Problemen met PBR bij ACI oplossen

Inhoud

Inleiding

In dit document wordt beschreven hoe u problemen kunt oplossen met Application Centric Infrastructure (ACI)-omgevingen met PBR (Policy-Based Redirect) in één pod-fabric.

Voorwaarden

Vereisten

Voor dit artikel is het aan te raden dat je algemene kennis hebt van deze onderwerpen:

- ACI-concepten: toegangsbeleid, eindpuntleren, contracten en L3out

Gebruikte componenten

Deze probleemoplossingsoefening werd gemaakt op ACI versie 6.0 (8f) met behulp van de tweede generatie Nexus-switches N9K-C93180YC-EX en N9K-C93240YC-FX2.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Afkortingen

- BD: Bridge-domein
- EPG: Eindpuntgroep
- Klasse-ID: tag die een EPG identificeert
- PBR-node: L4-L7-apparaat dat wordt gebruikt voor een PBR-bestemming
- Consumentenconnector: PBR-knooppuntinterface aan de consumentenzijde
- Provider-connector: PBR-knooppuntinterface die naar de kant van de provider is gericht

PBR-geschiedenis

Versie	Belangrijkste kenmerken
2,0(1m)	• Servicegrafieken bieden de PBR-functie.
3.x en eerder	• Ondersteuning voor beleidsgebaseerde omleiding (PBR) met meerdere knooppunten • PBR Resilient Hashing
3,2(x)	• One-node Firewall PBR wordt ondersteund in omgevingen met meerdere locaties.
4,0(x)	• Firewall PBR met twee knooppunten wordt ondersteund in omgevingen met meerdere sites.
4.2(1)	• Een back-upbeleid voor het maken van stand-by PBR-nodes wordt nu ondersteund.
4.2(3)	• De optie Filter-from-contract is beschikbaar in de servicegrafieksjabloon met behulp van de GUI.
5.0(1)	• L3Outs worden ondersteund aan alle kant van de provider van de service nodes. • Active Active Active Deployment/ECMP-paden worden ondersteund voor PBR-apparaten van Layer 1/Layer 2.
5.2(1)	• Een PBR-bestemming kan nu in een L3Out zijn. • U kunt serviceknooppunten volgen met behulp van de HTTP URI. • Servicegrafieken en beheerde hybride modi worden niet langer ondersteund. • Het dynamische MAC-adres van de PBR-node wordt ondersteund.

6.0(1)	• Op gewicht gebaseerde symmetrische beleidsgebaseerde omleiding (PBR)

Ontwerpoverwegingen

- PBR werkt met zowel fysieke als virtuele apparaten
- PBR kan worden gebruikt tussen L3Out EPG en EPG, tussen EPG's en tussen L3Out EPG's. PBR wordt niet ondersteund als L2Out EPG deel uitmaakt van het contract
- PBR wordt ondersteund in Cisco ACI Multi-Pod-, Multi-Site- en Remote Leaf-omgevingen.
- De Cisco ACI-fabric moet de gateway zijn voor de servers en voor de PBR-node
- Het L4-L7-apparaat moet worden ingezet in de go-to-modus (gerouteerde modus)
- PBR node wordt niet ondersteund op FEX switches
- Een speciaal Bridge-domein is nodig voor PBR-knooppunt
- Het dynamische MAC-adres voor de PBR-node wordt nu ondersteund met behulp van controlegroepen.
- Het wordt aanbevolen om GARP-gebaseerde detectie in te schakelen op het PBR-knoopbrugdomein
- Een gemeenschappelijk standaardfilter dat ARP, ethernetverkeer en ander niet-IP-verkeer omvat, mag niet worden gebruikt voor PBR
- Het PBR-knooppunt kan zich tussen VRF-instanties bevinden of binnen een van de VRF-instanties. Voor deze topologie wordt de PBR-node niet ondersteund om te worden geconfigureerd op een derde VRF, die moet worden geconfigureerd in de VRF van de consument of de provider

Achtergrondinformatie

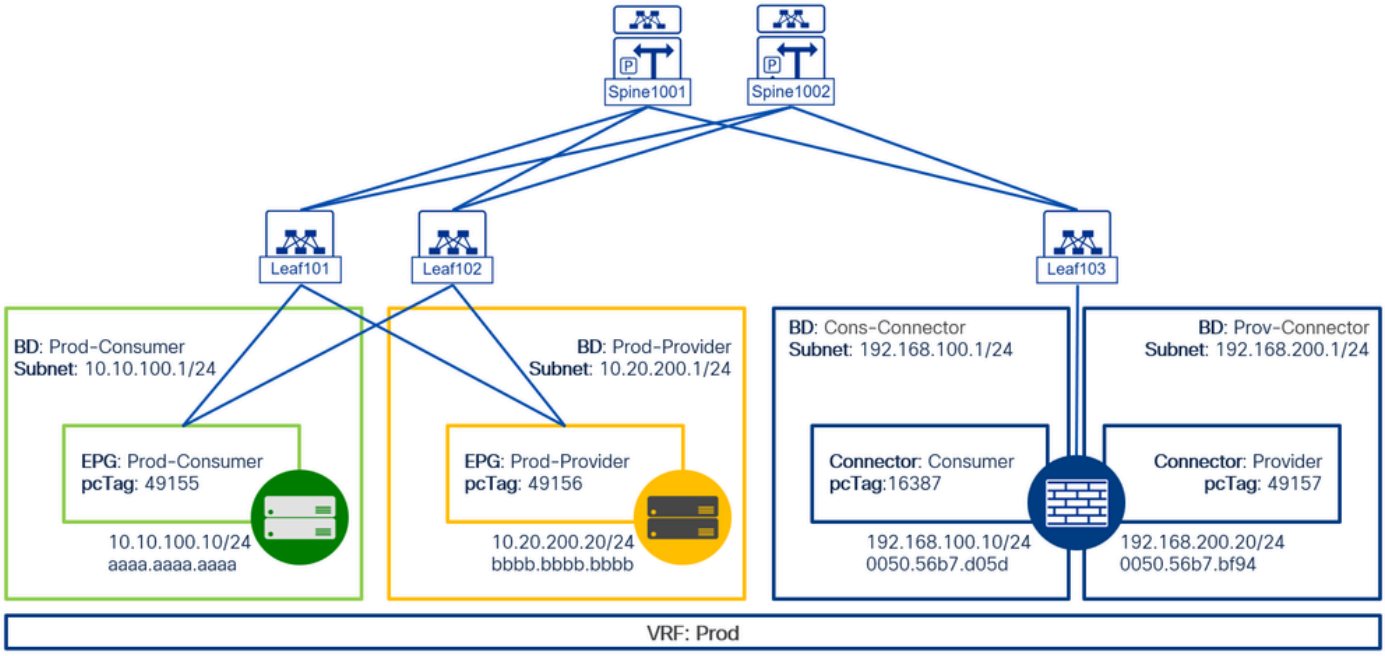
Diepere uitleg van ELAM en Ftriage is te vinden in de CiscoLive On-Demand bibliotheek in sessie BRKDCN-3900b.

Bovendien zijn alle configuratierichtlijnen te vinden in het witboek Cisco Application Centric Infrastructure Policy-Based Redirect Service Graph Design White Paper.

Scenario: Single VRF in een enkele Pod Fabric

Netwerkdiagram

Fysische topologie:



Probleemoplossing

Stap 1: fouten

ACI genereert een fout wanneer er een probleem is met de configuratie of beleidsinteracties. Er zijn specifieke fouten vastgesteld voor het PBR-renderingsproces in geval van een storing:

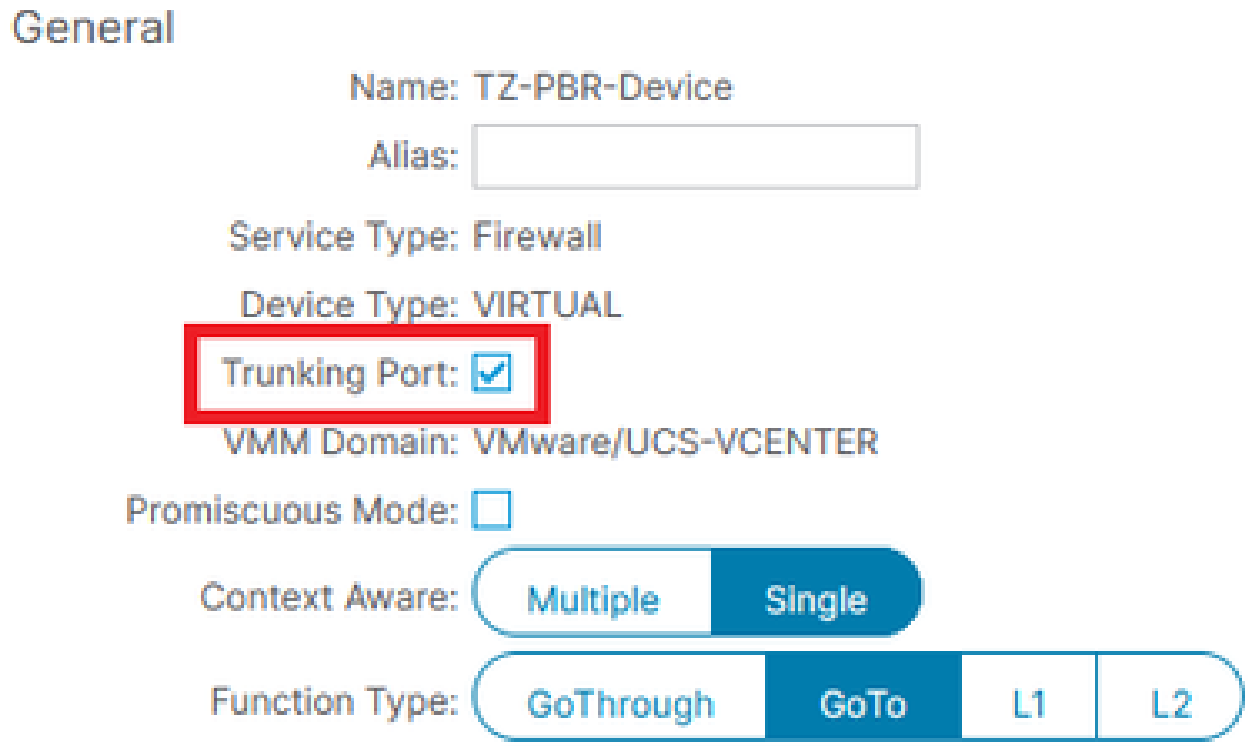
F1690: Configuratie is ongeldig vanwege:

- Mislukte toewijzing van id

  Deze fout betekent dat het ingekapselde VLAN voor de serviceknooppunt niet beschikbaar is. Er kan bijvoorbeeld geen dynamisch VLAN beschikbaar zijn in de VLAN-pool die is gekoppeld aan het VMM-domein (Virtual Machine Manager) dat wordt gebruikt door het logische apparaat.

  Oplossing: controleer de VLAN-pool binnen het domein dat wordt gebruikt door het logische apparaat. Als de Logical Device-interface zich binnen een fysiek domein bevindt, moet u ook de ingekapselde VLAN-configuratie controleren. U vindt deze instellingen onder Huurder > Services > L4-L7 > Apparaten en structuur > Toegangsbeleid > Pools > VLAN.

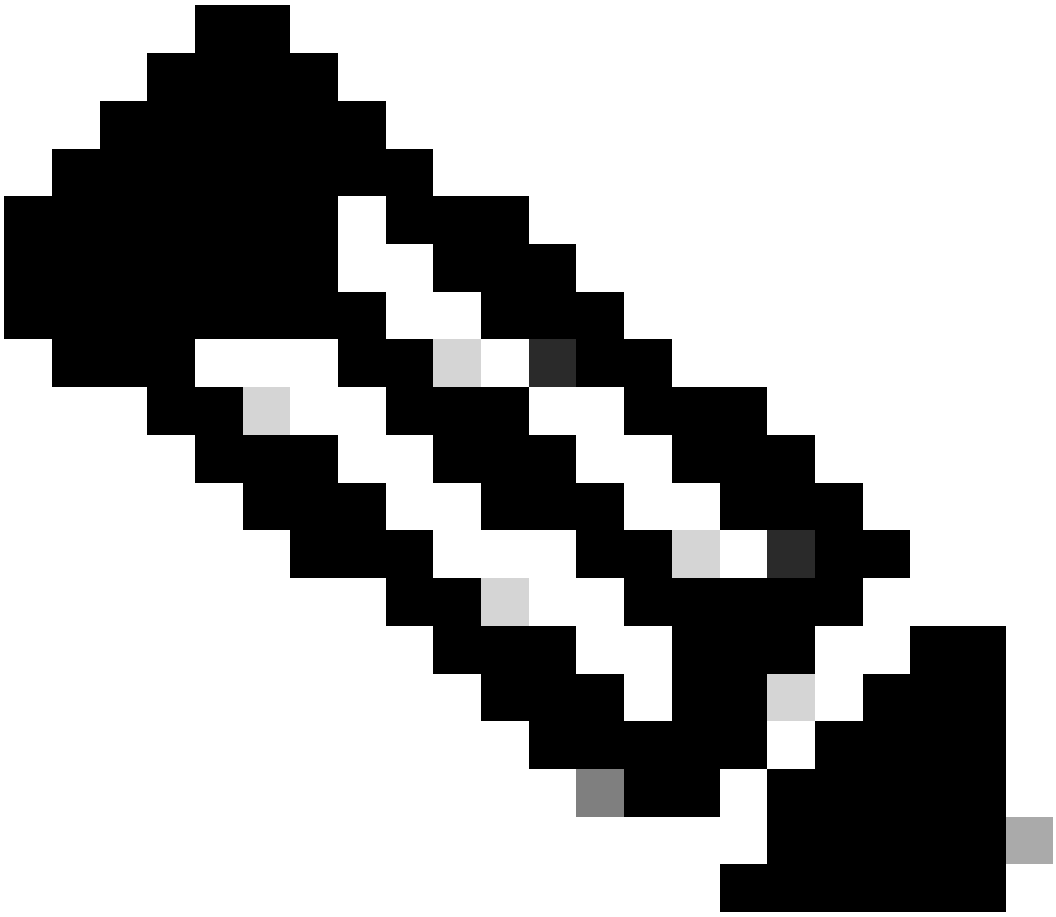
  Omgekeerd, als de Logical Device-interface zich in een virtueel domein bevindt en via een trunkinterface verbinding maakt met uw ESXi-hosts, moet u ervoor zorgen dat de optie trunkpoort is ingeschakeld.



- Geen apparaatcontext gevonden voor LDev

Deze fout geeft aan dat het logische apparaat niet kan worden gevonden voor de rendering van de servicegrafiek. Er kan bijvoorbeeld geen apparaatselectiebeleid zijn dat overeenkomt met het contract dat is gekoppeld aan de servicegrafiek.

Oplossing: controleer of er een apparaatselectiebeleid is gedefinieerd. In het apparaatselectiebeleid worden selectiecriteria voor een serviceapparaat en de connectoren opgegeven op basis van de contractnaam, de naam van de servicegrafiek en de nodenaam in de servicegrafiek. U vindt dit onder Huurder > Services > L4-L7 > Apparaatselectiebeleid.

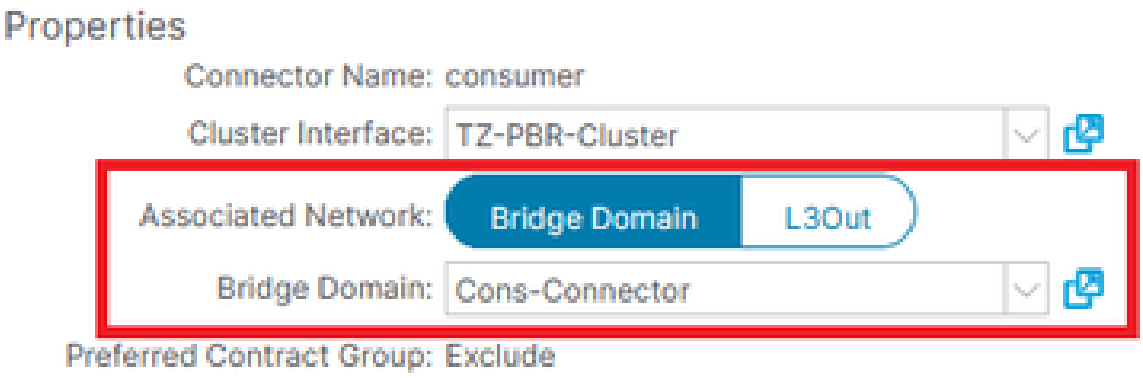


Opmerking: wanneer u een servicegrafieksjabloon implementeert, selecteert ACI vooraf het brugdomein voor de bron-EPG. U moet dit brugdomein wijzigen voor de PBR-consumentenconnector. Hetzelfde geldt voor de provider connector.

- Geen BD gevonden

  Deze fout geeft aan dat het Bridge Domain (BD) voor het serviceknooppunt niet kan worden gevonden. De BD is bijvoorbeeld niet opgegeven in het beleid Apparaatselectie.

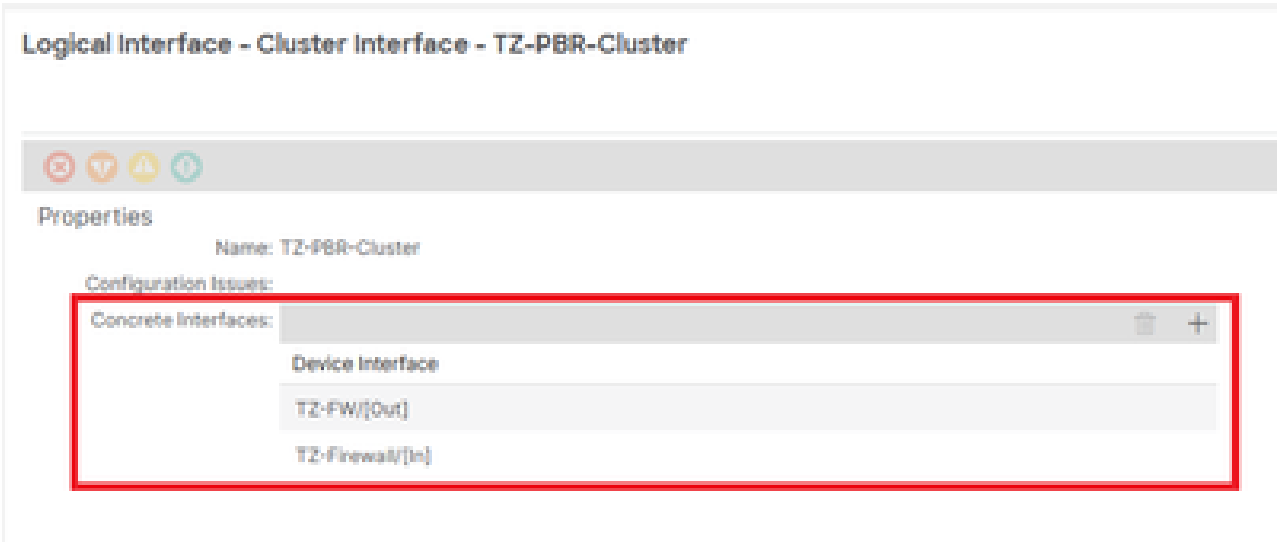
  Resolutie: Controleer of de BD is opgegeven in het beleid voor apparaatselectie en of de naam van de connector correct is. Deze configuratie bevindt zich onder Huurder > Services > L4-L7 > Apparaatselectiebeleid > [Contract + SG] > [Consument | Aanbieder] .



- LIf heeft geen relatie met CIf en LIf heeft een ongeldig CIf
- Geen clusterinterface gevonden

  Deze fouten geven aan dat het apparaat geen relatie heeft met de clusterinterfaces.

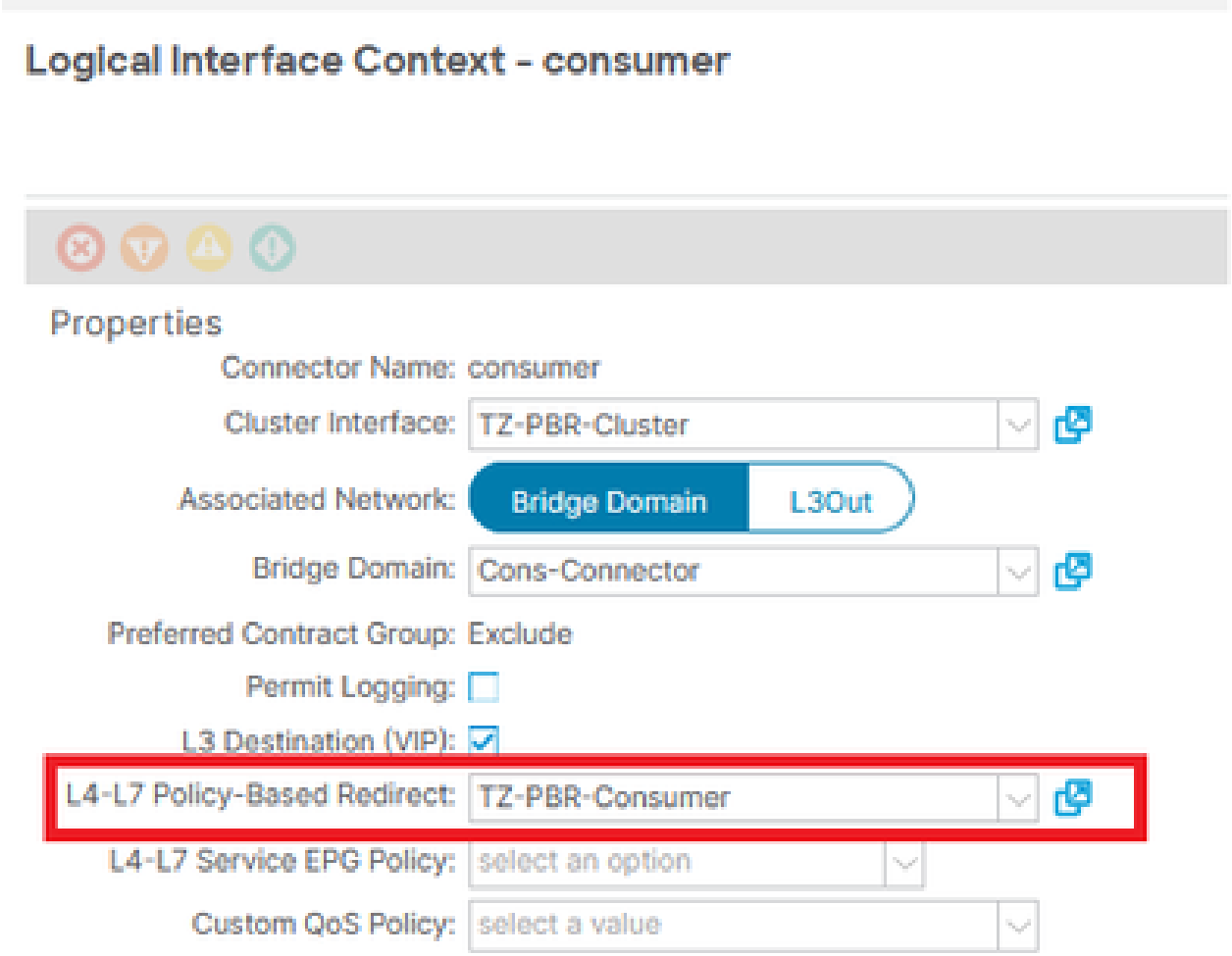
  Resolutie: Zorg ervoor dat de configuratie van het Layer 4 tot Layer 7 (L4-L7)-apparaat een specifieke concrete interfacekiezer bevat. Deze configuratie bevindt zich onder Huurder > Services > L4-L7 > Apparaten > [Apparaat] > Clusterinterfaces.



- Ongeldig omleidingsbeleid voor service

  Deze fout betekent dat het PBR-beleid niet is toegepast ondanks het feit dat de omleiding is geactiveerd op de servicefunctie in de servicegrafiek.

  Resolutie: zorg ervoor dat het PBR-beleid is geconfigureerd in de instellingen van het Beleid voor apparaatselectie. Deze configuratie bevindt zich onder Huurder > Services > L4-L7 > Apparaatselectiebeleid > [Contract + SG] > [Consument | Aanbieder] .



F0759: graph-rendering-failure - "Servicegrafiek voor tenant < tenant > kon niet worden geïnstantieerd. Functie node < node > configuratie is ongeldig."

De servicegrafiek voor de opgegeven tenant kon niet worden geïnstantieerd vanwege een ongeldige configuratie van de naam van de functienode.

Deze fout suggereert dat er configuratieproblemen zijn met betrekking tot de bovengenoemde voorwaarden.

Bovendien kan deze fout tijdens de eerste implementaties tijdelijk optreden en vervolgens snel worden opgelost. Dit komt door het renderingsproces dat de ACI ondergaat om alle beleidsregels te implementeren.

Oplossing: onderzoek eventuele aanvullende fouten die zijn gemeld en los ze dienovereenkomstig op.

F0764: configuratie mislukt - "L4-L7 Apparaatconfiguratie < apparaat > voor tenant < tenant > is ongeldig."

De servicegrafiek voor de opgegeven tenant kon niet worden ingesteld vanwege een ongeldige configuratie van het PBR-apparaatbeleid.

Deze fout suggereert dat er configuratieproblemen zijn met betrekking tot de bovengenoemde voorwaarden.

Oplossing: onderzoek eventuele aanvullende fouten die zijn gemeld en los ze dienovereenkomstig op.

F0772: configuratie mislukt - "LIf-configuratie < cluster > voor L4-L7-apparaten < apparaat > voor tenant < tenant > is ongeldig."

De servicegrafiek voor de opgegeven tenant kon niet worden geïnstantieerd vanwege een ongeldige configuratie van de PBR Device Cluster-interfaceselectie.

Deze fout suggereert dat er configuratieproblemen zijn met betrekking tot de bovengenoemde voorwaarden.

Oplossing: onderzoek eventuele aanvullende fouten die zijn gemeld en los ze dienovereenkomstig op.

Stap 2: Bron- en bestemmingseindpunt leren

Zorg ervoor dat uw bron- en bestemmingseindpunten worden herkend in de fabric, wat basisconfiguratie vereist:

- Een object Virtual Routing and Forwarding (VRF).
- Een Bridge Domain (BD)-object met Unicast Routing ingeschakeld. Hoewel het inschakelen van IP Data Plane-leren als beste praktijk wordt beschouwd, is het niet verplicht.
- Een object Endpoint Group (EPG), dat zowel op virtuele als op fysieke domeinen van toepassing is.
- Toegangsbeleid: controleer of de configuratieketen van uw toegangsbeleid volledig is en of er geen fouten in de EPG worden gemeld.

Om het leren van het eindpunt op de juiste EPG en interface te bevestigen, voert u deze opdracht uit op het blad waar het eindpunt is geleerd, ook bekend als compute leaf:

<#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#
```

Met deze opdracht kunt u de pcTag (sclass) identificeren die is gekoppeld aan de EPG waar het eindpunt is geclassificeerd, evenals de interface, het VRF-bereik en MAC-adresinformatie ophalen.

Als u de locatie van uw bron- of bestemmingseindpunt niet weet, kunt u zichzelf altijd helpen met dit commando op de APIC:

<#root>

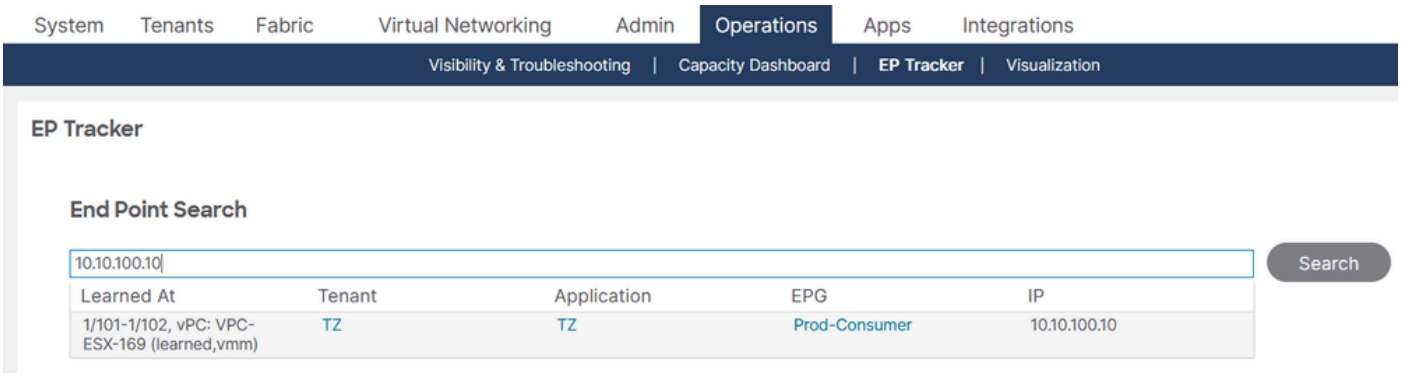
```
show endpoint [ ip | mac ] [ x.x.x.x | eeee.eeee.eeee ]
```

<#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#
```

In de GUI kan de EP Tracker-functie worden gebruikt om naar Operations > EP Tracker te navigeren voor bewaking en beheer van het eindpunt.



Met de informatie die is verzameld uit de bron- en bestemmingseindpunten, kunt u zich nu richten op de implementatie van PBR-beleid.

Stap 3: Contract omleiden

PBR is geïntegreerd in het Service Graph framework. Dientengevolge moet een servicegrafieksjabloon worden geïmplementeerd en geconfigureerd op zowel de bron- als de bestemmings-switch in overeenstemming met een contract. Met behulp van de pcTags-informatie die in de vorige stap is verzameld, kunt u nagaan of een Endpoint Group (EPG) wordt omgeleid naar een Service Graph-groep door deze opdracht uit te voeren.

<#root>

show zoning-rule scope [vrf_scope]

In de bestemmingsplannen moeten deze regels in acht worden genomen:

1. Bron EPG naar bestemming EPG met een bijbehorende omleidingsgroep
2. Bron PBR-node schaduw-EPG naar bron-EPG
3. Bestemmings-EPG naar bron-EPG met een bijbehorende omleidingsgroep. Deze groep kan identiek zijn aan of verschillen van de vorige configuratie.

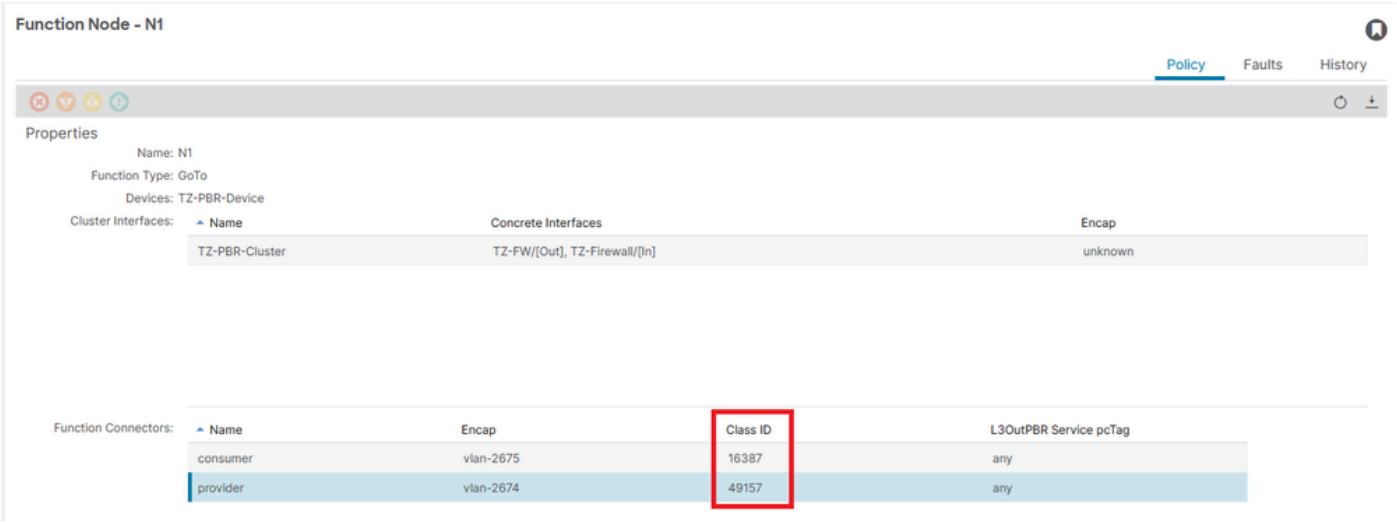
4. Schaduw-EPG van PBR-node naar bestemming-EPG

<#root>

```
Leaf101#

show zoning-rule scope 2162692
```

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

Als u de pcTag van de schaduw-EPG's wilt verifiëren die zijn gemaakt tijdens het implementatieproces voor beleidsgebaseerde routering (PBR), gaat u naar Tenants > [TENANT_NAME] > Services > L4-L7 > Deployed Graph Instance > [SG_NAME] > Function Node - N1.



- Contractparser

Het script correleert bestemmingsregels, filters, statistieken en EPG-namen. U kunt dit script veilig rechtstreeks uitvoeren op een ACI-blad of APIC. Wanneer het wordt uitgevoerd op de APIC, verzamelt het concrete objecten over alle switches van bladeren, wat enkele minuten kan duren voor grote beleidsimplementaties.

Vanaf ACI versie 3.2 wordt de contract_parser gebundeld in de afbeelding en beschikbaar op het blad. Voer gewoon contract_parser.py in vanuit de iBash-shell.

<#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#
```

Deze opdracht bevat details zoals de contractactie, bron- en bestemmings-EPG's, de gebruikte contractnaam en het aantal treffers.

Stap 4: Omleidingsgroep

Nadat de omleidingsgroep is geïdentificeerd op basis van het contract dat is toegepast op de bestemmingsregels, is de volgende stap het bepalen van de IP- en MAC-adressen van het (de) apparaat(en) waarop de omleiding is (zijn) gericht. Om te helpen met dit, voert u het commando:

<#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#
```

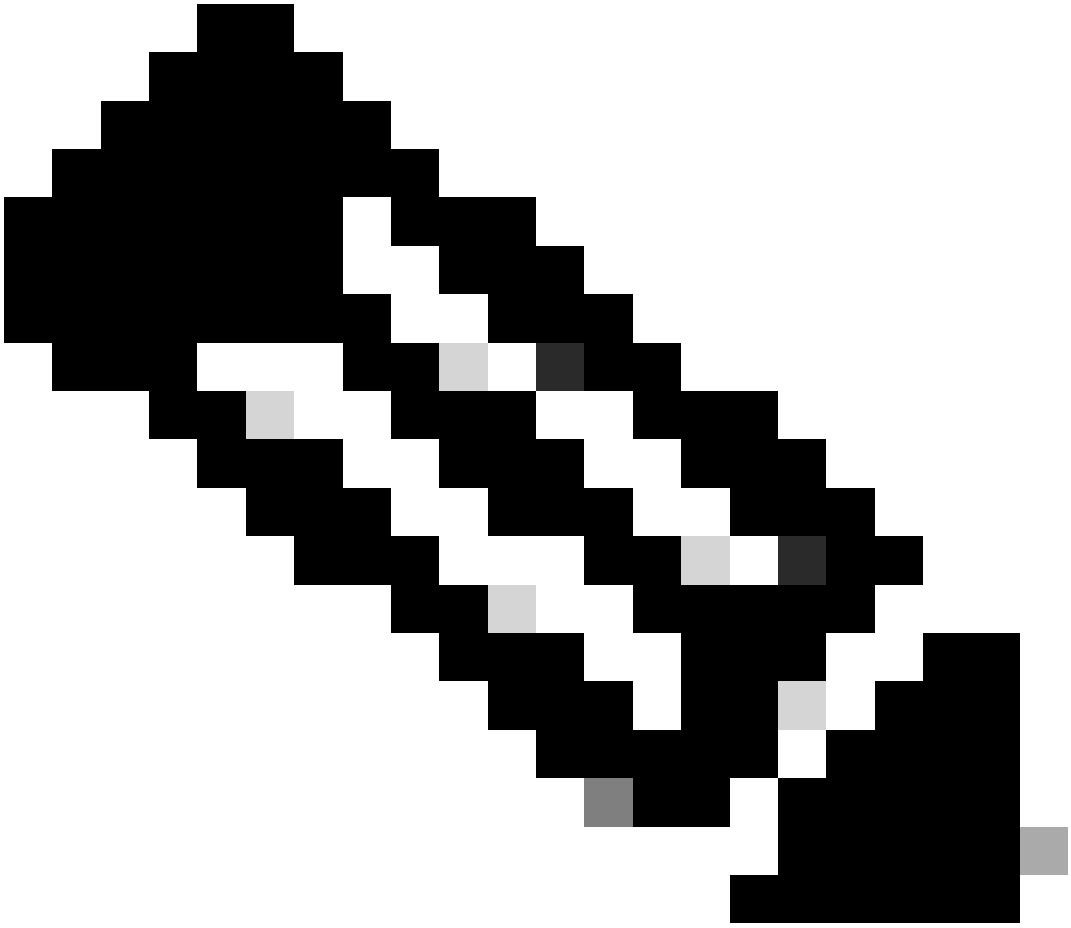
Met deze opdracht kunnen we de operationele status (OperSt) van onze omleidingsgroep bepalen, het IP-adres dat is geconfigureerd in de sectie L4-L7 PBR en de VNID van de VRF die is gekoppeld aan de PBR-node bridge-domeinen. U moet nu het geconfigureerde MAC-adres bepalen:

<#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#
```

Naast de eerder genoemde details biedt deze opdracht waardevolle inzichten, waaronder de VRF-naam, BD VNID en het geconfigureerde MAC-adres van de PBR-node.



Opmerking: Het is belangrijk op te merken dat zowel het IP- als het MAC-adres in dit stadium door de gebruiker zijn geconfigureerd, wat betekent dat typografische fouten kunnen optreden tijdens de L4-L7-definitie van routering op basis van beleid.

Stap 5: PBR-node ontvangt geen verkeer.

Een veel voorkomend probleem met PBR-doorsturen is de afwezigheid van verkeer dat de PBR-node bereikt. Een veelvoorkomende oorzaak van dit probleem is een onjuist opgegeven MAC-adres in de L4-L7-configuratie op basis van beleidsregels.

Om de nauwkeurigheid van het MAC-adres te controleren dat is geconfigureerd in de L4-L7-beleidsgebaseerde routering, voert u de eerder gebruikte opdracht uit vanaf stap 2. Dit commando kan worden uitgevoerd op de leaf switch die is aangewezen als het serviceblad, waar de node naar verwachting zal worden aangeleerd.

<#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#
```

Controleer of het MAC-adres in de EPM-tabel overeenkomt met het adres dat is geconfigureerd in de serviceredirectiegroep. Zelfs kleine typografische fouten moeten worden gecorrigeerd om een goede verkeersroutering naar de bestemming van de PBR-node te garanderen.

Stap 6: Verkeersstroom.

- FTRIAGE

Een CLI-tool voor de APIC die is ontworpen om de configuratie en interpretatie van ELAM-processen end-to-end te automatiseren. Met de tool kunnen gebruikers een bepaalde stroom en de switch van het blad opgeven waar de stroom vandaan komt. Het voert achtereenvolgens ELAM's uit op elk knooppunt om het doorstuurpad van de stroom te analyseren. Deze tool is vooral nuttig in complexe topologieën waar het pakketpad niet gemakkelijk te onderscheiden is.

<#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:

De Embedded Logic Analyzer Module (ELAM) is een diagnostisch hulpmiddel dat gebruikers in staat stelt om specifieke omstandigheden in hardware vast te stellen om het eerste pakket of

frame vast te leggen dat aan die criteria voldoet. Wanneer een opname succesvol is, wordt de ELAM-status aangegeven als geactiveerd. Bij het activeren wordt de ELAM uitgeschakeld, waardoor een datadump kan worden verzameld, wat de analyse van de vele doorstuurbeslissingen die door de ASIC van de switch voor dat pakket of frame worden uitgevoerd, vergemakkelijkt. ELAM werkt op het ASIC-niveau en zorgt ervoor dat het geen invloed heeft op de CPU of andere bronnen van de switch.

Structuur van de commando syntaxis. Deze structuur is verzameld uit het boek Problemen oplossen 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]
```

Voorwaarden instellen om te activeren

```
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]
```

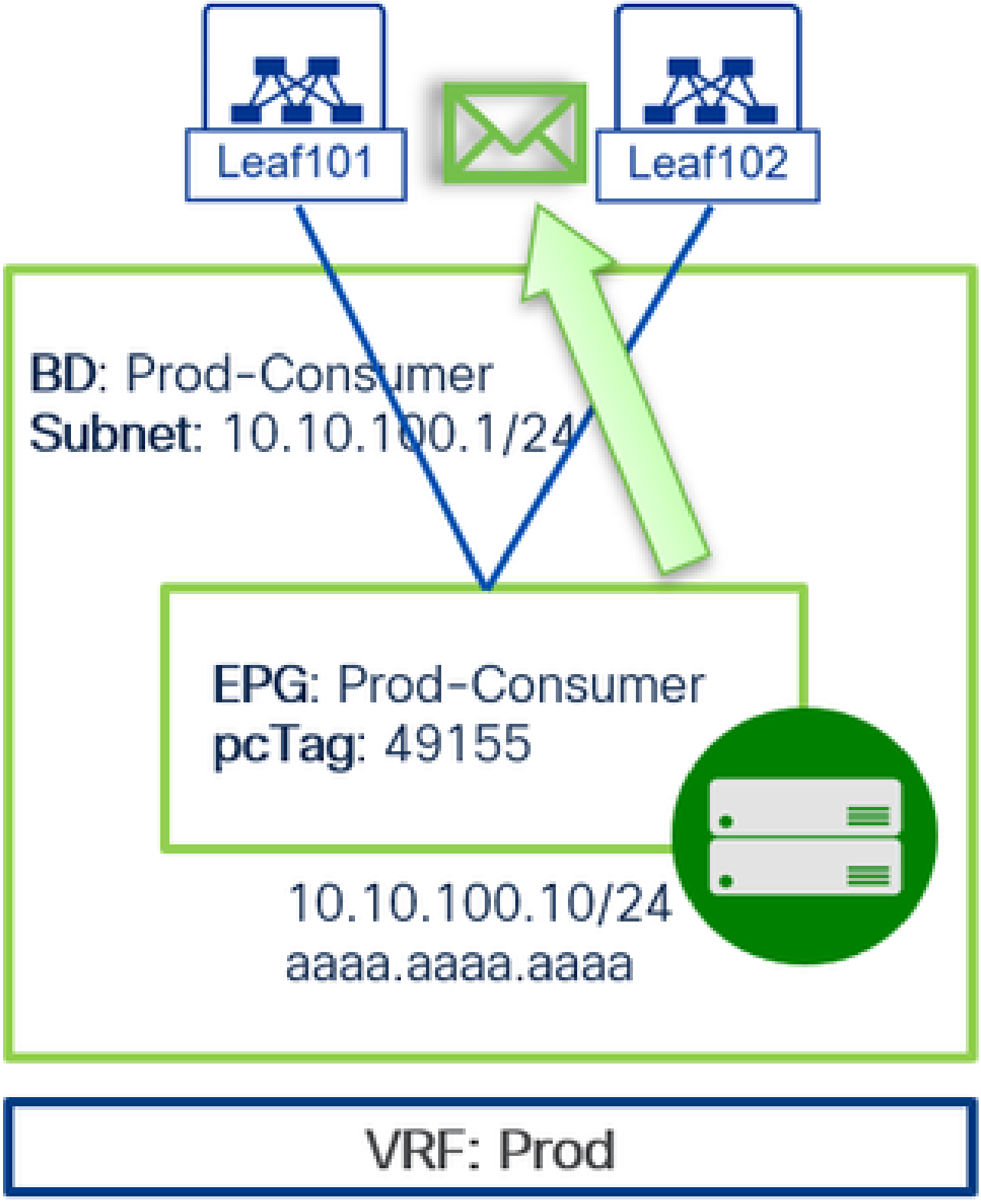
Genereer de dump met de pakketanalyse.

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

- Verkeersstroom

Het is van cruciaal belang om de verkeersstroom over alle apparaten in kwestie te begrijpen. De Ftriage tool geeft een uitstekende samenvatting van deze flow. Echter, voor een gedetailleerde stapsgewijze validatie en om dieper inzicht te krijgen in het pakketontvangstproces, kunt u Embedded Logic Analyzer Module (ELAM) uitvoeren op elk punt binnen de netwerktopologie.

1. Ingress-verkeer vindt plaats op het computerblad waar de bronserver wordt aangeleerd. In dit specifieke scenario moet ELAM worden geconfigureerd op de vPC-peers, aangezien de bron zich achter een vPC-interface bevindt. Dit is nodig omdat de fysieke interface die is geselecteerd door het hashing-algoritme onbepaald is.



<#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


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

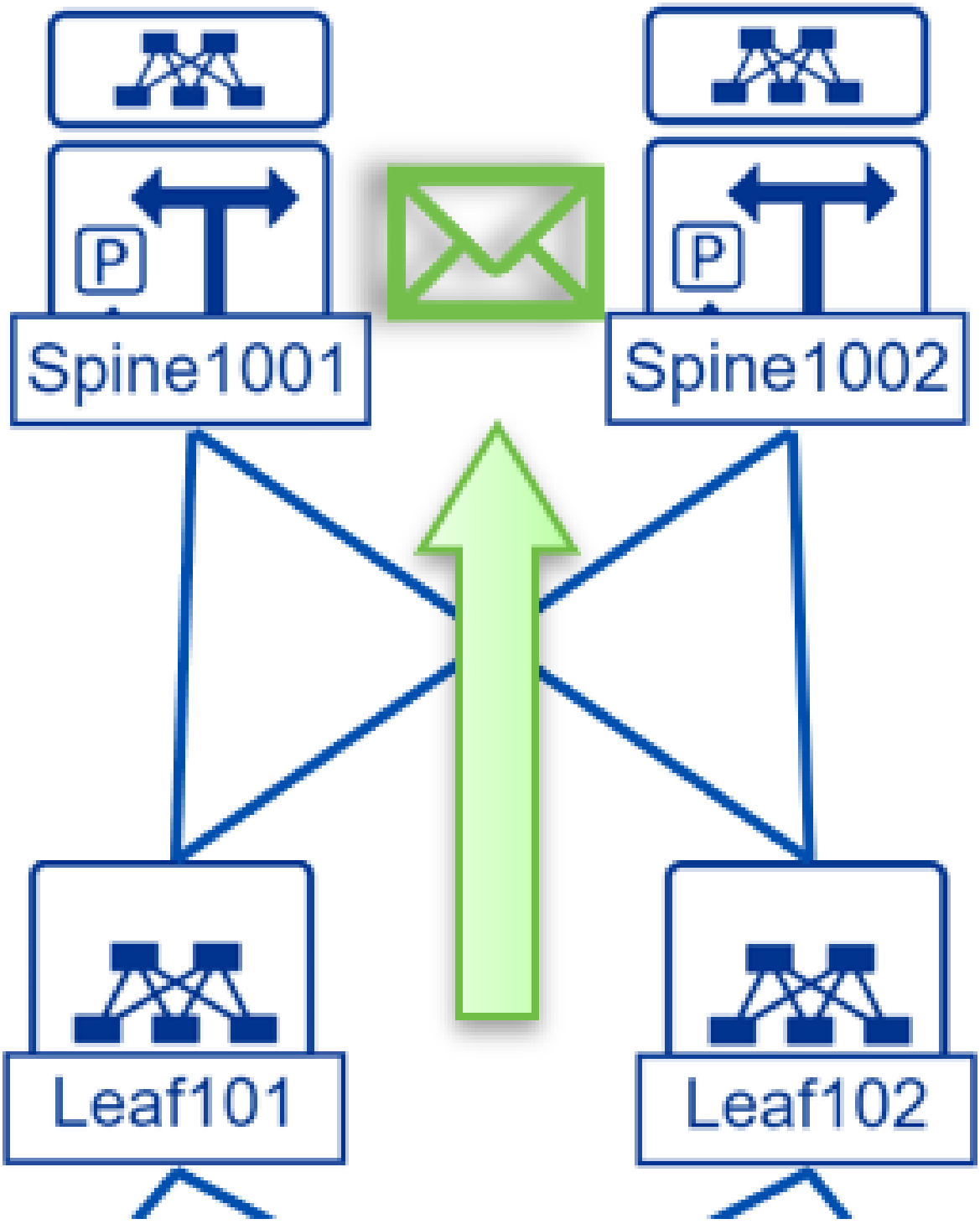
Op basis van de verstrekte informatie is het duidelijk dat het pakket wordt omgeleid via Policy-Based Routing (PBR), omdat de service_revisor-optie is ingeschakeld. Bovendien haalt u de klasse- en dclass-waarden op. In dit specifieke geval herkent de switch de dclass. Als het bestemmingseindpunt echter niet in de EPM-tabel aanwezig is, wordt de waarde voor dclass standaard 1.

Bovendien wordt de ingress-interface bepaald door de SRCID en wordt de uitgang-interface geïdentificeerd door de vectorwaarden. Deze waarden kunnen worden vertaald naar een voorpoort door deze opdracht op het niveau vsh_lc uit te voeren:

<#root>

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

2. De volgende stap in de stroom omvat het bereiken van de switch van de wervelkolom om het MAC-adres van de bestemming aan de PBR-node toe te wijzen. Aangezien het verkeer is ingekapseld in VXLAN-headers, is voor het uitvoeren van ELAM op een ruggengraat of extern blad het gebruik van in-select 14 vereist om de inkapseling goed te decoderen.



<#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

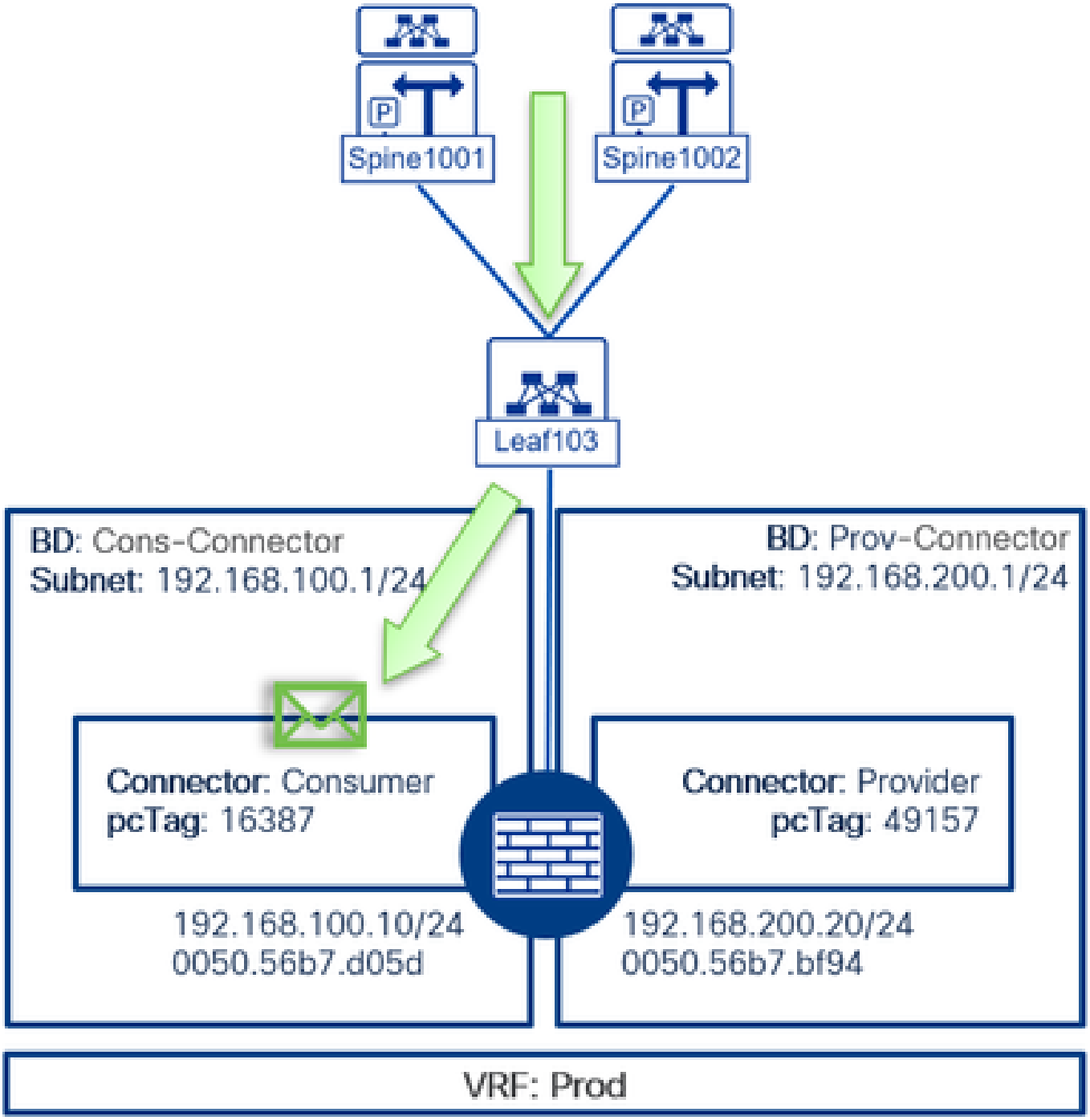
Uit de vorige uitvoer blijkt dat het MAC-adres van de bestemming wordt herschreven naar het MAC-adres van de firewall. Vervolgens wordt een COOP-zoekopdracht uitgevoerd om de bestemmingspublicator van de MAC te identificeren en wordt het pakket vervolgens doorgestuurd naar de corresponderende interface van de switch.

U kunt dit opzoeken op de wervelkolom simuleren door deze opdracht uit te voeren met behulp van de Bridge Domain VNID en het MAC-adres van de 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. Het verkeer bereikt het serviceblad waar het MAC-adres van de firewall wordt herkend en vervolgens wordt doorgestuurd naar de PBR-node.



<#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 )
```

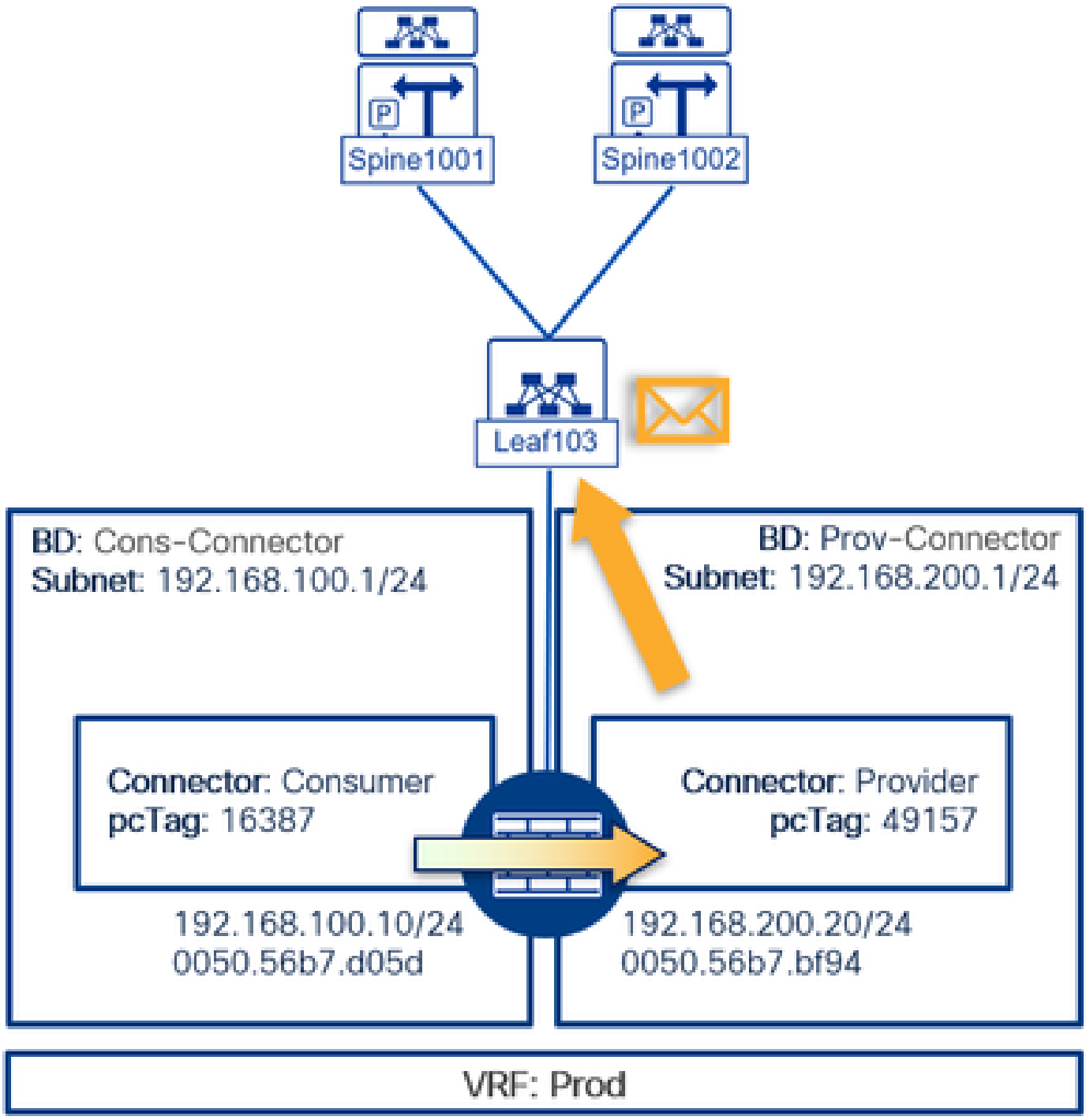
sclass (src pcTag) : 49155(0xC003) >>> Prod-Consumer EPG

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. Voor de verpakker die wordt geretourneerd door de PBR-node, moet deze eerst zijn eigen zorgvuldigheid maken en de VRF, interface of VLAN laten wijzigen. Het pakket wordt vervolgens teruggestuurd naar ACI op de Provider-connector:



<#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

---

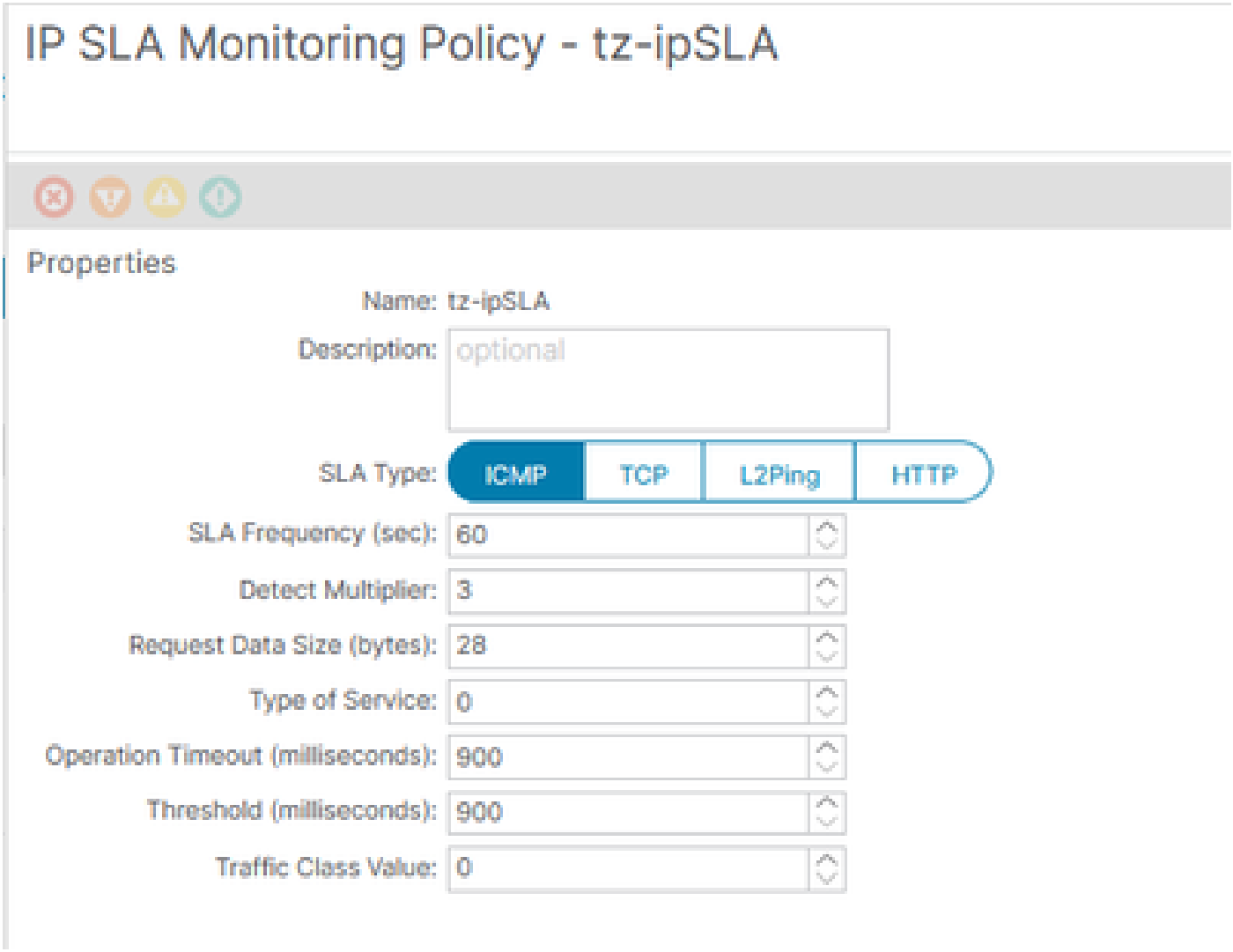
5. Het resterende netwerkverkeer voldoet aan de tot nu toe genoemde vastgestelde stappen, waarbij pakketten terugkeren naar de switches van de wervelkolom om de uiteindelijke serverbestemming te bepalen, op basis van de coop-zoekopdracht. Vervolgens worden pakketten naar de compute leaf switch geleid die de lokale leervlag heeft en deze informatie naar de COOP-tabel op de stekels heeft verspreid. De ELAM-uitvoering voor stap 2 en stap 3 is consistent voor de distributie van het pakket naar de eindbestemming. Het is essentieel om deze te valideren via de bestemming EPG pcTag en de uitgang-interface om een nauwkeurige levering te garanderen.

IP-SLA

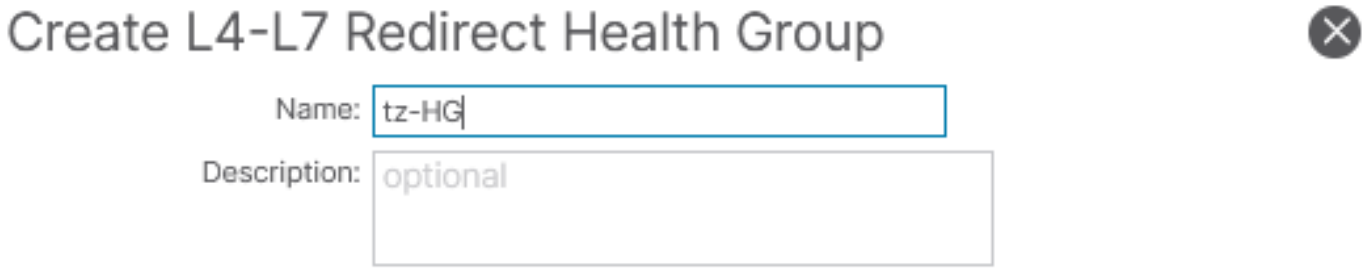
IP SLA wordt gebruikt om de operationele status en prestaties van netwerkpaden te beoordelen. Het helpt ervoor te zorgen dat het verkeer efficiënt wordt gerouteerd volgens het gedefinieerde beleid, op basis van realtime netwerkomstandigheden. In ACI maakt PBR gebruik van IP SLA om weloverwogen routeringsbeslissingen te nemen. Als de IP SLA-statistieken aangeven dat een pad minder goed presteert, kan PBR het verkeer omleiden via alternatieve paden die voldoen aan de vereiste prestatiecriteria.

Vanaf versie 5.2(1) kunt u Dynamic MAC-tracking inschakelen voor IP SLA, dit is handig voor scenario's waarbij een PBR-knooppunt omvalt en het MAC-adres voor hetzelfde IP-adres wijzigt, in statische implementaties moet elke keer dat de PBR-knooppunt zijn MAC-adres wijzigt om het verkeer te blijven verzenden, een wijziging in het beleid voor beleidsgebaseerde omleiding worden uitgevoerd. Met IP SLA wordt het MAC-adres dat in dit beleid wordt gebruikt, doorgegeven aan de sondereactie. Verschillende sondes kunnen worden gebruikt om te bepalen of de PBR-node gezond is of niet, op het moment van dit schrijven, deze omvatten: ICMP, TCP, L2Ping en HTTP.

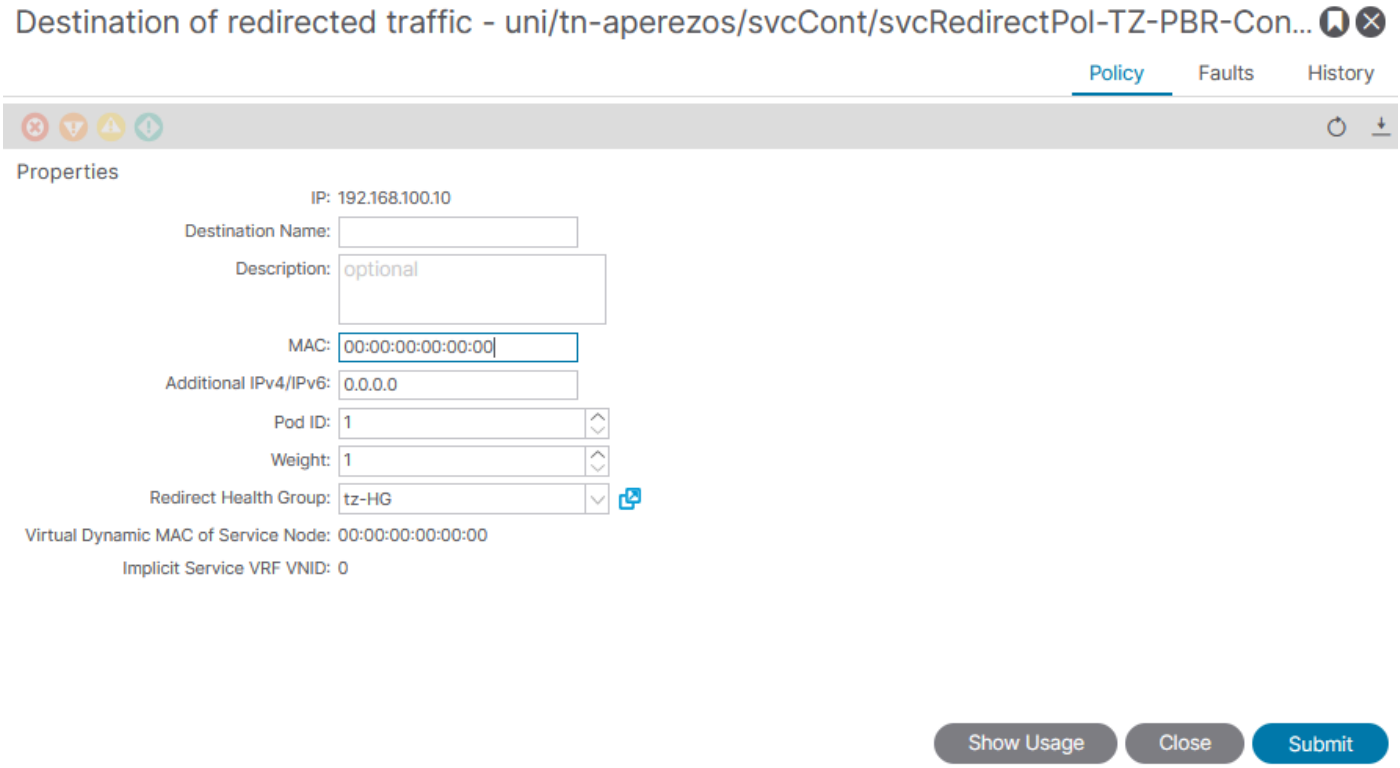
De algemene configuratie van een IP SLA-beleid moet er als volgt uitzien:



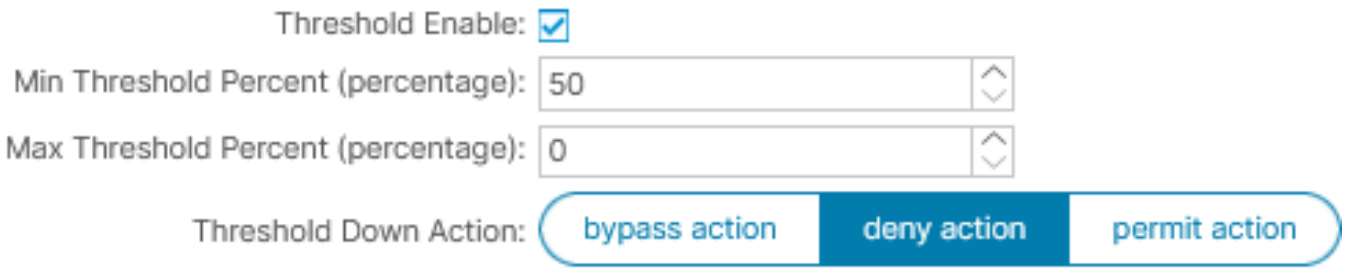
Het IP SLA-beleid moet worden gekoppeld aan de PBR-node IP door middel van een Health Group.



Als IP SLA wordt gebruikt om dynamisch het MAC-adres te detecteren, kan dit veld niet leeg zijn, maar worden ingesteld op alle 0s:



Zodra een gezondheidsgroep via de L3-bestemming in het L4-L7 Policy Based Redirect-beleid is gekoppeld aan de PBR-node IP, stelt u drempels in om het IP SLA-gedrag te definiëren wanneer het niet bereikbaar is. Geef een minimumaantal actieve L3-bestemmingen op dat vereist is om de omleiding te behouden. Als het aantal actieve PBR-knooppunten onder of boven het drempelpercentage valt, wordt de hele groep beïnvloed door de geselecteerde drempelwaardeverlaging, waardoor herverdeling wordt gestopt. Deze aanpak ondersteunt het omzeilen van de PBR-node tijdens het oplossen van problemen zonder de verkeersstroom te beïnvloeden.



Gezondheidsgroepen verbinden alle IP's die zijn gedefinieerd in L3 Bestemmingen van één L4-L7 Beleidsbasis-omleidingsbeleid of meerdere L4-L7 Beleidsbasis-omleidingsbeleid zolang hetzelfde beleid van de Gezondheidsgroep wordt gebruikt.

```
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#
```

Gerelateerde informatie

- Whitepaper over het ontwerp van de op het beleid gebaseerde redirect-servicegrafiek van Cisco Application Centric Infrastructure
- ACI Layer 4-7 Policy-Based Redirect (PBR) Diepduiken en tips (Cisco Live Presentatie)
- Problemen oplossen met IP SLA op multipod PBR

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.