排除ACI中的PBR故障

目錄

簡介

本文描述如何在單個Pod交換矩陣中使用基於策略的重定向(PBR)對以應用為中心的基礎設施(ACI)環境進行故障排除。

必要條件

需求

建議您瞭解以下主題的一般知識：

- ACI概念：訪問策略、終端學習、合約和L3out

採用元件

本故障排除練習是在ACI 6.0(8f)版上進行的，使用的是第二代Nexus交換機N9K-C93180YC-EX和N9K-C93240YC-FX2。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

縮寫

- BD:網橋域
- EPG:終端組

- 類ID:標識EPG的標籤
- PBR節點：用於PBR目的地的L4-L7裝置
- 使用者聯結器：面向使用者端的PBR節點介面
- 提供程式聯結器：面向提供商端的PBR節點介面

PBR歷史記錄

版本	主要功能
2.0（1米）	• 服務圖提供PBR功能。
3.x及更低版本	• 多節點基於策略的重定向(PBR)支援 • PBR彈性雜湊
3.2(x)	• 多站點環境中支援單節點防火牆PBR。
4.0(x)	• 多站點環境中支援雙節點防火牆PBR。
4.2(1)	• 現在支援用於建立備用PBR節點的備份策略。
4.2(3)	• 使用GUI的Service Graph模板中提供了Filter-from-contract選項。
5.0(1)	• 服務節點的所有提供商端都支援L3Outs。 • 第1層/第2層PBR裝置支援主動 — 主動部署/ECMP路徑。
5.2(1)	• PBR目標現在可位於L3Out中。 • 您可以使用HTTP URI跟蹤服務節點。 • 不再支援服務圖託管和混合模式。 • 支援動態PBR節點mac地址。
6.0(1)	• 基於權重的對稱原則型重新導向(PBR)

設計注意事項

- PBR可與物理裝置和虛擬裝置配合使用
- PBR可以在L3Out EPG和EPG之間、EPG之間以及L3Out EPG之間使用。如果L2Out EPG是合約的一部分，則不支援PBR
- 思科ACI多Pod、多站點和遠端枝葉環境支援PBR。
- 思科ACI交換矩陣必須是伺服器和PBR節點的網關
- L4-L7裝置必須在轉到模式（路由模式）下部署

- FEX交換機不支援PBR節點
- PBR節點需要專用的網橋域
- 現在，使用健康組支援PBR節點的動態MAC地址。
- 建議在PBR節點網橋域上啟用基於GARP的檢測
- 包括ARP、乙太網流量和其他非IP流量的通用預設過濾器不得用於PBR
- PBR節點可以在VRF例項之間或在一個VRF例項內。對於此拓撲，不支援在第三個VRF上使用PBR節點，必須在使用者或提供商VRF中配置PBR節點

背景資訊

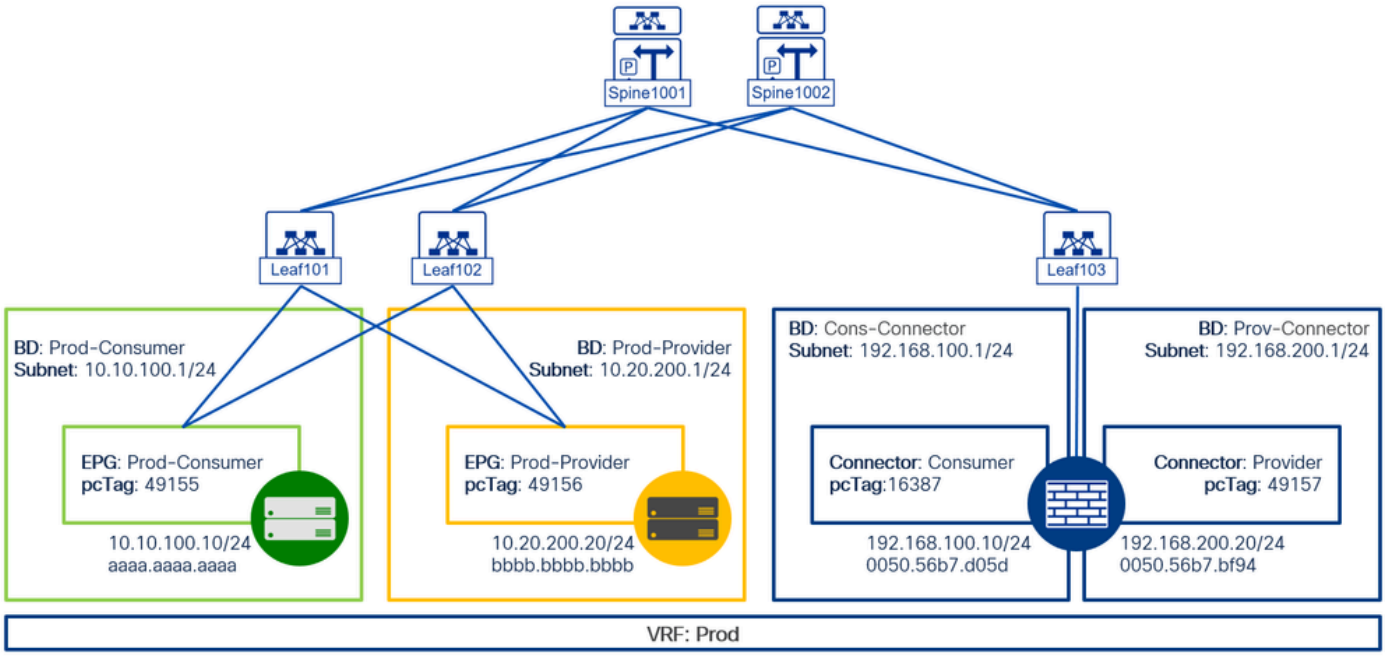
有關ELAM和Ftriage的更多說明，請參閱會話BRKDCN-3900b中的CiscoLive點播庫。

此外，所有配置准則都可以在白皮書思科以應用為中心的基礎架構基於策略的重定向服務圖設計白皮書中找到。

案例：單個Pod交換矩陣中的單個VRF

網路圖表

物理拓撲：



疑難排解

步驟 1:故障

當配置或策略互動存在問題時，ACI會生成故障。在出現故障時，已為PBR呈現過程識別出特定故障：

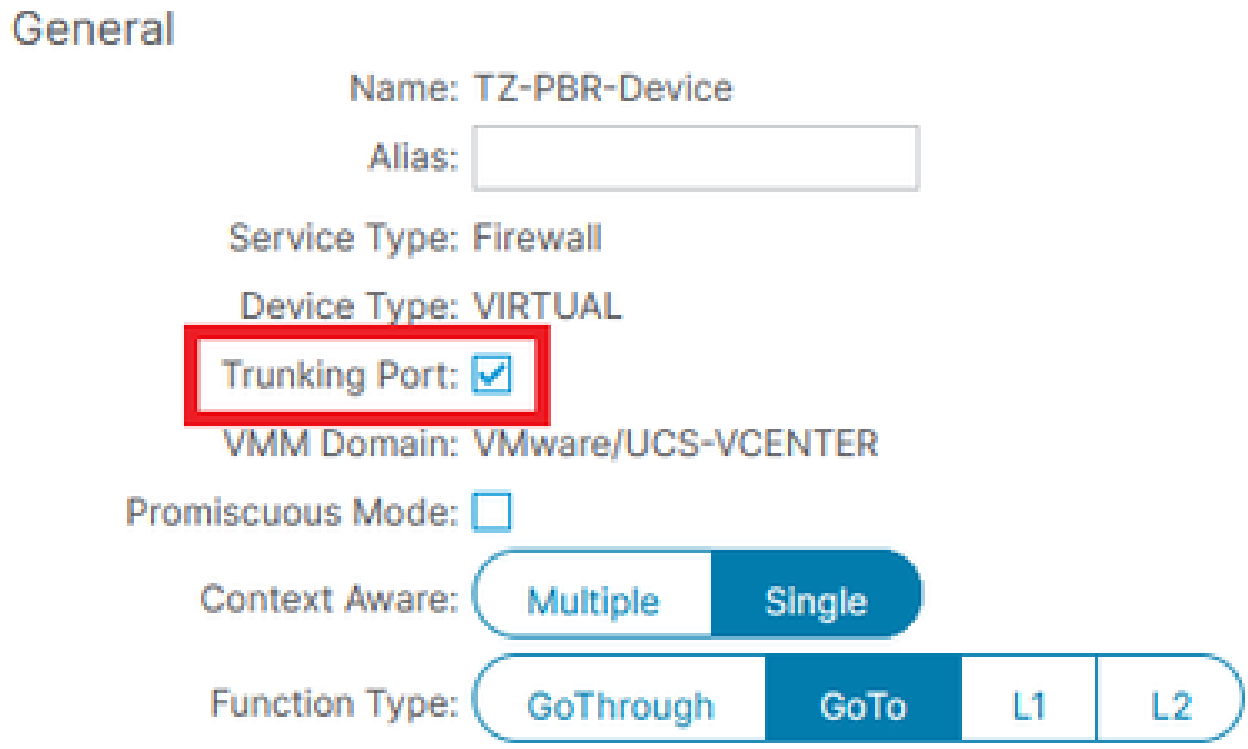
F1690:配置無效，原因是：

- ID分配失敗

此故障表示服務節點的封裝VLAN不可用。例如，與邏輯裝置使用的Virtual Machine Manager(VMM)域關聯的VLAN池中可能沒有可用的動態VLAN。

解析度：驗證邏輯裝置使用的域內的VLAN池。如果邏輯裝置介面在物理域內，還要檢查封裝的VLAN配置。這些設定可在Tenant > Services > L4-L7 > Devices and Fabric > Access Policies > Pools > VLAN下找到。

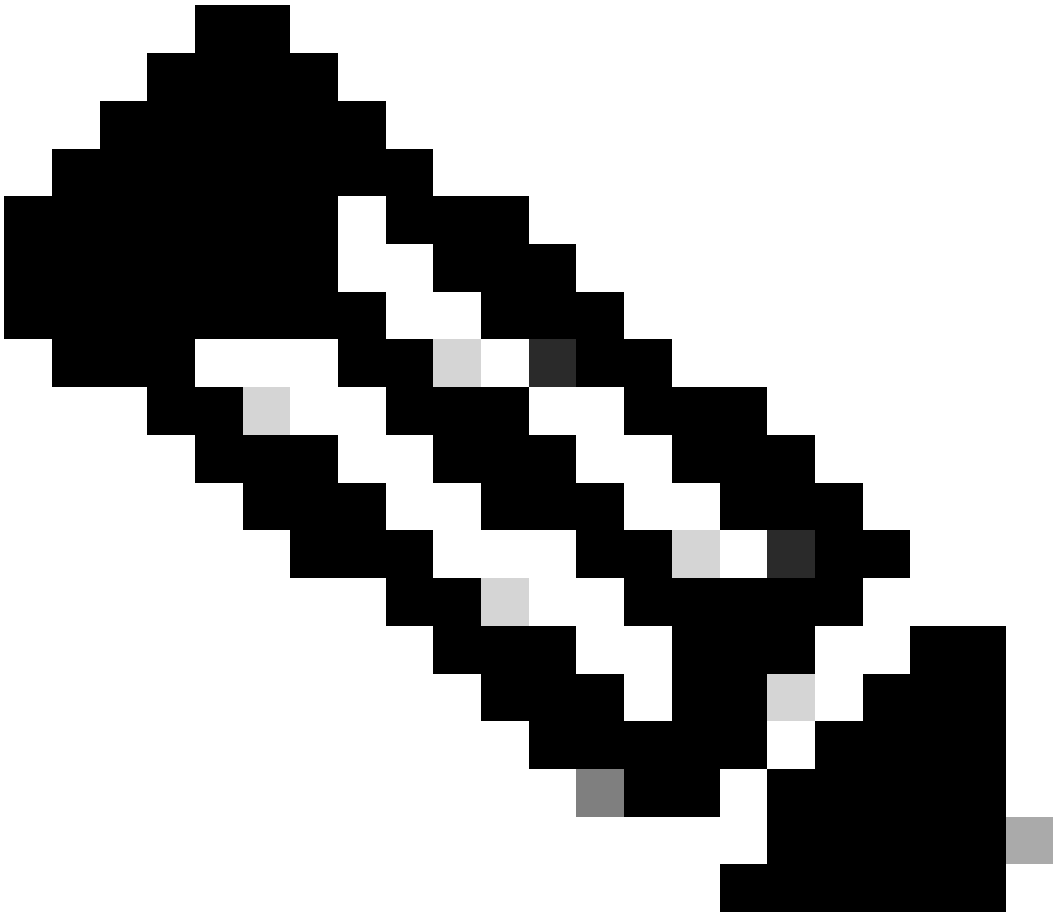
相反，如果邏輯裝置介面位於虛擬域中，並通過中繼介面連線到ESXi主機，請確保已啟用中繼端口選項。



- 找不到LDev的裝置上下文

此故障表示邏輯裝置不可定位用於服務圖形呈現。例如，可能沒有與服務圖關聯的合約相匹配的裝置選擇策略。

解析度：驗證是否已定義裝置選擇策略。裝置選擇策略根據服務圖中的合約名稱、服務圖名稱和節點名稱，指定服務裝置及其聯結器的選擇標準。可在Tenant > Services > L4-L7 > Device Selection Policy下找到此項。

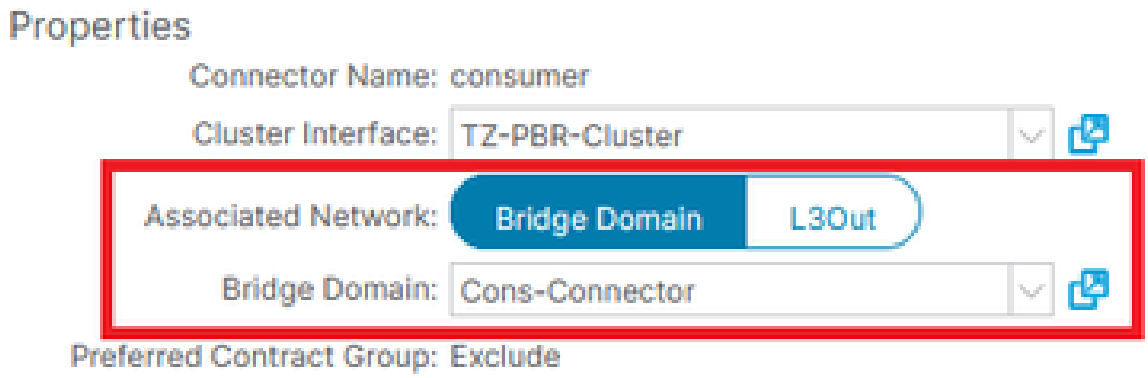


附註：部署服務圖模板時，ACI會預先為源EPG選擇網橋域。您必須更改PBR使用者聯結器的此網橋域。這同樣適用於提供商聯結器。

- 未找到BD

此故障表示找不到服務節點的橋接域(BD)。例如，未在裝置選擇策略中指定BD。

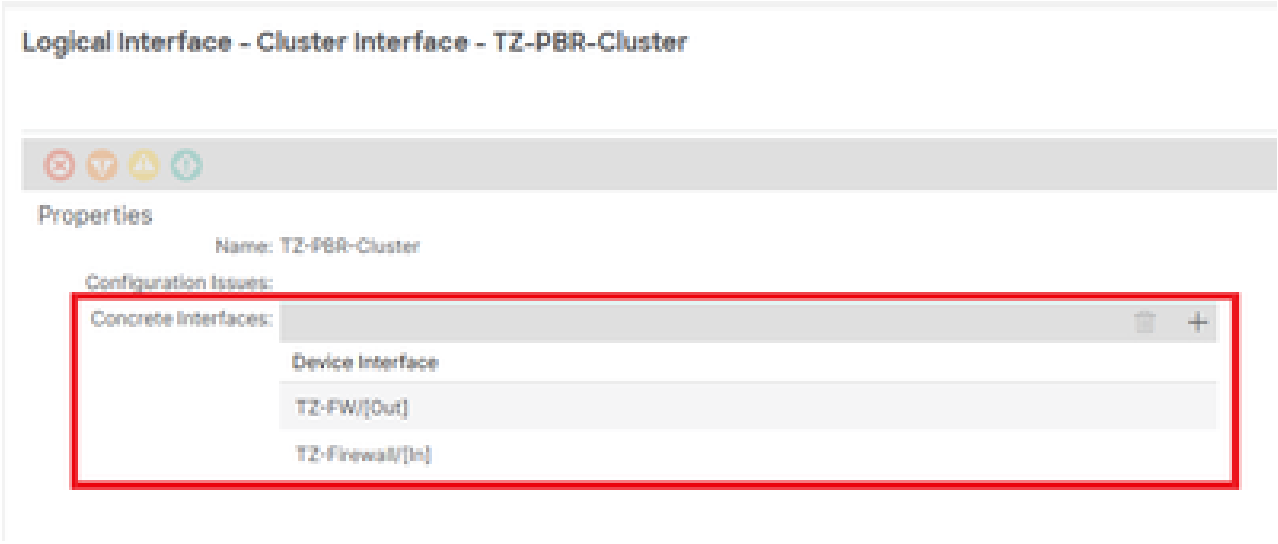
解析度：確保在裝置選擇策略中指定BD並且聯結器名稱正確。此配置位於Tenant > Services > L4-L7 > Devices Selection Policy > [Contract + SG] > [Consumer |提供程式].



- LIf與CIf無關，並且LIf具有無效的CIf
- 找不到群集介面

這些故障表明裝置與群集介面沒有關係。

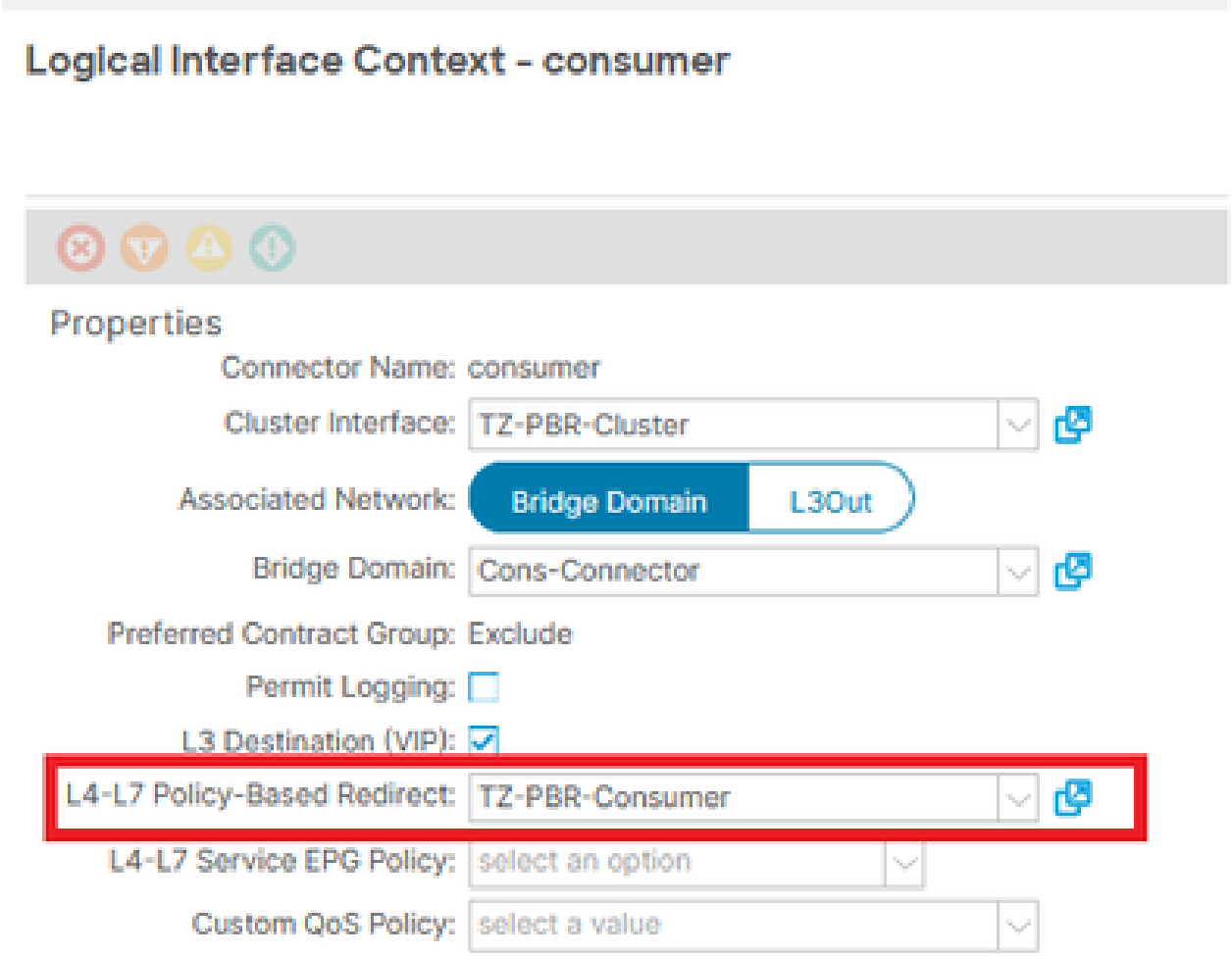
解析度：確保第4層到第7層(L4-L7)裝置配置包括指定的具體介面選擇器。此配置位於Tenant > Services > L4-L7 > Devices > [Device] > Cluster Interfaces下。



- 服務重定向策略無效

此故障表示儘管已在服務圖中的服務功能上啟用重定向，但尚未應用PBR策略。

解析度：確保PBR策略在裝置選擇策略設定中配置。此配置位於Tenant > Services > L4-L7 > Devices Selection Policy > [Contract + SG] > [Consumer |提供程式].



F0759:graph-rendering-failure — 「無法例項化租戶< tenant >的服務圖形。Function node < node > configuration is invalid."

由於函式節點名稱配置無效，無法例項化指定租戶的服務圖。

此錯誤表示存在與上述條件相關的組態問題。

此外，在初始部署期間，此故障可能暫時出現，然後立即解決。這是由於ACI部署所有策略所經歷的呈現過程所致。

解析度：調查已報告的任何其他故障，並相應地加以解決。

F0764:configuration-failed - "L4-L7裝置配置< device > for tenant < tenant >無效。"

由於PBR裝置策略的配置無效，無法例項化指定租戶的服務圖。

此錯誤表示存在與上述條件相關的組態問題。

解析度：調查已報告的任何其他故障，並相應地加以解決。

F0772:configuration-failed - "LIf configuration < cluster > for L4-L7 Devices < device > for tenant < tenant > is invalid。"

由於PBR裝置群集介面選擇的配置無效，無法例項化指定租戶的服務圖。

此錯誤表示存在與上述條件相關的組態問題。

解析度：調查已報告的任何其他故障，並相應地加以解決。

步驟 2:源和目標終端學習

確保在交換矩陣中識別您的源端點和目標端點，這就需要進行基本配置：

- 虛擬路由和轉送(VRF)對象。
- 已啟用單點傳送路由的橋接域(BD)對象。雖然啟用IP資料平面學習被認為是最佳實踐，但並非強制性的。
- 終端組(EPG)對象，適用於虛擬域和物理域。
- 訪問策略：驗證您的訪問策略配置鏈是否完整，以及EPG上是否未報告任何故障。

要在正確的EPG和介面上確認終端學習，請在獲知終端後的枝葉上執行此命令，也稱為計算枝葉：

<#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#
```

此命令允許您標識與終端被分類的EPG關聯的pcTag（類），以及檢索介面、VRF範圍和MAC地址資訊。

如果您不知道源或目標端點的位置，可以隨時在APIC上使用此命令：

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

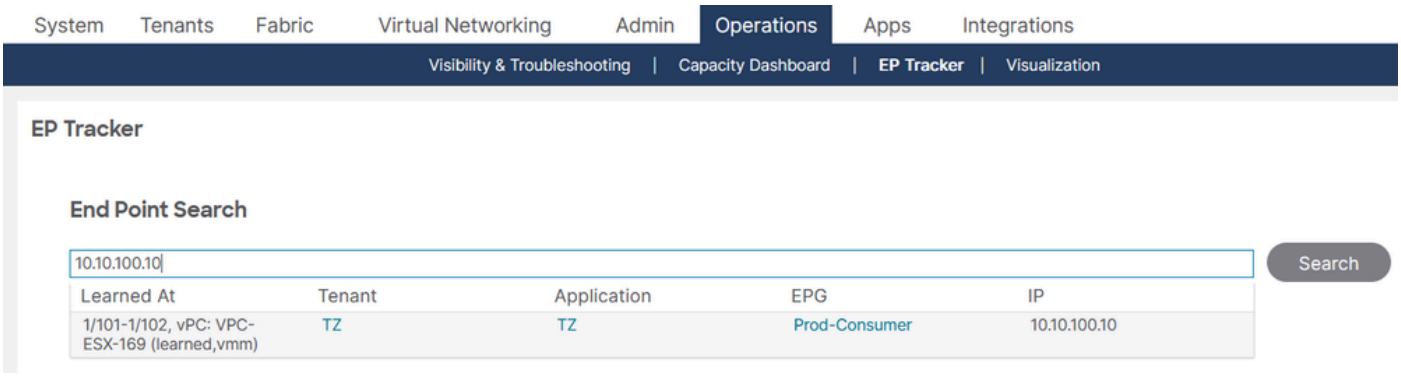
AA:AA:AA:AA:AA:AA 10.10.100.10

```
                              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#
```

在GUI中，可以導航到操作(Operations)> EP跟蹤器(EP Tracker)訪問EP跟蹤器功能，以便進行端點監視和管理。



利用從源和目標終端收集的資訊，您現在可以集中精力進行PBR策略部署。

步驟 3:重新導向合約

PBR整合在服務圖框架中。因此，必須根據合約在源交換機和目標交換機上部署和配置Service Graph模板。利用在上一步中收集的pcTags資訊，您可以通過執行此命令來確定是否已將終端組(EPG)重定向到服務圖組。

<#root>

show zoning-rule scope [vrf_scope]

在分割槽規則中，必須考慮以下規則：

1. 源EPG到目標EPG與關聯的重定向組
2. 源PBR節點影子EPG到源EPG
3. 目標EPG到源EPG以及關聯的重定向組。此組可以與以前的配置相同或不同。
4. 目標PBR節點影子EPG到目標EPG

<#root>

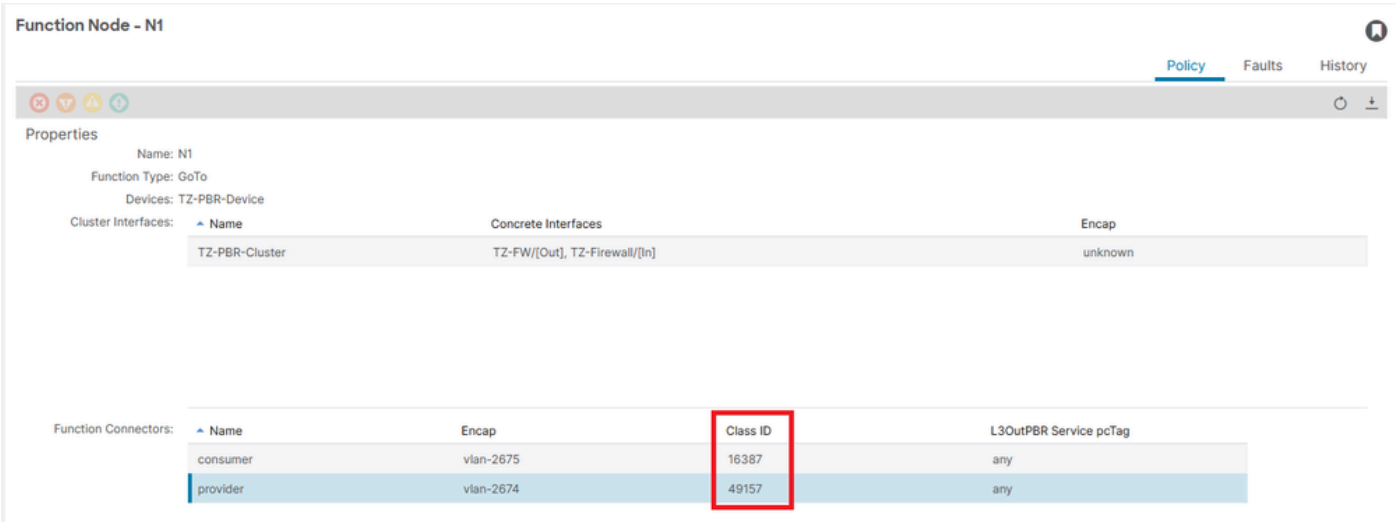
Leaf101#

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#
```

要驗證在基於策略的路由(PBR)部署過程中建立的影子EPG的pcTag，請導航到Tenants > [TENANT_NAME] > Services > L4-L7 > Deployed Graph Instance > [SG_NAME] > Function

Node - N1。



- 合約分析器

該指令碼將分割槽規則、過濾器、統計資訊和EPG名稱相關聯。您可以安全地直接在ACI枝葉或APIC上執行此指令碼。在APIC上運行時，它會收集所有枝葉交換機上的具體對象，對於大型策略部署，這可能需要幾分鐘的時間。

從ACI版本3.2開始，contract_parser捆綁在映像中並在枝葉上可用。只需從iBash shell輸入contract_parser.py。

<#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#

此命令提供合約操作、源和目標EPG、使用的合約名稱以及命中計數等詳細資訊。

步驟 4:重定向組

根據應用於分割槽規則的合約識別重定向組後，下一步是確定重定向目標裝置的IP和MAC地址。為了協助達成此目的，請執行以下命令：

<#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#
```

此命令使我們能夠確定重定向組的操作狀態(OperSt)、在L4-L7 PBR部分配置的IP地址，以及與PBR節點網橋域關聯的VRF的VNID。現在需要確定已配置的MAC地址：

<#root>

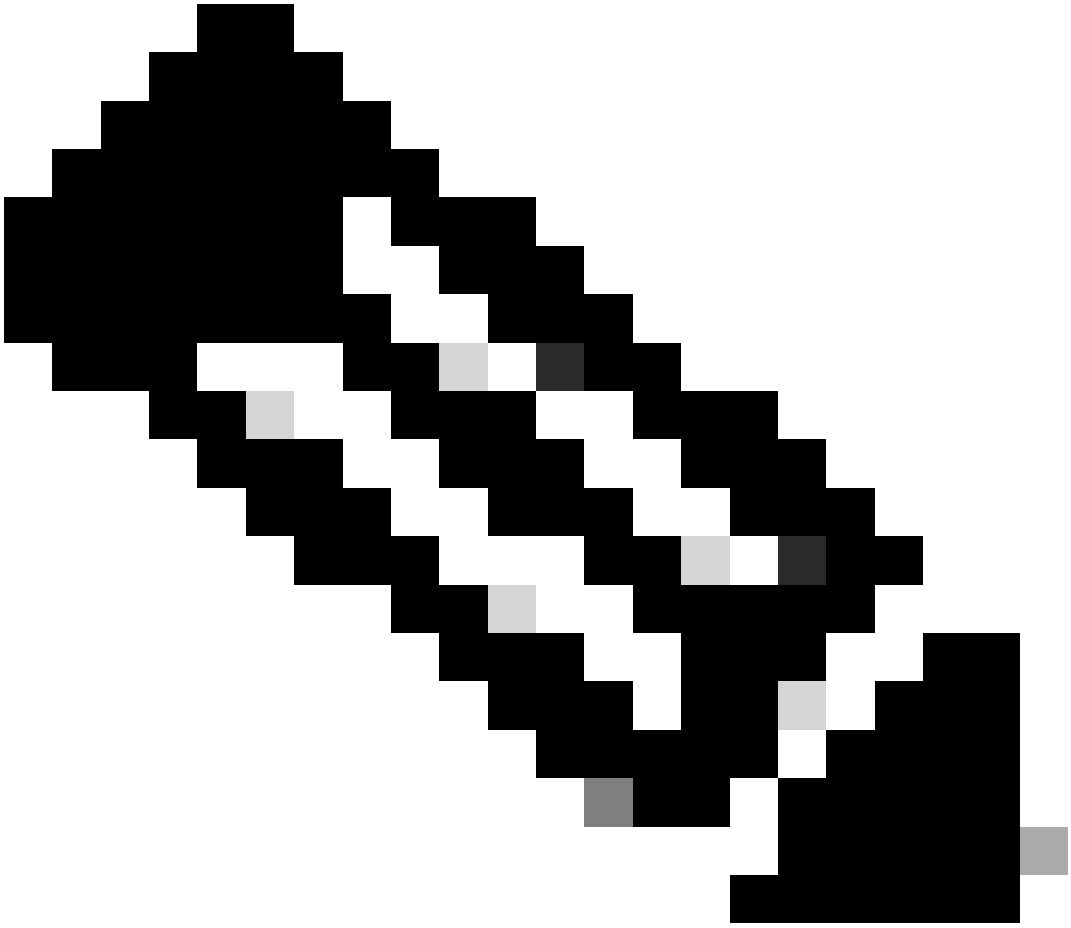
show service redir info destinations ip [PBR-node IP] vnid [VRF_VNID]

<#root>

```
Leaf101#

show service redir info destination ip 192.168.100.10 vnid 2162692


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

192.168.100.10

]-[vxlan-

2162692

] vxlan-

15826939


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

 TZ:Prod

enabled

 no-oper-dest Not attached
Leaf101#
```

```
Leaf101# show service redir info destination ip 192.168.200.20 vnid 2162692
==========================================================================================================
LEGEND
TL: Threshold(Low) | TH: Threshold(High) | HP: HashProfile | HG: HealthGrp | BAC: Backup-Dest | TRA: Tr
==========================================================================================================
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#
```

除了前面提到的詳細資訊，此命令還提供有價值的見解，包括VRF名稱、BD VNID以及PBR節點已設定的MAC位址。



附註：必須注意的是，在此階段，IP和MAC地址都是使用者配置的，這意味著在L4-L7基於策略的路由定義期間可能會發生拼字錯誤。

步驟 5:PBR節點未接收任何流量。

PBR轉發遇到的普遍問題是沒有流量到達PBR節點。此問題的一個常見原因是L4-L7基於策略的路由配置中指定的MAC地址不正確。

要驗證在L4-L7基於策略的路由中配置的MAC地址的準確性，請執行步驟2中以前使用的命令。此命令可在指定為服務枝葉的枝葉交換機上執行，該節點應在該枝葉交換機上獲取。

<#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#
```

驗證EPM表中記錄的MAC地址是否與服務重定向組中配置的MAC地址匹配。即使是次要的排版錯誤也必須糾正，以確保正確的流量路由到PBR節點目標。

步驟 6:流量。

- FTRIAGE

用於APIC的CLI工具旨在自動配置和解釋ELAM端到端流程。該工具允許使用者指定特定流以及流源所在的枝葉交換機。它按順序在每個節點上執行ELAM以分析流的轉發路徑。此工具在封包路徑不易識別的複雜拓撲中尤其有用。

```
<#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:

嵌入式邏輯分析器模組(ELAM)是一種診斷工具，使使用者能夠在硬體中建立特定條件，以捕獲滿足這些條件的初始資料包或幀。捕獲成功後，ELAM狀態顯示為「已觸發」。觸發時，ELAM被禁用，允許收集資料轉儲，這有助於分析交換機ASIC為該資料包或幀執行的眾多轉發決策。ELAM在ASIC級別運行，確保它不會影響交換機的CPU或其他資源。

命令語法的結構。此結構摘自排除ACI交換矩陣內轉發工具故障

```
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]
```

設定觸發條件

```
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]
```

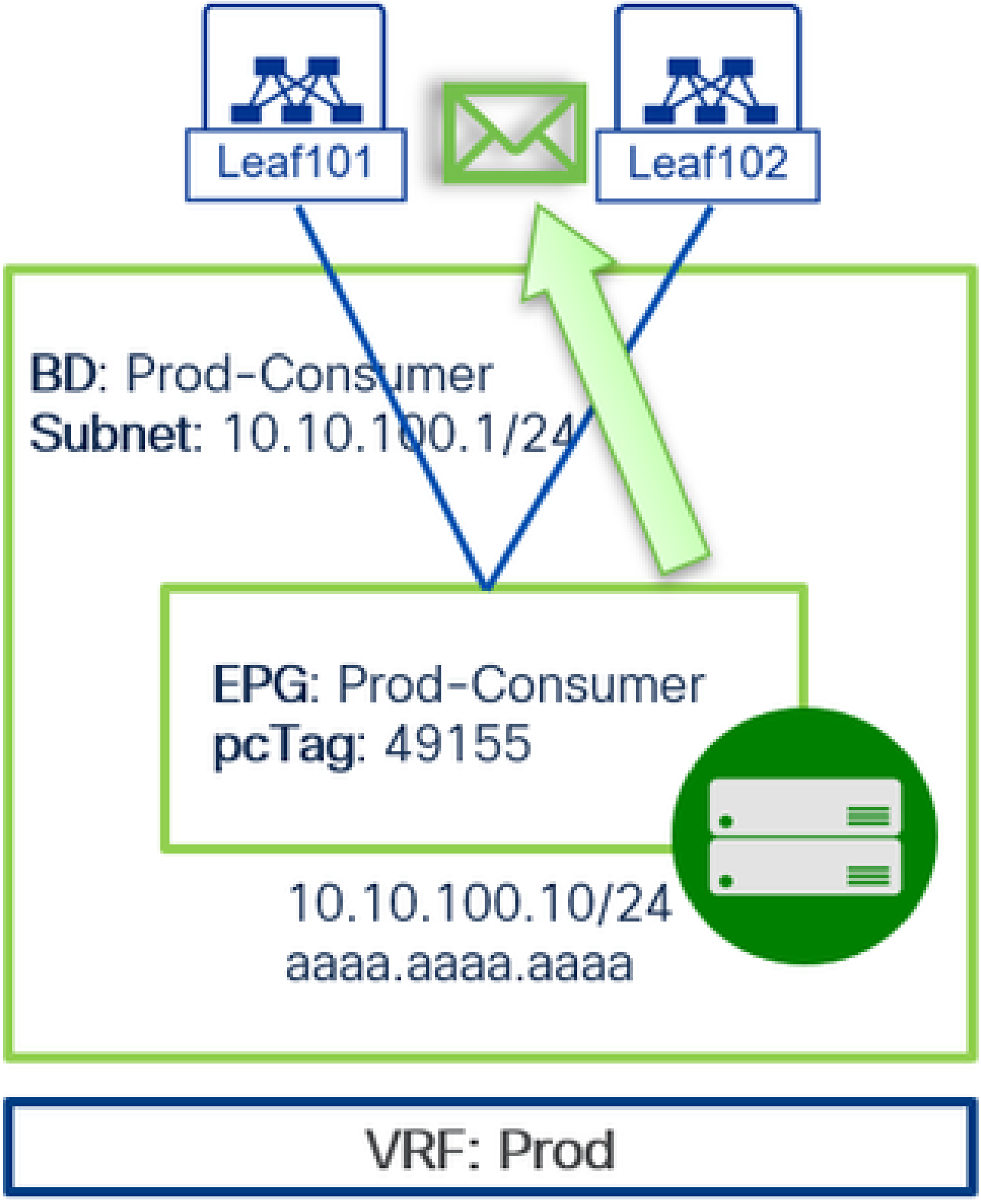
生成包含資料包分析的轉儲。

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

- 流量

理解流經所有有問題的裝置的流量至關重要。Ftriage工具提供了此流程的極佳摘要。但是，要獲得詳細的逐步驗證並更深入地瞭解資料包接收過程，您可以在網路拓撲中的每一點執行嵌入式邏輯分析器模組(ELAM)。

1.輸入流量發生在獲知源伺服器的計算枝葉。在此特定情況下，由於來源位於vPC介面之後，因此必須在vPC對等點上設定ELAM。這是必要的，因為雜湊演算法選擇的物理介面是不確定的。



<#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

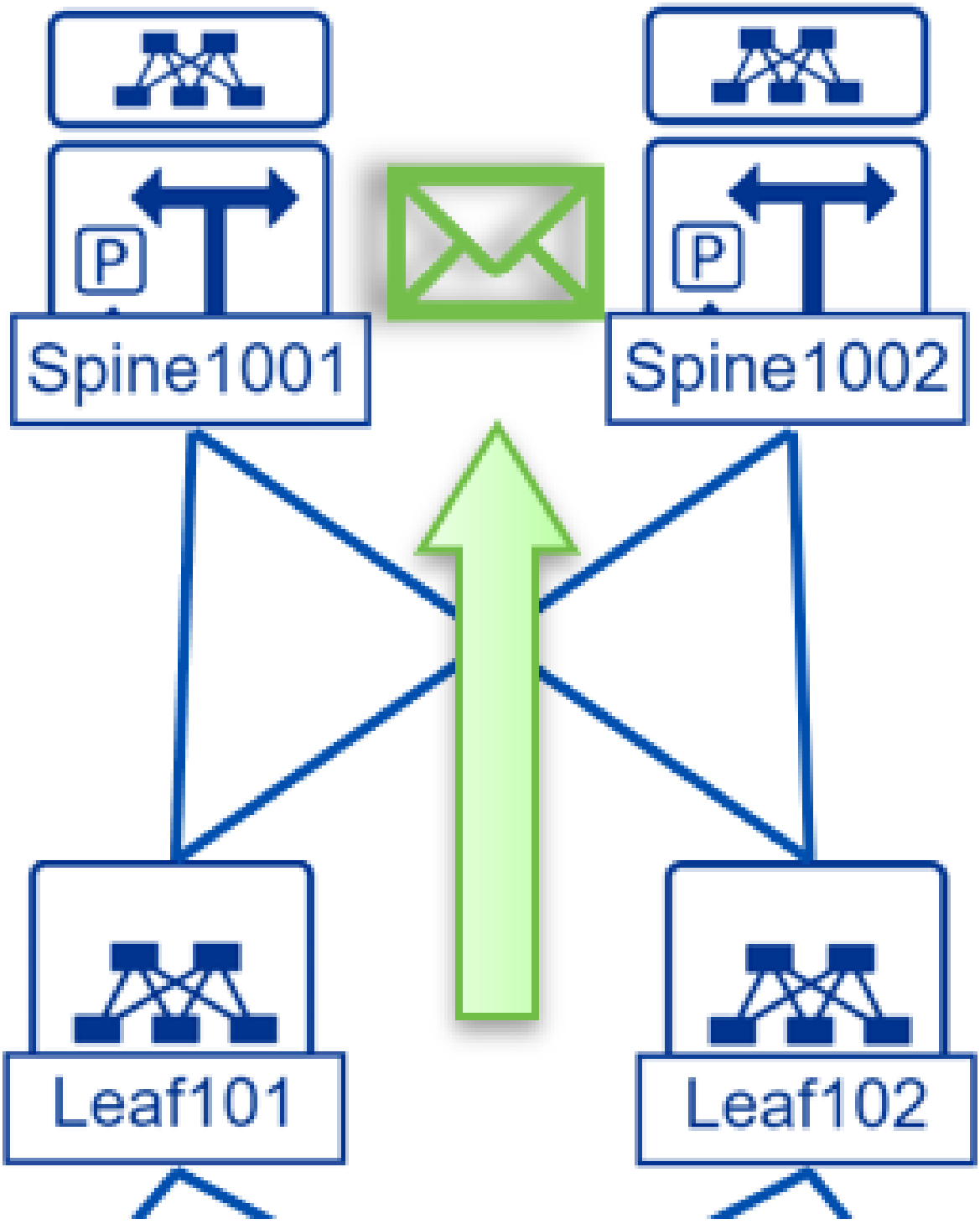
```
Ovec in "show plat int hal l2 port gpd"

Opcode : OPCODE_UC


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

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


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

根據所提供的資訊，顯然封包透過原則型路由(PBR)重新導向，因為service_redir選項已啟用。此外，還可以檢索sclass和dclass值。在此特定案例中，交換器會識別dclass。但是，如果EPM表中不存在目標終結點，則dclass值預設為1。

此外，輸入介面由SRCID確定，輸出介面由向量值標識。通過在vsh_lc級別執行此命令，可以將這些值轉換為前端埠：

```
<#root>

show platform internal hal l2 port gpd
```

2.流程中的後續步驟涉及到達主幹交換機，以將目標MAC地址對映到PBR節點。由於流量封裝在VXLAN標頭中，因此在脊柱或遠端枝葉上執行ELAM需要使用內選14來正確解碼封裝。



<#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.

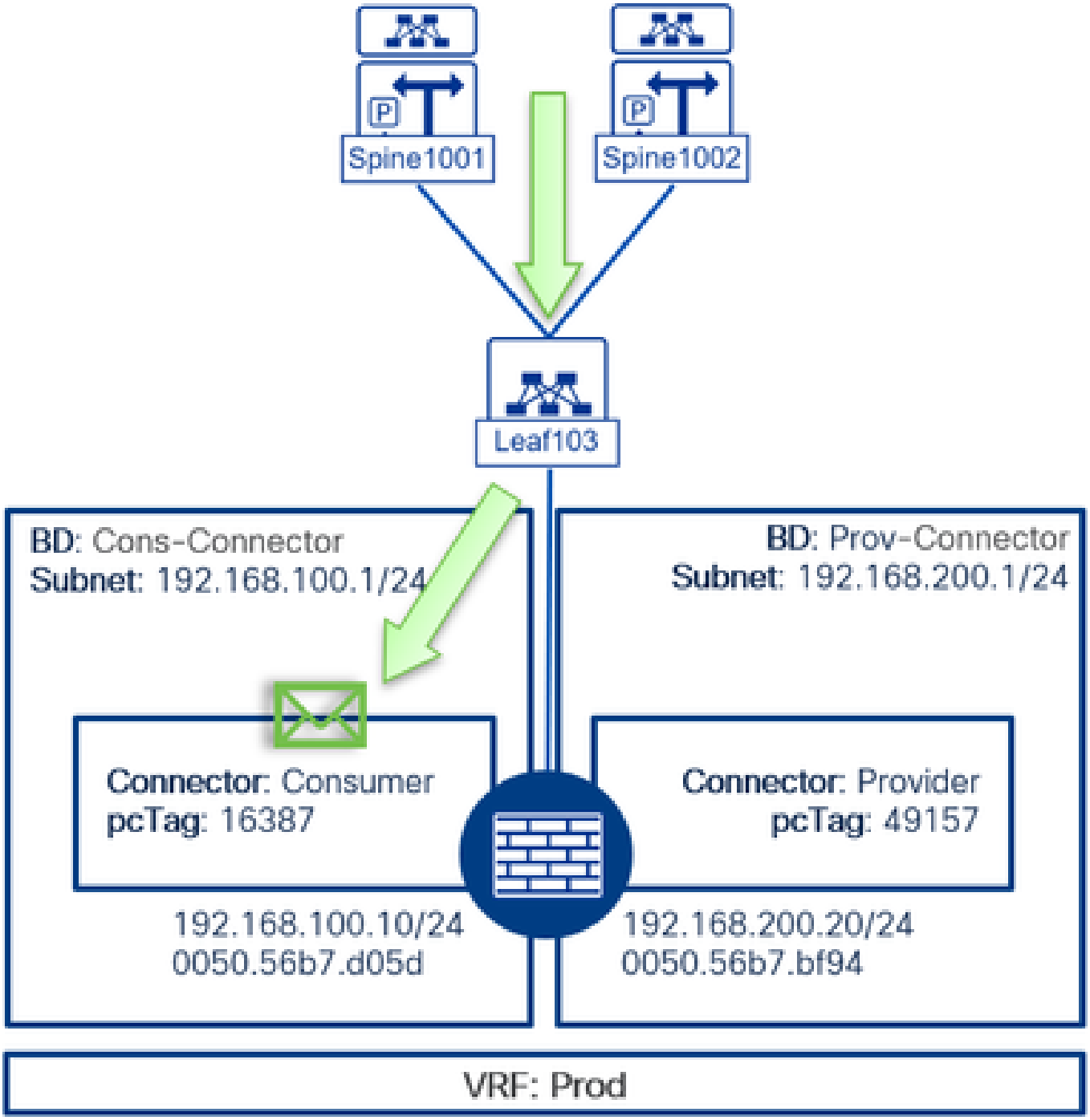
ovector_idx: 0x1F0 >>> Eth1/10

從先前的輸出中，很明顯，目的地MAC位址會重新寫入防火牆的MAC位址。隨後，執行COOP查詢以標識MAC的目標發佈者，然後將資料包轉發到交換機的相應介面。

您可以通過執行以下命令，利用網橋域VNID和防火牆的MAC地址在脊柱上模擬此查詢：

```
<#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.流量到達識別防火牆MAC地址的服務枝葉，然後轉發到PBR節點。



<#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 )
```

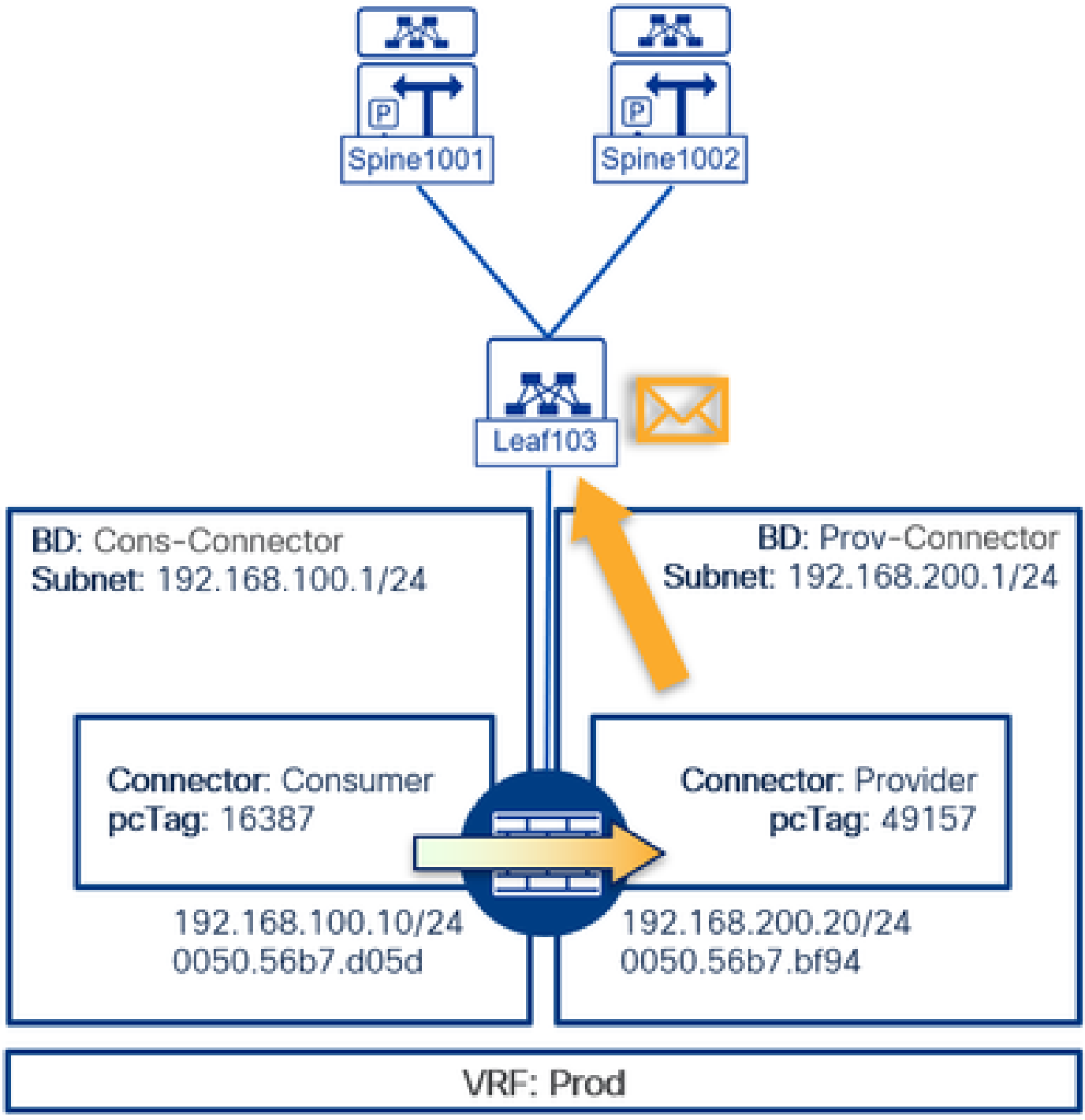
sclass (src pcTag) : 49155(0xC003) >>> Prod-Consumer EPG

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.對於由PBR節點返回的打包程式，首先這個節點必須自己進行偵錯，並更改VRF、介面或VLAN。然後將資料包轉發回提供商聯結器上的ACI:



<#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


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

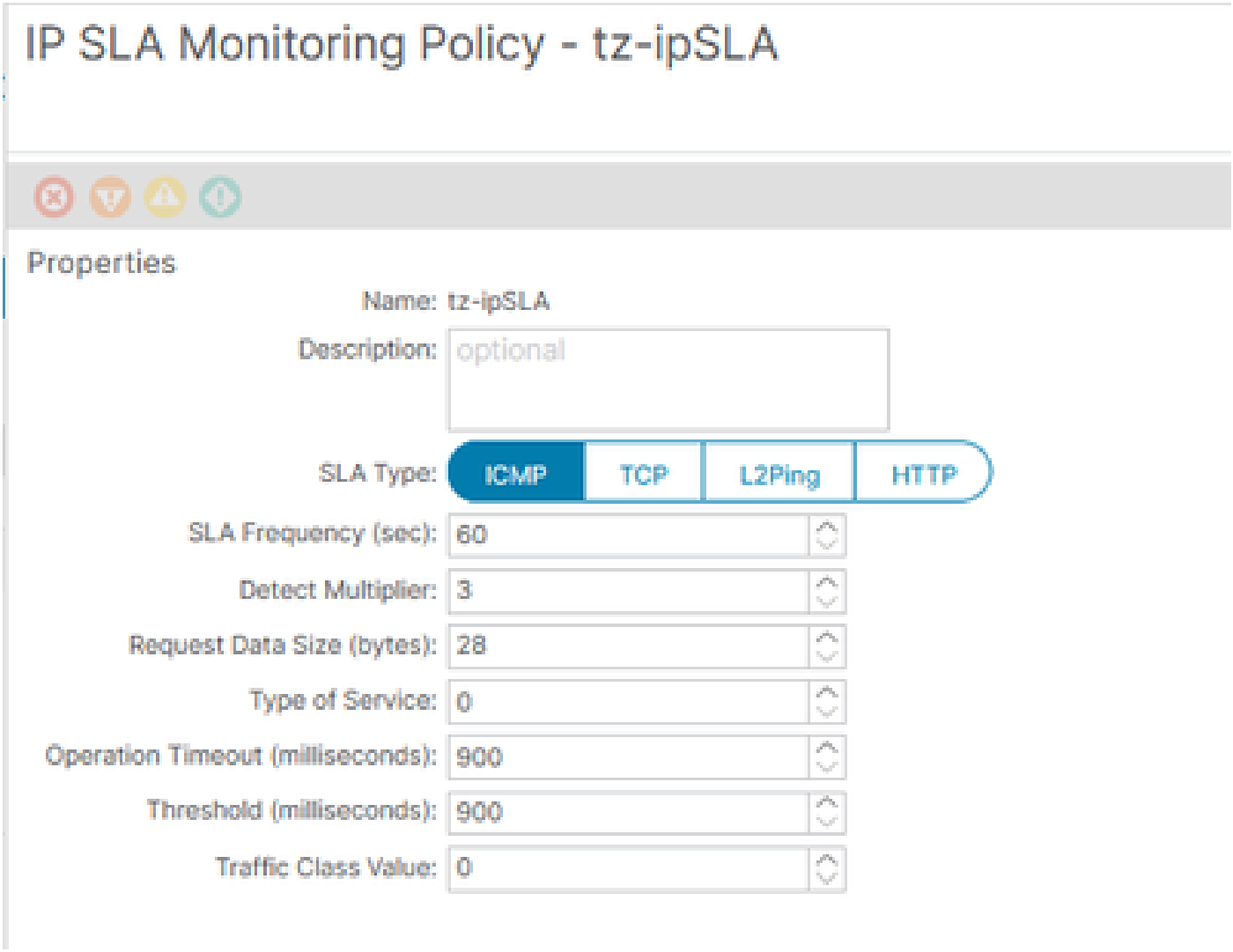
5. 剩餘的網路流量遵循目前為止提到的既定步驟，其中資料包返回主幹交換機，以便根據連線埠查詢確定最終的伺服器目的地。隨後，將資料包定向到具有本地學習標誌的電腦枝葉交換機，並將該資訊傳播到主幹上的COOP表。步驟2和步驟3的ELAM執行對於將資料包分發到其最終目的地是一致的。驗證這些目的EPG pcTag和出口介面以確保準確交付至關重要。

IP SLA

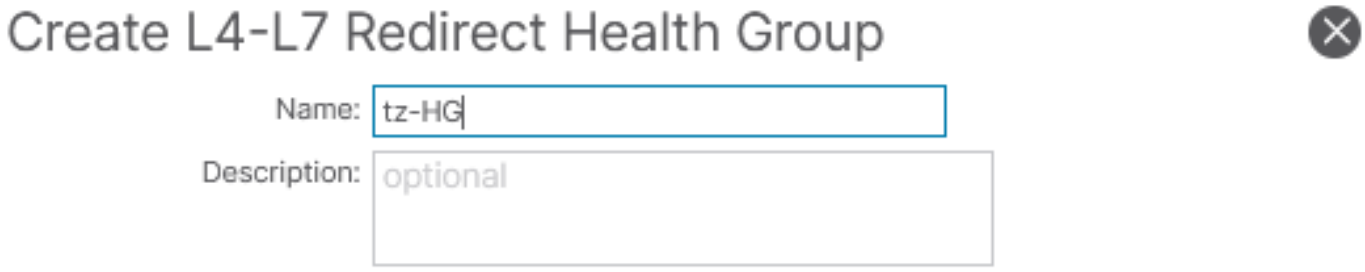
IP SLA用於評估網路路徑的運行狀態和效能。它有助於確保根據定義的策略基於即時網路條件有效地路由流量。在ACI中，PBR利用IP SLA做出明智的路由決策。如果IP SLA度量指示某個路徑正在執行中，則PBR可以通過滿足所需效能條件的備用路徑重新路由流量。

從版本5.2(1)開始，您可以為IP SLA啟用動態MAC跟蹤，這對於PBR節點進行故障轉移並更改同一IP地址的MAC地址的情況非常有用。在靜態部署中，每次更改PBR節點的MAC地址以繼續傳送流量時，都需要更改基於策略的重定向策略。使用IP SLA時，此策略中使用的MAC地址將中繼到探測響應。在撰寫本文時，可以使用不同的探測器來確定PBR節點是否正常，這些探測器包括：ICMP、TCP、L2Ping和HTTP。

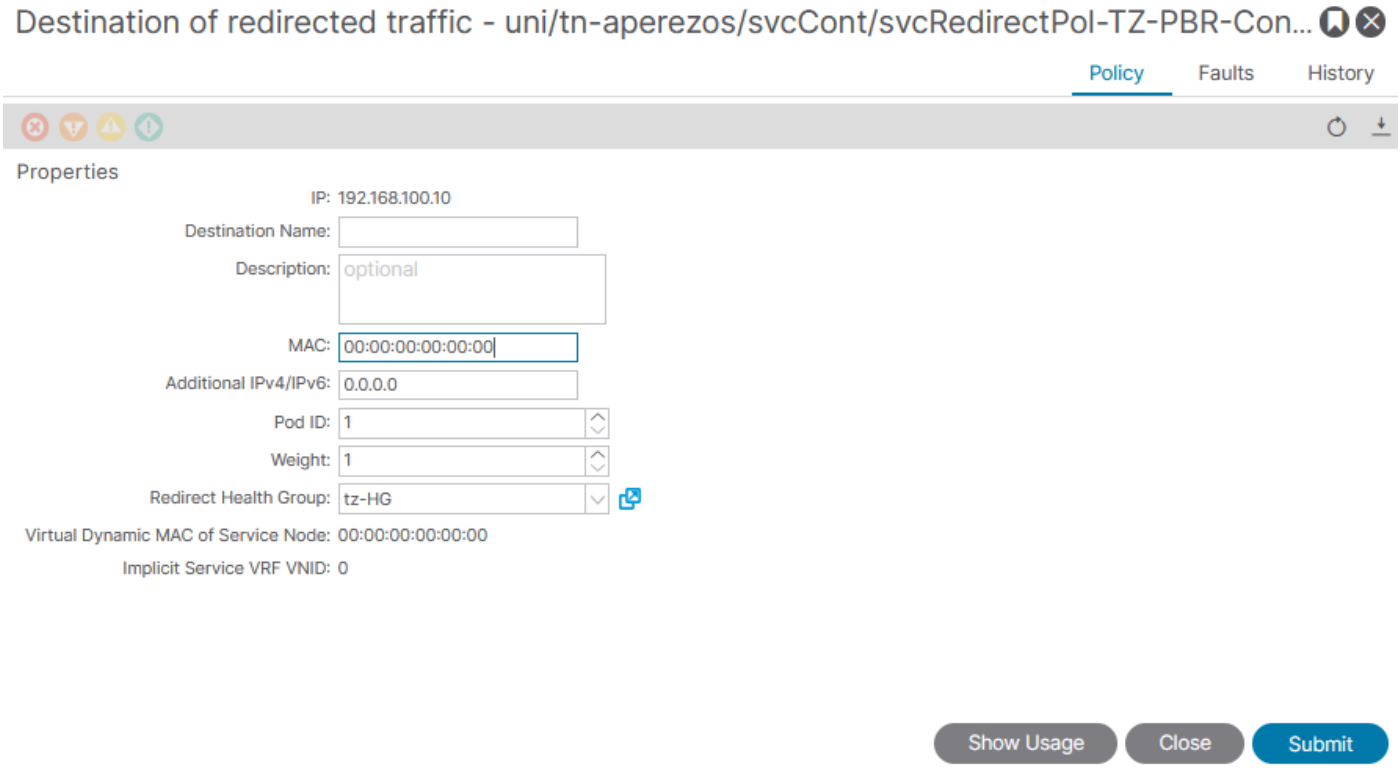
IP SLA策略的常規配置必須如下所示：



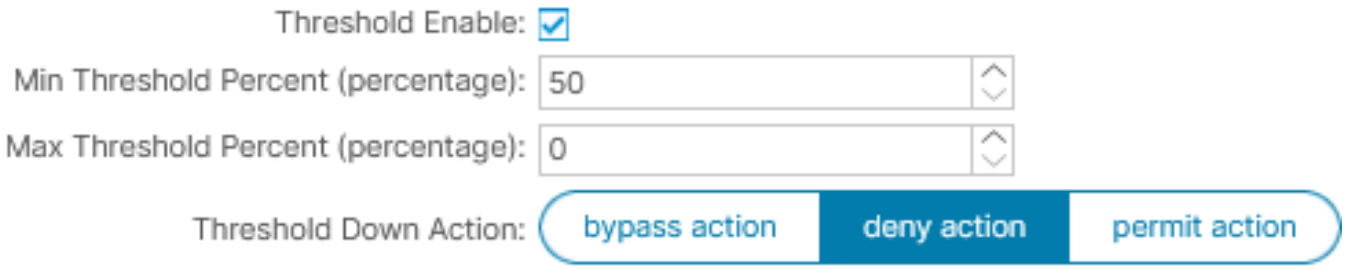
必須通過健康組將IP SLA策略對映到PBR節點IP。



如果使用動態發現MAC地址的IP SLA，此欄位不能為空，但設定為所有0:



一旦運行狀況組通過L4-L7基於策略的重定向策略中的L3目標與PBR節點IP關聯，請設定閾值以定義無法到達時的IP SLA行為。指定維護重定向所需的最小活動L3目標數。如果活動PBR節點的計數低於或超過閾值百分比，則整個組都會受到所選的Threshold Down Action的影響，正在停止重新分發。此方法支援在故障排除期間繞過PBR節點，而不會影響流量。



運行狀況組將單個L4-L7策略庫重定向策略或多個L4-L7策略庫重定向策略的第3層目標中定義的所有IP繫結在一起，只要使用相同的運行狀況組策略即可。

```
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#
```

相關資訊

- 思科以應用為中心的基礎架構基於策略的重定向服務圖設計白皮書
- ACI第4-7層基於策略的重定向(PBR)深入探討和提示（Cisco Live演示）
- 排除Multipod PBR上的IP SLA故障

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。