

Configurazione e verifica della PBR L1 attiva/attiva in ACI

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Topologia](#)

[Perché in ACI è necessario il grafico del servizio L1?](#)

[Informazioni sulla periferica L1](#)

[Attivo/Attivo L1 PBR](#)

[Grafico Configurazione per il servizio L1](#)

[Grafico della verifica per il servizio L1 su GUI APIC](#)

[Grafico della verifica per il servizio L1 su CLI APIC](#)

[Convalida traffico](#)

Introduzione

In questo documento viene descritto come configurare e verificare il grafico dei servizi L1 attivi/attivi in ACI (Application Centric Infrastructure).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Informazioni sul funzionamento di Layer 3 Service Graph in ACI
- Informazioni su come configurare il gruppo di criteri Endpoint, i domini bridge e il contratto in ACI

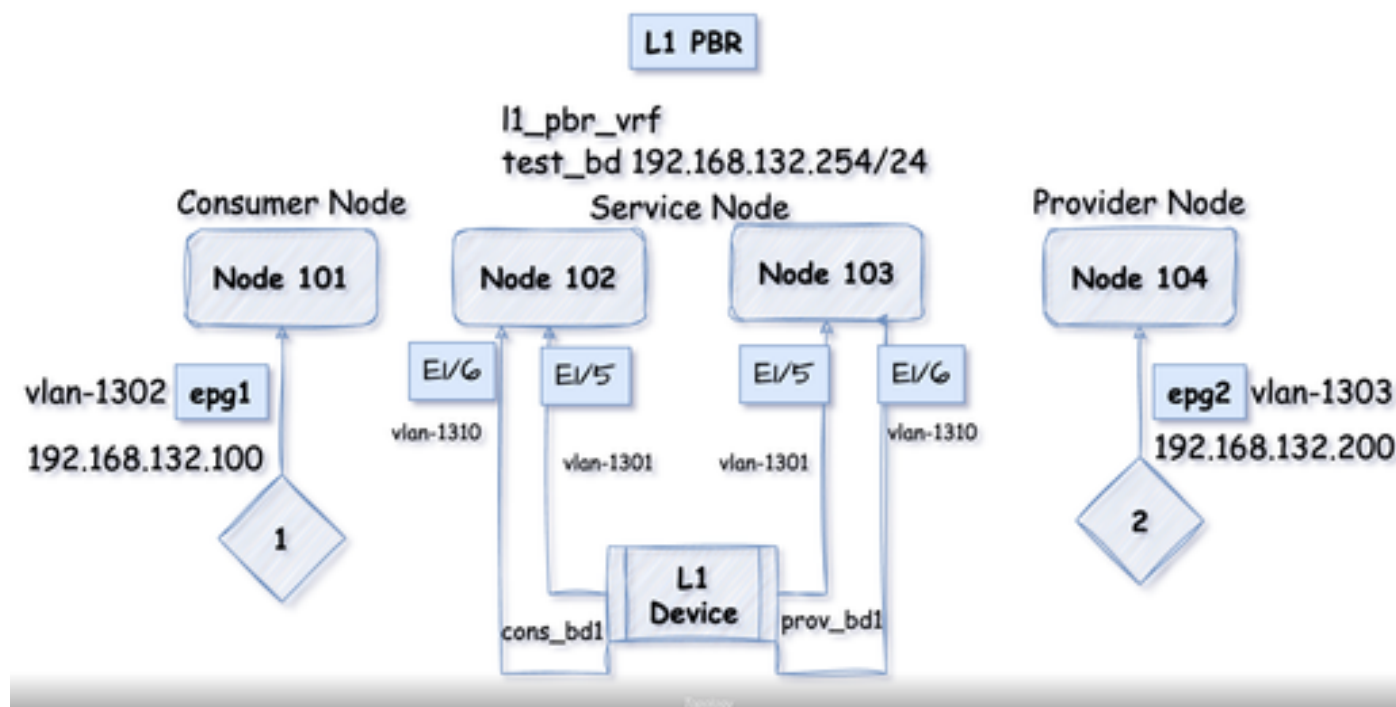
Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Versione APIC: 5.3(2a)
- H/W foglia: N9K-C93180YC-FX , N9K-C93180YC-EX
- Foglia S/W: n9000-15.3(2a)
- Nodo foglia 101, 102, 103, 104

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

Topologia



La configurazione di EPG1 ed EPG2 non è illustrata in questo documento, ma deve essere configurata prima di procedere con l'apprendimento dell'endpoint.

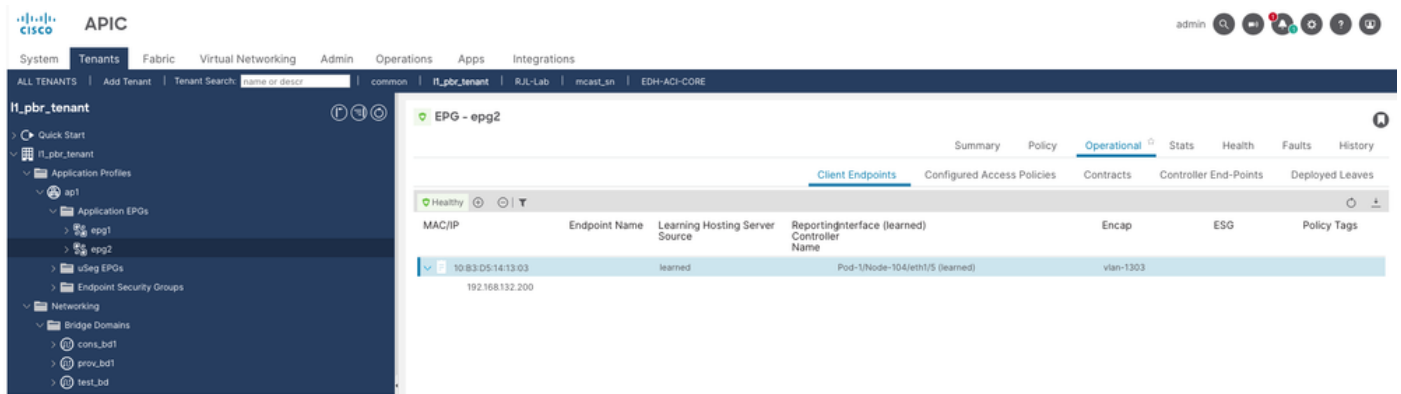
1. convalidare l'endpoint di tipo EPG1 haş 192.168.132.100 appreso (nodo 101).

The screenshot shows the APIC interface with the following details:

- System** tab is selected.
- Tenants** section shows **it_pbr_tenant** selected.
- Application Profiles** section shows **epg1** selected.
- Client Endpoints** tab is active, showing a table of endpoints.

MAC/IP	Endpoint Name	Learning Source	Reporting Host (learned)	Reporting Interface (learned)	Encap	ESG	Policy Tags
10.83.D5:14:13:02		learned	Pod-1/Node-101/eth1/5 (learned)		vlan-1302		
192.168.132.100							

2. La convalida di EPG2 ha appreso l'endpoint 192.168.132.200 (nodo 104).



Perché in ACI è necessario il grafico del servizio L1?

In Cisco ACI è possibile inserire il dispositivo di servizio L4-L7 come L3/L2/L1. Il layer 3 indica che il dispositivo esterno è in grado di eseguire la decisione di routing per inoltrare il traffico, mentre il layer 2 indica che il traffico deve essere inoltrato solo sulla base dell'indirizzo MAC. In ACI è possibile inserire una periferica L2 come IPS (Intrusion Prevention System)/Firewall trasparente. Si pensi a uno scenario in cui il dispositivo che si sta per reindirizzare il traffico non è in grado di prendere alcuna decisione di inoltro, quindi in questi casi è possibile distribuire L1 Policy-Based Routing (PBR).

L'inoltro del traffico è lo stesso per i casi L3 e L2 PBR, l'unica differenza è nel caso in cui il traffico L3 PBR viene reindirizzato a un indirizzo IP dove, come per il traffico L1/L2 PBR, viene reindirizzato a un indirizzo MAC. Questi indirizzi MAC sono associati in modo statico all'interfaccia foglia per l'inoltro. Vedrete di più su questo andare oltre.

Per ulteriori informazioni sui casi di utilizzo di Active/Standby o Active/Active L1/L2 PBR, fare riferimento al collegamento [White paper PBR](#).

Informazioni sulla periferica L1

In questo modello di implementazione, non viene eseguita alcuna conversione VLAN sul dispositivo di servizio ed entrambe le interfacce funzionano sulla stessa VLAN. Questo approccio è comunemente noto come modalità in linea o modalità wire ed è generalmente utilizzato per i firewall e i sistemi di prevenzione delle intrusioni (IPS). È ideale quando il dispositivo di servizio deve eseguire funzioni di sicurezza senza partecipare all'inoltro di livello 2 o 3.

Attivo/Attivo L1 PBR

A partire dalla versione ACI 5.0, è supportata la distribuzione di un grafico dei servizi con dispositivi L4-L7 in modalità attiva/attiva. Questo risultato si ottiene assegnando un'encap unica a ogni interfaccia di dispositivo L4-L7 (interfaccia concreta) e sfruttando la configurazione automatica di ACI di 'Flood in encap' sul servizio nascosto EPG. Questo servizio nascosto EPG viene creato da ACI per associare l'interfaccia di periferica L4-L7 al dominio del Service Bridge.

Non è necessario che gli amministratori configurino manualmente il servizio nascosto EPG, in

quanto ACI abilita automaticamente 'Flood in encap' durante il processo di rendering del grafico del servizio.

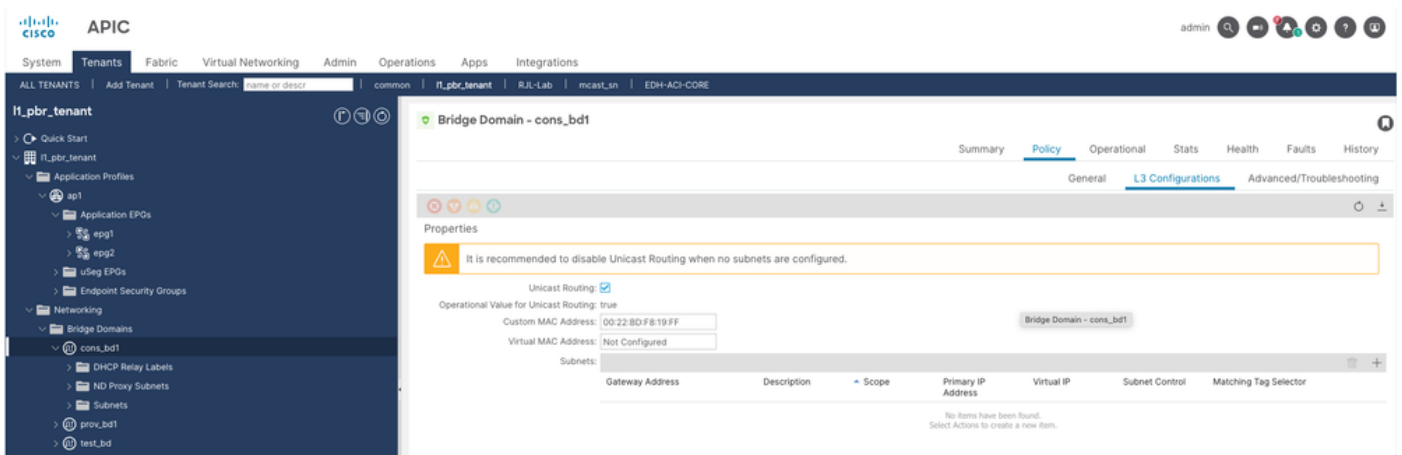
Per le distribuzioni L1 PBR active-active, è necessario configurare l'ambito locale della porta. È quindi necessario collocare le interfacce cluster (connettori) consumer e provider del dispositivo L4-L7 in domini fisici separati, ciascuno con il proprio pool VLAN, mantenendo lo stesso intervallo VLAN su entrambi i domini.

Riferimento: [White Paper PBR](#).

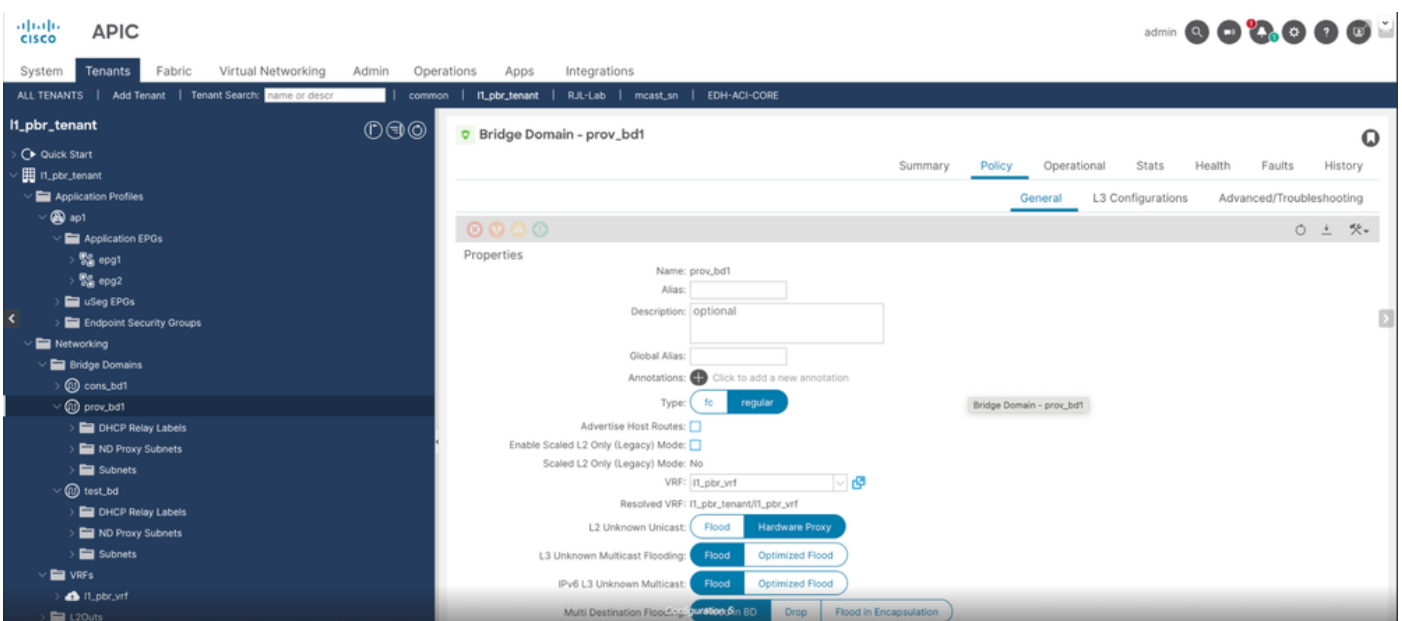
Grafico Configurazione per il servizio L1

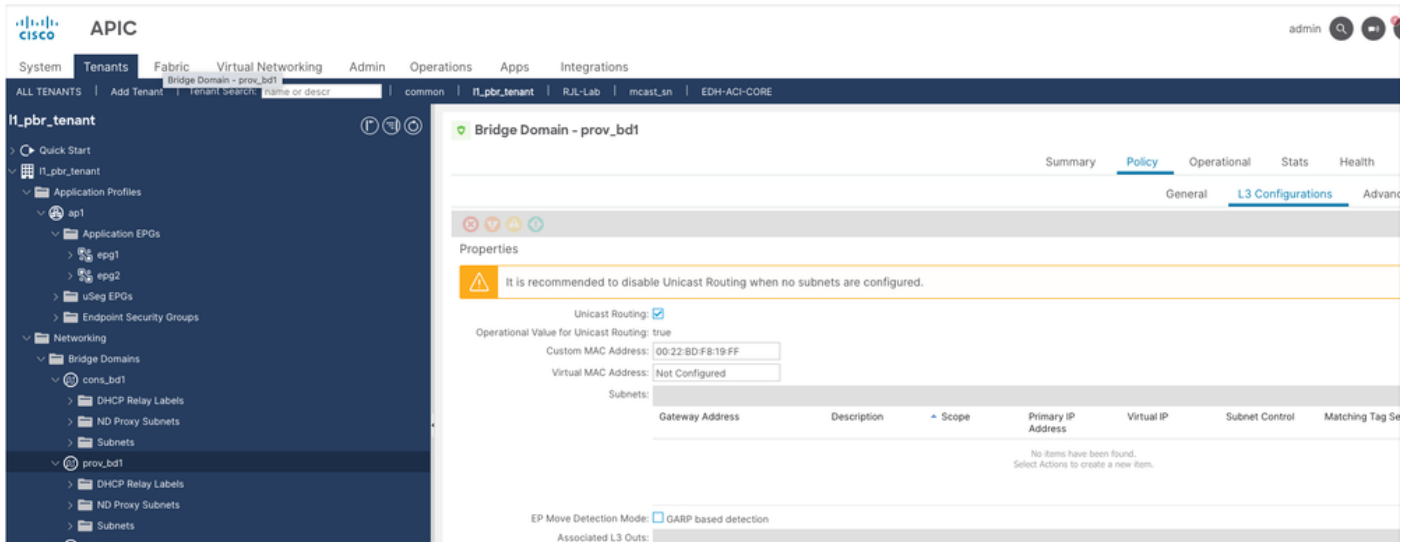
È necessario abilitare il routing unicast, impostare l'unicast sconosciuto L2 sul proxy hardware e non è necessaria alcuna subnet per i domini con e prov bridge.

Passaggio 1. Configurare il dominio del bridge di consumer denominato cons_bd1.



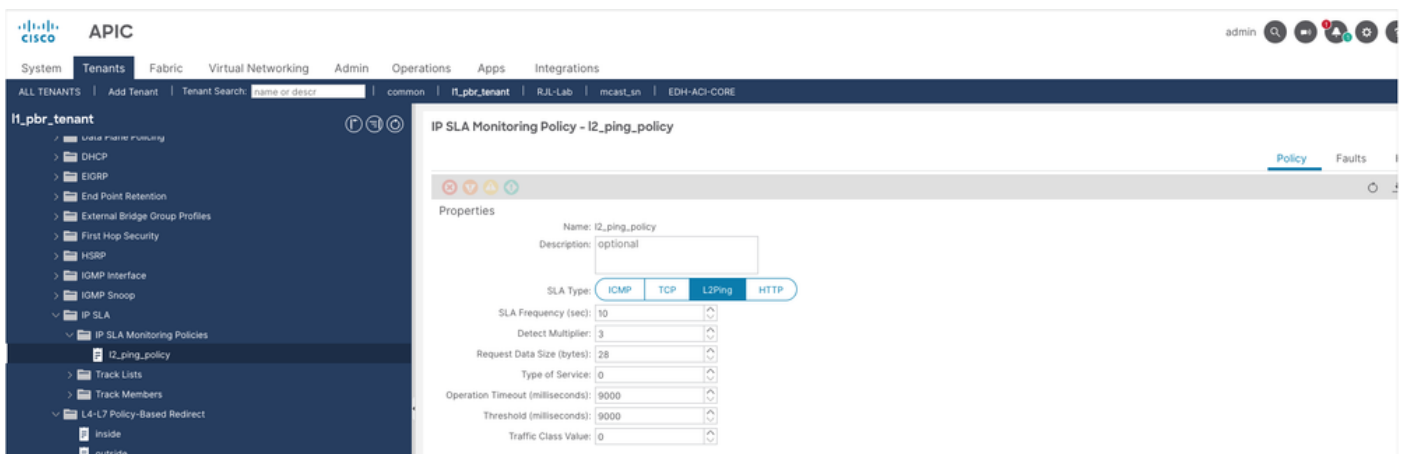
Passaggio 2. Configurare il dominio del bridge del provider denominato prov-bd1.





Passaggio 3. Configurare i criteri del contratto di servizio IP con il tipo di contratto di servizio L2Ping.

Selezionare Tenant > Policies > Protocol > IP SLA > IP SLA Monitoring Policies, quindi fare clic con il pulsante destro del mouse e creare il criterio.



Passaggio 4. Configurare il dispositivo L4/L7.

Passare a Tenant > Servizi > Dispositivi, quindi fare clic con il pulsante destro del mouse e creare il dispositivo L4-L7.

APIC

admin

System

Tenants

Fabric

Virtual Networking

Admin

Operations

Apps

Integrations

ALL TENANTS

Add Tenant

Tenant Search: name or device

common

it_pbr_tenant

R/L-Lab

micast_sn

EDH-ACI-CORE

it_pbr_tenant

Match Rules

MLD Snoop

ND Interface

OSPF

PIM

Route Maps for Multicast

Route Maps for Route Control

Route Tag

Set Rules

Troubleshooting

Host Protection

Monitoring

NetFlow

VMM

Endpoint Tags

Services

L4-L7

Service Graph Templates

gbr1

Router configurations

Devices

pk_l1_pbr

L4-L7 Devices - pk_l1_pbr

Policy

Faults

History

General

Devices

Cluster

Name: pk_l1_pbr

Alias:

Service Type: Other

Device Type: PHYSICAL

Promiscuous Mode:

Context Aware: Multiple Single

Function Type: GoThrough GoTo L1 L2

Active-Active Mode: true

Devices

Name	Interfaces	Encap
it_device_1	inside1 (Pod-1/Node-102/eth1/5)	vlan-1301
it_device_2	outside1 (Pod-1/Node-103/eth1/5)	vlan-1301
it_device_3	inside2 (Pod-1/Node-102/eth1/6)	vlan-1310
it_device_4	outside2 (Pod-1/Node-103/eth1/6)	vlan-1310

Cluster

Cluster Interfaces:

Name	Concrete Interfaces	Physical Domain
consumer	it_device_1[inside1], it_device_2[inside2]	it_pbr_dom_inside
provider	it_device_1[outside1], it_device_2[outside2]	it_pbr_dom_outside

Nota: Per il dispositivo L1, ogni interfaccia cluster deve trovarsi in domini fisici diversi per l'ambito locale della porta.

Passaggio 5. Configurare il reindirizzamento basato su criteri L4-L7 per l'interfaccia interna ed esterna.

Passare a Tenant > Criteri > Protocollo > Reindirizzamento basato su criteri L4-L7, quindi fare clic con il pulsante destro del mouse e creare il criterio.

Il nome del criterio ++ si trova all'interno

++ Abbiamo due destinazioni L1, una per ciascun dispositivo L1

The screenshot shows the APIC interface with the 'L4-L7 Policy-Based Redirect - inside' configuration page. The left sidebar shows the navigation tree with 'L4-L7 Policy-Based Redirect' expanded, showing 'inside' and 'outside' options. The main panel displays the configuration for the 'inside' policy.

Properties

- Name: inside
- Description: optional
- Destination Type: L1, L2, L3 (L1 is selected)
- Rewrite source MAC: ☐
- IP SLA Monitoring Policy: i2_ping_policy
- Oper Status: Enabled
- Threshold Enable: ☒
- Min Threshold Percent (percentage): 40
- Max Threshold Percent (percentage): 100
- Threshold Down Action: bypass action, deny action, permit action (bypass action is selected)
- Enable Pod ID Aware Redirection: ☐
- Hashing Algorithm: Destination IP, Source IP, Source IP, Destination IP and Protocol number (Destination IP is selected)
- Resilient Hashing Enabled: ☐
- L1/L2 Destinations:

Destination Name	IP	MAC	Redirect Health Group	CIF	Description	Oper Status
inside2	ceda:aaaa2d2-4c8293ff-d53376f3-4741	10 83 D5:14 88 88	HG2	[inside2]		Enabled
inside	8301bb59-e940-4233-81c6-e007-437e-45f	10 83 D5:14 99 99	HG1	[inside1]		Enabled

Il nome del criterio ++ è esterno

++ Abbiamo due destinazioni L1, una per ciascun dispositivo L1

The screenshot shows the APIC interface with the 'L4-L7 Policy-Based Redirect - outside' configuration page. The left sidebar shows the navigation tree with 'L4-L7 Policy-Based Redirect' expanded, showing 'inside' and 'outside' options. The main panel displays the configuration for the 'outside' policy.

Properties

- Name: outside
- Description: optional
- Destination Type: L1, L2, L3 (L1 is selected)
- Rewrite source MAC: ☐
- IP SLA Monitoring Policy: i2_ping_policy
- Oper Status: Enabled
- Threshold Enable: ☒
- Min Threshold Percent (percentage): 40
- Max Threshold Percent (percentage): 100
- Threshold Down Action: bypass action, deny action, permit action (bypass action is selected)
- Enable Pod ID Aware Redirection: ☐
- Hashing Algorithm: Destination IP, Source IP, Source IP, Destination IP and Protocol number (Destination IP is selected)
- Resilient Hashing Enabled: ☐
- L1/L2 Destinations:

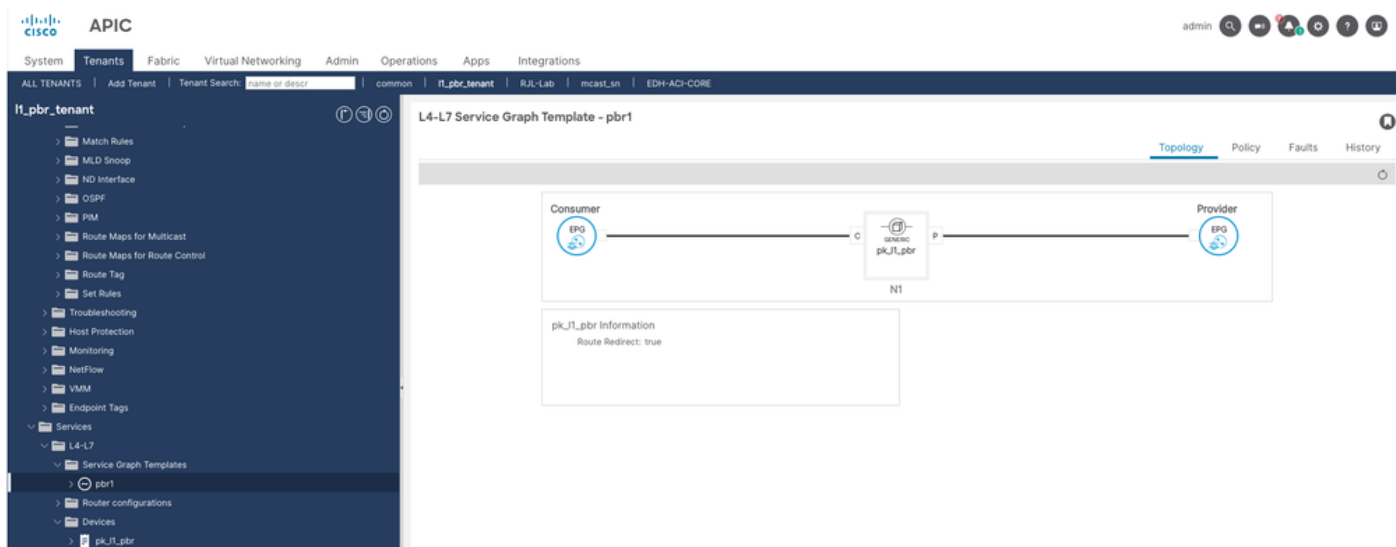
Destination Name	IP	MAC	Redirect Health Group	CIF	Description	Oper Status
outside	2958-ddd3-6eda-4ede-8bb4-1b66-8b19-1eb4	10 83 D5:14 66 66	HG1	[outside1]		Enabled
outside2	13fc:5458-d1ef-46a4-b17b-63b5-4946-ae3f	10 83 D5:14 77 77	HG2	[outside2]		Enabled



Nota: L'azione di riduzione della soglia deve essere la stessa per entrambi i criteri di reindirizzamento L4-L7.

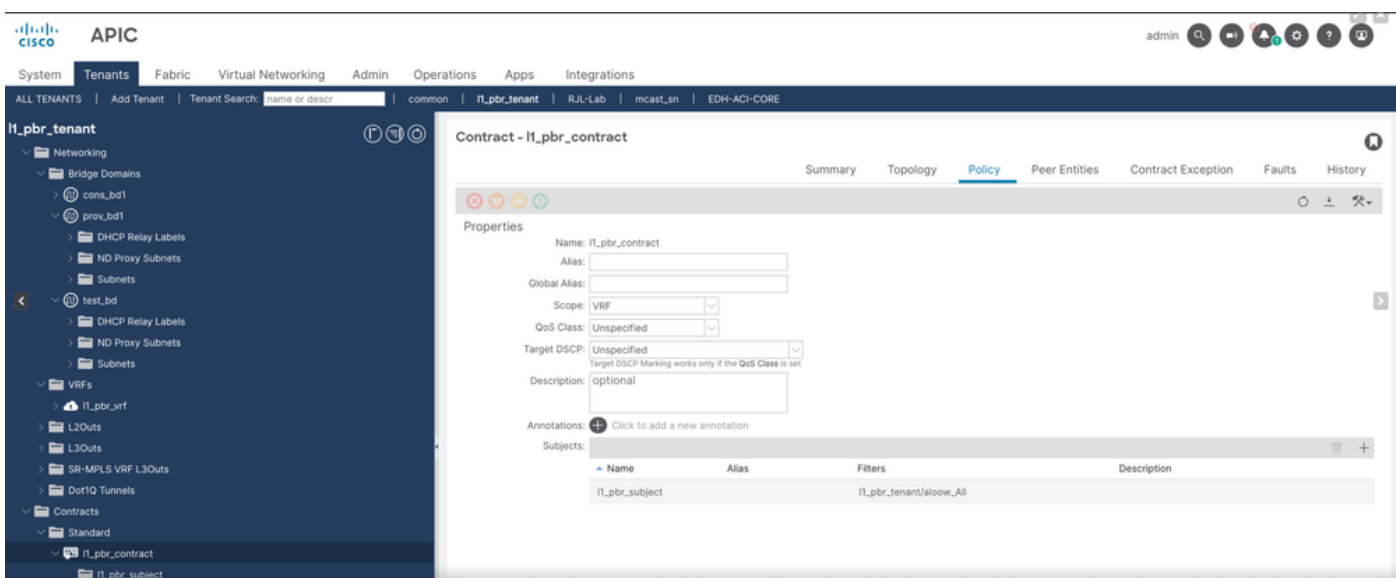
Passaggio 6. Configurare il modello di grafico del servizio.

Passare a Tenant > Servizi > Modello di grafico servizi, quindi fare clic con il pulsante destro del mouse e creare il modello di grafico servizi L4-L7.

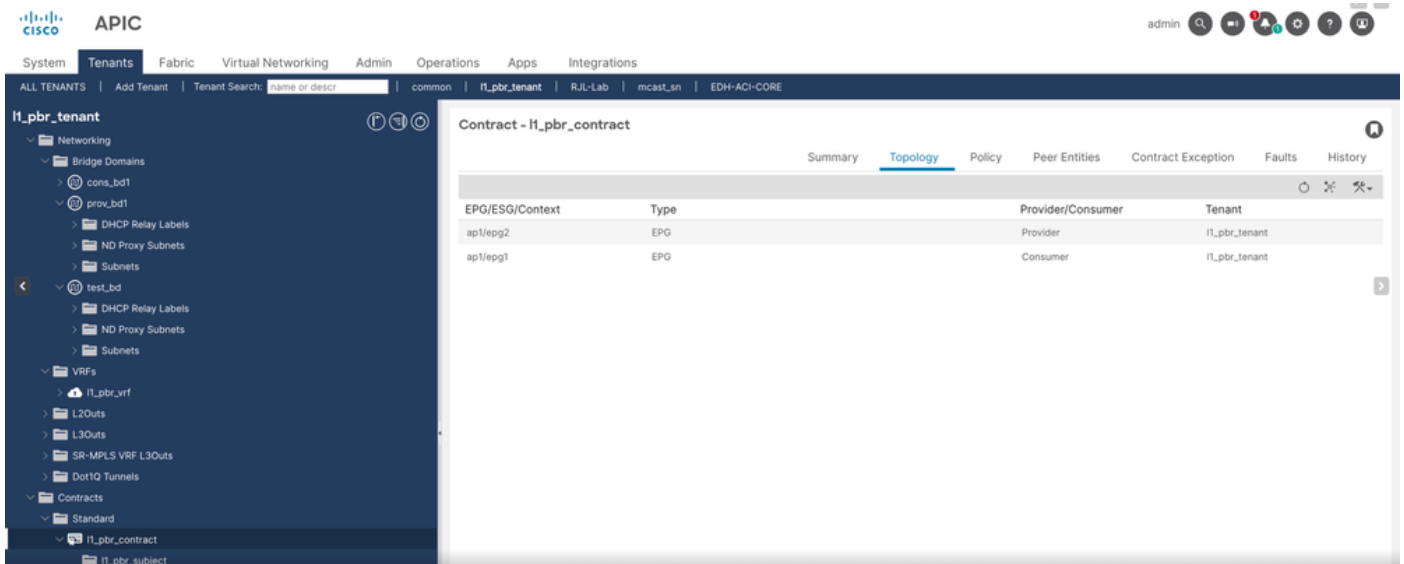


Passaggio 7. Creazione di un contratto.

Passare a Tenant > Contratto > Standard, quindi fare clic con il pulsante destro del mouse e creare il contratto.

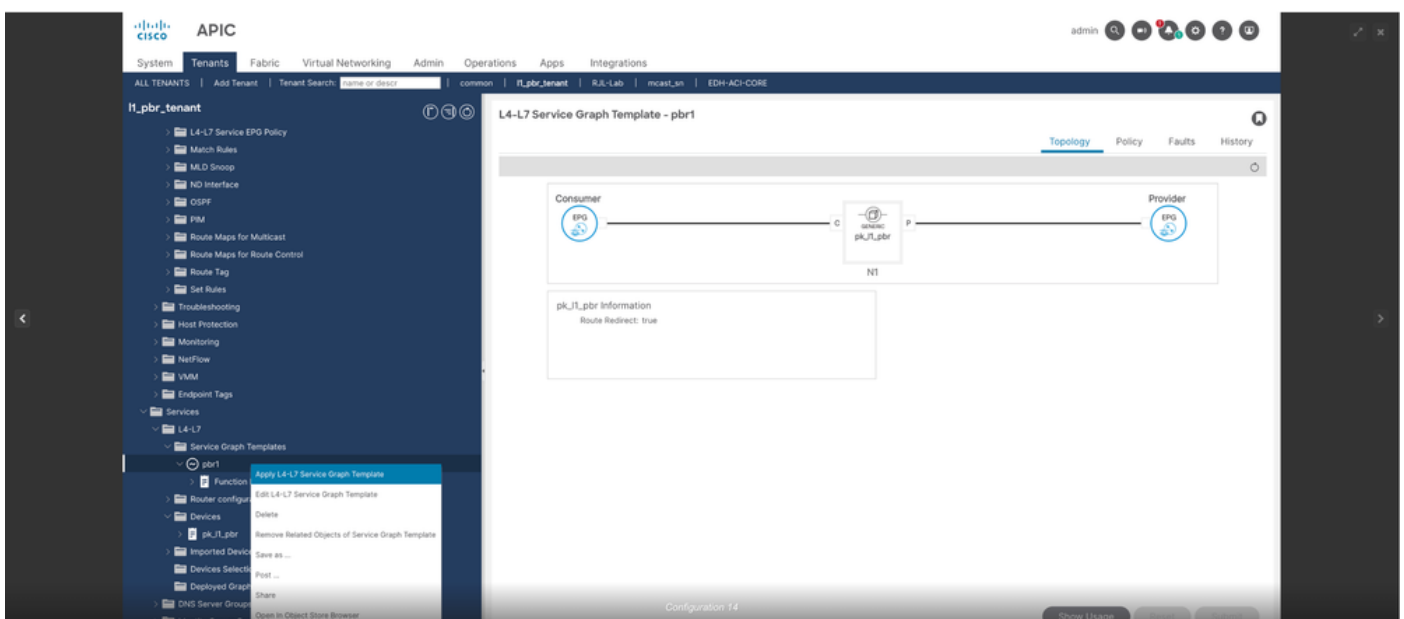


Passaggio 8. Applicare il contratto come consumatore e fornitore rispettivamente a EPG1 ed EPG2.



Passaggio 9. Applicare il modello di grafico del servizio L4-L7.

Passare a Tenant > Servizi > Modello di grafico servizi, quindi fare clic con il pulsante destro del mouse su PBR1 e applicare il modello di grafico servizi L4-L7.



++ Aggiungi EPG consumer e provider

++ Specifica contratto

Apply L4-L7 Service Graph Template to EPG/ESG(s)

STEP 1 > Contract

Endpoint Group Type

Group Type: **Endpoint Policy Group (EPG)** Endpoint Security Group (ESG)

Endpoint Group Configuration

Configure an Intra-Endpoint Contract: ☐

Consumer EPG / External Network:

Provider EPG / Internal Network:

Contract Information

Contract Type: **New Contract** Select Existing Contract Subject

Existing Contracts with Subjects:

Configuration 15

Previous

Cancel

Next

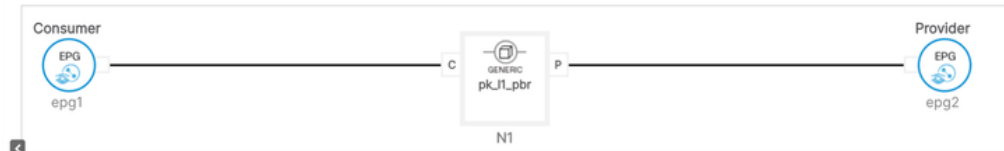
++ clic su Avanti

++ Specificare i dettagli del connettore consumer

Apply L4-L7 Service Graph Template to EPG/ESG(s)

STEP 2 > Graph

Service Graph Template:



pk_i1_pbr Information

Policy-Based Redirect: true

Consumer Connector

Type: **General** Route Peering

BD:

BD that connects the two devices

L3 Destination (VIP): ☒

Redirect Policy:

Service EPG Policy:

Cluster Interface:

++ Specificare i dettagli del connettore del provider

Apply L4-L7 Service Graph Template to EPG/ESG(s)

STEP 2 > Graph

1. Contract 2. Graph

Service Graph Template:

Consumer EPG: epg1

Provider EPG: epg2

Service EPG Policy:

Cluster Interface:

Provider Connector

Type: ☒ General ☐ Route Peering

BD:

BD that connects the two devices

L3 Destination (VIP): ☒

Redirect Policy:

Service EPG Policy:

Cluster Interface:

Configuration 17

Previous Cancel Finish

++ Fare clic sul pulsante Fine

Grafico della verifica per il servizio L1 su GUI APIC

Passaggio 1. Verificare i criteri di selezione dei dispositivi creati dopo l'applicazione del modello di

System Tenants Fabric Virtual Networking Admin Operations Apps Integrations

ALL TENANTS | Add Tenant | Tenant Search: | common | it_pbr_tenant | R/L-Lab | mcast_Lan | EDH-ACI-CORE

it_pbr_tenant

- ND Interface
- OSPF
- IPM
- Route Maps for Multicast
- Route Maps for Route Control
- Route Tag
- Set Rules
- Troubleshooting
- Host Protection
- Monitoring
- NetFlow
- VMM
- Endpoint Tags
- Services
 - L4-L7
 - Service Graph Templates
 - pbr1
 - Function Node - N1
 - Router configurations
 - Devices
 - pk_it_pbr
 - Imported Devices
 - Devices Selection Policies
 - it_pbr_contract-pbr1-N1
 - consumer
 - provider

Logical Device Context - it_pbr_contract-pbr1-N1

Policy Faults History

Properties

Contract Name: it_pbr_contract

Graph Name: pbr1

Node Name: N1

Alias:

Context Name:

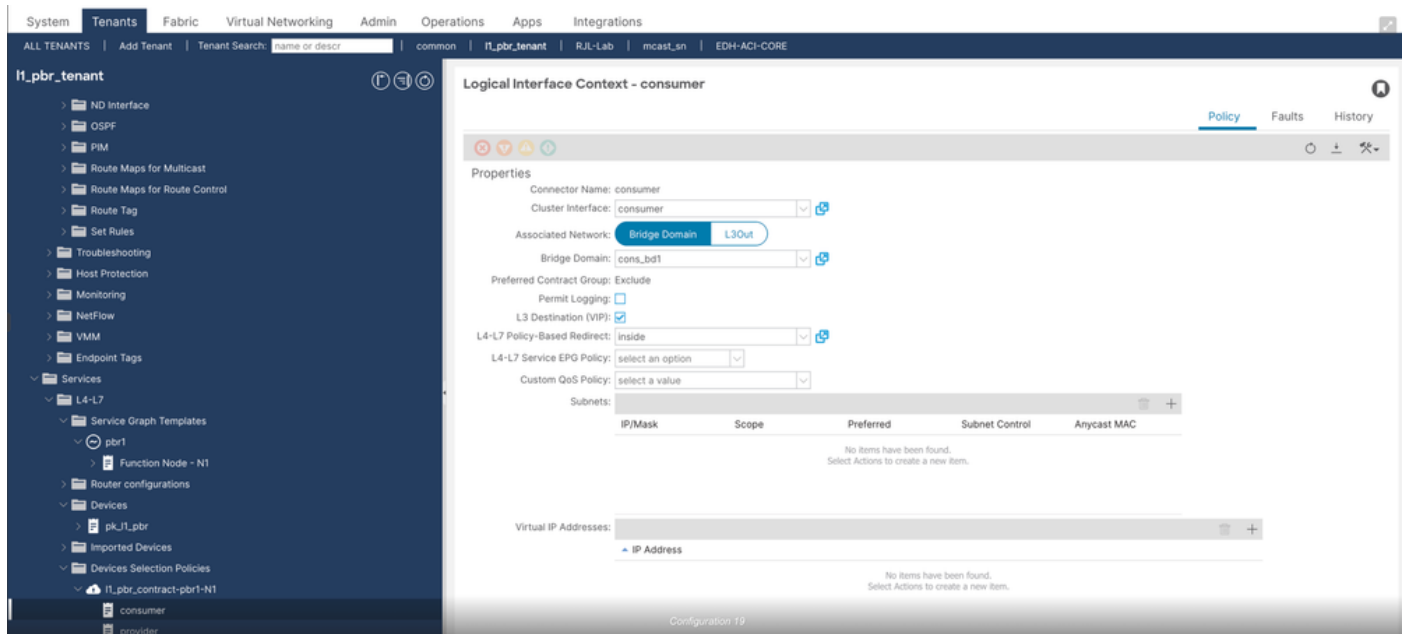
Devices:

Router Config:

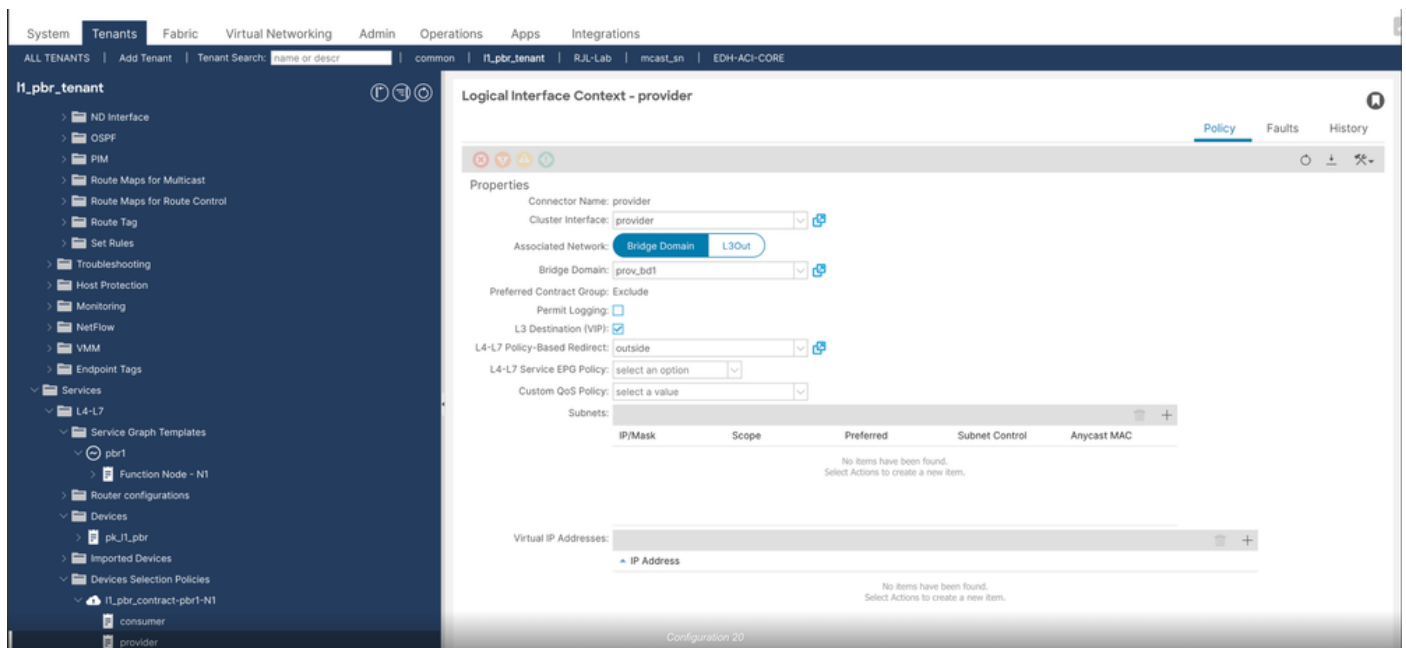
Configuration 18

grafico del servizio.

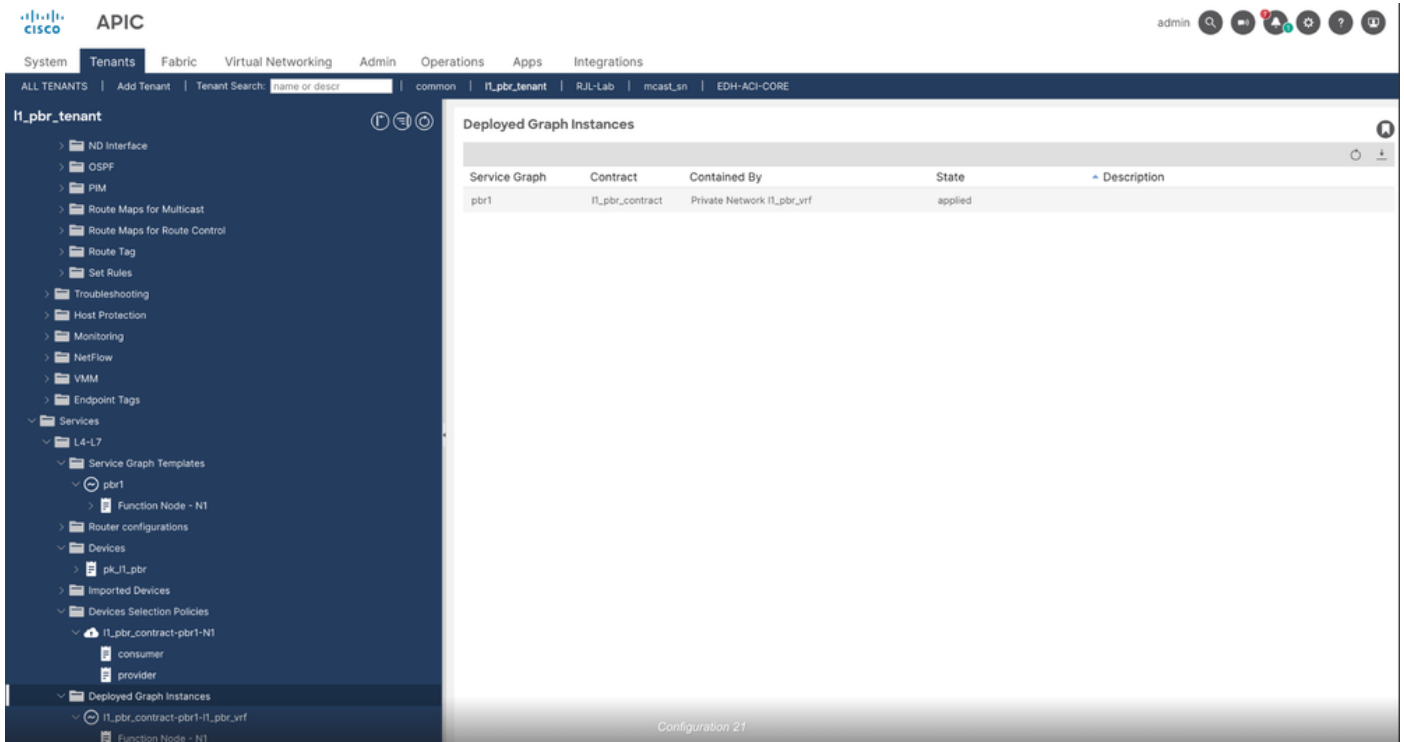
++ Verifica connettore consumer



++ Configura connettore provider



Passaggio 2. Verificare le istanze del grafico distribuite. Se si desidera visualizzare un'istanza, è necessario che sia in stato applicato.



++ Controllare le interfacce di dispositivo e i connettori di funzione dove si sta per vedere PCTAG associato al servizio EPG

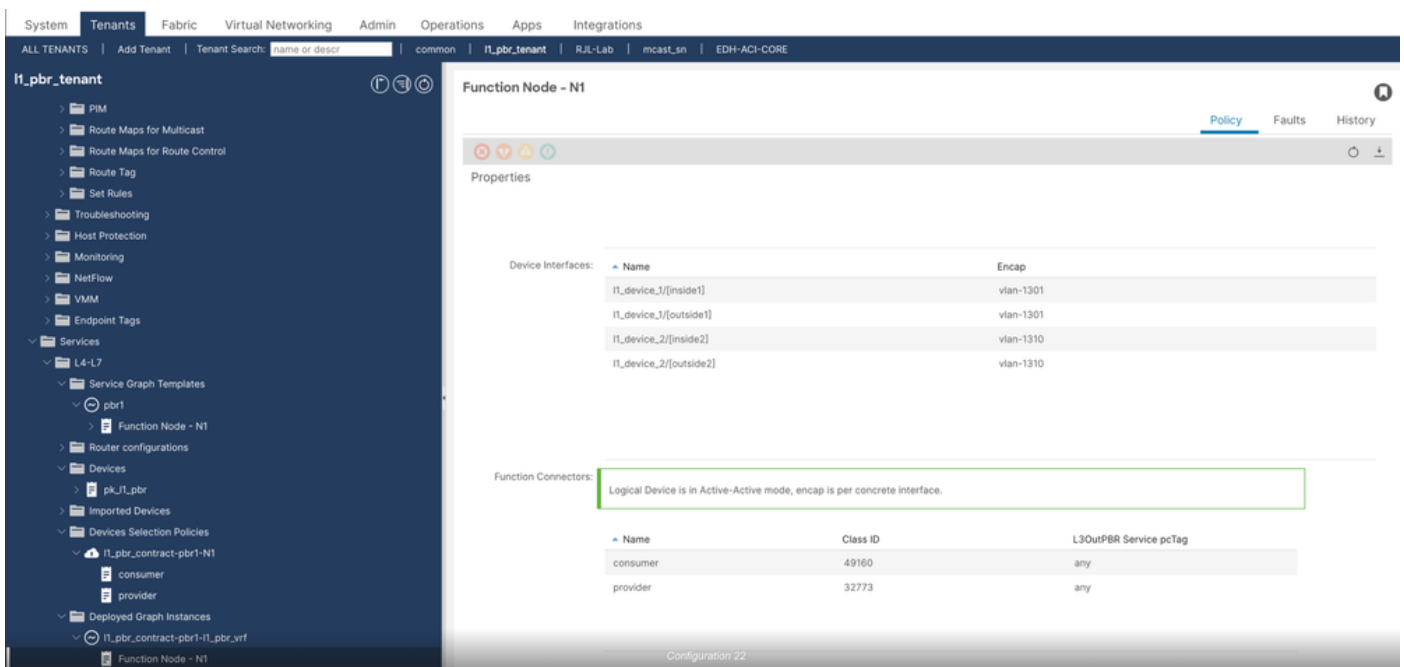


Grafico della verifica per il servizio L1 su CLI APIC

Passaggio 1. Verificare se il grafico del servizio è applicato al nodo consumer e provider insieme allo stato del gruppo di integrità.

```
<#root>
```

```
apic01#
```

fabric 101,104 show service redir info

Node 101

=====

LEGEND

TL: Threshold(Low) | TH: Threshold(High) | HP: HashProfile | HG: HealthGrp | BAC: Backup-Dest |

=====

List of Dest Groups

GrpID	Name	destination	HG-name
=====	=====	=====	=====
10	destgrp-10	dest-[476f:9be9:5aab:4454:a5d6:8c9e:7017:61eb]-[vxlan-2490369]	11_pbr_tenant::HG2
		dest-[8301:bb59:e940:4233:81c6:e007:437e:45f]-[vxlan-2490369]	11_pbr_tenant::HG1
2	destgrp-2	dest-[2958:ddd3:6eda:4ede:8bb4:1b66:8b19:1eb4]-[vxlan-2490369]	11_pbr_tenant::HG1
		dest-[d438:790d:6fdb:4485:bab7:197d:ef61:9a59]-[vxlan-2490369]	11_pbr_tenant::HG2

List of destinations

Name	bdVnid	vMac	vrf
=====	=====	=====	=====
dest-[8301:bb59:e940:4233:81c6:e007:437e:45f]-[vxlan-2490369]	vxlan-16252846	10:B3:D5:14:99:99	11_
dest-[476f:9be9:5aab:4454:a5d6:8c9e:7017:61eb]-[vxlan-2490369]	vxlan-16252846	10:B3:D5:14:77:77	11_
dest-[2958:ddd3:6eda:4ede:8bb4:1b66:8b19:1eb4]-[vxlan-2490369]	vxlan-15794150	10:B3:D5:14:66:66	11_
dest-[d438:790d:6fdb:4485:bab7:197d:ef61:9a59]-[vxlan-2490369]	vxlan-15794150	10:B3:D5:14:77:77	11_

List of Health Groups

HG-Name	HG-OperSt	HG-Dest
=====	=====	=====
11_pbr_tenant::HG1	enabled	dest-[2958:ddd3:6eda:4ede:8bb4:1b66:8b19:1eb4]-[v
		dest-[8301:bb59:e940:4233:81c6:e007:437e:45f]-[vx
11_pbr_tenant::HG2	enabled	dest-[d438:790d:6fdb:4485:bab7:197d:ef61:9a59]-[v
		dest-[476f:9be9:5aab:4454:a5d6:8c9e:7017:61eb]-[v

Node 104

=====

LEGEND

TL: Threshold(Low) | TH: Threshold(High) | HP: HashProfile | HG: HealthGrp | BAC: Backup-Dest |

=====

List of Dest Groups

GrpID	Name	destination	HG-name
=====	=====	=====	=====
3	destgrp-3	dest-[d438:790d:6fdb:4485:bab7:197d:ef61:9a59]-[vxlan-2490369]	11_pbr_tenant::HG2
		dest-[2958:ddd3:6eda:4ede:8bb4:1b66:8b19:1eb4]-[vxlan-2490369]	11_pbr_tenant::HG1
4	destgrp-4	dest-[476f:9be9:5aab:4454:a5d6:8c9e:7017:61eb]-[vxlan-2490369]	11_pbr_tenant::HG2
		dest-[8301:bb59:e940:4233:81c6:e007:437e:45f]-[vxlan-2490369]	11_pbr_tenant::HG1

List of destinations

Name	bdVnid	vMac	vrf
=====	=====	=====	=====
dest-[2958:ddd3:6eda:4ede:8bb4:1b66:8b19:1eb4]-[vxlan-2490369]	vxlan-15794150	10:B3:D5:14:66:66	11_
dest-[d438:790d:6fdb:4485:bab7:197d:ef61:9a59]-[vxlan-2490369]	vxlan-15794150	10:B3:D5:14:77:77	11_
dest-[476f:9be9:5aab:4454:a5d6:8c9e:7017:61eb]-[vxlan-2490369]	vxlan-16252846	10:B3:D5:14:77:77	11_
dest-[8301:bb59:e940:4233:81c6:e007:437e:45f]-[vxlan-2490369]	vxlan-16252846	10:B3:D5:14:99:99	11_

List of Health Groups

HG-Name	HG-OperSt	HG-Dest
=====	=====	=====
l1_pbr_tenant::HG1	enabled	dest-[2958:ddd3:6eda:4ede:8bb4:1b66:8b19:1eb4]-[vx dest-[8301:bb59:e940:4233:81c6:e007:437e:45f]-[vx
l1_pbr_tenant::HG2	enabled	dest-[476f:9be9:5aab:4454:a5d6:8c9e:7017:61eb]-[vx dest-[d438:790d:6fdb:4485:bab7:197d:ef61:9a59]-[vx

Passaggio 2. Verificare se il binding MAC statico è stato creato nei nodi del servizio (102 e 103).

<#root>

apic01#

fabric 102-103 show endpoint vrf l1_pbr_tenant:l1_pbr_vrf

Node 102

Legend:

S - static s - arp L - local O - peer-attached

V - vpc-attached a - local-aged p - peer-aged M - span

B - bounce H - vtep R - peer-attached-r1 D - bounce-to-proxy

E - shared-service m - svc-mgr

+-----+-----+-----+-----+-----+				
VLAN/	Encap	MAC	Address	MAC Info/ Interface
Domain	VLAN	IP	Address	IP Info
+-----+-----+-----+-----+-----+				
23/l1_pbr_tenant:l1_pbr_vrf	vlan-1310	10b3.d514.7777	LS	eth1/6
24/l1_pbr_tenant:l1_pbr_vrf	vlan-1301	10b3.d514.9999	LS	eth1/5

Node 103

Legend:

S - static s - arp L - local O - peer-attached

V - vpc-attached a - local-aged p - peer-aged M - span

B - bounce H - vtep R - peer-attached-r1 D - bounce-to-proxy

E - shared-service m - svc-mgr

+-----+-----+-----+-----+-----+				
VLAN/	Encap	MAC	Address	MAC Info/ Interface
Domain	VLAN	IP	Address	IP Info
+-----+-----+-----+-----+-----+				
40/l1_pbr_tenant:l1_pbr_vrf	vlan-1310	10b3.d514.7777	LS	eth1/6
1/l1_pbr_tenant:l1_pbr_vrf	vlan-1301	10b3.d514.6666	LS	eth1/5

Convalida traffico

1. Da EP1 a EP2 vengono generati 2000 pacchetti ping ICMP che verranno reindirizzati al dispositivo L1.

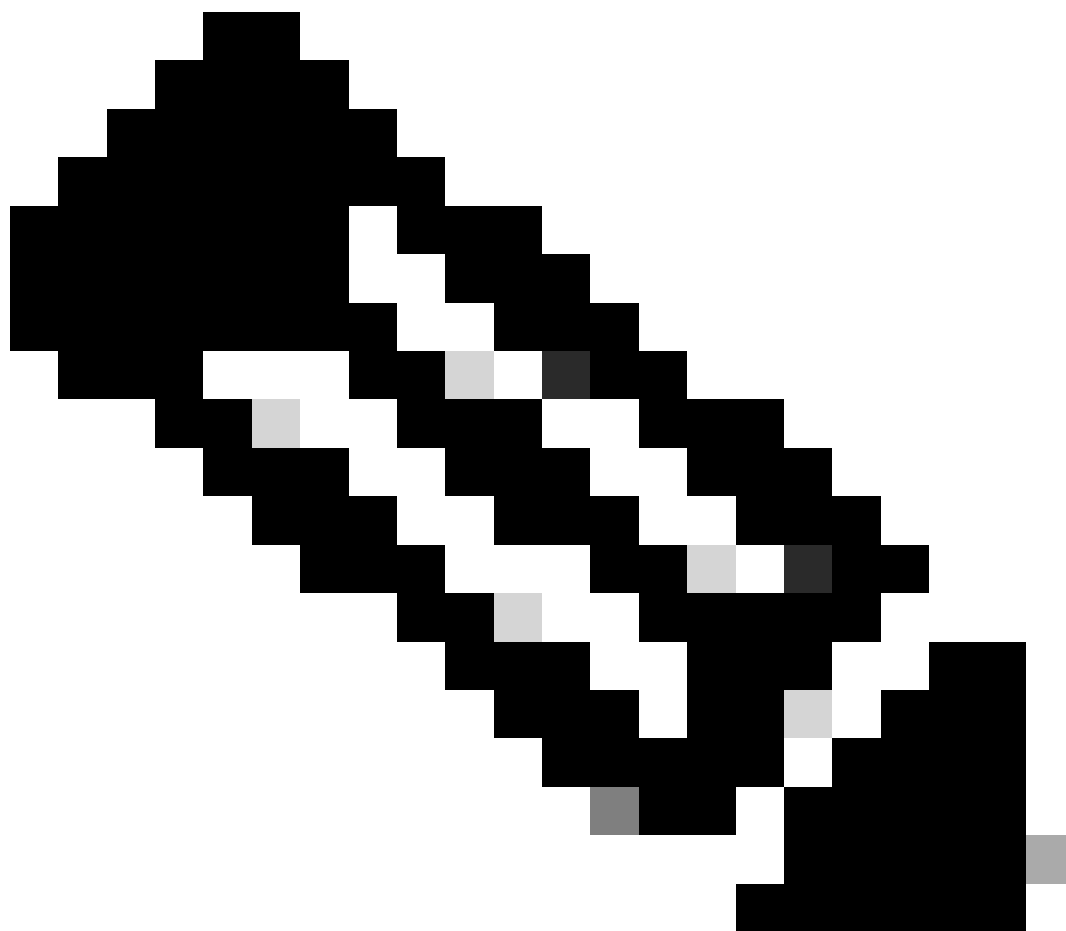
```
switch1# ping 192.168.132.200 vrf l1_pbr1 count 2000 >>>> sending 2000 packets
64 bytes from 192.168.132.200: icmp_seq=464 ttl=251 time=0.859 ms
64 bytes from 192.168.132.200: icmp_seq=465 ttl=251 time=0.872 ms
64 bytes from 192.168.132.200: icmp_seq=466 ttl=251 time=0.844 ms
64 bytes from 192.168.132.200: icmp_seq=467 ttl=251 time=0.821 ms
64 bytes from 192.168.132.200: icmp_seq=468 ttl=251 time=0.814 ms
64 bytes from 192.168.132.200: icmp_seq=469 ttl=251 time=0.846 ms
64 bytes from 192.168.132.200: icmp_seq=470 ttl=251 time=0.863 ms
64 bytes from 192.168.132.200: icmp_seq=471 ttl=251 time=0.819 ms
64 bytes from 192.168.132.200: icmp_seq=472 ttl=251 time=0.802 ms
64 bytes from 192.168.132.200: icmp_seq=473 ttl=251 time=0.851 ms
64 bytes from 192.168.132.200: icmp_seq=474 ttl=251 time=0.815 ms
```

2. Convalidare i contatori delle interfacce sui nodi 102 e 103 collegati al dispositivo L1.

```
apic01# fabric 102-103 show interface ethernet 1/5-6 | grep "Node\|Ethernet\|RX\|packets\|TX"
Node 102
Ethernet1/5 is up
Hardware: 100/1000/10000/25000/auto Ethernet, address: 10b3.d5c5.8f25 (bia 10b3.d5c5.8f25)
30 seconds input rate 0 bits/sec, 0 packets/sec
30 seconds output rate 64 bits/sec, 0 packets/sec
RX
2008 unicast packets 2 multicast packets 0 broadcast packets >>>>>2000 packets recieved from L1 device
2010 input packets 213180 bytes
0 jumbo packets 0 storm suppression bytes
TX
2009 unicast packets 1 multicast packets 0 broadcast packets >>>>> 2000 packets transmitted towards L1
2010 output packets 213003 bytes
0 jumbo packets
Ethernet1/6 is up
Hardware: 100/1000/10000/25000/auto Ethernet, address: 10b3.d5c5.8f26 (bia 10b3.d5c5.8f26)
30 seconds input rate 0 bits/sec, 0 packets/sec
30 seconds output rate 64 bits/sec, 0 packets/sec
RX
9 unicast packets 2 multicast packets 0 broadcast packets
11 input packets 1286 bytes
0 jumbo packets 0 storm suppression bytes
TX
9 unicast packets 1 multicast packets 0 broadcast packets
10 output packets 1003 bytes
0 jumbo packets

Node 103
Ethernet1/5 is up
Hardware: 100/1000/10000/25000/auto Ethernet, address: a453.0e75.9a85 (bia a453.0e75.9a85)
30 seconds input rate 0 bits/sec, 0 packets/sec
30 seconds output rate 64 bits/sec, 0 packets/sec
RX
2009 unicast packets 1 multicast packets 0 broadcast packets >>>>> 2000 packets recieved from L1 device
2010 input packets 213003 bytes
0 jumbo packets 0 storm suppression bytes
TX
2008 unicast packets 1 multicast packets 0 broadcast packets >>> 2000 packets transmitted towards L1 de
2009 output packets 212897 bytes
0 jumbo packets
Ethernet1/6 is up
Hardware: 100/1000/10000/25000/auto Ethernet, address: a453.0e75.9a86 (bia a453.0e75.9a86)
30 seconds input rate 0 bits/sec, 0 packets/sec
```

30 seconds output rate 64 bits/sec, 0 packets/sec
RX
9 unicast packets 1 multicast packets 0 broadcast packets
10 input packets 1003 bytes
0 jumbo packets 0 storm suppression bytes
TX
9 unicast packets 1 multicast packets 0 broadcast packets
10 output packets 1003 bytes
0 jumbo packets



Nota: I contatori di interfaccia sono stati azzerati sui nodi 102 e 103 prima del test del traffico.

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).