenda el nodo.

<#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 que la dirección MAC registrada en la tabla de EPM coincida con la configurada en el grupo de redirección de servicios. Incluso los errores tipográficos menores deben corregirse para garantizar el ruteo correcto del tráfico al destino del nodo PBR.

Paso 6: Flujo de tráfico.

- FRAGMENTO

Herramienta CLI para el APIC diseñada para automatizar la configuración y la interpretación de los procesos ELAM de extremo a extremo. La herramienta permite a los usuarios especificar un flujo determinado y el switch de hoja donde se origina el flujo. Ejecuta secuencialmente los ELAM en cada nodo para analizar la trayectoria de reenvío del flujo. Esta herramienta es especialmente útil en topologías complejas en las que la ruta del paquete no es fácilmente perceptible.

<#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) es una herramienta de diagnóstico que permite a los usuarios establecer condiciones específicas en el hardware para capturar el paquete o la trama

inicial que cumple esos criterios. Cuando una captura es exitosa, el estado de ELAM se indica como disparado. Al activarse, el ELAM se inhabilita, lo que permite que se recopile un volcado de datos, lo que facilita el análisis de las numerosas decisiones de reenvío ejecutadas por el ASIC del switch para ese paquete o trama. ELAM funciona en el nivel ASIC, asegurándose de que no afecte a la CPU ni a otros recursos del switch.

Estructura de la sintaxis del comando. Esta estructura se recopiló del libro Troubleshooting de ACI Intra-Fabric Forwarding Tools

```
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]
```

Establecer condiciones para activar

```
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]
```

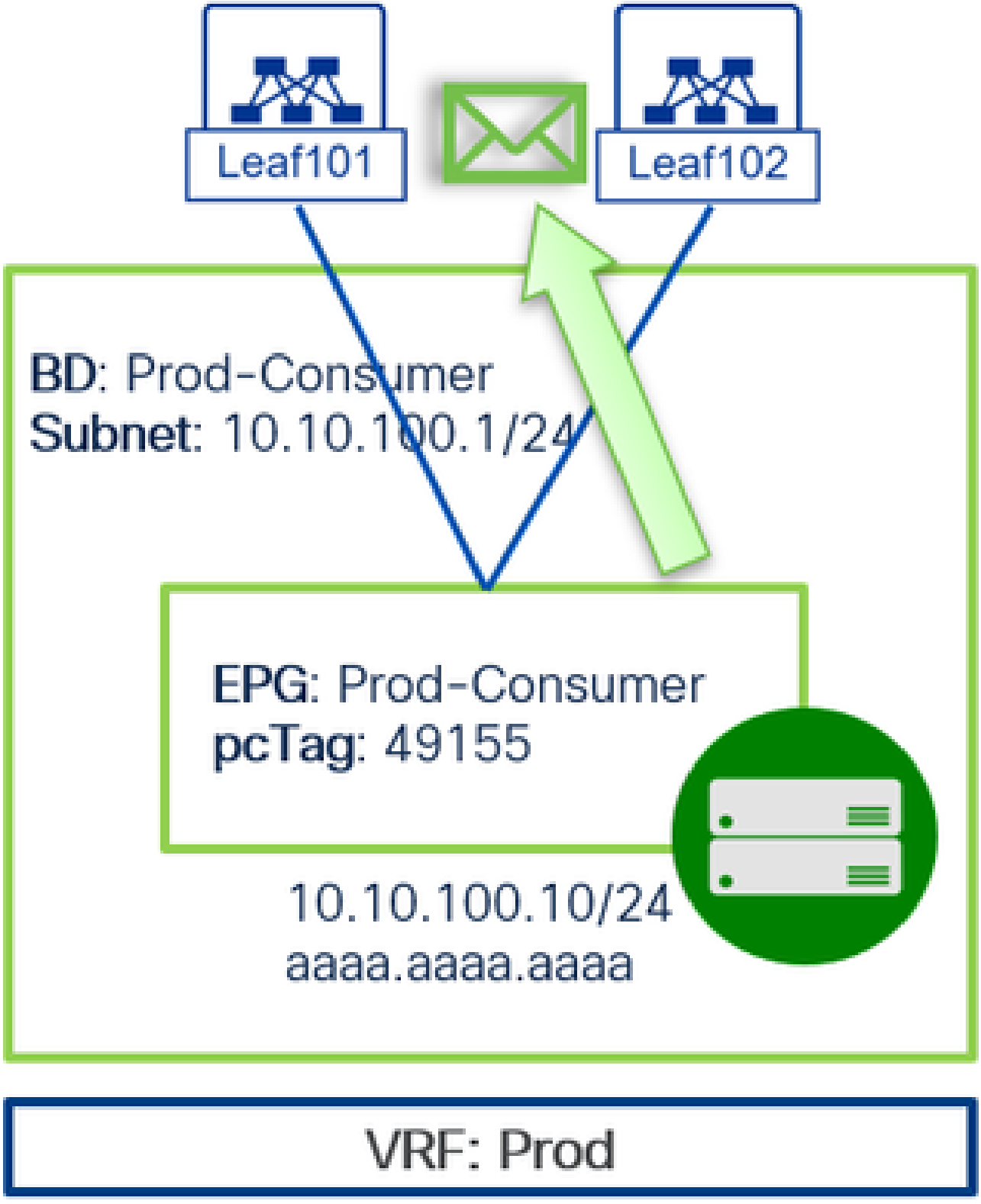
Genere el volcado que contiene el análisis de paquetes.

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

- Flujo de tráfico

Es fundamental comprender el flujo de tráfico en todos los dispositivos en cuestión. La herramienta Ftriage proporciona un excelente resumen de este flujo. Sin embargo, para realizar una validación detallada paso a paso y obtener información más detallada sobre el proceso de recepción de paquetes, puede ejecutar el módulo analizador de lógica incorporada (ELAM) en cada punto de la topología de red.

1. El tráfico de entrada se produce en la hoja de cálculo donde se aprende el servidor de origen. En este escenario específico, como el origen se coloca detrás de una interfaz vPC, la ELAM se debe configurar en los pares vPC. Esto es necesario porque la interfaz física seleccionada por el algoritmo hash es 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

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

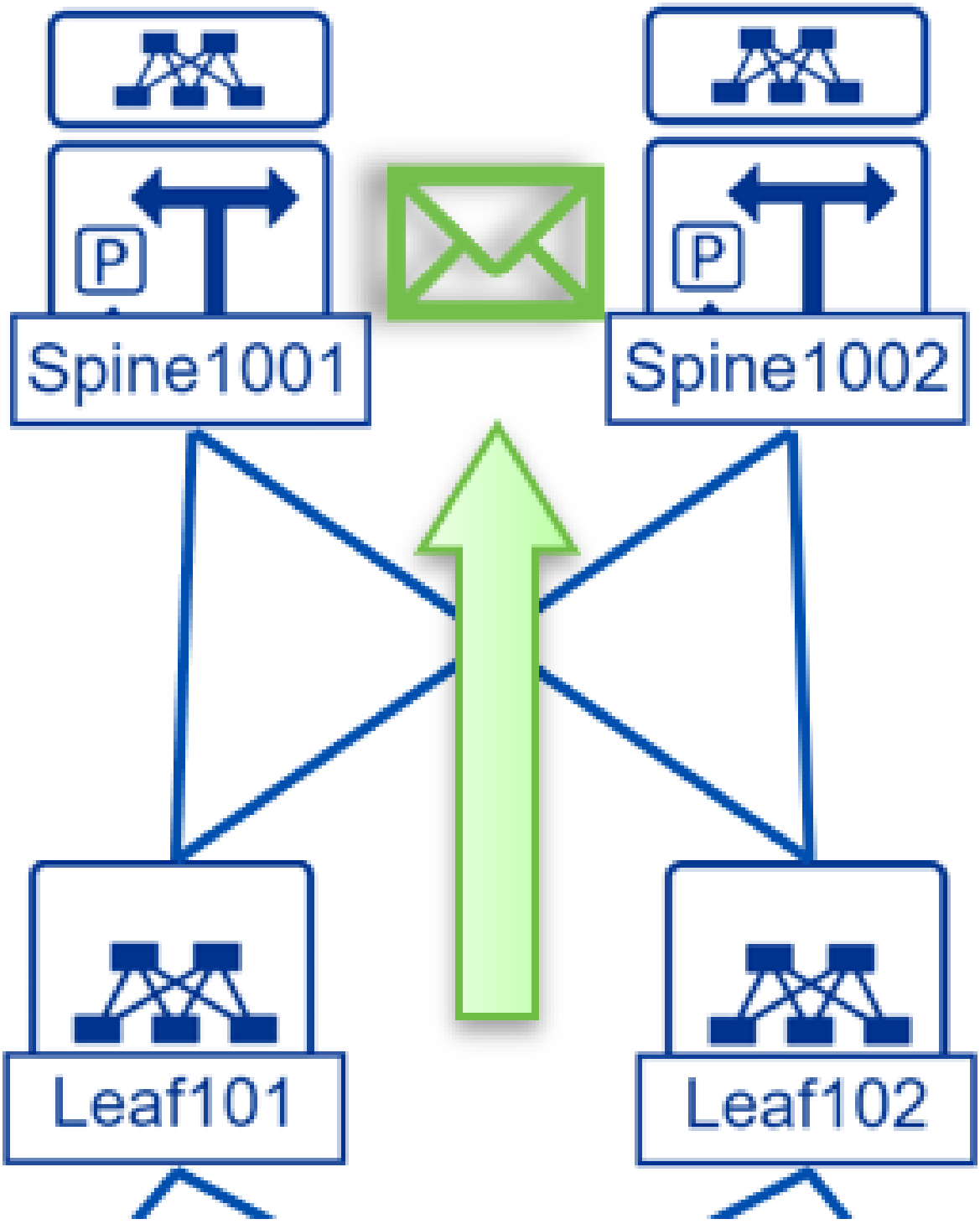
Según la información proporcionada, es evidente que el paquete se está redirigiendo a través del routing basado en políticas (PBR), ya que la opción service_redir está habilitada. Además, se recuperan los valores sclass y dclass. En este escenario en particular, el switch reconoce la dclass. Sin embargo, si el extremo de destino no está presente en la tabla de EPM, el valor predeterminado de dclass es 1.

Además, la interfaz de ingreso es determinada por el SRCID, y la interfaz de egreso es identificada por los valores del vector. Estos valores se pueden traducir a un puerto frontal ejecutando este comando en el nivel vsh_lc:

<#root>

show platform internal hal l2 port gpd

2. El paso subsiguiente en el flujo implica alcanzar el switch de columna para mapear la dirección MAC de destino al nodo PBR. Dado que el tráfico se encapsula en encabezados VXLAN, la ejecución de ELAM en una columna o una hoja remota requiere el uso de in-select 14 para decodificar correctamente la encapsulación.



<#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.

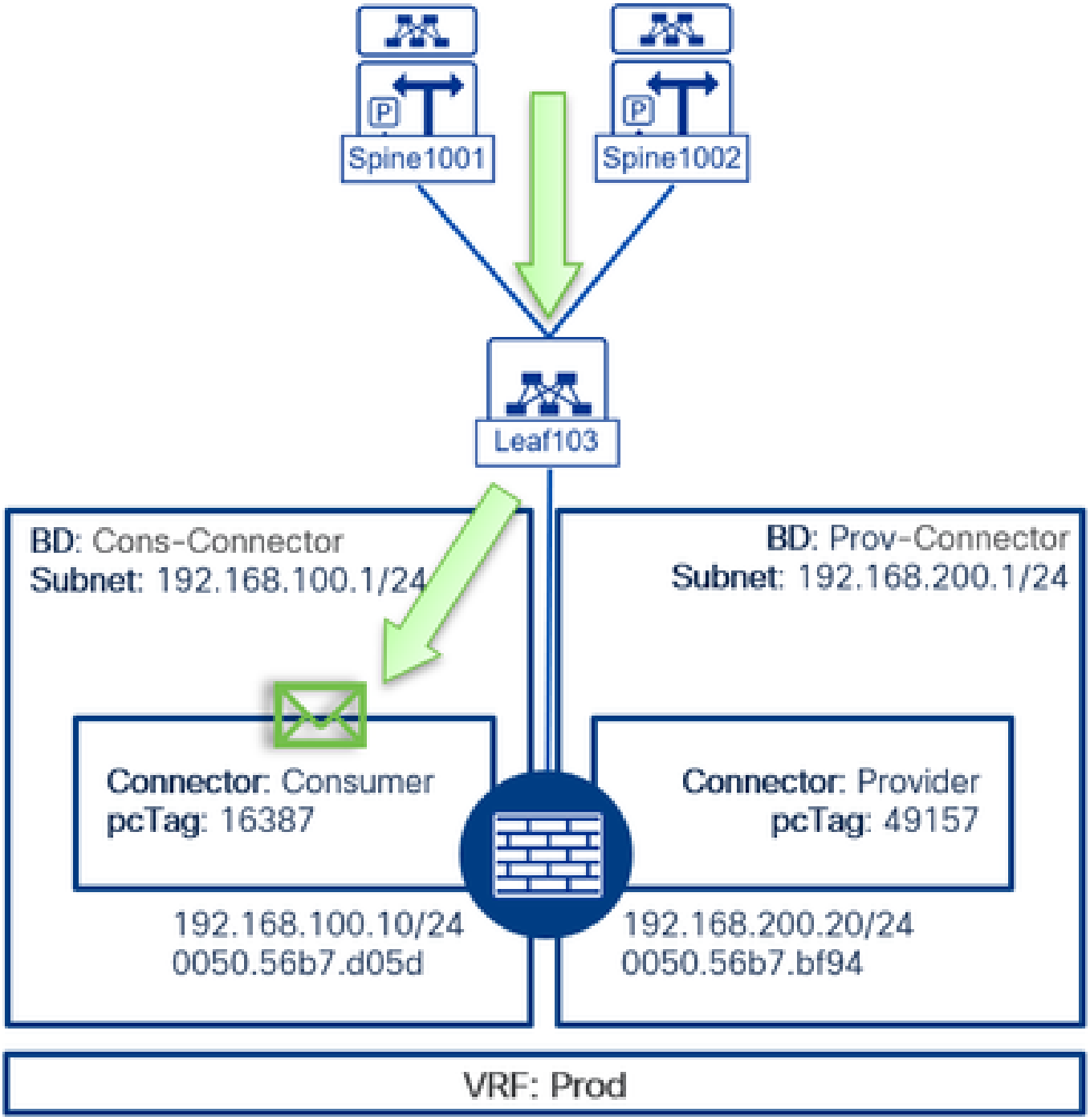
ovector_idx: 0x1F0 >>> Eth1/10

A partir del resultado anterior, es evidente que la dirección MAC de destino se reescribe en la dirección MAC del firewall. Posteriormente, se realiza una búsqueda COOP para identificar el editor de destino del MAC, y el paquete se reenvía a la interfaz correspondiente del switch.

Puede simular esta búsqueda en la columna ejecutando este comando, utilizando el VNID de dominio de puente y la dirección MAC del 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. El tráfico llega a la hoja de servicio donde se reconoce la dirección MAC del firewall y posteriormente se reenvía al nodo 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 )
```

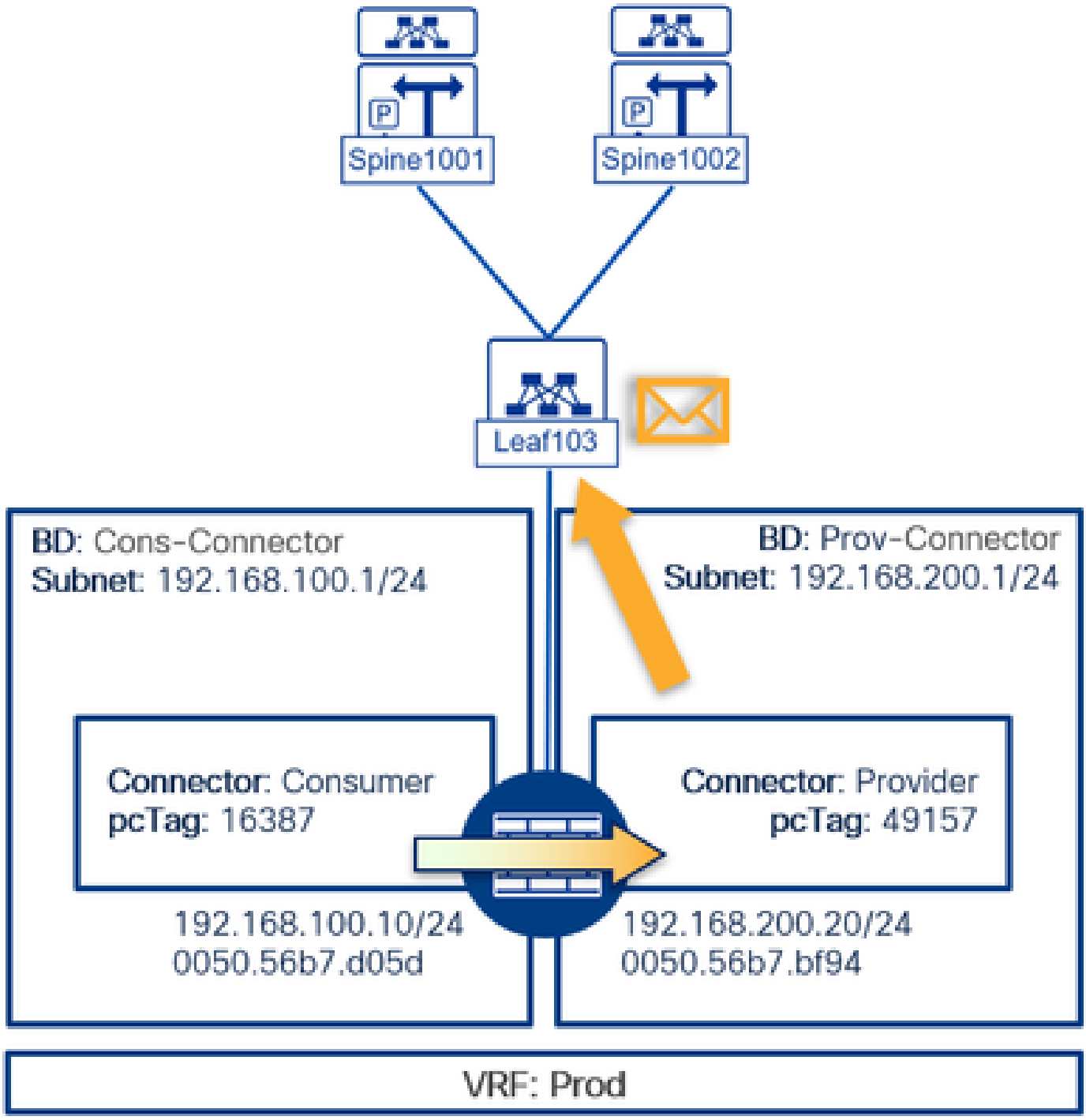
sclass (src pcTag) : 49155(0xC003) >>> Prod-Consumer EPG

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 que el empaquetador sea devuelto por el nodo PBR, primero, éste tiene que hacer su propia diligencia y tener el VRF, la interfaz o la VLAN cambiada. A continuación, el paquete se reenviará de nuevo a ACI en el conector del proveedor:



<#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

---

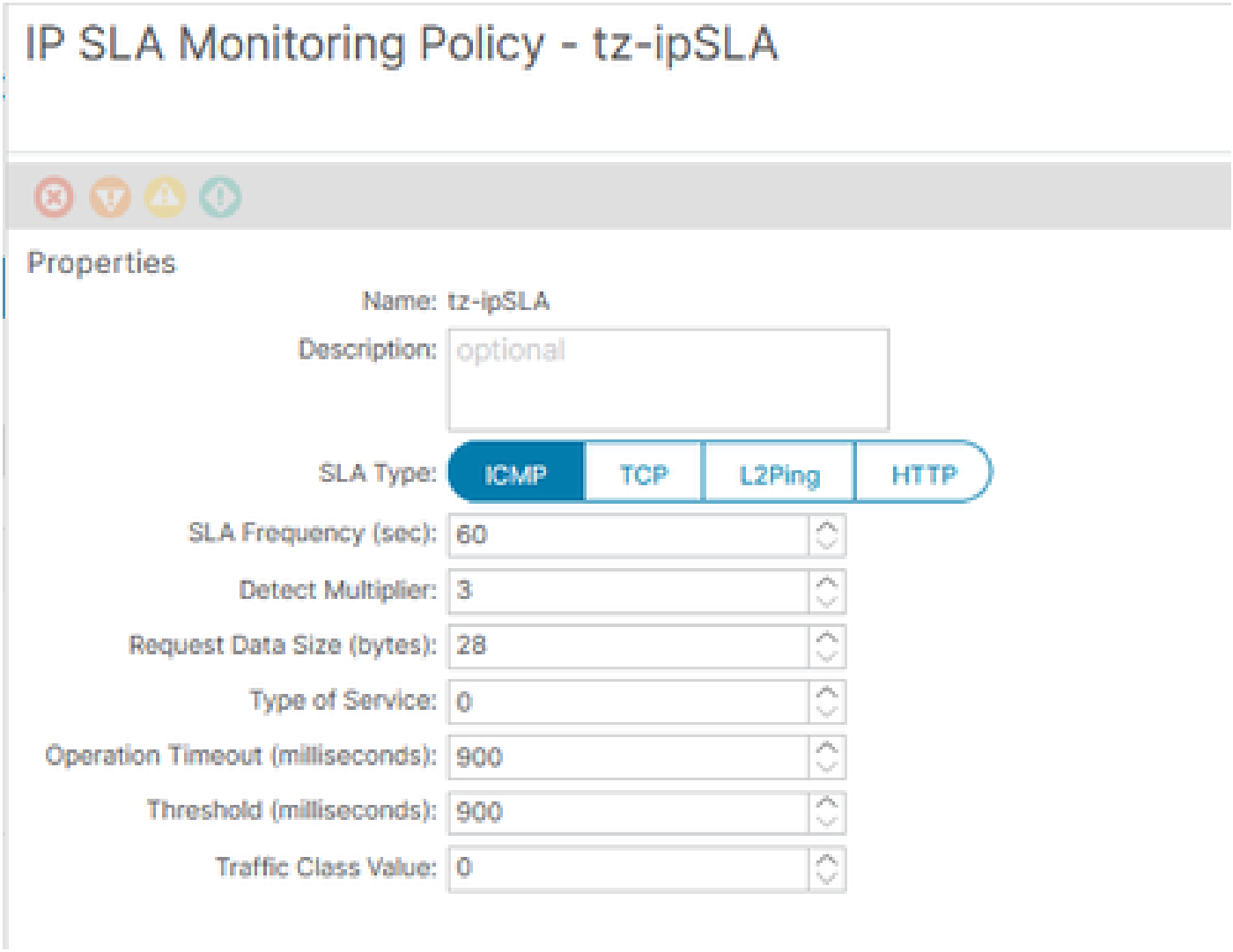
5. El tráfico de red restante se adhiere a los pasos establecidos mencionados hasta el momento, en los que los paquetes regresan a los switches de columna para determinar el destino final del servidor, en función de la búsqueda de coop. Posteriormente, los paquetes se dirigen al switch de hoja de cálculo que tiene el indicador de aprendizaje local y disemina esta información a la tabla COOP en las columnas. La ejecución de ELAM para los pasos 2 y 3 es consistente para la distribución del paquete hacia su destino final. Es esencial validarlas en la pcTag de EPG de destino y en la interfaz de salida para garantizar una entrega precisa.

SLA de IP

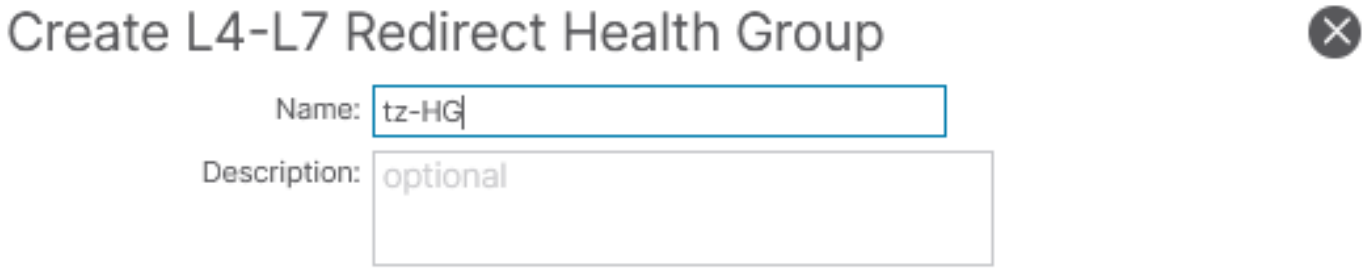
SLA de IP se utiliza para evaluar el estado operativo y el rendimiento de las rutas de red. Ayuda a garantizar que el tráfico se enruta de forma eficaz según las políticas definidas, en función de las condiciones de la red en tiempo real. En ACI, PBR aprovecha IP SLA para tomar decisiones de routing fundamentadas. Si las métricas de SLA de IP indican que una trayectoria está en ejecución, PBR puede volver a rutear el tráfico a través de trayectorias alternativas que cumplan con los criterios de rendimiento requeridos.

A partir de la versión 5.2(1), puede habilitar el seguimiento de MAC dinámico para IP SLA. Esto es útil para escenarios donde un nodo PBR conmuta por error y cambia la dirección MAC para la misma dirección IP; en implementaciones estáticas, se debe realizar un cambio en la política de redirección basada en políticas cada vez que el nodo PBR cambia su dirección MAC para continuar enviando tráfico. Con IP SLA, la dirección MAC utilizada en esta política se transmite a la respuesta de sondeo. Se pueden utilizar diferentes sondas para determinar si el nodo PBR está sano o no, en el momento de escribir este artículo, estas incluyen: ICMP, TCP, L2Ping y HTTP.

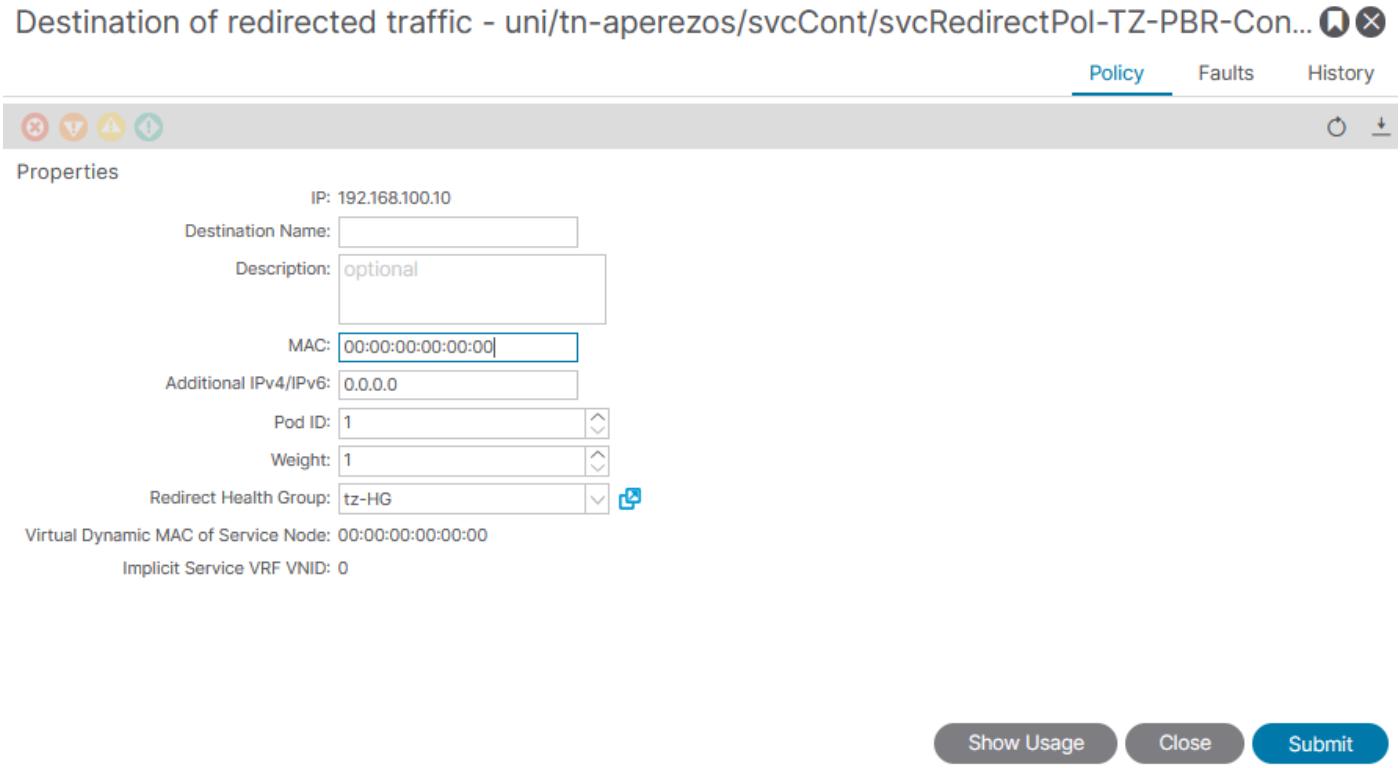
La configuración general de una política de IP SLA debe ser similar a:



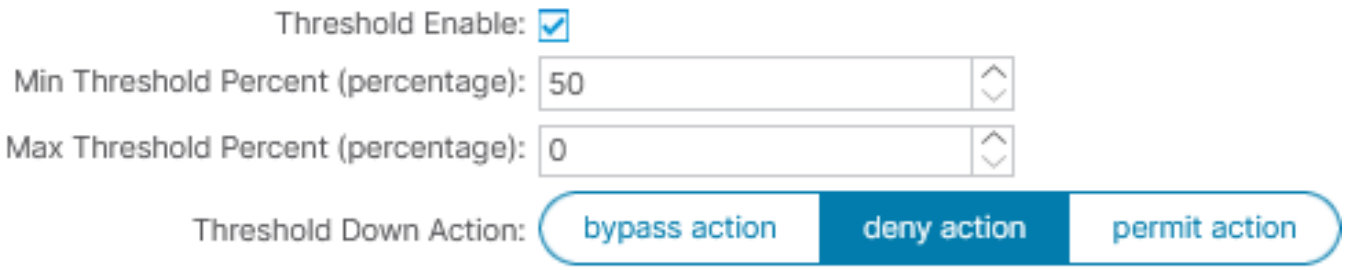
La política de SLA de IP debe asignarse a la IP del nodo PBR por medio de un grupo de estado.



Si se utiliza IP SLA para detectar dinámicamente la dirección MAC, este campo no puede estar vacío, sino configurado en todos los ceros:



Una vez que un grupo de estado se asocie con la IP del nodo PBR a través del destino L3 en la política de redirección basada en políticas L4-L7, establezca umbrales para definir el comportamiento de IP SLA en caso de indisponibilidad. Especifique un número mínimo de destinos L3 activos necesarios para mantener la redirección. Si el recuento de nodos PBR activos cae por debajo o excede el porcentaje de umbral, todo el grupo se verá afectado por la acción de umbral descendente seleccionada, deteniendo la redistribución. Este enfoque admite la omisión del nodo PBR durante la resolución de problemas sin afectar al flujo de tráfico.



Los grupos de estado unen todas las IP definidas en Destinos L3 de una única política de redireccionamiento de base de políticas L4-L7 o varias políticas de redireccionamiento de base de políticas L4-L7 siempre que se utilice la misma política de grupo de estado.

```
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#
```

Información Relacionada

- Informe técnico de diseño de gráfico de servicios de redirección basados en políticas de Cisco Application Centric Infrastructure
- Perspectiva en profundidad y consejos sobre la redirección basada en políticas (PBR) de las capas 4 a 7 de ACI (presentación de Cisco Live)
- Troubleshooting de IP SLA en Multipod PBR

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).