Risoluzione dei problemi relativi a PBR in ACI

Sommario

Introduzione

Prerequisiti

- Requisiti
- Componenti usati
- Abbreviazioni
- Cronologia PBR
- Considerazioni sulla progettazione

Premesse

Scenario: Singola VRF in un singolo fabric per pod

- Esempio di rete
- Risoluzione dei problemi

SLA IP

Informazioni correlate

Introduzione

In questo documento viene descritto come risolvere i problemi relativi agli ambienti ACI (Application Centric Infrastructure) con Policy-Based Redirect (PBR) in un'unica struttura pod.

Prerequisiti

Requisiti

Per questo articolo è consigliabile avere una conoscenza generale dei seguenti argomenti:

- Concetti ACI: Criteri di accesso, apprendimento degli endpoint, contratti e L3out

Componenti usati

Questo esercizio di risoluzione dei problemi è stato eseguito su ACI versione 6.0(8f) con switch Nexus di seconda generazione N9K-C93180YC-EX e N9K-C93240YC-FX2.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Abbreviazioni

- BD: Dominio bridge
- EPG: Gruppo endpoint
- ID classe: Tag che identifica un EPG
- Nodo PBR: Dispositivo L4-L7 utilizzato per una destinazione PBR
- Connettore consumer: Interfaccia del nodo PBR rivolta verso il lato consumer
- Connettore provider: Interfaccia del nodo PBR rivolta verso il lato del provider

Cronologia PBR

Version	Caratteristiche principali
2,0(1 m)	• I grafici dei servizi forniscono la funzione PBR.
3.x e versioni precedenti	• Supporto PBR (Policy-Based Redirect) a più nodi • Hashing resiliente PBR
3,2 (x)	• Il PBR del firewall a nodo singolo è supportato in ambienti multisito.
4,0 (x)	• Firewall PBR a due nodi è supportato in ambienti multisito.
4.2(1)	• È ora supportato un criterio di backup per la creazione di nodi PBR in standby.
4.2(3)	• L'opzione Filtra da contratto è disponibile nel modello di Service Graph tramite GUI.
5.0(1)	• Le estensioni L3T sono supportate su tutti i lati del provider dei nodi del servizio. • I percorsi di distribuzione attiva-attiva/ECMP sono supportati per i dispositivi PBR di layer 1/2.
5.2(1)	• Una destinazione PBR può ora trovarsi in un'uscita L3D. • È possibile tenere traccia dei nodi di servizio utilizzando l'URI HTTP. • Le modalità gestite e ibride del grafico dei servizi non sono più supportate. • L'indirizzo MAC del nodo PBR dinamico è supportato.
6.0(1)	• Weight-Based Symmetric Policy-Based Redirect (PBR)

Considerazioni sulla progettazione

- PBR funziona sia con dispositivi fisici che virtuali
- Il PBR può essere utilizzato tra EPG L3Out e EPG, tra EPG e tra EPG L3Out. PBR non è supportato se L2Out EPG fa parte del contratto
- Il PBR è supportato negli ambienti Cisco ACI Multi-Pod, Multi-Site e Remote Leaf.
- La struttura Cisco ACI deve essere il gateway per i server e per il nodo PBR
- Il dispositivo L4-L7 deve essere implementato in modalità go-to (routing)
- Nodo PBR non supportato sugli switch FEX
- È necessario un dominio Bridge dedicato per il nodo PBR
- L'indirizzo MAC dinamico per il nodo PBR è ora supportato utilizzando i gruppi di integrità.
- Si consiglia di abilitare il rilevamento basato su GARP sul dominio bridge del nodo PBR
- Il filtro predefinito comune che include ARP, traffico Ethernet e altro traffico non IP non deve essere utilizzato per PBR
- Il nodo PBR può trovarsi tra istanze VRF o all'interno di una delle istanze VRF. Per questa topologia, il nodo PBR non è supportato per trovarsi su un terzo VRF, deve essere configurato nel VRF consumer o provider

Premesse

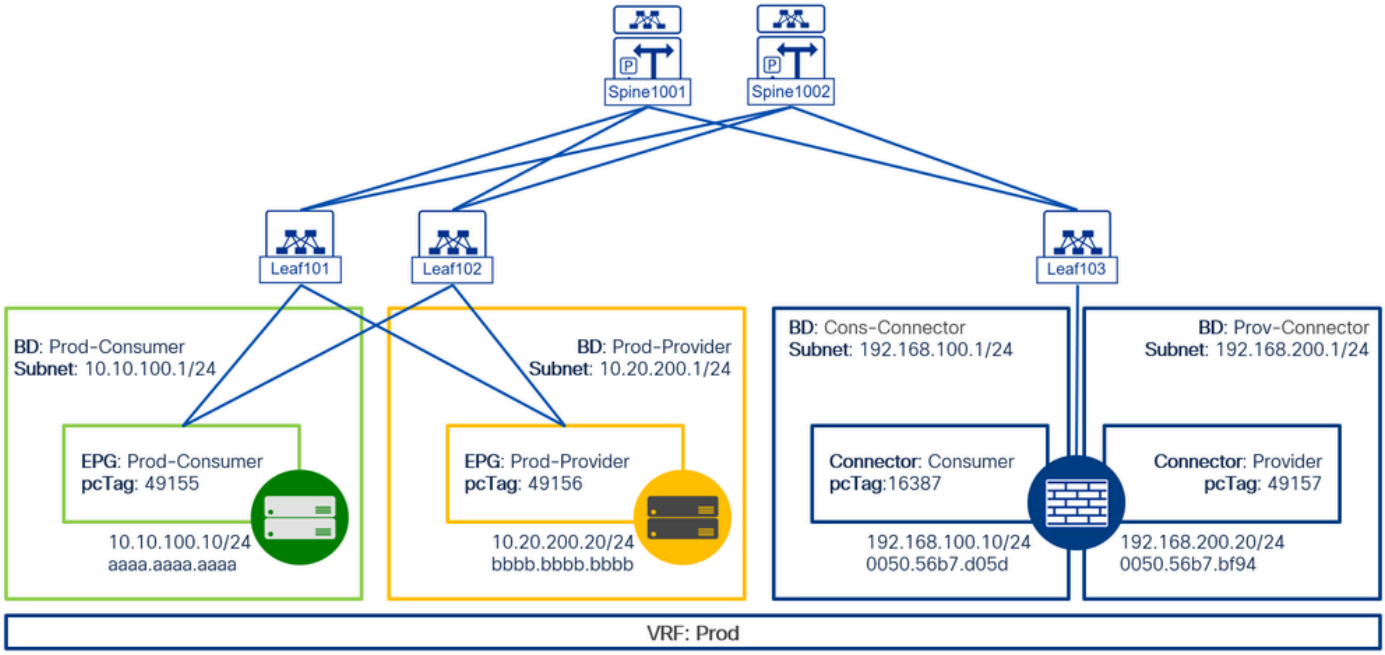
Spiegazioni più dettagliate su ELAM e Ftriage sono disponibili nella libreria on-demand CiscoLive nella sessione BRKDCN-3900b.

Inoltre, tutte le linee guida per la configurazione sono disponibili nel white paper Cisco Application Centric Infrastructure Policy-Based Redirect Service Graph Design.

Scenario: Singola VRF in un singolo fabric per pod

Esempio di rete

Topologia fisica:



Risoluzione dei problemi

Passaggio 1: Errori

ACI genera un errore quando si verifica un problema con la configurazione o con le interazioni dei criteri. Sono stati identificati guasti specifici per il processo di rendering PBR in caso di guasto:

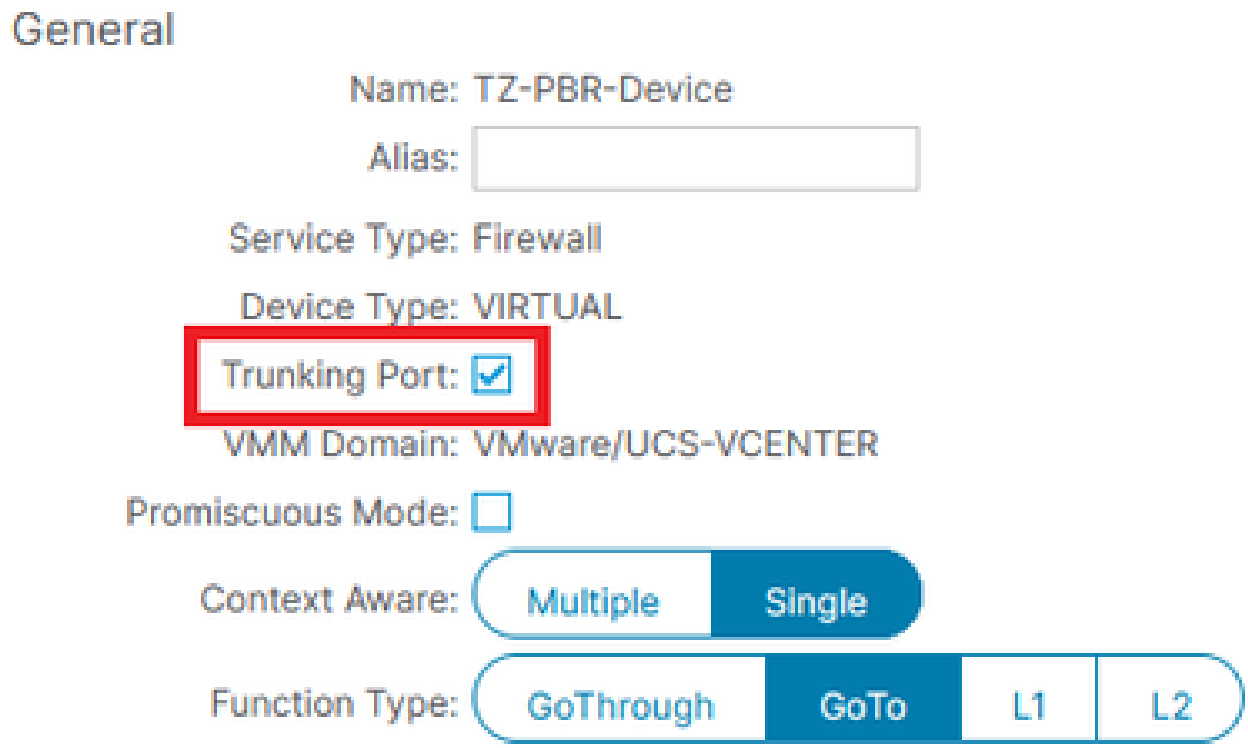
F1690: Configurazione non valida a causa di:

- Errore di allocazione ID

  Questo errore indica che la VLAN incapsulata per il nodo del servizio non è disponibile. Ad esempio, potrebbe non essere disponibile alcuna VLAN dinamica nel pool VLAN associato al dominio Virtual Machine Manager (VMM) utilizzato dal dispositivo logico.

  Risoluzione: Verificare il pool VLAN all'interno del dominio utilizzato dal dispositivo logico. Se l'interfaccia del dispositivo logico si trova all'interno di un dominio fisico, controllare anche la configurazione della VLAN incapsulata. Queste impostazioni sono disponibili in Tenant > Servizi > L4-L7 > Dispositivi e infrastruttura > Criteri di accesso > Pool > VLAN.

  Al contrario, se l'interfaccia del dispositivo logico risiede all'interno di un dominio virtuale e si connette agli host ESXi tramite un'interfaccia trunk, verificare che l'opzione della porta trunking sia abilitata.

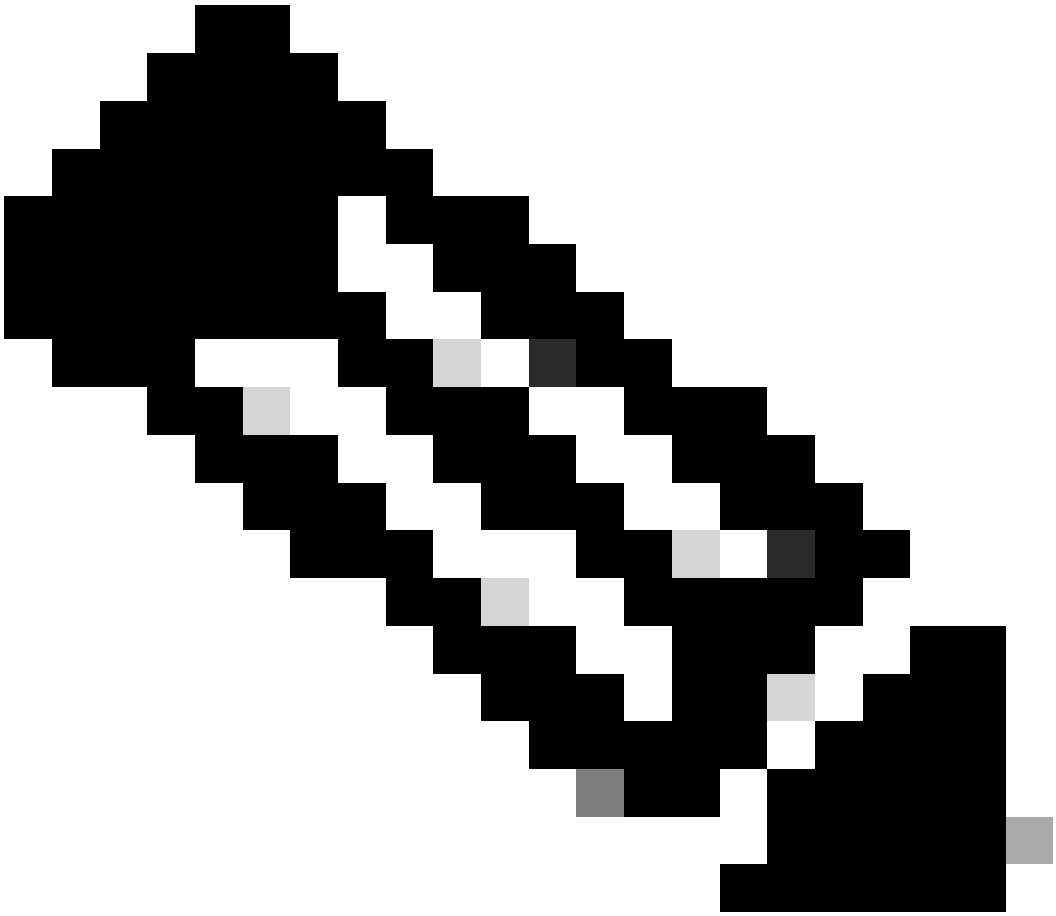


- Nessun contesto di dispositivo trovato per LDev

  Questo errore indica che il dispositivo logico non è individuabile per il rendering di Service Graph. Ad esempio, potrebbero non esistere criteri di selezione del dispositivo corrispondenti

al contratto associato al grafico del servizio.

Risoluzione: Verificare che sia definito un criterio di selezione del dispositivo. I criteri di selezione dei dispositivi specificano i criteri di selezione per un dispositivo di servizio e i relativi connettori, in base al nome del contratto, al nome del grafico del servizio e al nome del nodo all'interno del grafico del servizio. In Tenant > Servizi > L4-L7 > Criteri di selezione dispositivi.

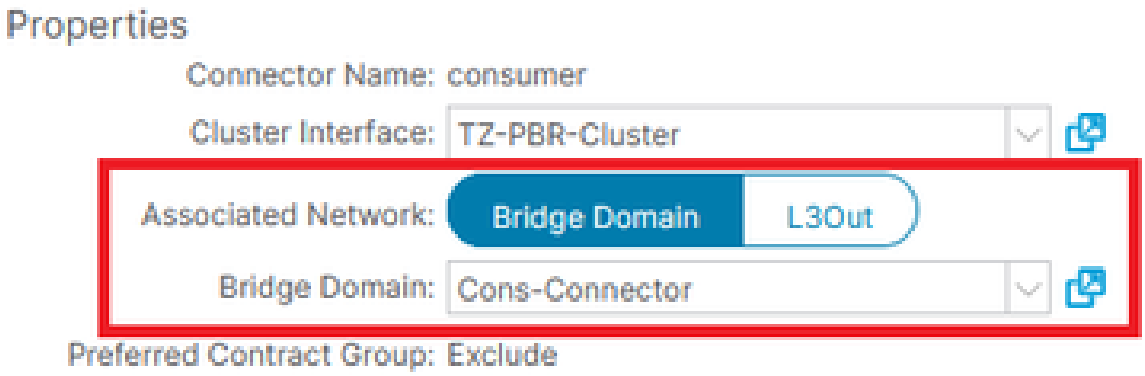


Nota: Quando si distribuisce un modello di Service Graph, ACI preseleziona il dominio bridge per l'EPG di origine. È necessario modificare questo dominio bridge per il connettore consumer PBR. Lo stesso vale per il connettore del provider.

- Nessun BD trovato

Questo errore indica che non è possibile individuare il dominio bridge (BD) per il nodo del servizio. Ad esempio, BD non è specificato in Criteri di selezione dispositivi.

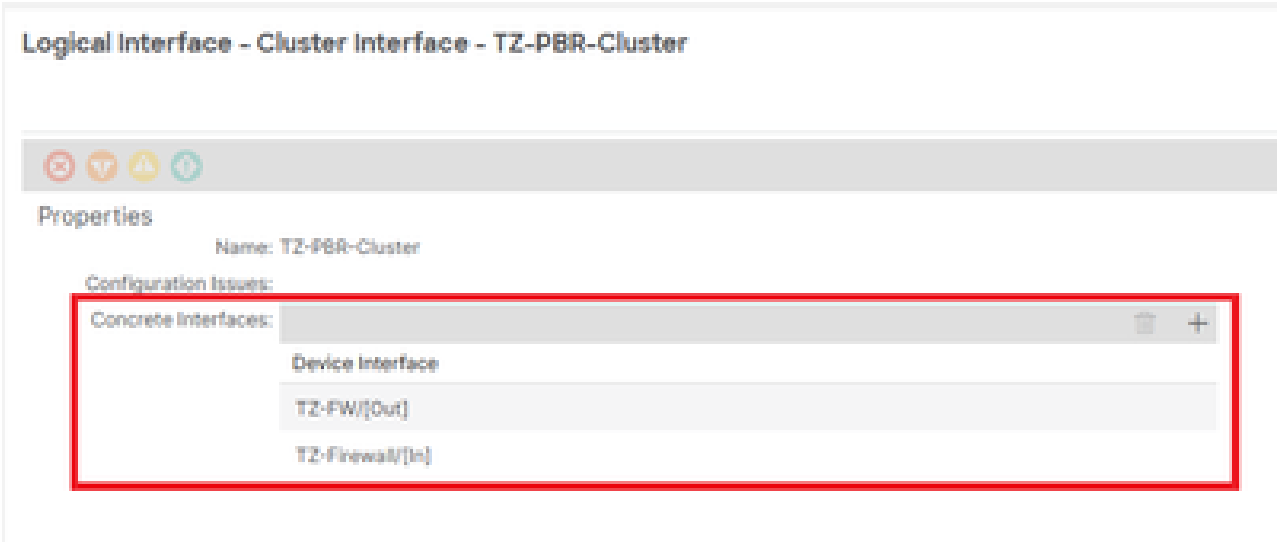
Risoluzione: Verificare che il BD sia specificato nei criteri di selezione dei dispositivi e che il nome del connettore sia corretto. Questa configurazione si trova in Tenant > Servizi > L4-L7 > Criteri di selezione dispositivi > [Contratto + SG] > [Consumer | Provider].



- LIf non ha alcuna relazione con CIf e LIf ha un CIf non valido
- Nessuna interfaccia cluster trovata

Questi errori indicano che il dispositivo non ha alcuna relazione con le interfacce del cluster.

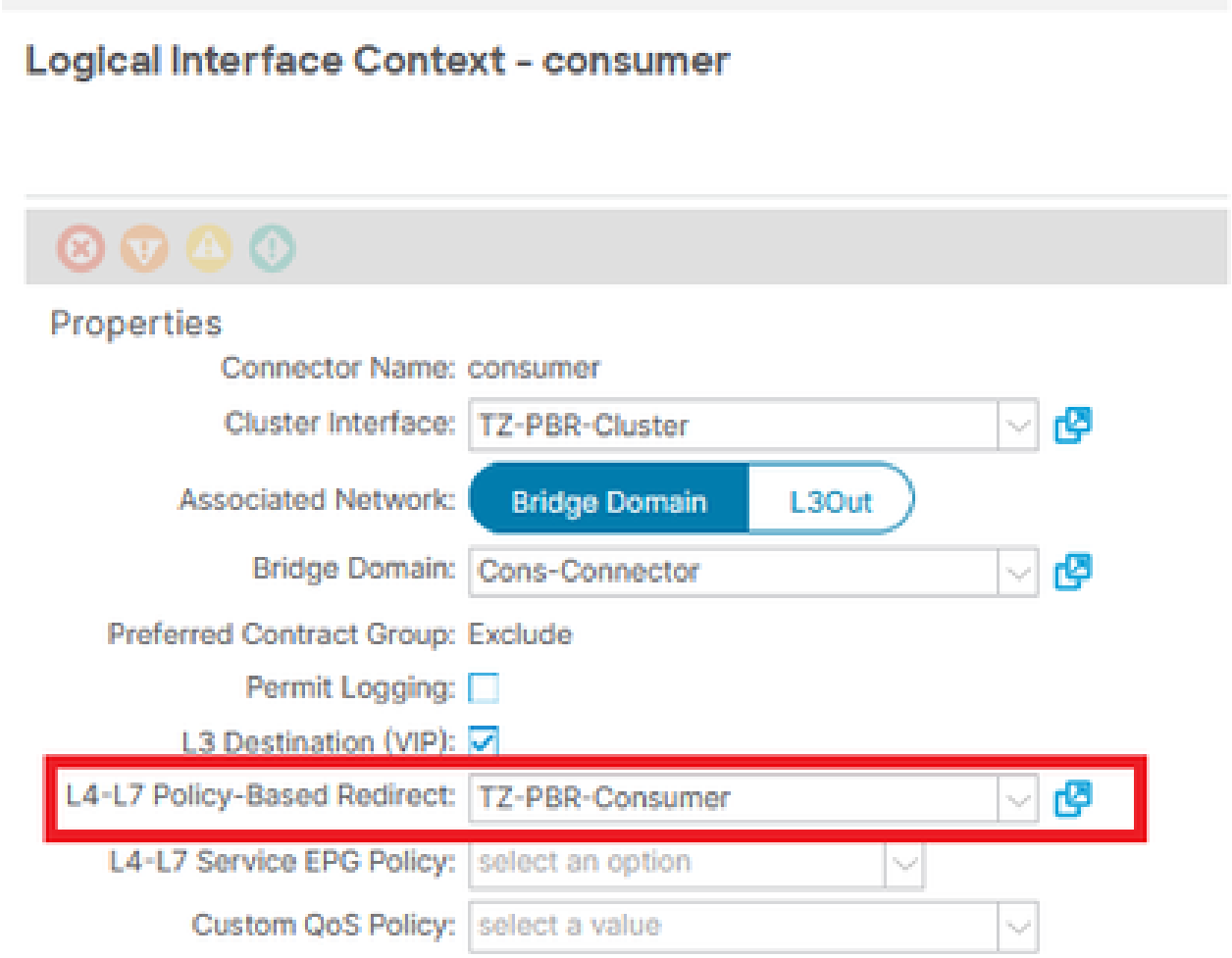
Risoluzione: Verificare che la configurazione dei dispositivi dal layer 4 al layer 7 (L4-L7) includa un selettore di interfaccia concreto specificato. Questa configurazione si trova in Tenant > Servizi > L4-L7 > Dispositivi > [Dispositivo] > Interfacce cluster.



- Criteri di reindirizzamento del servizio non validi

  Questo errore indica che il criterio PBR non è stato applicato nonostante il reindirizzamento sia stato attivato sulla funzione di servizio all'interno del grafico del servizio.

  Risoluzione: Verificare che il criterio PBR sia configurato nelle impostazioni del criterio di selezione del dispositivo. Questa configurazione si trova in Tenant > Servizi > L4-L7 > Criteri di selezione dispositivi > [Contratto + SG] > [Consumer | Provider].



F0759: graph-rendering-failure: "Impossibile creare un'istanza del grafico del servizio per tenant < tenant >. La configurazione del nodo funzione < nodo > non è valida."

Impossibile creare un'istanza del grafico del servizio per il tenant specificato a causa di una configurazione non valida del nome del nodo della funzione.

Questo errore suggerisce che vi sono problemi di configurazione relativi alle condizioni sopra menzionate.

Inoltre, durante le installazioni iniziali, questo errore può verificarsi temporaneamente e quindi essere risolto rapidamente. Questo si verifica a causa del processo di rendering che l'ACI esegue per distribuire tutti i criteri.

Risoluzione: Esaminare eventuali altri errori segnalati e risolverli di conseguenza.

F0764 configurazione non riuscita - "La configurazione dei dispositivi L4-L7 < dispositivo > per il tenant < tenant > non è valida".

Impossibile creare un'istanza del grafico del servizio per il tenant specificato a causa di una configurazione non valida del criterio di dispositivo PBR.

Questo errore suggerisce che vi sono problemi di configurazione relativi alle condizioni sopra menzionate.

Risoluzione: Esaminare eventuali altri errori segnalati e risolverli di conseguenza.

F072: configurazione non riuscita - "La configurazione di LIf < cluster > per dispositivi L4-L7 < dispositivo > per tenant < tenant > non è valida."

Impossibile creare un'istanza del grafico del servizio per il tenant specificato a causa di una configurazione non valida della selezione dell'interfaccia del cluster di dispositivi PBR.

Questo errore suggerisce che vi sono problemi di configurazione relativi alle condizioni sopra menzionate.

Risoluzione: Esaminare eventuali altri errori segnalati e risolverli di conseguenza.

Passaggio 2: Apprendimento degli endpoint di origine e destinazione

Verificare che gli endpoint di origine e di destinazione siano riconosciuti nell'infrastruttura, il che richiede una configurazione di base:

- Oggetto VRF (Virtual Routing and Forwarding).
- Oggetto Bridge Domain (BD) con il routing unicast abilitato. L'abilitazione dell'apprendimento IP Data Plane è considerata una best practice, ma non è obbligatoria.
- Oggetto Endpoint Group (EPG), applicabile sia ai domini virtuali che a quelli fisici.
- Criteri di accesso: Verificare che la catena di configurazione dei criteri di accesso sia completa e che non vengano segnalati errori nell'EPG.

Per confermare l'apprendimento dell'endpoint con l'EPG e l'interfaccia corretti, eseguire questo comando sulla foglia quando si apprende l'endpoint, noto anche come foglia di calcolo:

<#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#

Questo comando consente di identificare il pcTag (classe) associato all'EPG in cui l'endpoint è classificato, nonché di recuperare le informazioni sull'interfaccia, l'ambito VRF e l'indirizzo MAC.

Se non si conosce la posizione dell'endpoint di origine o di destinazione, è sempre possibile utilizzare questo comando sull'interfaccia APIC:

<#root>

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

<#root>

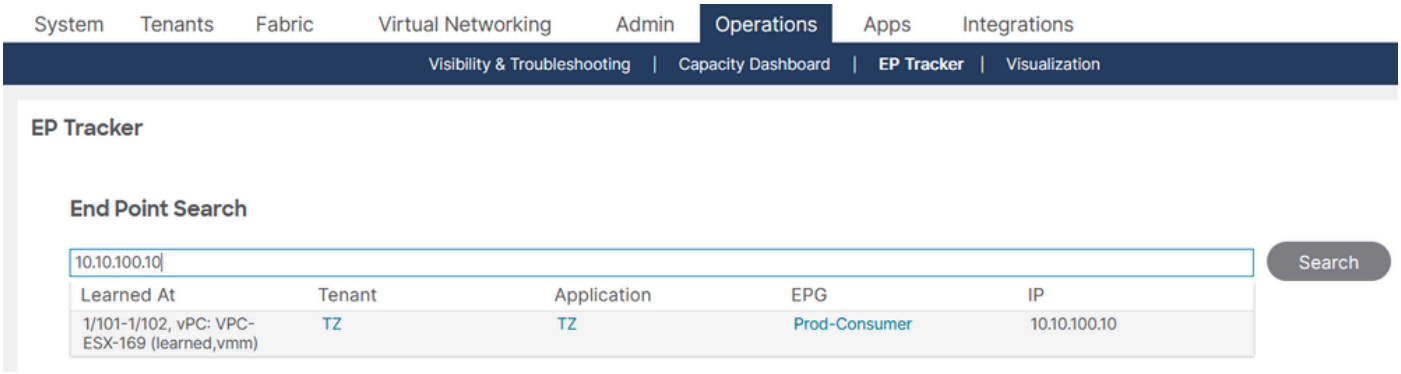
APIC#

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#
```

Nella GUI, è possibile accedere alla funzione EP Tracker passando a Operazioni > EP Tracker per il monitoraggio e la gestione degli endpoint.



Con le informazioni raccolte dagli endpoint di origine e di destinazione, è ora possibile concentrarsi sulla distribuzione dei criteri PBR.

Passaggio 3: Reindirizza contratto

Il PBR è integrato nel framework Service Graph. Di conseguenza, un modello di Service Graph deve essere distribuito e configurato sia sullo switch di origine che su quello di destinazione in conformità a un contratto. Utilizzando le informazioni pcTags raccolte nel passaggio precedente, è possibile verificare se un gruppo di endpoint (EPG, Endpoint Group) viene reindirizzato a un gruppo di Service Graph eseguendo questo comando.

<#root>

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

Nelle regole di zonizzazione, tali regole devono essere considerate:

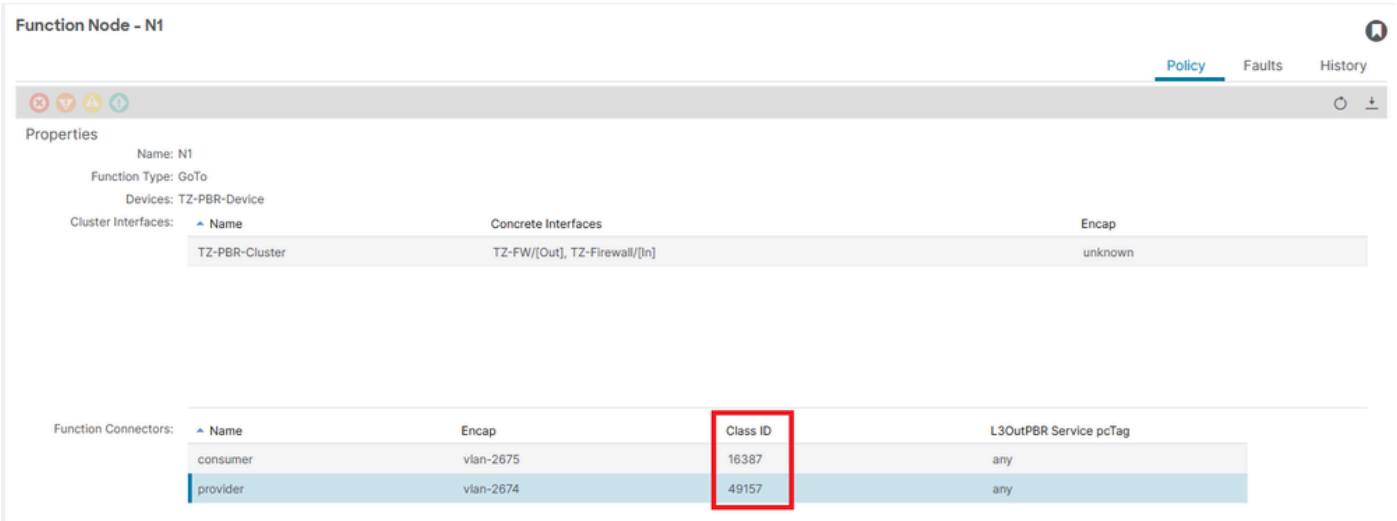
1. EPG di origine-destinazione con un gruppo di reindirizzamento associato
2. Origine PBR-node shadow EPG a origine EPG
3. EPG di destinazione a EPG di origine con un gruppo di reindirizzamento associato. Questo gruppo può essere identico o diverso dalla configurazione precedente.
4. Destinazione PBR-node shadow EPG a destinazione 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#
```

Per verificare il pcTag degli EPG shadow creati durante il processo di distribuzione di Policy-Based Routing (PBR), selezionare Tenants > [NOME_TENANT] > Services > L4-L7 > Deployed Graph Instance > [NOME_SG] > Function Node - N1.



- Parser contratto

Lo script mette in correlazione le regole di zoning, i filtri, le statistiche e i nomi EPG. È possibile eseguire questo script in modo sicuro direttamente su un elemento ACI leaf o APIC. Quando viene eseguito sull'APIC, raccoglie oggetti concreti su tutti gli switch foglia, operazione che può richiedere alcuni minuti per distribuzioni di criteri di grandi dimensioni.

A partire dalla versione ACI 3.2, contract_parser è incluso nell'immagine ed è disponibile nella foglia. Immettere contract_parser.py dalla shell iBash.

<#root>

Leaf101#

contract_parser.py --sepg 49155

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

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

redir

ip tn-TZ/ap-TZ/epg-

Prod-Consumer(49155)

tn-TZ/ap-TZ/epg-

Prod-Provideer(49156)

[contract:uni/tn-TZ/brc-

TZ-PBR-Contract

] [

hit=81

]

destgrp-8

vrf:TZ:Prod ip:

192.168.100.10

mac:

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

bd:uni/tn-TZ/

BD-Cons-Connector

Leaf101#

Questo comando fornisce dettagli quali l'azione del contratto, gli EPG di origine e di destinazione, il nome del contratto in uso e il numero di accessi.

Passaggio 4: Gruppo di reindirizzamento

Dopo aver identificato il gruppo di reindirizzamento in base al contratto applicato alle regole di zoning, il passaggio successivo è determinare gli indirizzi IP e MAC dei dispositivi di destinazione del reindirizzamento. A tale scopo, eseguire il 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#
```

Questo comando consente di determinare lo stato operativo (OperSt) del gruppo di reindirizzamento, l'indirizzo IP configurato nella sezione L4-L7 PBR e il VNID del VRF associato ai domini bridge del nodo PBR. A questo punto, è necessario determinare l'indirizzo MAC configurato:

<#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: Tr
================================================================================================================
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: Tr
================================================================================================================
Name                                 bdVnid         vMac              vrf     operSt  operStQual   HG-
====                                 ======         ====              ====    =====   =========    ===
dest-[
```

192.168.200.20

```
]-[vxlan-
```

2162692

```
] vxlan-
```

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

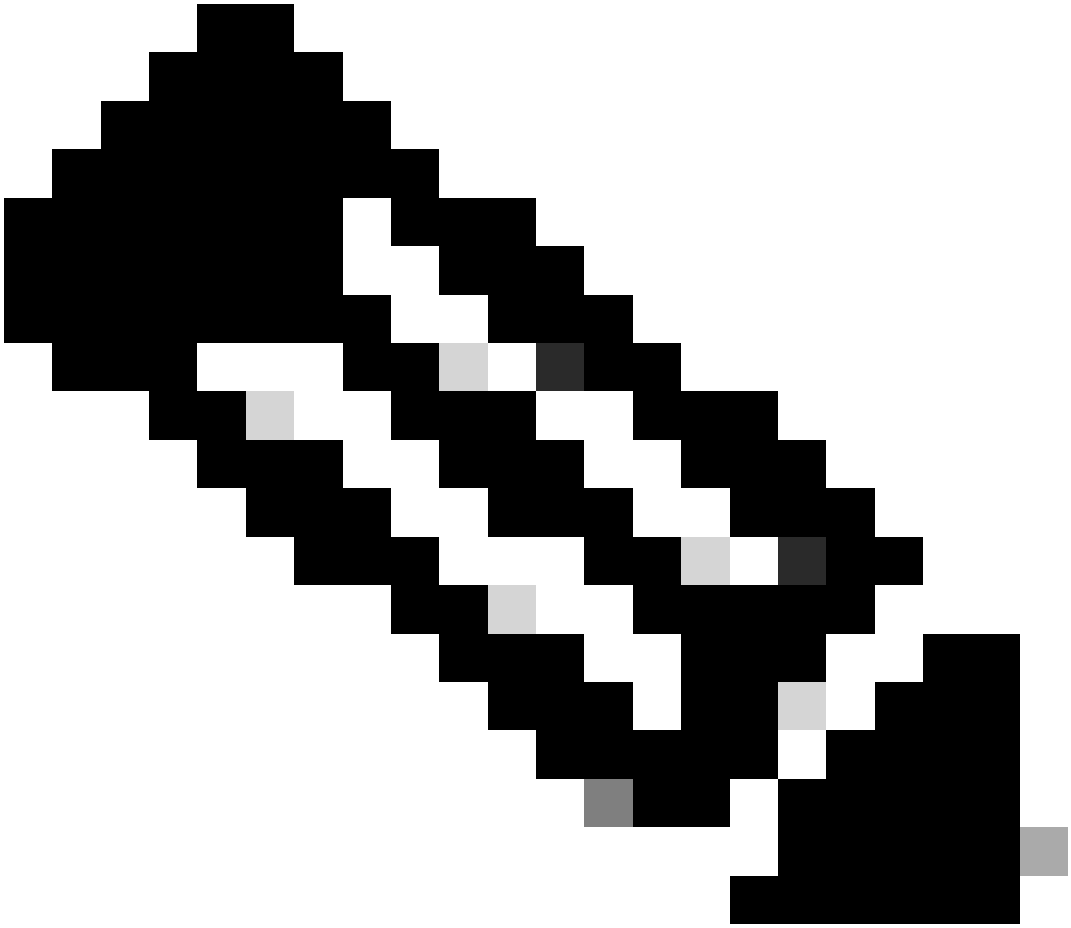
```
 TZ:Prod
```

enabled

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

Oltre ai dettagli precedentemente menzionati, questo comando fornisce informazioni preziose, tra

cui il nome VRF, il VNID BD e l'indirizzo MAC configurato del nodo PBR.



> Nota: È importante notare che in questa fase sia gli indirizzi IP che MAC sono configurati dall'utente, il che significa che possono verificarsi errori tipografici durante la definizione del routing basato sui criteri L4-L7.

Passaggio 5: Il nodo PBR non riceve traffico.

Un problema prevalente rilevato con l'inoltro PBR è l'assenza di traffico che raggiunge il nodo PBR. Una causa frequente di questo problema è un indirizzo MAC specificato in modo errato nella configurazione del routing basato su criteri L4-L7.

Per verificare l'accuratezza dell'indirizzo MAC configurato nel routing basato su criteri L4-L7, eseguire il comando utilizzato in precedenza dal passaggio 2. Questo comando può essere eseguito sullo switch foglia designato come foglia di servizio, dove si prevede che il nodo venga appreso.

<#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#
```

Verificare che l'indirizzo MAC registrato nella tabella EPM corrisponda a quello configurato nel gruppo di reindirizzamento del servizio. È necessario correggere anche errori tipografici minori per garantire un corretto routing del traffico verso la destinazione del nodo PBR.

Passaggio 6: Flusso del traffico.

- FTRIAGE

Uno strumento CLI per l'APIC progettato per automatizzare la configurazione e l'interpretazione dei processi ELAM end-to-end. Lo strumento consente agli utenti di specificare un particolare flusso e lo switch foglia da cui ha origine il flusso. Esegue in sequenza gli ELAM su ciascun nodo per analizzare il percorso di inoltro del flusso. Questo strumento è particolarmente utile nelle topologie complesse in cui il percorso del pacchetto non è facilmente distinguibile.

<#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

Il modulo ELAM (Embedded Logic Analyzer Module) è uno strumento diagnostico che consente agli utenti di stabilire condizioni specifiche nell'hardware per acquisire il pacchetto o il frame iniziale che soddisfa tali criteri. Quando un'acquisizione viene completata correttamente, lo stato ELAM viene indicato come attivato. All'attivazione, l'ELAM viene disabilitato, consentendo la raccolta di un dump di dati, che semplifica l'analisi delle numerose decisioni di inoltro eseguite dall'ASIC dello switch per quel pacchetto o frame. ELAM opera a livello ASIC, garantendo che non influisca sulla CPU o su altre risorse dello switch.

Struttura della sintassi del comando. Questa struttura è stata raccolta dal libro Risoluzione dei problemi 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]
```

Imposta condizioni da attivare

```
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]
```

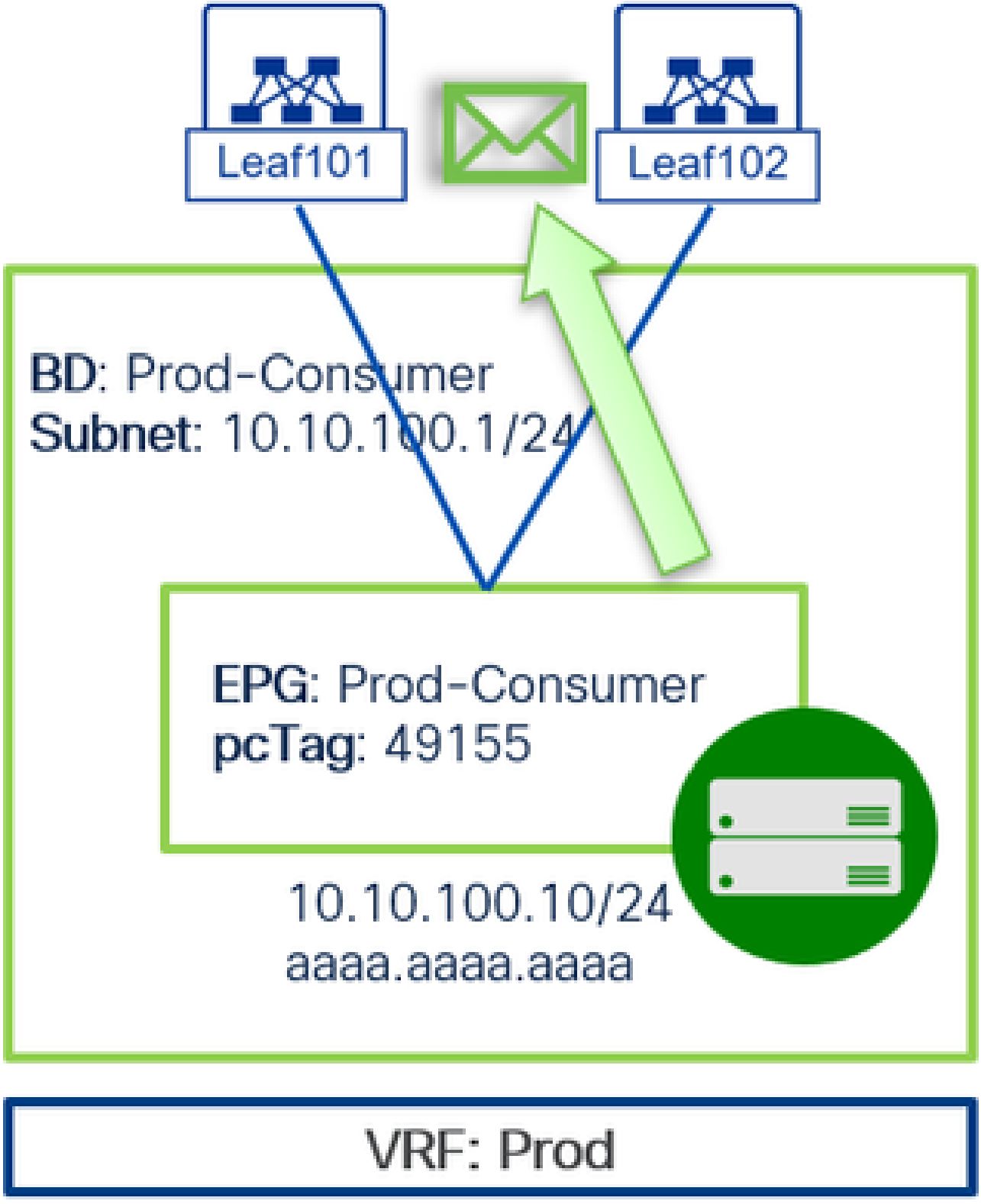
Generare il dump contenente l'analisi del pacchetto.

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

- Flusso del traffico

È fondamentale comprendere il flusso del traffico tra tutti i dispositivi in questione. Lo strumento Ftriage fornisce un eccellente riepilogo di questo flusso. Tuttavia, per una convalida dettagliata e per ottenere informazioni più dettagliate sul processo di ricezione dei pacchetti, è possibile eseguire Embedded Logic Analyzer Module (ELAM) in ogni punto della topologia di rete.

1. Il traffico in entrata si verifica alla foglia di calcolo in cui viene appreso il server di origine. In questo scenario specifico, poiché l'origine è posizionata dietro un'interfaccia vPC, è necessario configurare ELAM sui peer vPC. Questa operazione è necessaria perché l'interfaccia fisica selezionata dall'algoritmo di hashing è indeterminata.



<#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

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

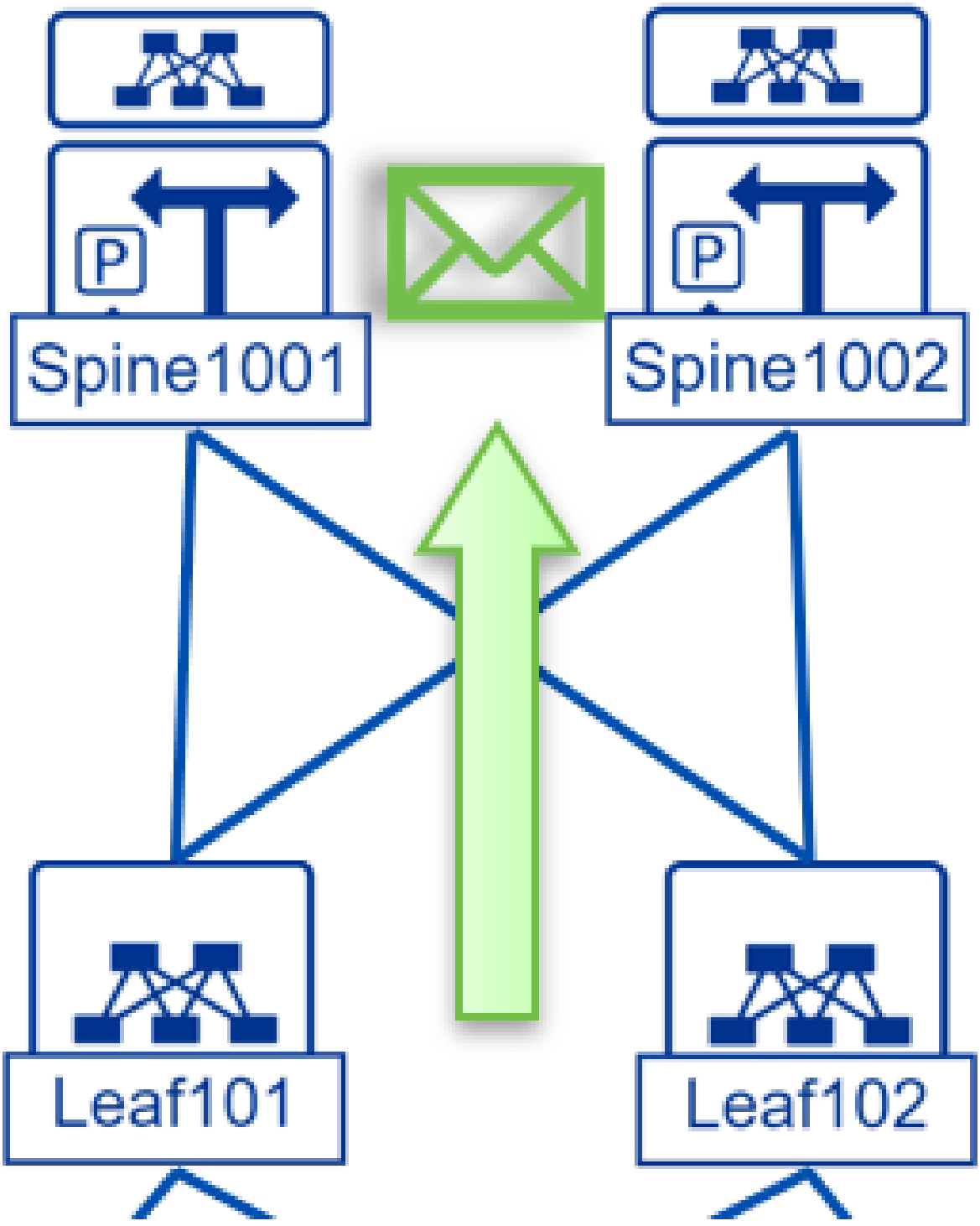
In base alle informazioni fornite, è evidente che il pacchetto viene reindirizzato tramite Policy-Based Routing (PBR), poiché l'opzione service_redir è abilitata. Inoltre, è possibile recuperare i valori di sclass e dclass. In questo scenario particolare, lo switch riconosce la dclass. Tuttavia, se l'endpoint di destinazione non è presente nella tabella EPM, il valore predefinito di dclass è 1.

Inoltre, l'interfaccia in entrata è determinata dall'SRCID e l'interfaccia in uscita è identificata dai valori del vettore. Questi valori possono essere convertiti in una porta frontale eseguendo questo comando a livello vsh_lc:

<#root>

show platform internal hal l2 port gpd

2. Il passaggio successivo del flusso prevede il raggiungimento dello switch dorso per mappare l'indirizzo MAC di destinazione sul nodo PBR. Poiché il traffico è incapsulato nelle intestazioni VXLAN, per eseguire ELAM su una spine o una foglia remota è necessario usare in-select 14 per decodificare correttamente l'incapsulamento.



<#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

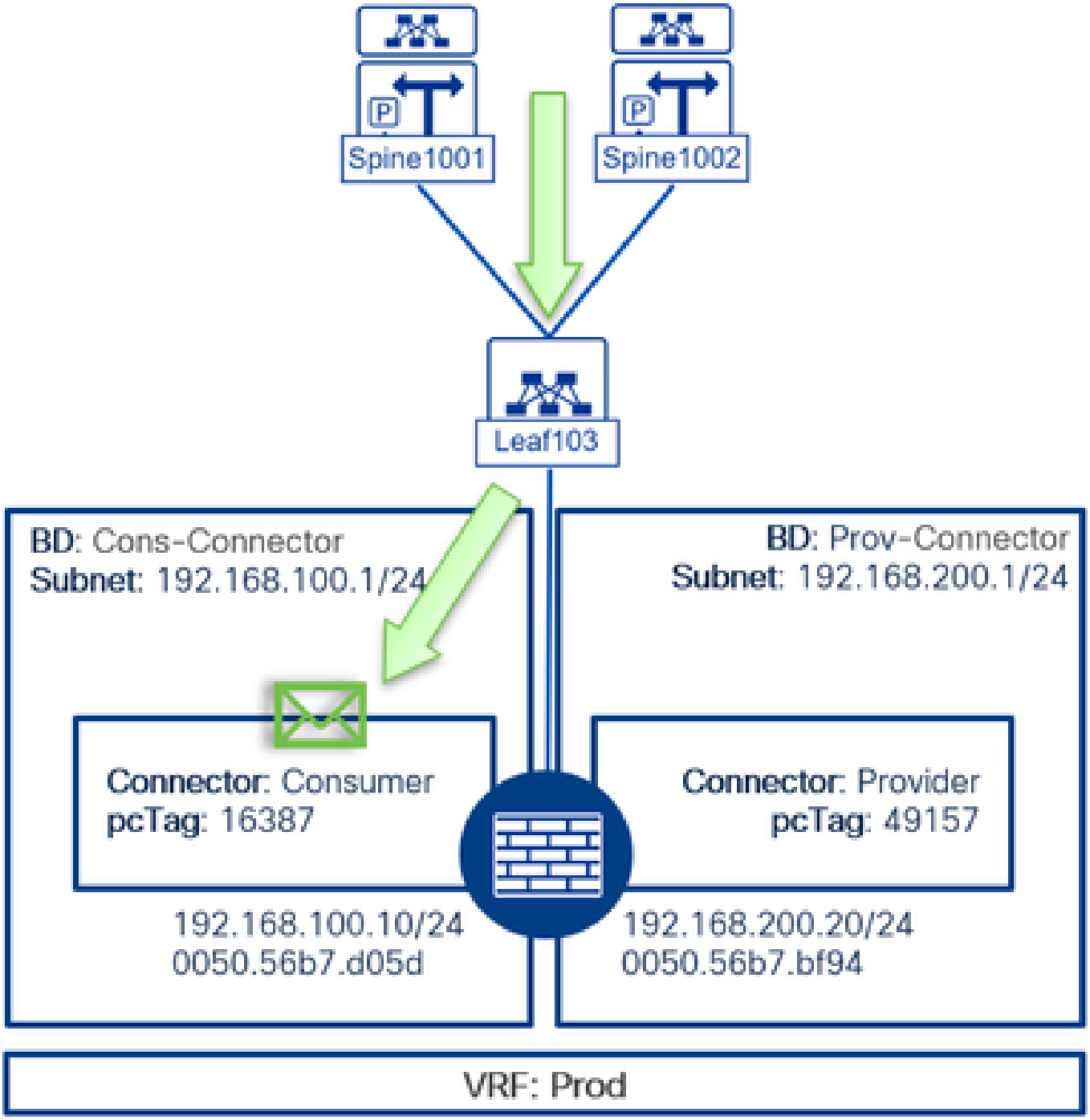
Dall'output precedente, è evidente che l'indirizzo MAC di destinazione viene riscritto sull'indirizzo MAC del firewall. Successivamente, viene eseguita una ricerca COOP per identificare l'autore di destinazione dell'indirizzo MAC e il pacchetto viene inoltrato all'interfaccia corrispondente dello switch.

È possibile simulare questa ricerca sul dorso eseguendo questo comando, utilizzando il VNID del dominio del bridge e l'indirizzo 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. Il traffico raggiunge la foglia di servizio dove l'indirizzo MAC del firewall viene riconosciuto e successivamente inoltrato 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 )
```

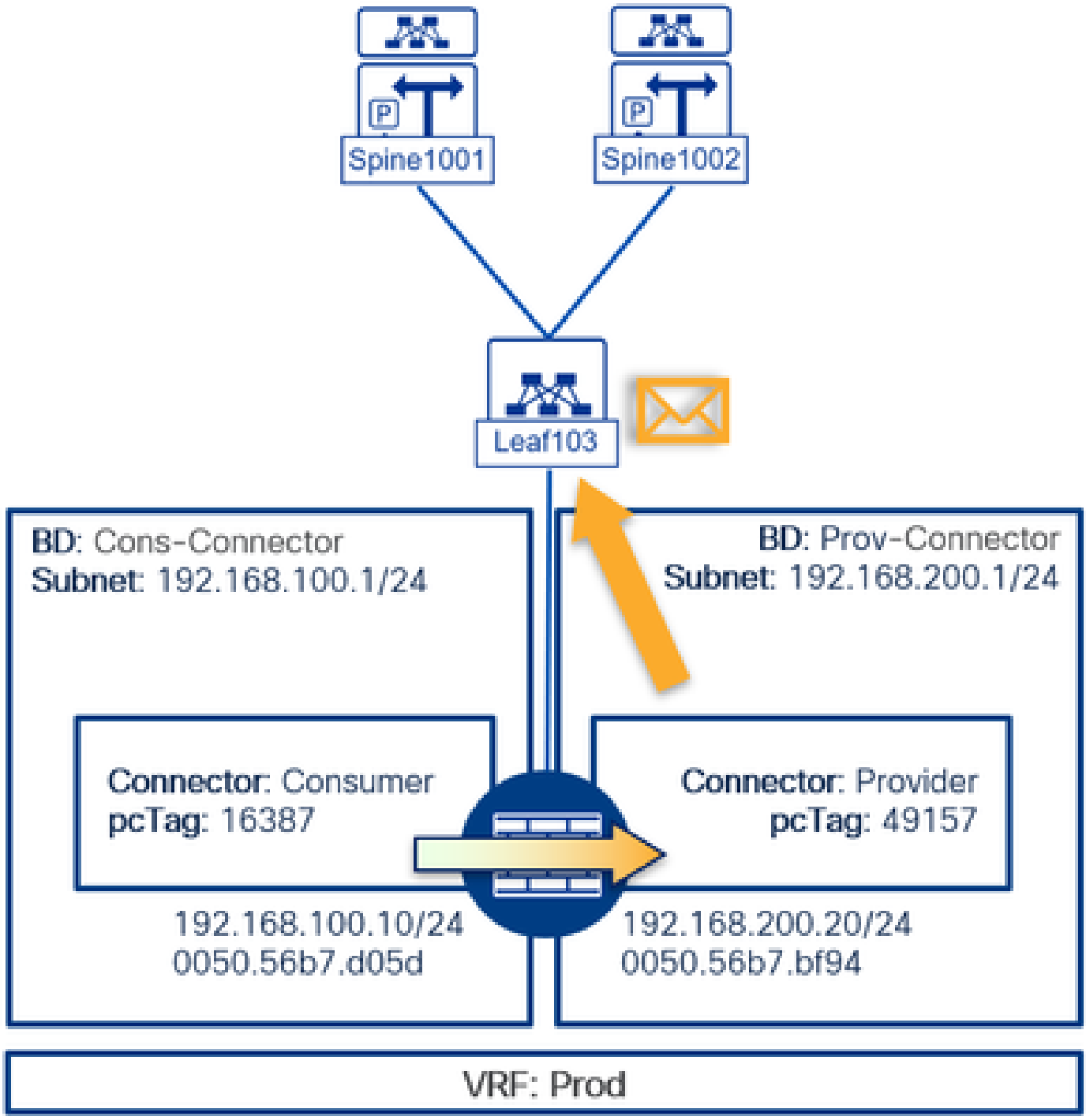
sclass (src pcTag) : 49155(0xC003) >>> Prod-Consumer EPG

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. Per il imballatore che viene restituito dal nodo PBR, in primo luogo, questo deve fare la propria diligenza e far modificare il VRF, l'interfaccia o la VLAN. Il pacchetto verrà quindi inoltrato nuovamente all'ACI sul connettore Provider:



<#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

---

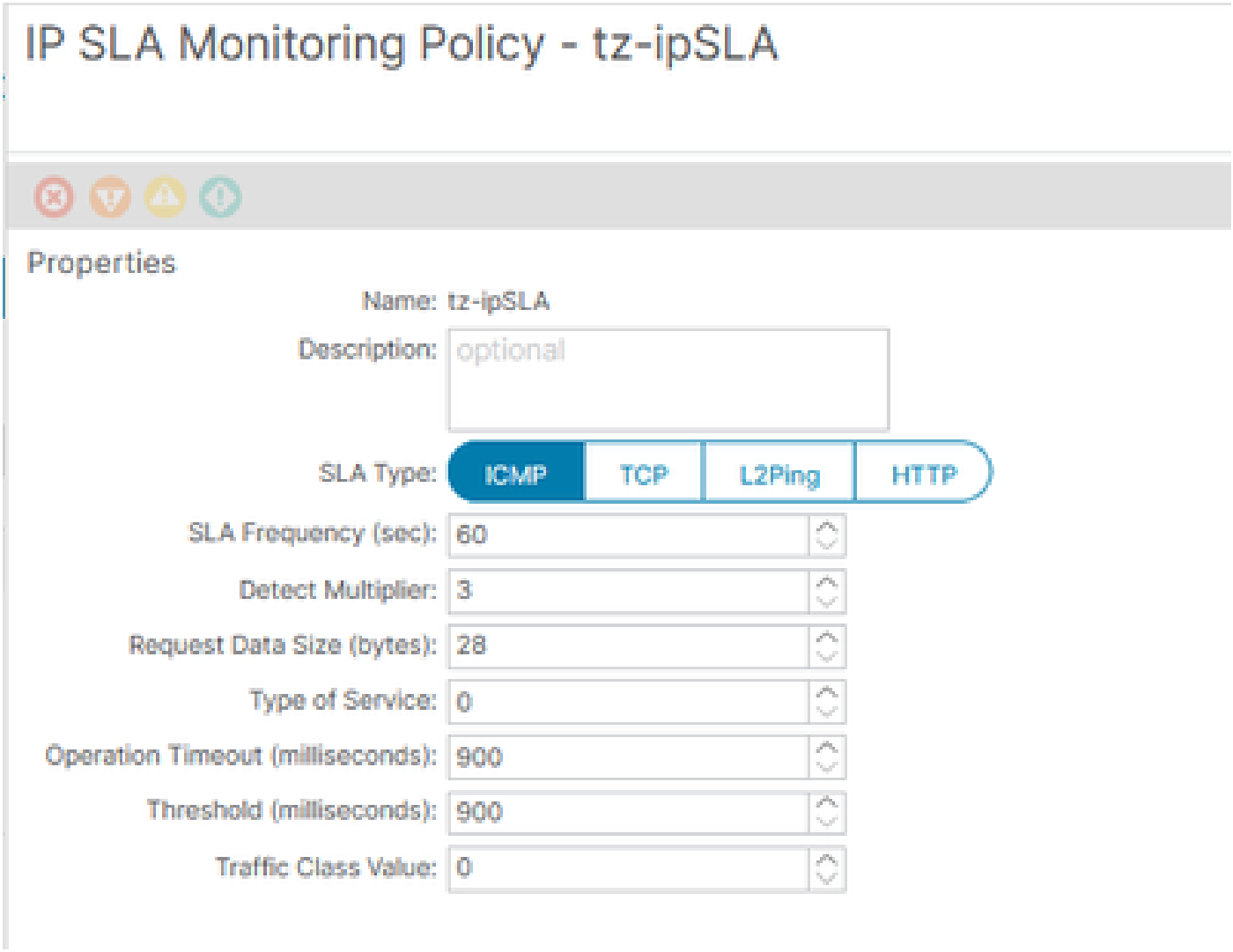
5. Il rimanente traffico di rete rispetta le fasi stabilite menzionate finora, in cui i pacchetti ritornano agli switch sul dorso per determinare la destinazione finale del server, in base alla ricerca del coop. Successivamente, i pacchetti vengono indirizzati allo switch foglia di calcolo che ha il flag di apprendimento locale e hanno diffuso queste informazioni alla tabella COOP sugli aculei. L'esecuzione ELAM per i passi 2 e 3 è coerente per la distribuzione del pacchetto verso la sua destinazione finale. Per garantire una consegna accurata, è essenziale convalidare questi dati sulla destinazione EPG pcTag e sull'interfaccia di uscita.

SLA IP

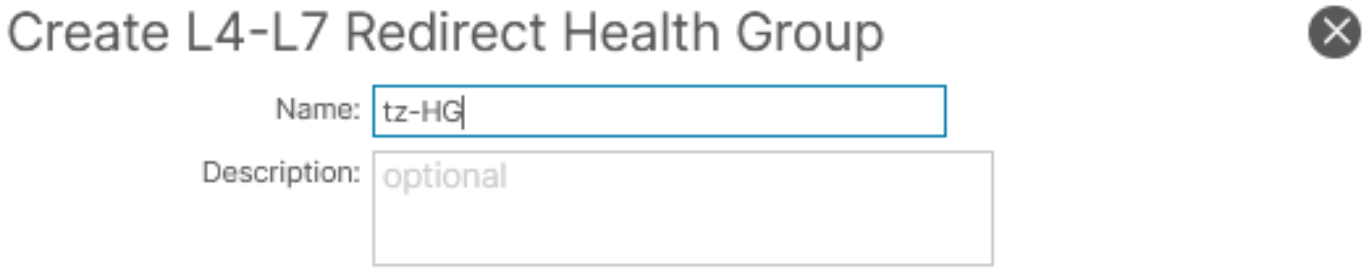
Lo SLA IP viene utilizzato per valutare lo stato operativo e le prestazioni dei percorsi di rete. Permette di instradare il traffico in modo efficiente in base a policy definite e a condizioni di rete in tempo reale. In ACI, il PBR sfrutta lo SLA IP per prendere decisioni informate sul routing. Se le metriche dello SLA IP indicano che un percorso è in esecuzione, PBR può reindirizzare il traffico su percorsi alternativi che soddisfano i criteri di prestazioni richiesti.

A partire dalla versione 5.2(1), è possibile abilitare il tracciamento MAC dinamico per lo SLA IP, utile per gli scenari in cui si verifica il failover di un nodo PBR e si modifica l'indirizzo MAC per lo stesso indirizzo IP. Nelle distribuzioni statiche, è necessario apportare una modifica alla regola di reindirizzamento basato su criteri ogni volta che il nodo PBR modifica il proprio indirizzo MAC per continuare l'invio del traffico. Con lo SLA IP, l'indirizzo MAC utilizzato in questo criterio inoltra la risposta della sonda. Al momento della stesura di questo documento, è possibile utilizzare diverse sonde per determinare se il nodo PBR è integro o meno. Tali sonde includono: ICMP, TCP, L2Ping e HTTP.

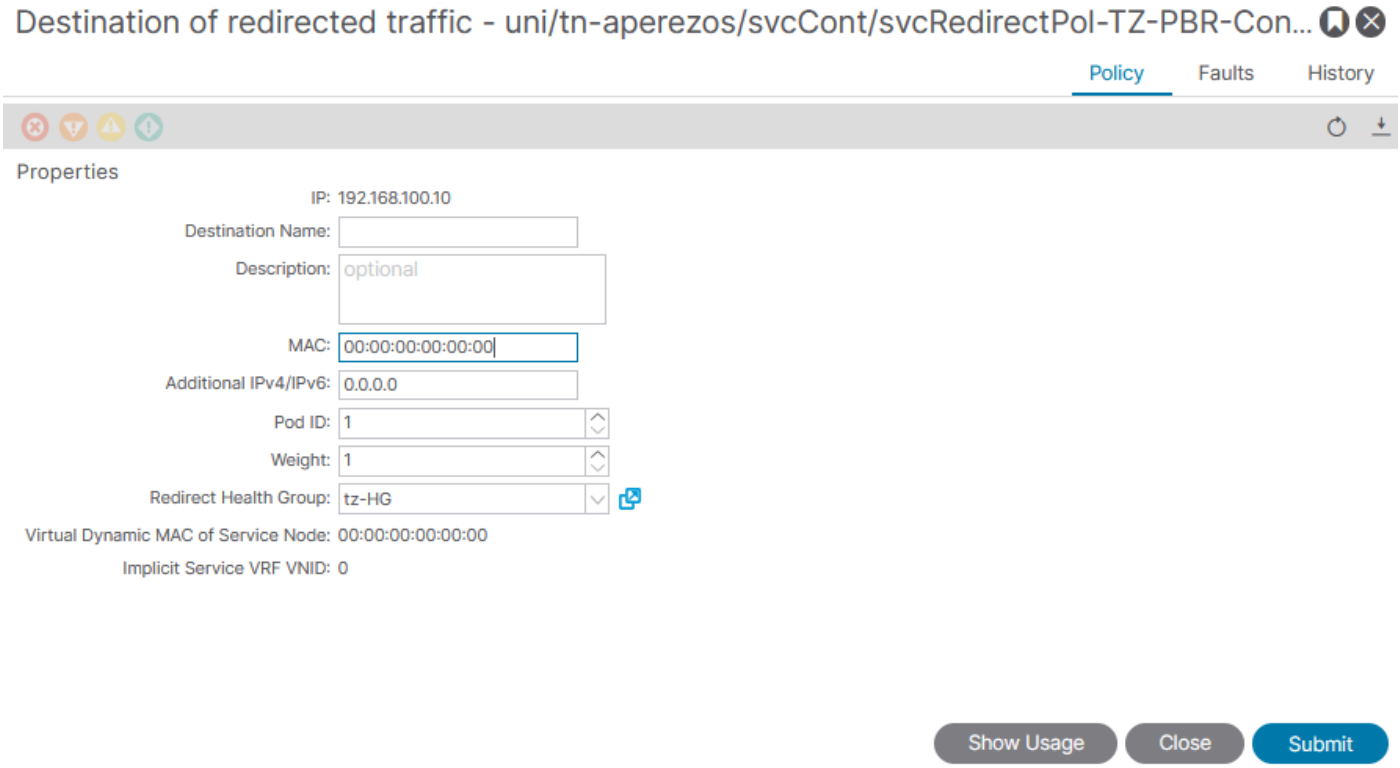
La configurazione generale di un criterio SLA IP deve essere simile alla seguente:



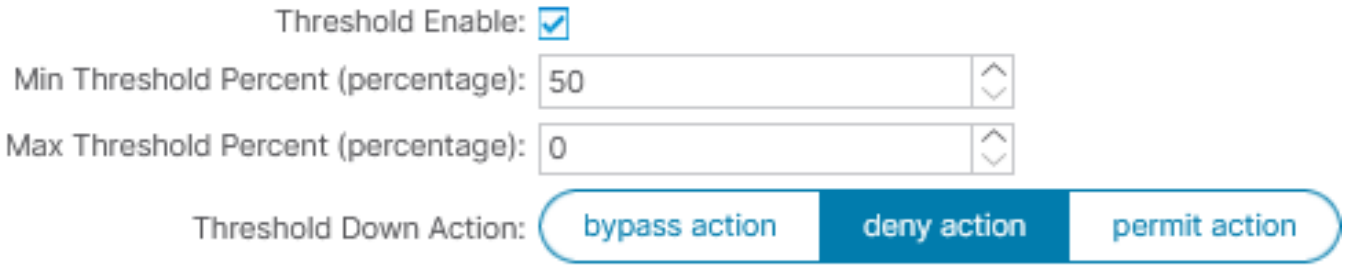
Il criterio SLA IP deve essere mappato all'IP del nodo PBR tramite un gruppo di integrità.



Se viene utilizzato lo SLA IP per individuare dinamicamente l'indirizzo MAC, questo campo non può essere vuoto, ma impostato su tutti gli 0:



Una volta che un gruppo di integrità si è associato all'IP del nodo PBR tramite la destinazione L3 nel criterio di reindirizzamento basato su criteri L4-L7, impostare delle soglie per definire il comportamento dello SLA IP in caso di irraggiungibilità. Specificare un numero minimo di destinazioni L3 attive necessarie per mantenere il reindirizzamento. Se il conteggio dei nodi PBR attivi è inferiore o superiore alla percentuale di soglia, l'intero gruppo viene interessato dall'azione di riduzione della soglia selezionata, interrompendo la ridistribuzione. Questo approccio supporta l'esclusione del nodo PBR durante la risoluzione dei problemi senza influire sul flusso del traffico.



I gruppi di integrità associano tutti gli IP definiti nelle destinazioni L3 di un singolo criterio di reindirizzamento di base dei criteri L4-L7 o più criteri di reindirizzamento di base dei criteri L4-L7, a condizione che venga utilizzato lo stesso criterio del gruppo di integrità.

```
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#
```

Informazioni correlate

- White paper sulla progettazione del grafico di reindirizzamento dell'infrastruttura basata su policy e incentrata sulle applicazioni Cisco
- ACI Layer 4-7 Policy-Based Redirect (PBR) Deep Dive and Tips (Cisco Live Presentation)
- Risoluzione dei problemi relativi allo SLA IP su PBR multipiattaforma

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).