Configurazione e verifica della configurazione del grafico di servizio di layer 2 con ASAv

Sommario

Introduzione

In questo documento viene descritto come configurare e verificare la configurazione del diagramma dei servizi di layer 2 in Cisco Application Centric Infrastructure (ACI).

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
- Informazioni su come configurare ASAv (Adaptive Security Appliance Virtual) come firewall trasparente

Componenti usati

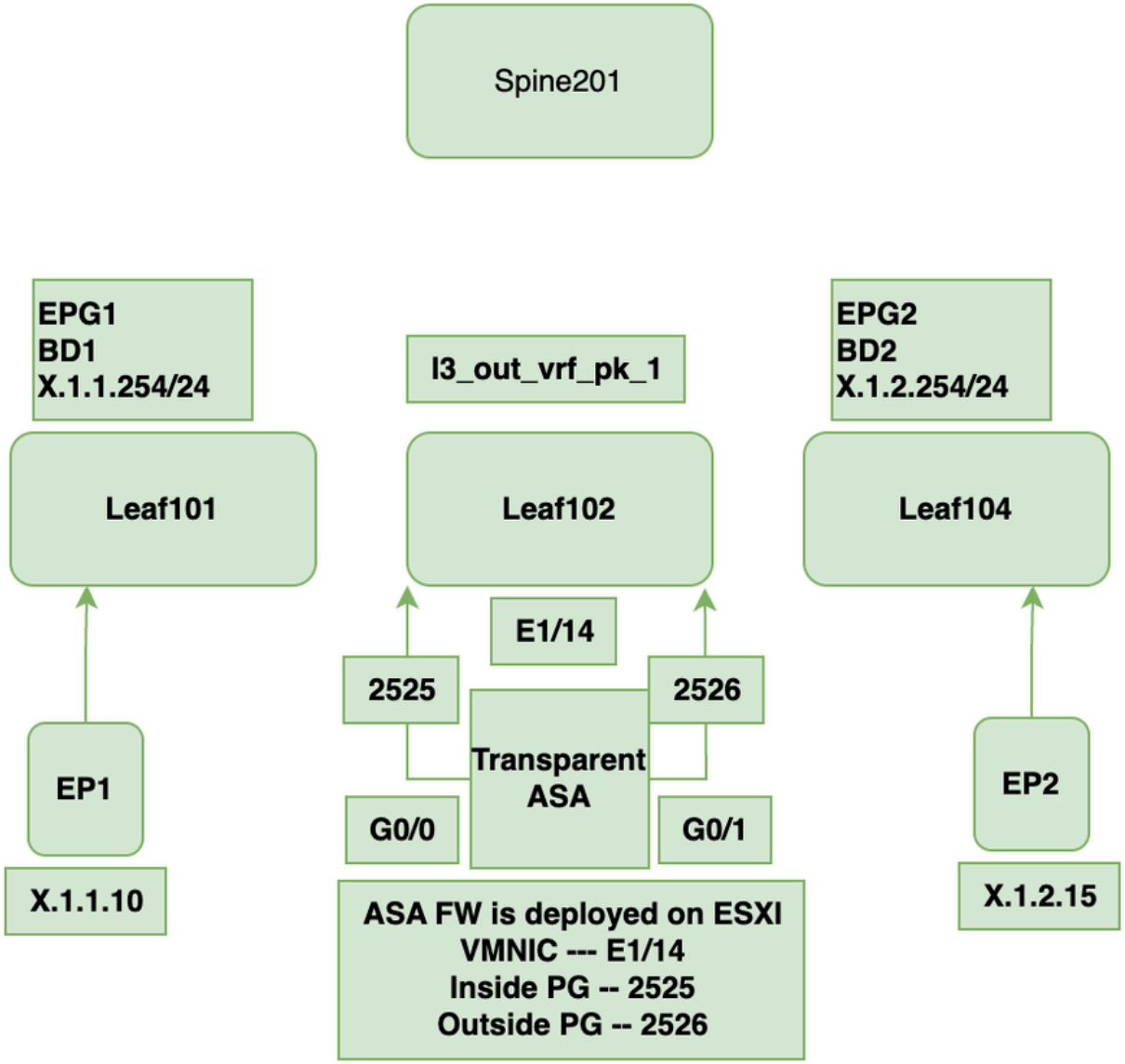
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Versione APIC: 6.0 (3g)

- H/W foglia: N9K-C93180YC-FX
- Bianco e nero foglia: n9000-16.0 (3g)
- Nodo foglia 101, 102, 103
- ASAv installato sul server ESXi

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.

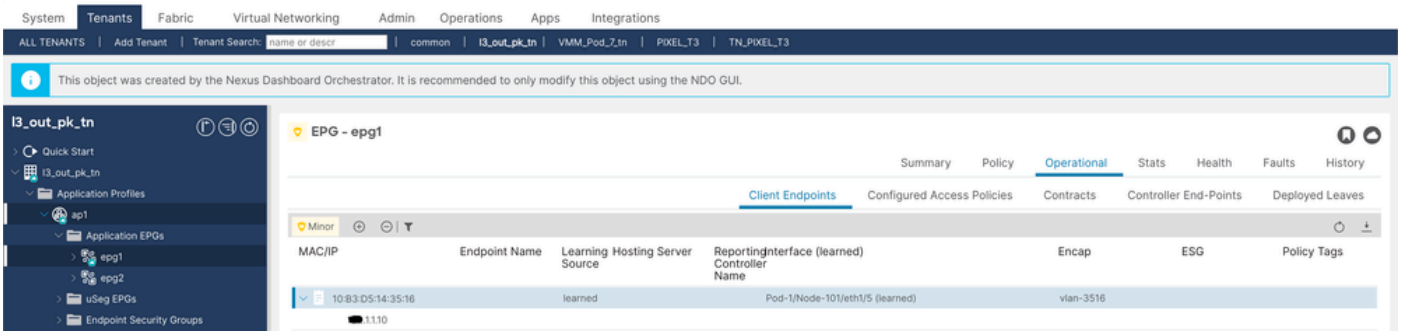
Topologia



Topologia

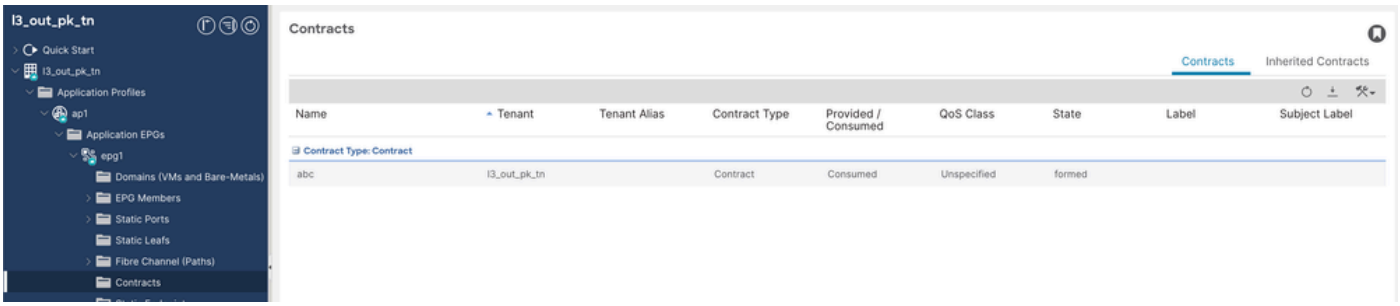
La configurazione di EPG1 ed EPG2 non è illustrata in questo documento, ma deve essere configurata prima di procedere con l'apprendimento dell'endpoint.

1. Convalidare l'endpoint di tipo EPG1 haș X.1.1.10 appreso (nodo 101).



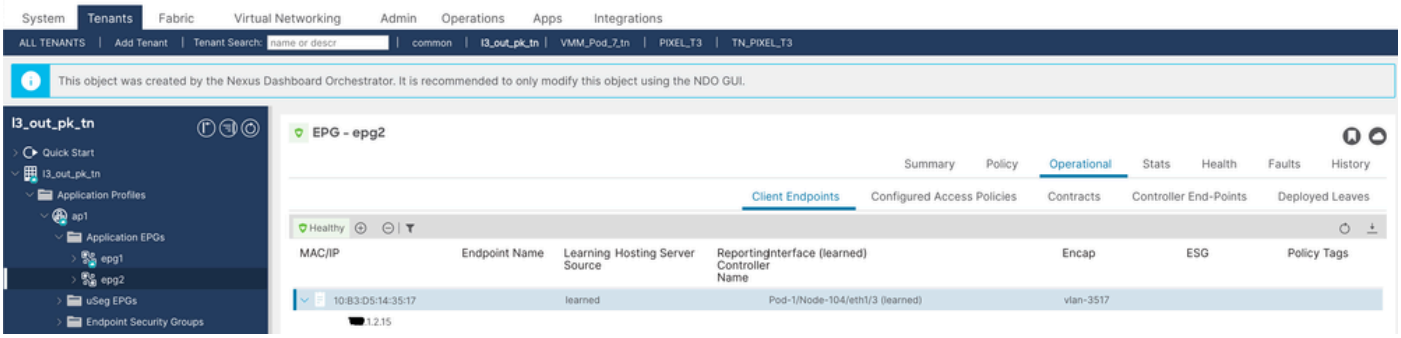
Endpoint client

2. Il contratto abc viene utilizzato da EPG1.



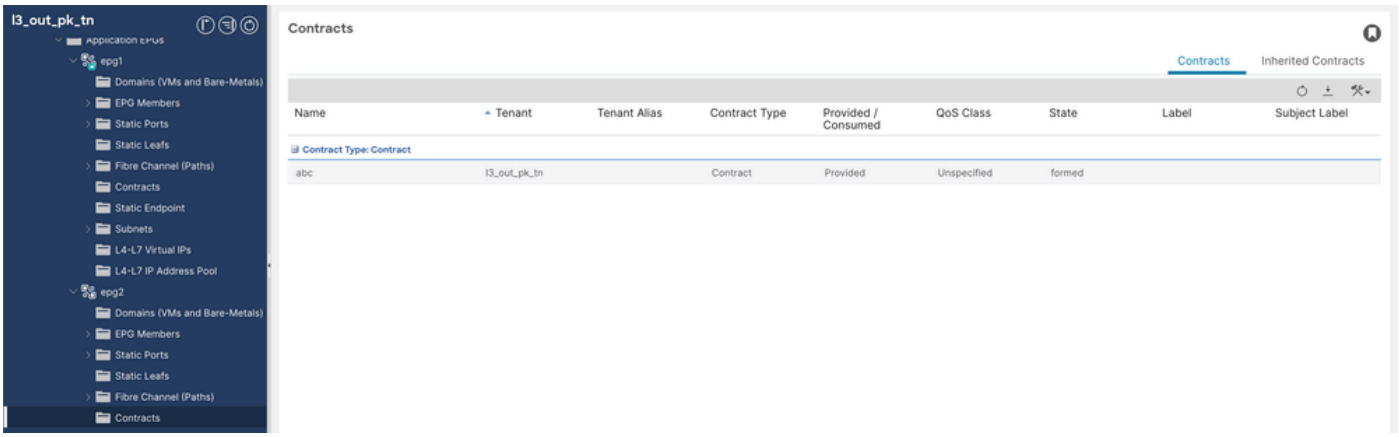
Contratto utilizzato

3. Convalida che l'endpoint di EPG2 è X.1.2.15appreso (Nodo 104).



Endpoint client

4. Il contratto abc è fornito da EPG2.



Contratto fornito

Perché in ACI è necessario il grafico del servizio L2?

- In Cisco ACI, i dispositivi di servizio L4-L7 possono essere inseriti sul layer 3 (L3), layer 2 (L2) o layer 1 (L1).
- Inserimento servizi Layer 3: Il dispositivo esterno (ad esempio, firewall, Intrusion Prevention System (IPS)) prende le decisioni relative al routing e inoltra il traffico in base agli indirizzi IP.
- Inserimento servizi Layer 2: Il traffico viene inoltrato in base agli indirizzi MAC senza coinvolgimento del routing. Ciò è utile per i firewall trasparenti o i dispositivi IPS.
- PBR (Policy-Based Routing) L2 viene utilizzato quando si inserisce un dispositivo di servizio L2, ad esempio un IPS o un firewall trasparente in ACI.
- Il meccanismo di inoltro del traffico rimane lo stesso sia per L3 che per L2 PBR.
- La differenza principale:
    - PBR L3: Il traffico viene reindirizzato a un indirizzo IP (il dispositivo partecipa al routing).
    - PBR L2: Il traffico viene reindirizzato a un indirizzo MAC (il dispositivo funziona sul layer 2).
- Nel PBR L2, gli indirizzi MAC sono associati in modo statico alle interfacce foglia per garantire un corretto inoltro del traffico.

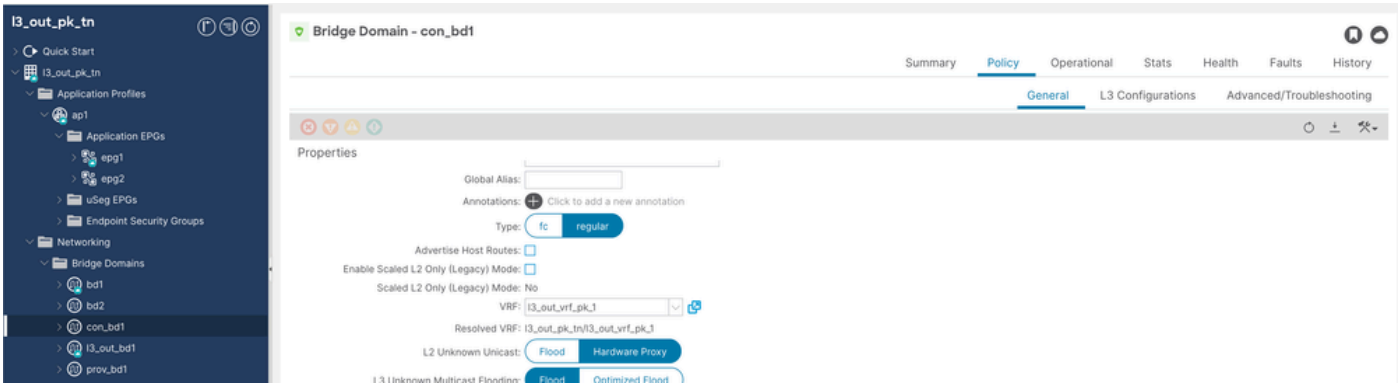
Per ulteriori informazioni sugli scenari di utilizzo di Active/Standby o Active/Active L1/L2 PBR, consultare il white paper PBR.

Grafico Configurazione per il servizio L2

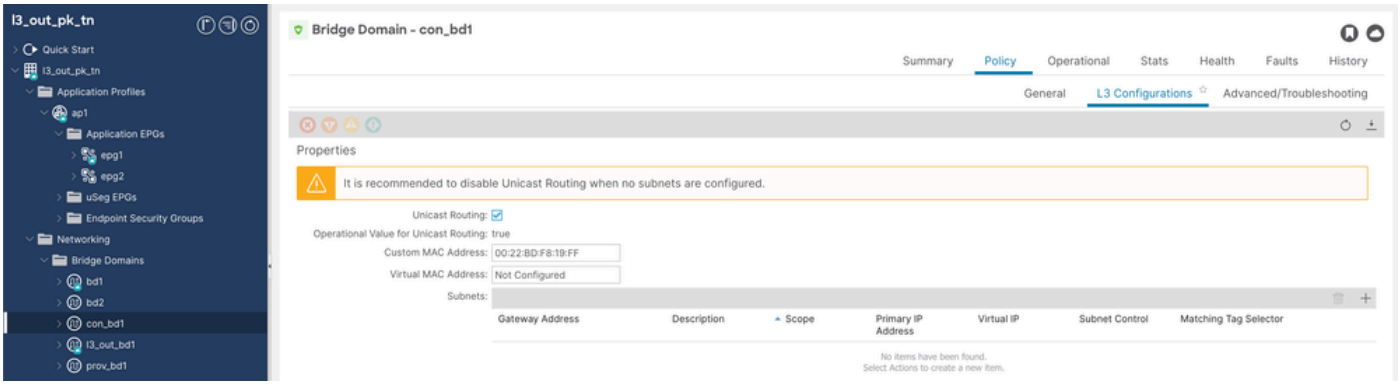
Passaggio 1. Configurare l'offerta consumer denominata con-bd1.

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 (BD).

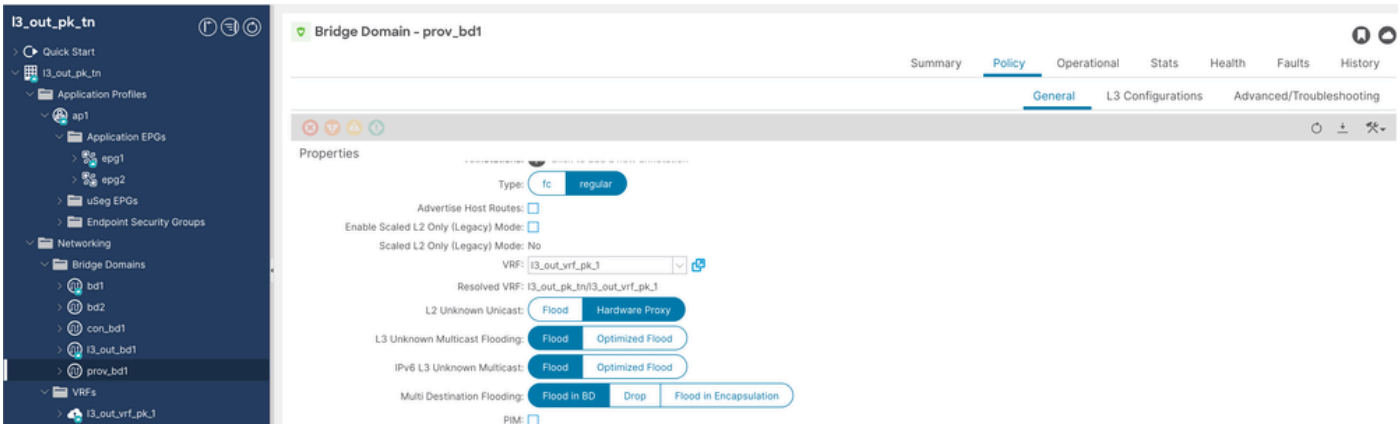


Config BD Cons

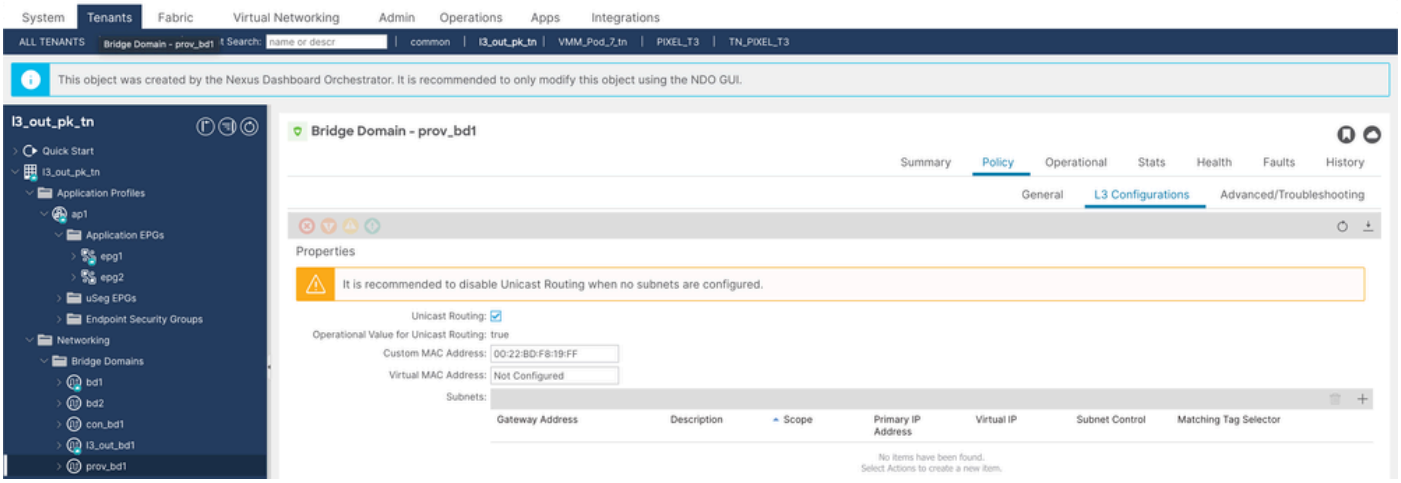


Config. BD 2

Passaggio 2. Configurare il provider bd denominato prov-bd1.



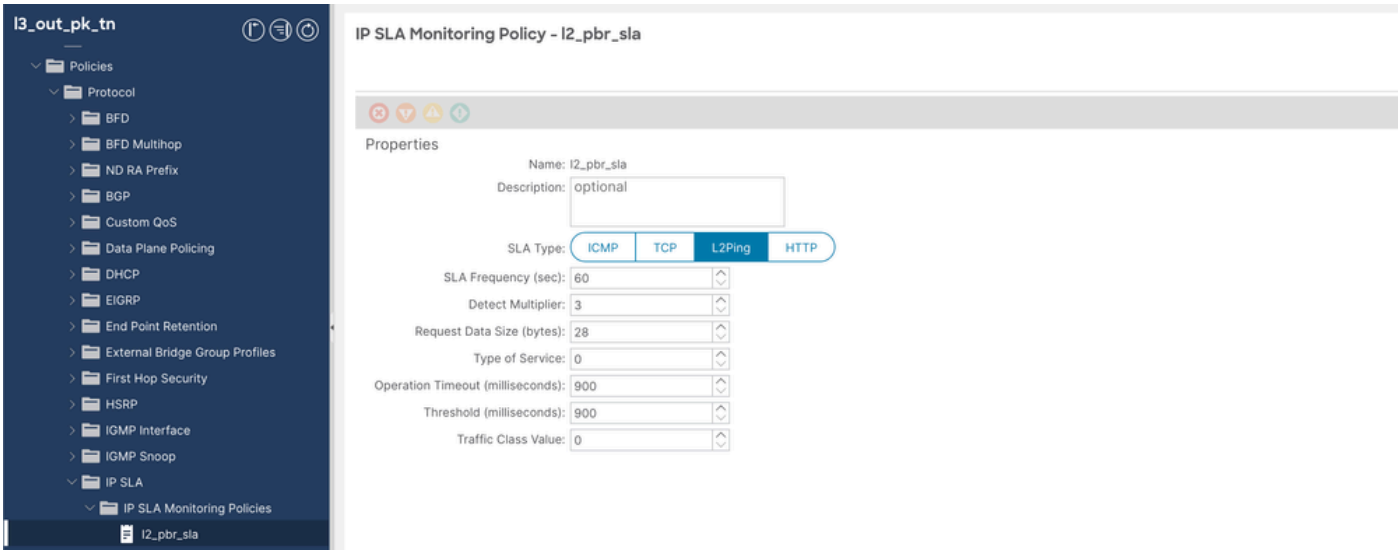
Configurazione BD di prova



Configurazione BD prov. 2

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

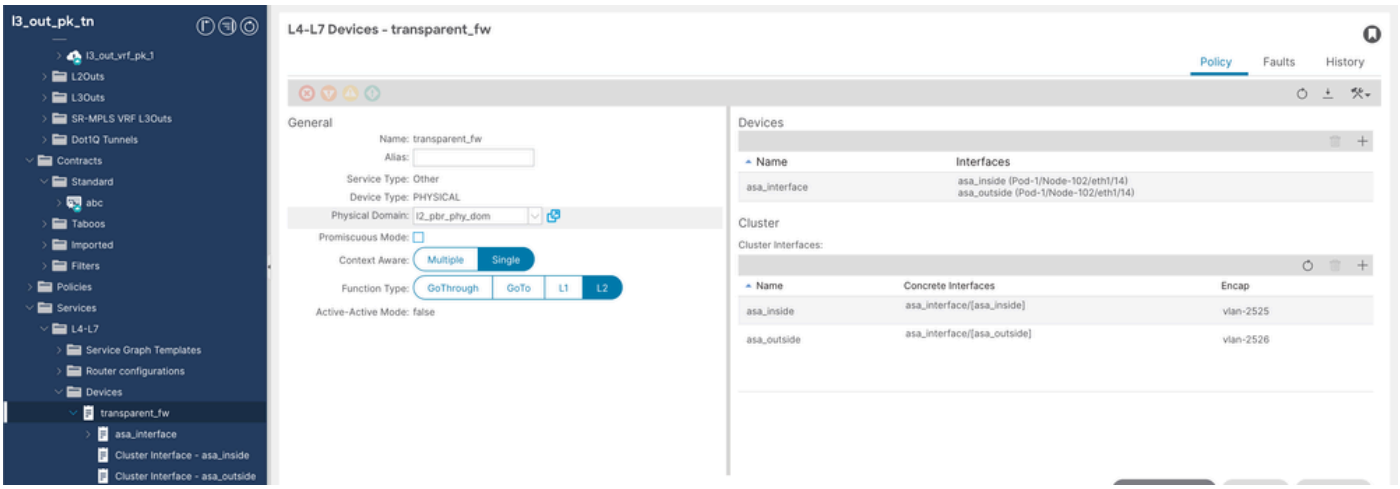
Selezionare Tenant > Policy > Protocollo > IP SLA > Policy di monitoraggio IP SLA, quindi fare clic con il pulsante destro del mouse e creare il criterio.



Criteri SLA IP

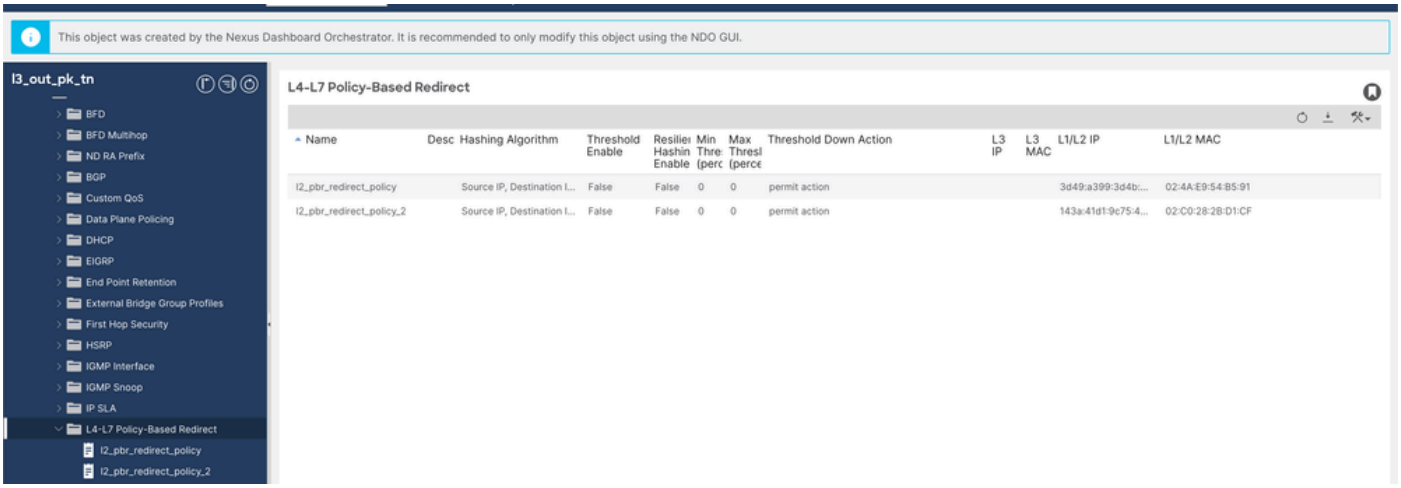
Passaggio 4. Configurare il dispositivo L4/L7.

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



Dispositivo L4-L7

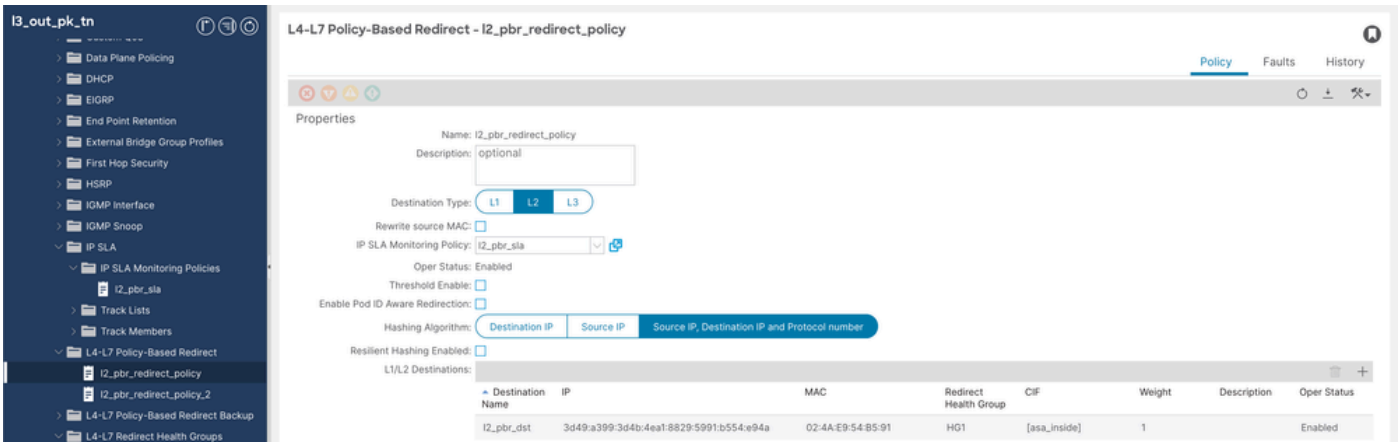
Passaggio 5. Convalidare la panoramica del reindirizzamento basato su criteri (è possibile verificare questa condizione dopo aver configurato 5a e 5b).



Criteri di reindirizzamento L4-L7

Passaggio 5.1. Configurare una policy di reindirizzamento basata su policy L4-L7 per ASA (Adaptive Security Appliance) all'interno dell'interfaccia (non è necessario specificare MAC o IP, ma l'interfaccia viene popolata dall'APIC stessa).

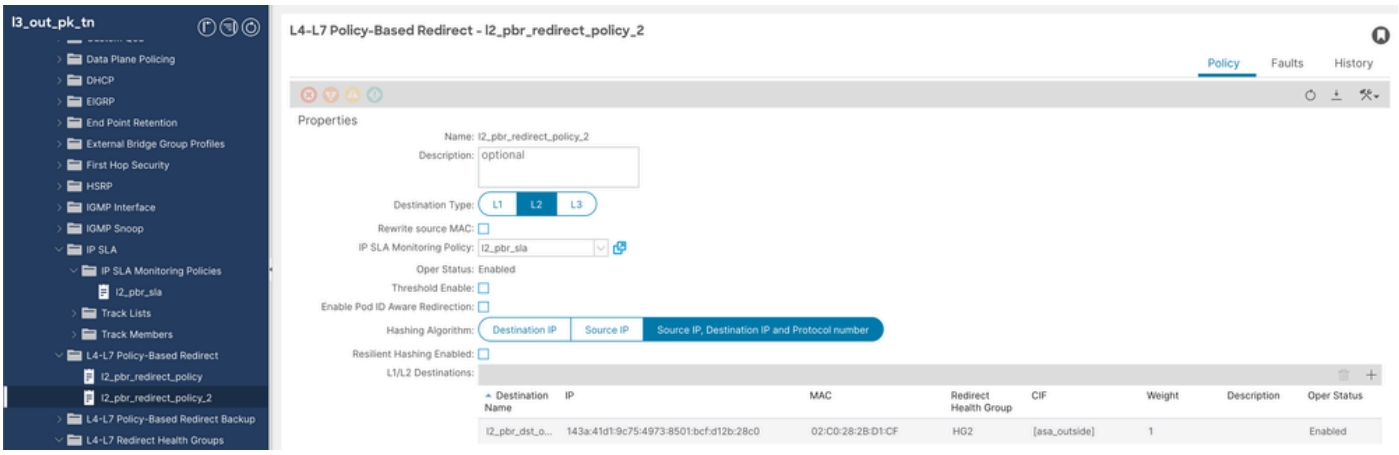
Passare a Tenant > Criteri > Protocollo > Reindirizzamento basato su criteri L4-L7, quindi fare clic con il pulsante destro del mouse e creare il criterio.



Configurazione criteri di reindirizzamento L4-L7

Passaggio 5.2. Configurare la policy di reindirizzamento L4-L7 basata su policy per l'interfaccia esterna ASA (non è necessario specificare l'indirizzo MAC o IP, ma l'indirizzo viene popolato dallo stesso APIC).

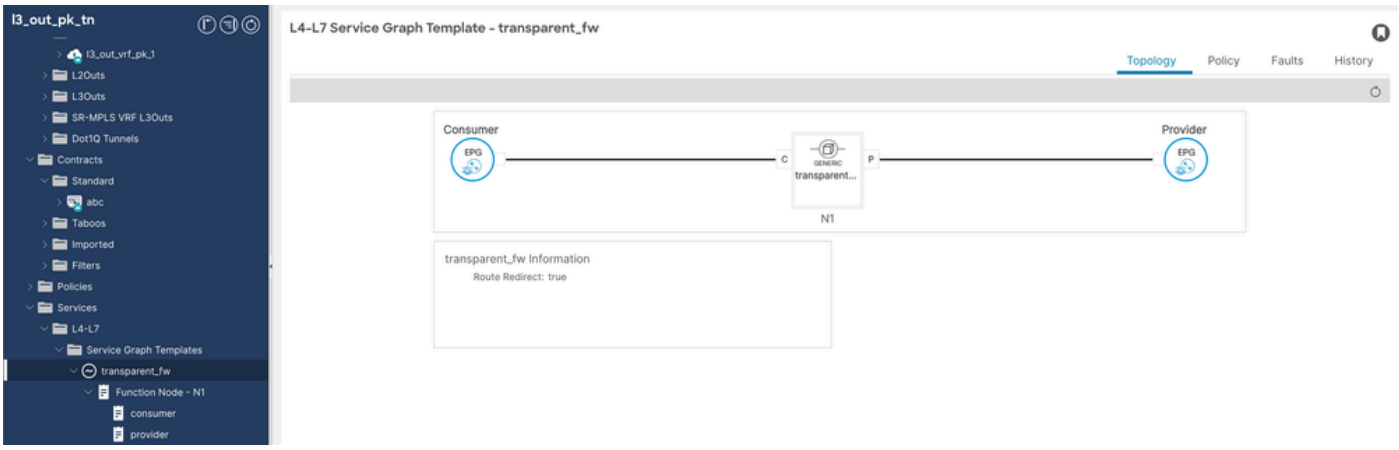
Passare a Tenant > Criteri > Protocollo > Reindirizzamento basato su criteri L4-L7, quindi fare clic con il pulsante destro del mouse e creare il criterio.



Configurazione 2 criteri di reindirizzamento L4-L7

Passaggio 6. Configurare il modello di grafico del servizio.

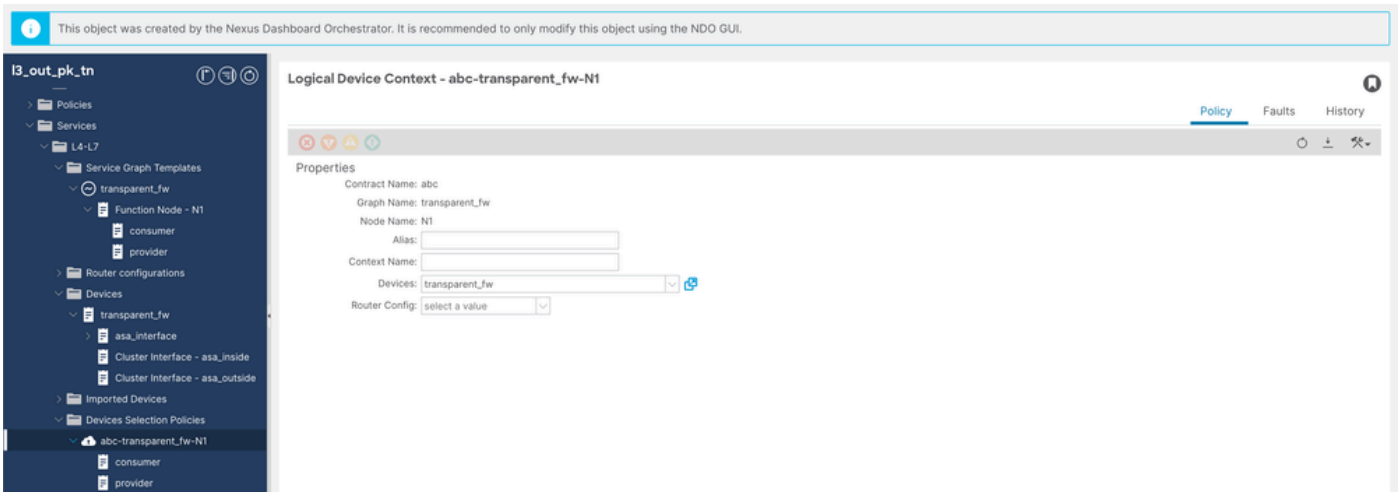
Passare a Tenant > Servizi > Modello di grafico servizi, quindi fare clic con il pulsante destro del mouse e creare il modello di grafico servizi L4-L7.



Configurazione del grafico del servizio

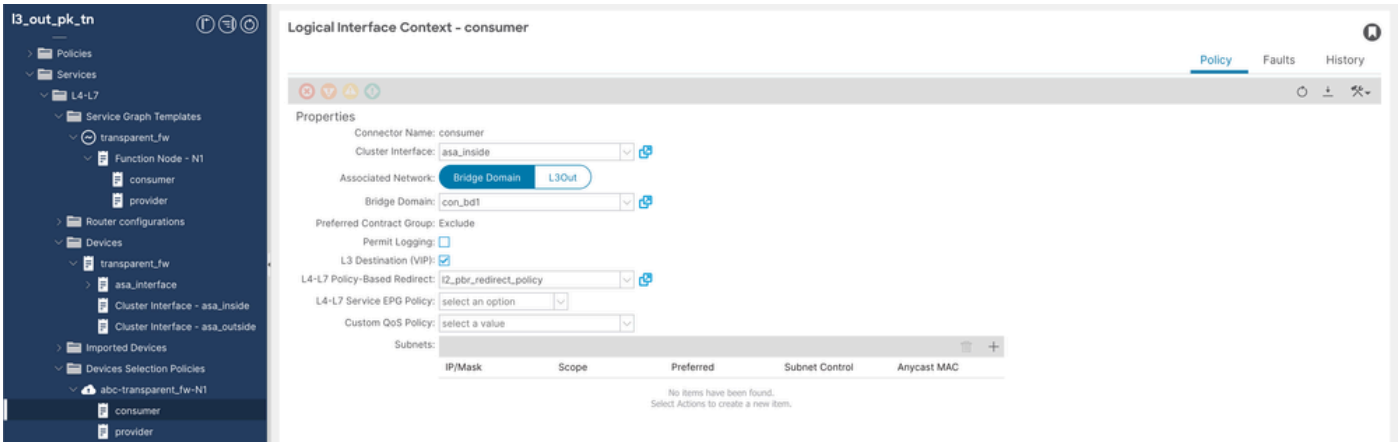
Passaggio 7. Configurare i criteri di selezione dei dispositivi.

Passare a Tenant > Servizi > Criterio di selezione del dispositivo, quindi fare clic con il pulsante destro del mouse e creare il criterio di selezione del dispositivo.



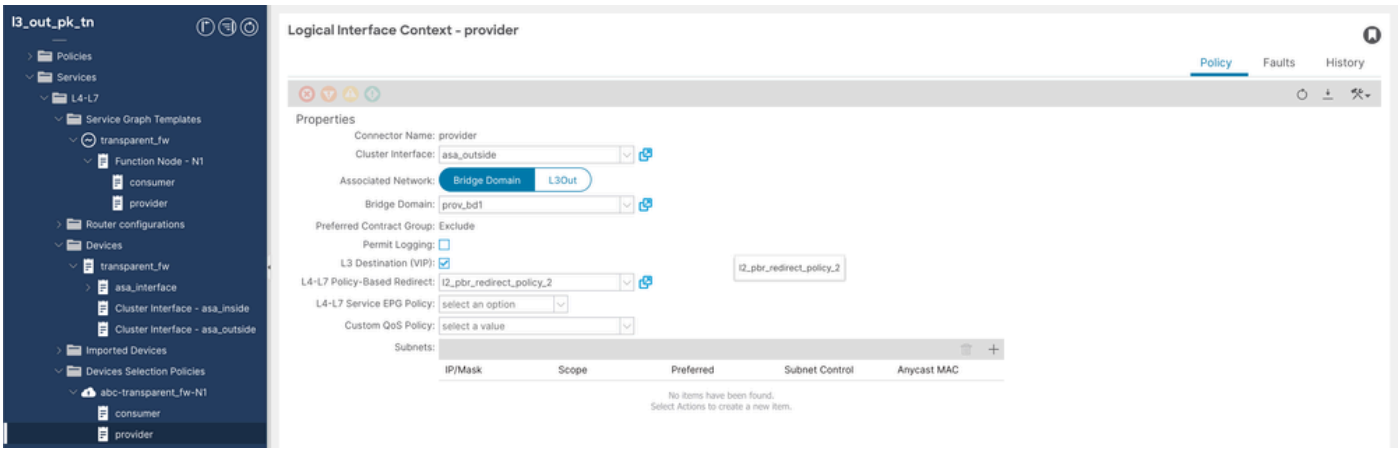
Configurazione 2 di Service Graph

Contesto interfaccia logica consumer ++

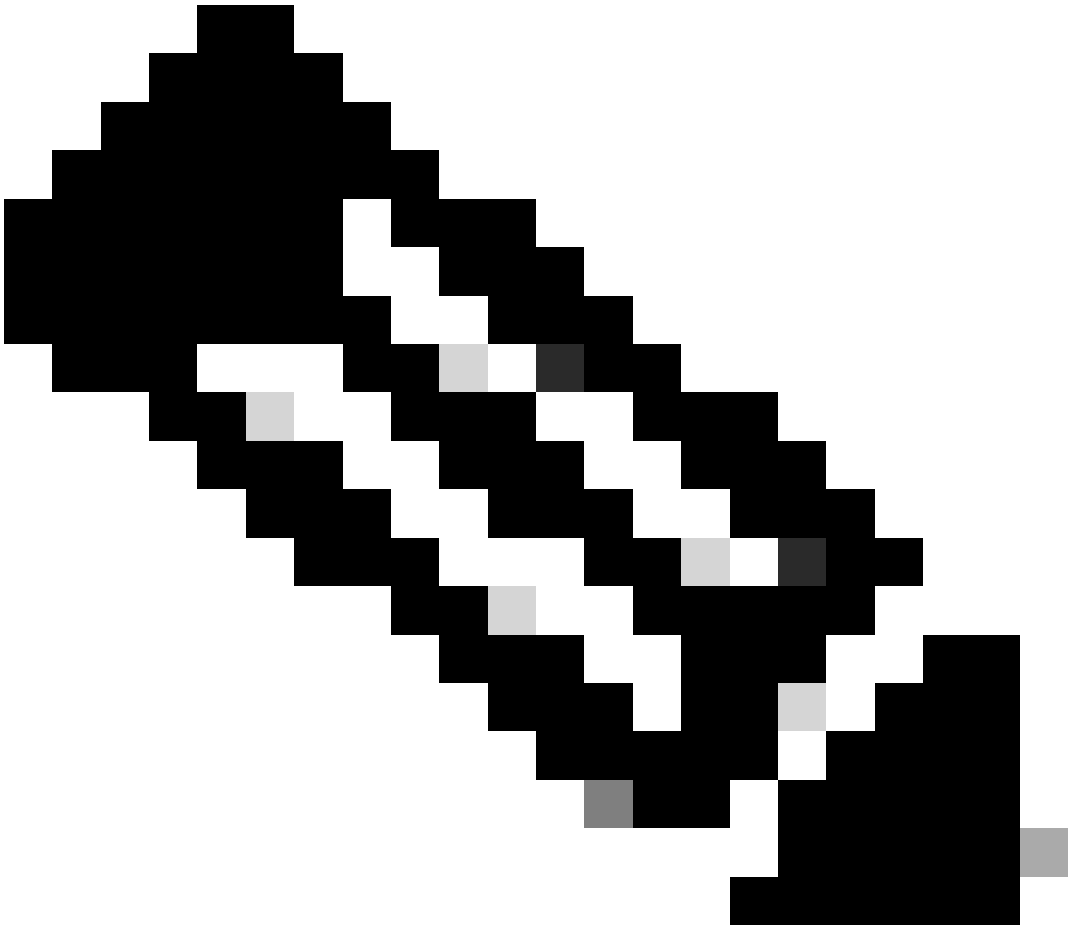


Configurazione consumer criteri di selezione dispositivi

Contesto interfaccia logica provider ++



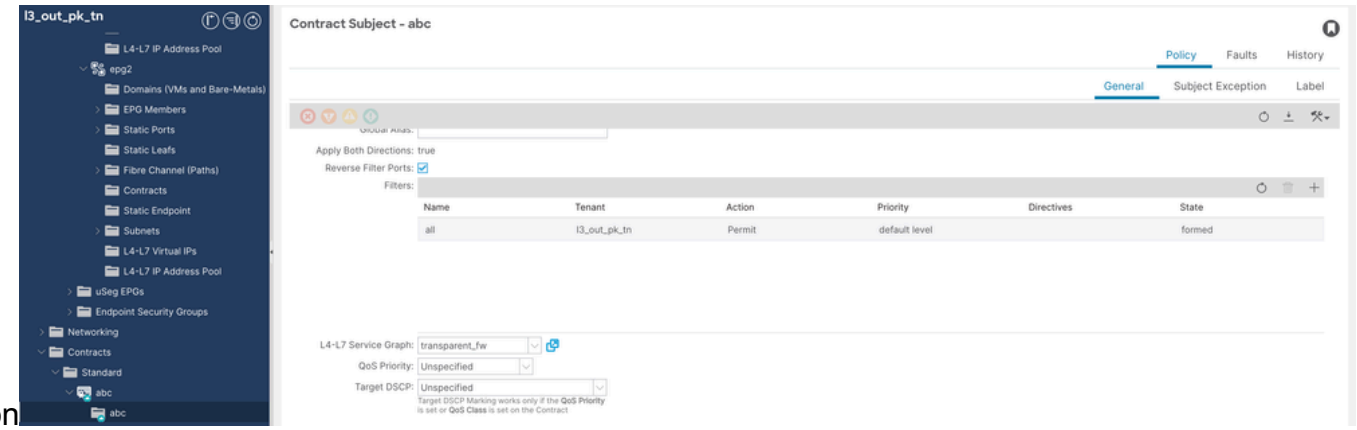
Configurazione provider criteri di selezione dispositivo



Nota: I criteri di selezione dei dispositivi verranno creati automaticamente nel caso in cui si utilizzi l'opzione Applica service graph.

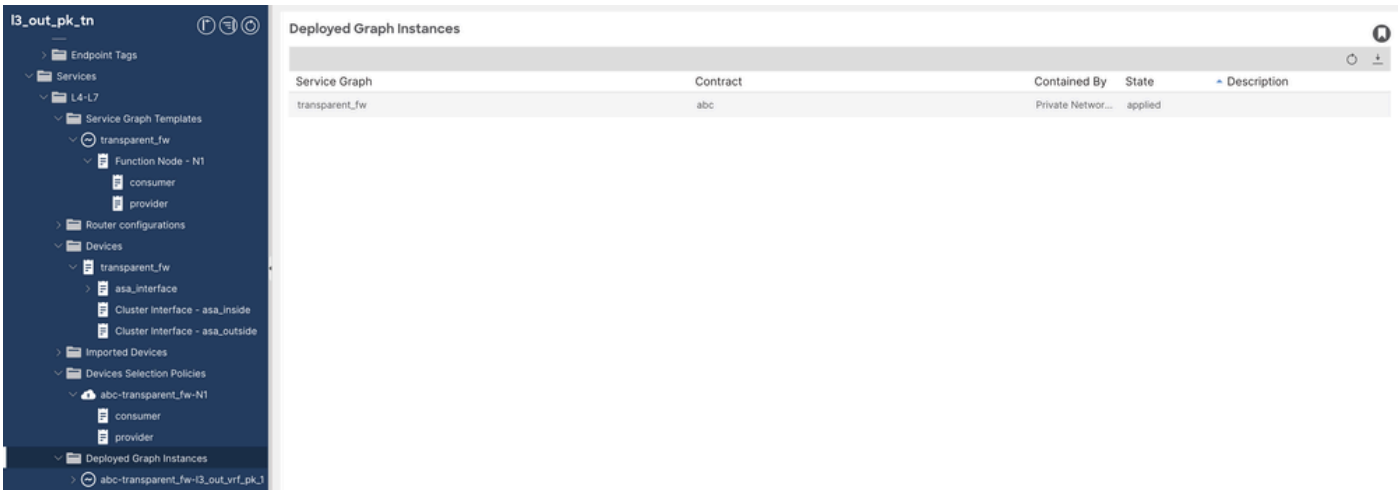
Passaggio 8. Applicare PBR per contrarre l'oggetto abc.

Passare a Tenant > Contratto > Oggetto contratto > Grafico servizio L4-L7 > transparent_fw.



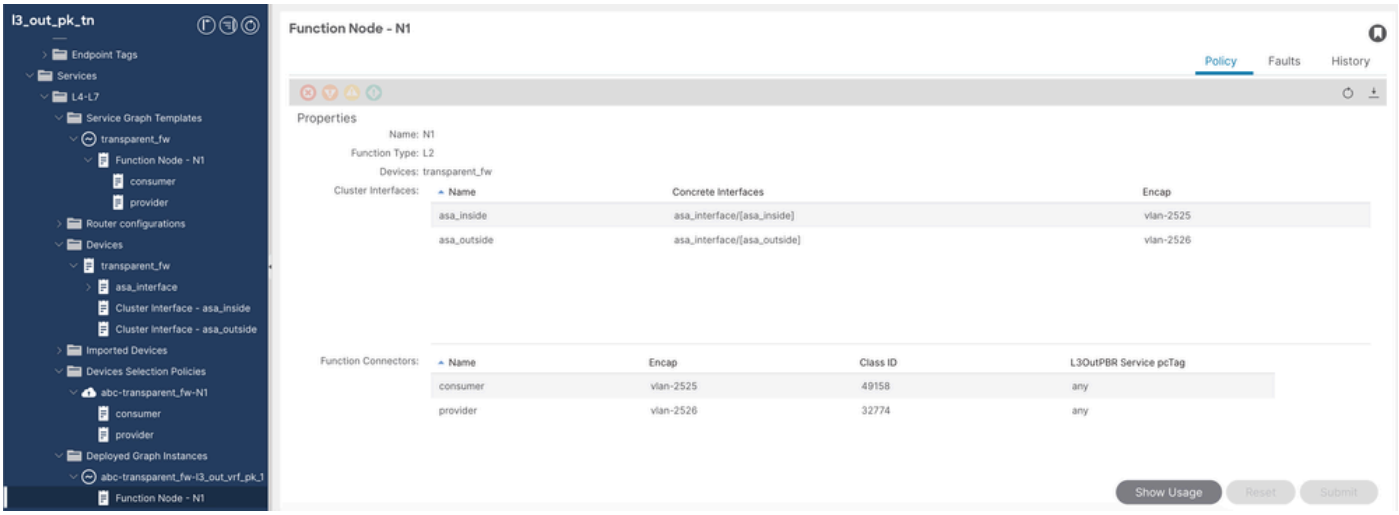
Configurazione contratto

Passaggio 9. Se la distribuzione è riuscita, eseguire la convalida nel grafico Istanza distribuita (cercare lo stato).



Convalida grafico servizi

++ Convalidare le interfacce cluster, le VLAN di incapsulamento e gli ID delle classi dei connettori di funzione.



Convalida grafico servizi 2

Convalida del traffico L2 PBR sull'appliance ASA

SSH (Secure Shell) tra l'endpoint Src e l'endpoint DST è visibile nella voce della tabella Conn sull'appliance ASA.

Convalida ASA

Verifica PBR L2 su foglia

1. Programmazione VLAN sul nodo foglia 102.

<#root>

```
PBR vlan 2525 and 2526 will get programmed on leaf node 102 and mac addresses will be statically tied t

bgl-aci07-apic100#

fabric 102 show endpoint


----------------------------------------------------------------
Node 102 (bgl-aci07-leaf2)
----------------------------------------------------------------
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-rl D - bounce-to-proxy
E - shared-service   m - svc-mgr
+----------------------------------+---------------+-----------------+--------------+-------------+
      VLAN/                           Encap           MAC Address       MAC Info/       Interface
      Domain                          VLAN            IP Address        IP Info
+----------------------------------+---------------+-----------------+--------------+-------------+
28/l3_out_pk_tn:l3_out_vrf_pk_1          vlan-2525    024a.e954.b591 LS                    eth1/14
1/l3_out_pk_tn:l3_out_vrf_pk_1           vlan-2526    02c0.282b.d1cf LS                    eth1/14
```

2. Reindirizzare la politica e la regola di zoning sul nodo consumer (101) e provider (104).

<#root>

```
++ Redirect policy on consumer node

bgl-aci07-apic100#

fabric 101 show service redir info


----------------------------------------------------------------
Node 101 (bgl-aci07-leaf1)
----------------------------------------------------------------
================================================================================================================
```

```
LEGEND
TL: Threshold(Low)  |  TH: Threshold(High) |  HP: HashProfile  |  HG: HealthGrp  | BAC: Backup-Dest |
================================================================================================================
List of Dest Groups
GrpID Name            destination                                                    HG-name
===== ====            ===========                                                    ==============
7     destgrp-7       dest-[3d49:a399:3d4b:4ea1:8829:5991:b554:e94a]-[vxlan-2228224] l3_out_pk_tn::HG1
8     destgrp-8       dest-[143a:41d1:9c75:4973:8501:bcf:d12b:28c0]-[vxlan-2228224]  l3_out_pk_tn::HG2

List of destinations
Name                                                          bdVnid          vMac                vrf
====                                                          ======          ====                ===
dest-[3d49:a399:3d4b:4ea1:8829:5991:b554:e94a]-[vxlan-2228224] vxlan-16744328  02:4A:E9:54:B5:91    l3_
dest-[143a:41d1:9c75:4973:8501:bcf:d12b:28c0]-[vxlan-2228224]  vxlan-16056296  02:C0:28:2B:D1:CF    l3_

List of Health Groups
HG-Name                                  HG-OperSt  HG-Dest
=======                                  =========  =======
l3_out_pk_tn::HG1                        enabled    dest-[3d49:a399:3d4b:4ea1:8829:5991:b554:e94a]-[v
l3_out_pk_tn::HG2                        enabled    dest-[143a:41d1:9c75:4973:8501:bcf:d12b:28c0]-[vx

List of Backup Destinations
Name                                                          primaryDestName
====                                                          ==============
List of AclRules
AclRuleVnid     DestGroup       OperSt   OperStQual
===========     =========       ======   ==========

++ Zoning rule on consumer Node

bgl-aci07-apic1OO#
```

`fabric 101 show zoning-rule  | grep redir`

```
|   4228  | 32771  | 49157  | default  |     bi-dir     | enabled | 2228224  |
|   4231  | 49157  | 32771  | default  | uni-dir-ignore | enabled | 2228224  |
|   4230  | 32771  |   15   | default  |    uni-dir     | enabled | 2228224  |
|   4229  | 16386  | 32771  | default  |    uni-dir     | enabled | 2228224  |
```

<#root>

```
++ Redirect Policy on Provider Node
bgl-aci07-apic1OO#
```

`fabric 104 show service redir info`

```
------------------------------------------------------------
Node 104 (bgl-aci07-leaf4)
------------------------------------------------------------
================================================================================================================
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-[3d49:a399:3d4b:4ea1:8829:5991:b554:e94a]-[vxlan-2228224] l3_out_pk_tn::HG1
4     destgrp-4       dest-[143a:41d1:9c75:4973:8501:bcf:d12b:28c0]-[vxlan-2228224]  l3_out_pk_tn::HG2
```

```
List of destinations
Name                                                                bdVnid          vMac                vrf
====                                                                ======          ====                ===
dest-[3d49:a399:3d4b:4ea1:8829:5991:b554:e94a]-[vxlan-2228224] vxlan-16744328  02:4A:E9:54:B5:91    l3_
dest-[143a:41d1:9c75:4973:8501:bcf:d12b:28c0]-[vxlan-2228224]  vxlan-16056296  02:C0:28:2B:D1:CF    l3_

List of Health Groups
HG-Name                                 HG-OperSt  HG-Dest
=======                                 =========  =======
l3_out_pk_tn::HG1                       enabled    dest-[3d49:a399:3d4b:4ea1:8829:5991:b554:e94a]-[v
l3_out_pk_tn::HG2                       enabled    dest-[143a:41d1:9c75:4973:8501:bcf:d12b:28c0]-[vx
List of Backup Destinations
Name                                                    primaryDestName
====                                                    ===============

++ Zoning rule on provider node
bgl-aci07-apic100#
```

fabric 104 show zoning-rule | grep redir

```
|   4220  | 32771  | 49157  | default  |     bi-dir     | enabled | 2228224  |
|   4221  | 49157  | 32771  | default  | uni-dir-ignore | enabled | 2228224  |
```

Errori rilevati in caso di errore di L2Ping

In caso di guasto dei ping L2P su un dispositivo PBR, si osserverà che il PBR è ancora in stato distribuito e che i guasti F4203, F2833 e F2911 generati dichiarano inattivo il gruppo di integrità/traccia.

Acquisizione Di Ping L2

È possibile acquisire i ping L2P utilizzando tcpdump sull'interfaccia utente per verificare che vengano inviati e ricevuti correttamente. Se solo la trasmissione della CPU è stata inviata e non è stata ricevuta, si prevedono gli errori sopra menzionati e si dovranno risolvere altri problemi dell'appliance ASA per comprenderne la causa (consultare la sezione sulla configurazione dell'appliance ASA).

<#root>

```
Capturing L2Pings using tcpdump on PBR Node 102

bgl-aci07-leaf2#
```

tcpdump -i tahoe0 -w /data/techsupport/l2_pbr1.pcap

```
tcpdump: listening on tahoe0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C4858 packets captured
4875 packets received by filter
0 packets dropped by kernel
```

In order to deocde the tcpdump

cat /data/techsupport/l2_pbr1.pcap | knet_parser.py --decode tahoe --pcap | less

** Search for mac 00ab.8752.3100

++ CPU transmit packets
Frame 505
Time: 2024-10-29T05:55:28.707136+00:00
Header: ieth

CPU Transmit

sup_tx:1, ttl_bypass:0, opcode:0x0, bd:0x207, outer_bd:0x0, dl:0, span:0, traceroute:0, tclass:5
src_idx:0x0, src_chip:0x0, src_port:0x0, src_is_tunnel:0, src_is_peer:0
dst_idx:0x0, dst_chip:0x0, dst_port:0x0, dst_is_tunnel:0
Len: 72
Eth:

00ab.8752.3100 > 024a.e954.b591

, len/

ethertype:0x721

Frame 506
Time: 2024-10-29T05:55:28.707297+00:00
Header: ieth CPU Transmit
sup_tx:1, ttl_bypass:0, opcode:0x0, bd:0x208, outer_bd:0x0, dl:0, span:0, traceroute:0, tclass:5
src_idx:0x0, src_chip:0x0, src_port:0x0, src_is_tunnel:0, src_is_peer:0
dst_idx:0x0, dst_chip:0x0, dst_port:0x0, dst_is_tunnel:0
Len: 72
Eth:

00ab.8752.3100 > 02c0.282b.d1cf

, len/

ethertype:0x721

++CPU recived packets

Frame 509
Time: 2024-10-10T20:16:37.580855+00:00
Header: ieth_extn

CPU Receive

sup_qnum:0x33, sup_code:0x4d, istack:

ISTACK_SUP_CODE_PBR_TRACK_REFRESH

(0x4d)
Header: ieth
sup_tx:0, ttl_bypass:0, opcode:0x0, bd:0x209, outer_bd:0x2, dl:0, span:0, traceroute:0, tclass:0
src_idx:0x32, src_chip:0x0, src_port:0x6, src_is_tunnel:0, src_is_peer:0
dst_idx:0x1, dst_chip:0x0, dst_port:0x3d, dst_is_tunnel:0
Len: 76
Eth:

00ab.8752.3100 > 024a.e954.b591

, len/ethertype:0x8100(802.1q)
802.1q:

vlan:2526

, cos:0, len/

ethertype:0x721

Frame 510
Time: 2024-10-10T20:16:37.580891+00:00
Header: ieth_extn

CPU Receive

sup_qnum:0x33, sup_code:0x4d, istack:

ISTACK_SUP_CODE_PBR_TRACK_REFRESH(0x4d)

Header: ieth
sup_tx:0, ttl_bypass:0, opcode:0x0, bd:0x20a, outer_bd:0x2, dl:0, span:0, traceroute:0, tclass:0
src_idx:0x32, src_chip:0x0, src_port:0x6, src_is_tunnel:0, src_is_peer:0
dst_idx:0x1, dst_chip:0x0, dst_port:0x3d, dst_is_tunnel:0
Len: 76
Eth:

00ab.8752.3100 > 02c0.282b.d1cf

, len/ethertype:0x8100(802.1q)
802.1q:

vlan:2525

, cos:0, len/

ethertype:0x721

Flusso Di Traffico Da Src All'Endpoint Dst

<#root>

++ Endpoint X.1.1.10 want to send traffic to X.1.2.15
++ If destination is not learned on consumer/source leaf, PBR will be performed on destination leaf
++ For this case we are assuming endpoint X.1.2.15 is learned on Leaf 101 so PBR/Redirection will be pe

bgl-aci07-apic100#

fabric 101 show endpoint

Node 101 (bgl-aci07-leaf1)

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-rl D - bounce-to-proxy
E - shared-service   m - svc-mgr
+----------------------------------+--------------+-----------------+-------------+-------------+
      VLAN/                          Encap          MAC Address       MAC Info/       Interface
      Domain                         VLAN           IP Address        IP Info
+----------------------------------+--------------+-----------------+-------------+-------------+
l3_out_pk_tn:l3_out_vrf_pk_1                            X.1.2.15                      tunnel6 ===> |
17                                   vlan-3516    10b3.d514.3516 L                    eth1/5 ===>
l3_out_pk_tn:l3_out_vrf_pk_1         vlan-3516        X.1.1.10 L                     eth1/5

++ EPM entry to get the PC TAG
bgl-aci07-apic100#
```

fabric 101 show system internal epm endpoint ip X.1.1.10

```
------------------------------------------------------------------
Node 101 (bgl-aci07-leaf1)
------------------------------------------------------------------
MAC : 10b3.d514.3516 ::: Num IPs : 1
IP# 0 : X.1.1.10 ::: IP# 0 flags :  ::: l3-sw-hit: No
Vlan id : 17 ::: Vlan vnid : 11792 ::: VRF name : l3_out_pk_tn:l3_out_vrf_pk_1
BD vnid : 16744307 ::: VRF vnid : 2228224
Phy If : 0x1a004000 ::: Tunnel If : 0
Interface : Ethernet1/5
Flags : 0x80005c04 ::: sclass :
```

32771

```
 ::: Ref count : 5 ==> sclass
EP Create Timestamp : 10/11/2024 09:15:44.430334
EP Update Timestamp : 10/29/2024 10:45:35.458416
EP Flags : local|IP|MAC|host-tracked|sclass|timer|

bgl-aci07-apic100#
```

fabric 101 show system internal epm endpoint ip X.1.2.15

```
------------------------------------------------------------------
Node 101 (bgl-aci07-leaf1)
------------------------------------------------------------------
MAC : 0000.0000.0000 ::: Num IPs : 1
IP# 0 : X.1.2.15 ::: IP# 0 flags :  ::: l3-sw-hit: No
Vlan id : 0 ::: Vlan vnid : 0 ::: VRF name : l3_out_pk_tn:l3_out_vrf_pk_1
BD vnid : 0 ::: VRF vnid : 2228224
Phy If : 0 ::: Tunnel If : 0x18010006
Interface : Tunnel6
Flags : 0x80004400 ::: sclass :
```

49157

```
 ::: Ref count : 3 ==> sclass
EP Create Timestamp : 10/29/2024 10:38:34.949150
EP Update Timestamp : 10/29/2024 10:45:55.571786
EP Flags : IP|sclass|timer|

++ Traffic will be redirected based on redir(destgrp-7)
bgl-aci07-apic100#
```

fabric 101 show zoning-rule src-epg 32771 dst-epg 49157

```
------------------------------------------------------------------
Node 101 (bgl-aci07-leaf1)
```

```
------------------------------------------------------------
+---------+--------+--------+----------+--------+---------+---------+------+------------------+--------
| Rule ID | SrcEPG | DstEPG | FilterID |  Dir   |  operSt |  Scope  | Name |      Action      |    Prio
+---------+--------+--------+----------+--------+---------+---------+------+------------------+--------
|   4228  | 32771  | 49157  | default  | bi-dir | enabled | 2228224 |      | redir(destgrp-7) | src_dst_
+---------+--------+--------+----------+--------+---------+---------+------+------------------+--------

++ Based on redirect policy traffic will be redirected to mac
```

02:4A:E9:54:B5:91

```
bgl-aci07-apic100#
```

fabric 101 show service redir info

```
------------------------------------------------------------
Node 101 (bgl-aci07-leaf1)
------------------------------------------------------------
================================================================================================================
LEGEND
TL: Threshold(Low)  |  TH: Threshold(High) |  HP: HashProfile  |  HG: HealthGrp  | BAC: Backup-Dest |  T
================================================================================================================
List of Dest Groups
GrpID Name            destination                                                 HG-name
===== ====            ===========                                                 ==============
7     destgrp-7       dest-[3d49:a399:3d4b:4ea1:8829:5991:b554:e94a]-[vxlan-2228224] l3_out_pk_tn::HG1
List of destinations
Name                                                        bdVnid          vMac                vrf
====                                                        ======          ====                ===
dest-[3d49:a399:3d4b:4ea1:8829:5991:b554:e94a]-[vxlan-2228224] vxlan-16744328
```

02:4A:E9:54:B5:91

```
    l3_out_pk_tn:l3_out_vrf_pk_1 enabled    no-oper-dest    l3_out_pk_tn::HG
1

++ PBR mac addresses are never learnt remotely as IP/MAC learning is disabled for PBR BD
++ PBR mac addresses are statically binded to interfaces where L4/L7 device is connected and reported t
++ Traffic will be forwarded to SPINE PROXY
++ Spine has an COOP entry for 02:4A:E9:54:B5:91

bgl-aci07-apic100#
```

fabric 201 show coop internal info repo ep key 16744328 02:4A:E9:54:B5:91

```
------------------------------------------------------------
Node 201 (bgl-aci07-spine1)
------------------------------------------------------------
Repo Hdr Checksum : 49503
Repo Hdr record timestamp : 10 29 2024 10:15:07 658496921
Repo Hdr last pub timestamp : 10 29 2024 10:15:07 661679296
Repo Hdr last dampen timestamp : 01 01 1970 00:00:00 0
Repo Hdr dampen penalty : 0
Repo Hdr flags : IN_OBJ ACTIVE
EP bd vnid : 16744328
EP mac :
```

02:4A:E9:54:B5:91

```
 <<<<========== ASA MAC
flags : 0x480
repo flags : 0x102
```

```
Vrf vnid : 2228224
PcTag : 0x100c006
EVPN Seq no : 0
Remote publish timestamp: 01 01 1970 00:00:00 0
Snapshot timestamp: 10 29 2024 10:15:07 658496921
Tunnel nh : 10.0.144.66
MAC Tunnel  : 10.0.144.66
IPv4 Tunnel : 10.0.144.66
IPv6 Tunnel : 10.0.144.66
ETEP Tunnel : 0.0.0.0
num of active ipv4 addresses : 0
num of anycast ipv4 addresses : 0
num of ipv4 addresses : 0
num of active ipv6 addresses : 0
num of anycast ipv6 addresses : 0
num of ipv6 addresses : 0
Primary Path:
Current published TEP :
```

10.0.144.66

```
Backup Path:
BackupTunnel nh : 0.0.0.0
Current Backup (publisher_id): 0.0.0.0
Anycast_flags : 0
Current citizen (publisher_id): 10.0.144.66
Previous citizen : 10.0.144.66
Prev to Previous citizen : 10.0.144.66
Synthetic Flags : 0x5
Synthetic Vrf : 411
Synthetic IP : X.X.83.223
Tunnel EP entry: 0x7f20900167a8
Backup Tunnel EP entry: (nil)
TX Status: COOP_TX_DONE\
Damp penalty: 0
Damp status: NORMAL
Exp status: 0
Exp timestamp: 01 01 1970 00:00:00 0
Hash: 3209430840 owner: 10.0.144.65

++ Spine will forward this to PBR Leaf Node 102 based on COOP entry
++ PBR Leaf Node will forward this to ASA FW on interface E1/14
++ ASA FW will forward the traffic based on mac address table and send it back to PBR Leaf Node 102
++ PBR Leaf Node will look for Dst IP in the traffic and route it to Leaf 104 if remote endpoint entry
++ Leaf 104 will get this traffic forwarded to actual EP X.1.2.15 (Leaf4 does not learn the client IP a
```

Configurazione ASA

Passaggio 1. Configurazione interfaccia.

<#root>

```
ASA(config)#
```

show running-config interface

```
!
interface GigabitEthernet0/0
 bridge-group 1
 nameif inside
 security-level 100
!
interface GigabitEthernet0/1
 bridge-group 1
 nameif outside
 security-level 0
!
interface BVI1
ip address 192.168.100.1 255.255.255.0 ==> In case BVI IP is not defined ASA will not switch the packet
!
```

Passaggio 2. L'apprendimento degli indirizzi MAC deve essere disabilitato.

<#root>

```
ASA(config)#
```

show run mac-learn

```
mac-learn inside disable
mac-learn outside disable
```

PBR:

Passaggio 3. Tabella degli indirizzi MAC statici per PBR Mac.

<#root>

```
The mac statically binded to inside interface is the PBR mac generated by provider and vice versa
ASA(config)#
```

show run mac-address-table

```
mac-address-table static outside 024a.e954.b591
mac-address-table static inside 02c0.282b.d1cf
```

Passaggio 4. Configurare l'Access Control List (ACL) per passare i ping L2L.

<#root>

```
ASA(config)#
```

show access-list

```
access-list L2_PBR ethertype permit 721
```

```
ASA(config)# show run access-group
access-group L2_PBR in interface inside
access-group L2_PBR in interface outside
```

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).