Configurar e verificar a configuração do gráfico de serviço de camada 2 com ASAv

Contents

Introdução

Este documento descreve como configurar e verificar a configuração do gráfico de serviço de camada 2 na Cisco Application Centric Infrastructure (ACI).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Compreensão de como o gráfico de serviço de camada 3 funciona na ACI
- Compreensão de como configurar o grupo de políticas de endpoint, domínios de ponte e contrato na ACI
- Compreensão de como configurar (Adaptive Security Appliance Virtual) ASAv como firewall transparente

Componentes Utilizados

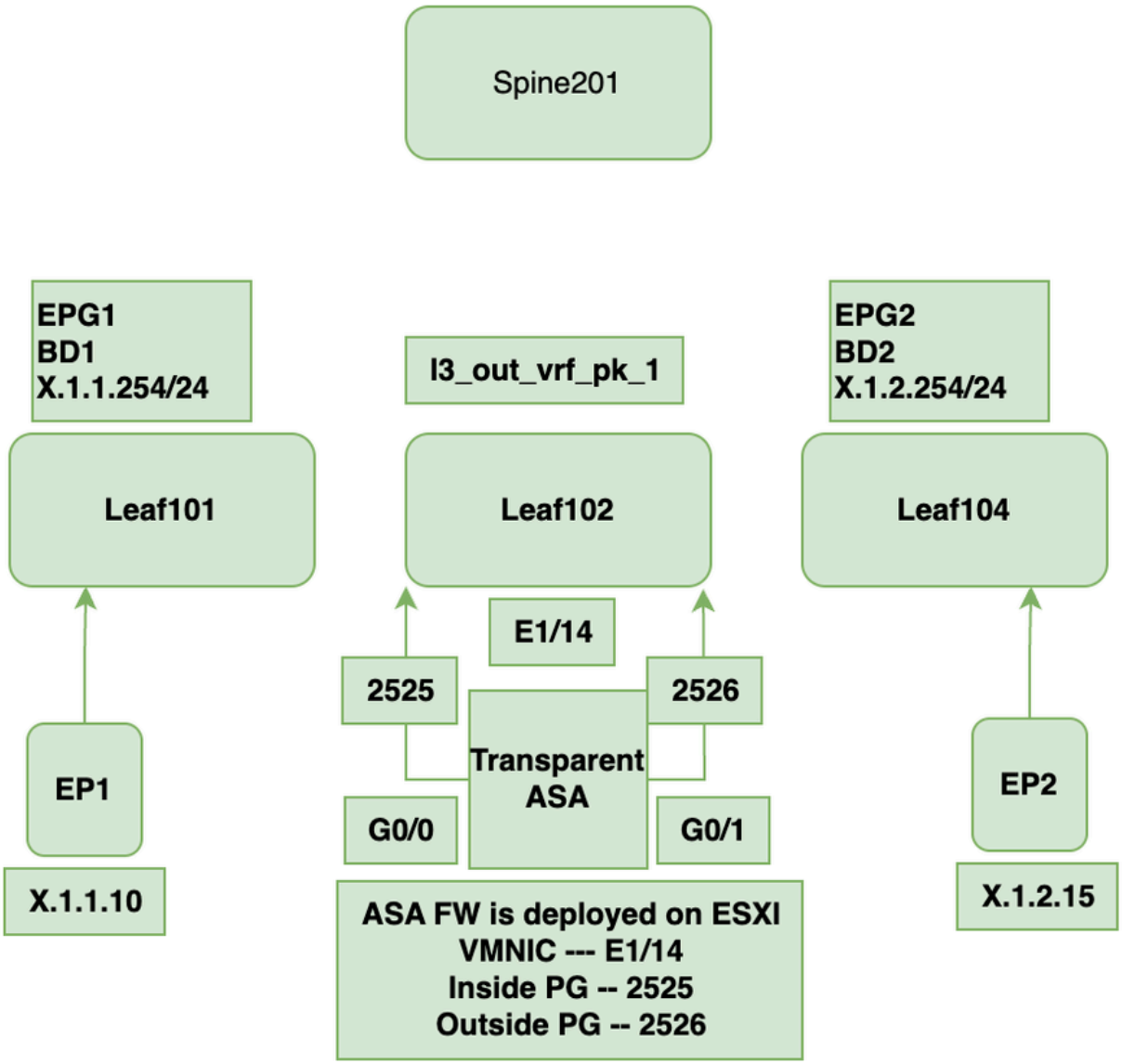
As informações neste documento são baseadas nestas versões de software e hardware:

- Versão do APIC: 6.0 (3g)
- Folha H/W: N9K-C93180YC-FX

- S/W da folha: n9000-16.0 (3g)
- Nó Folha 101, 102, 103
- ASAv implantado no servidor ESXi

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

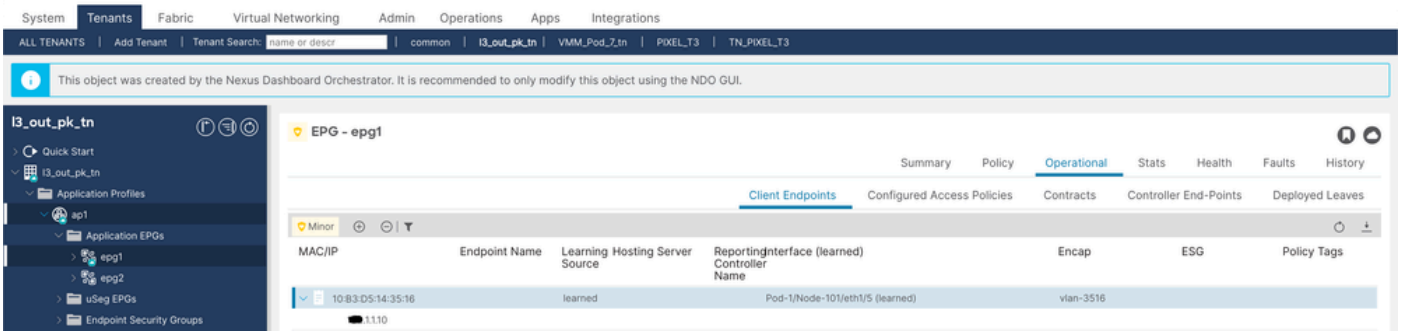
Topologia



Topologia

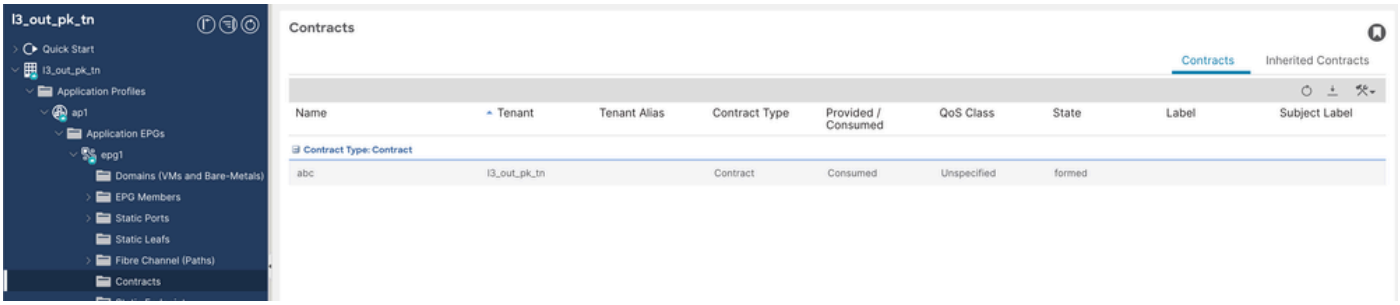
A configuração de EPG1 e EPG2 não é mostrada neste documento, ela deve ser configurada antes de ser usada e o endpoint deve ser aprendido.

1. Validar o ponto final de haș X.1.1.10 do EPG1 aprendido (Nó 101).



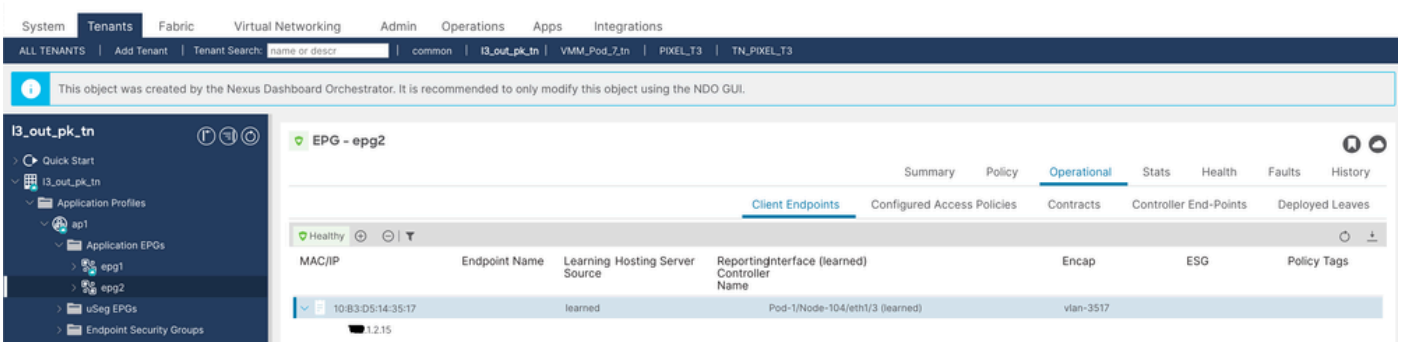
Pontos de Extremidade do Cliente

2. O contrato abc é consumido pelo EPG1.



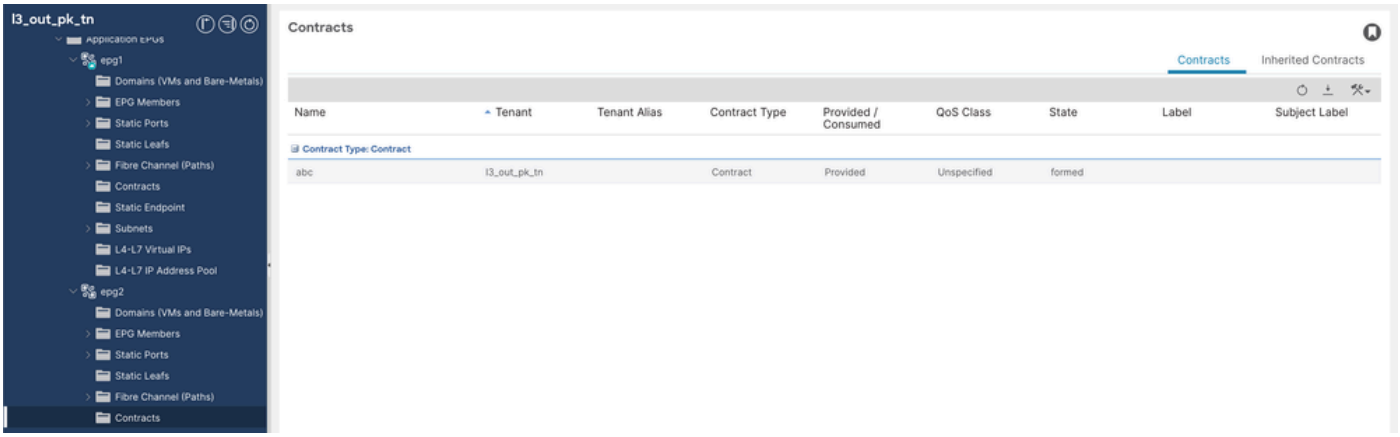
Contrato Consumido

3. Validar que o EPG2 tem o ponto final X.1.2.15aprendido (Nó 104).



Ponto de Extremidade do Cliente

4. O contrato abc é fornecido pelo EPG2.



Por que o gráfico de serviço L2 é necessário na ACI?

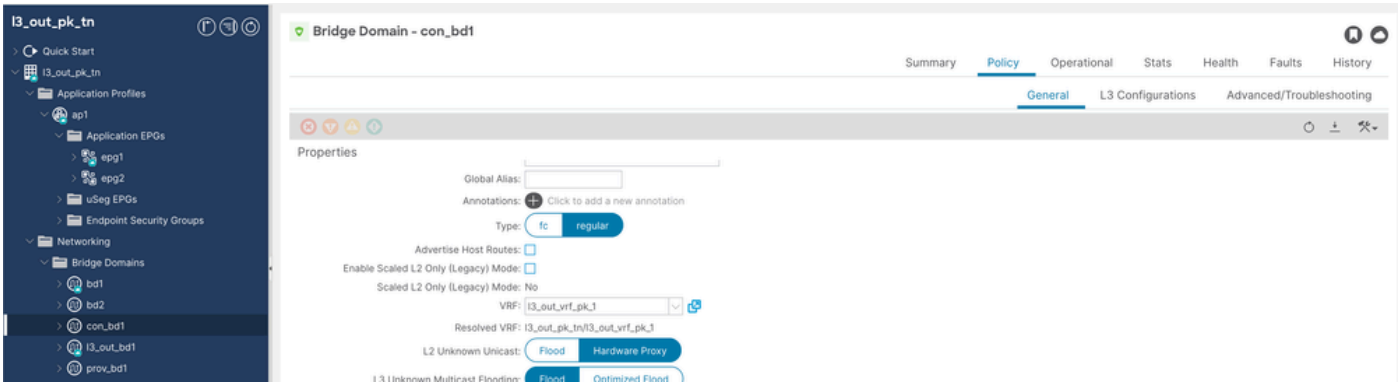
- Na Cisco ACI, os dispositivos de serviço L4-L7 podem ser inseridos na Camada 3 (L3), Camada 2 (L2) ou Camada 1 (L1).
- Inserção de serviço de camada 3: O dispositivo externo (por exemplo, firewall, Sistema de prevenção de intrusão (IPS)) toma decisões de roteamento e encaminha o tráfego com base nos endereços IP.
- Inserção de serviço de camada 2: O tráfego é encaminhado com base nos endereços MAC sem envolvimento de roteamento. Isso é útil para firewalls ou dispositivos IPS transparentes.
- O Roteamento Baseado em Políticas (PBR - Policy-Based Routing) da camada 2 é usado ao inserir um dispositivo de serviço da camada 2, como um IPS ou firewall transparente na ACI.
- O mecanismo de encaminhamento de tráfego permanece o mesmo para PBR L3 e L2.
- A principal diferença:
  - PBR L3: O tráfego é redirecionado para um endereço IP (o dispositivo participa do roteamento).
  - PBR L2: O tráfego é redirecionado para um endereço MAC (o dispositivo opera na Camada 2).
- No L2 PBR, os endereços MAC são vinculados estaticamente às interfaces leaf para garantir o encaminhamento de tráfego adequado.

Para obter mais informações sobre casos de uso de PBR L1/L2 ativo/em standby ou ativo/ativo, consulte o White Paper sobre PBR.

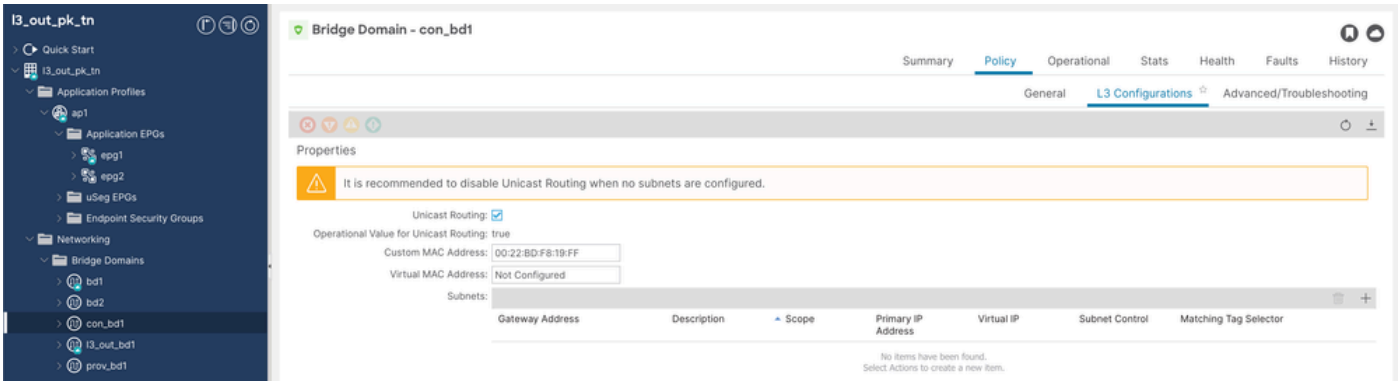
Configuração do gráfico de serviço L2

Etapa 1. Configure o bd de consumidor nomeado como con-bd1.

O roteamento unicast deve ser ativado, o unicast L2 desconhecido deve ser definido como proxy de Hardware e nenhuma sub-rede é necessária para Domínios de Bridge (BDs) con e prov.

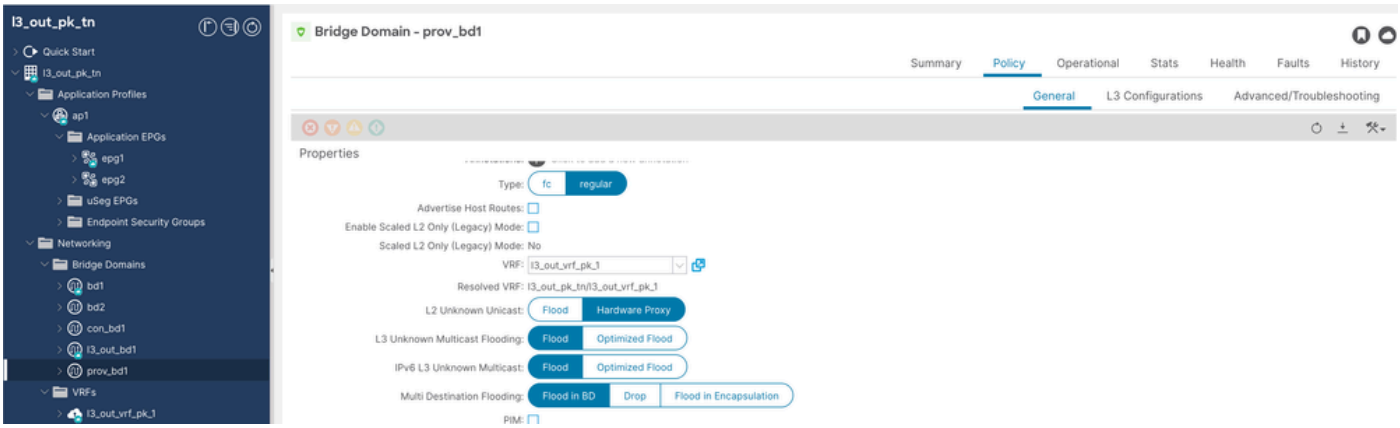


Configuração Cons BD

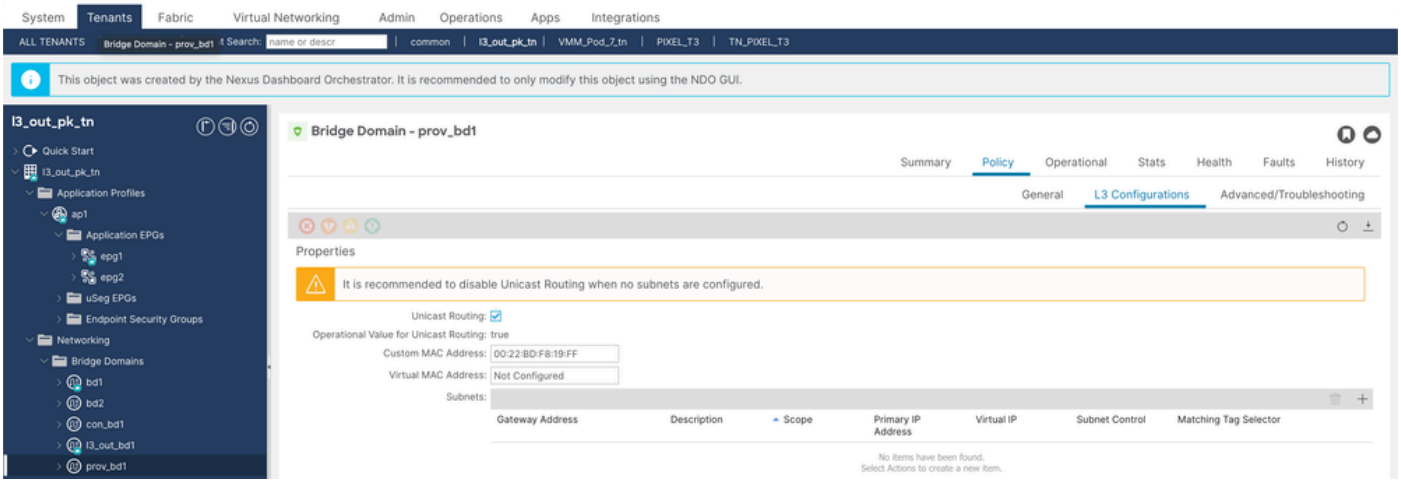


Configuração Cons BD 2

Etapa 2. Configure o bd do provedor nomeado como prov-bd1.



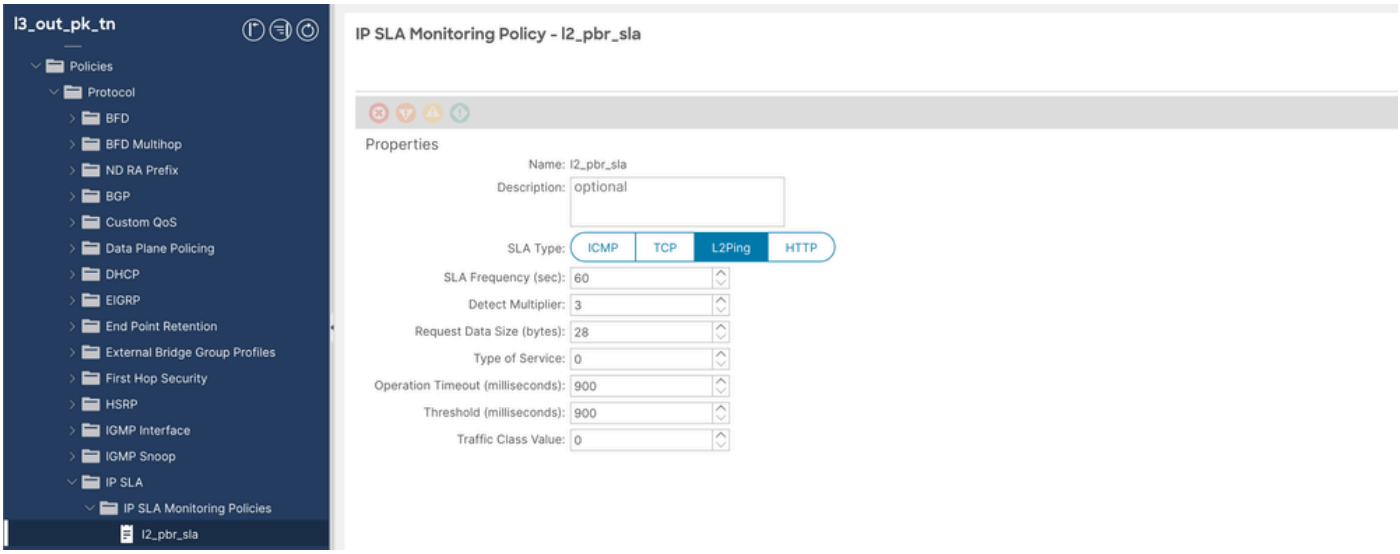
Configuração Prov BD



Prov BD Config 2

Etapa 3. Configurar a política de Contrato de Nível de Serviço (SLA - Service Level Agreement) IP com o tipo de SLA L2Ping.

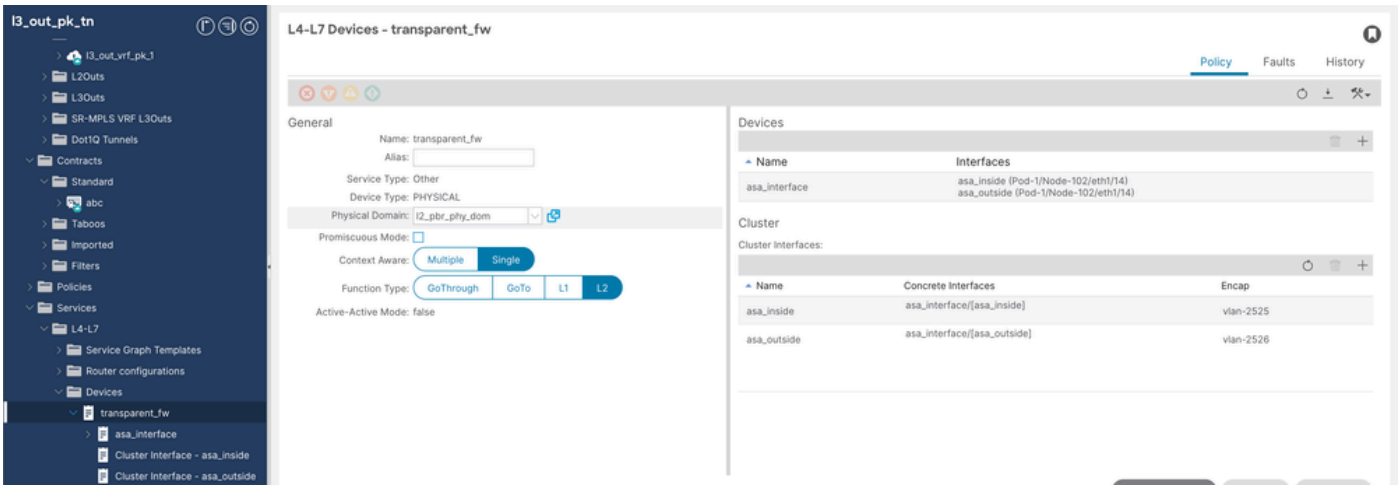
Navegue paraLocatário > Políticas > Protocolo > SLA IP > Políticas de monitoramento de SLA IP, clique com o botão direito do mouse e crie a política.



Política IP SLA

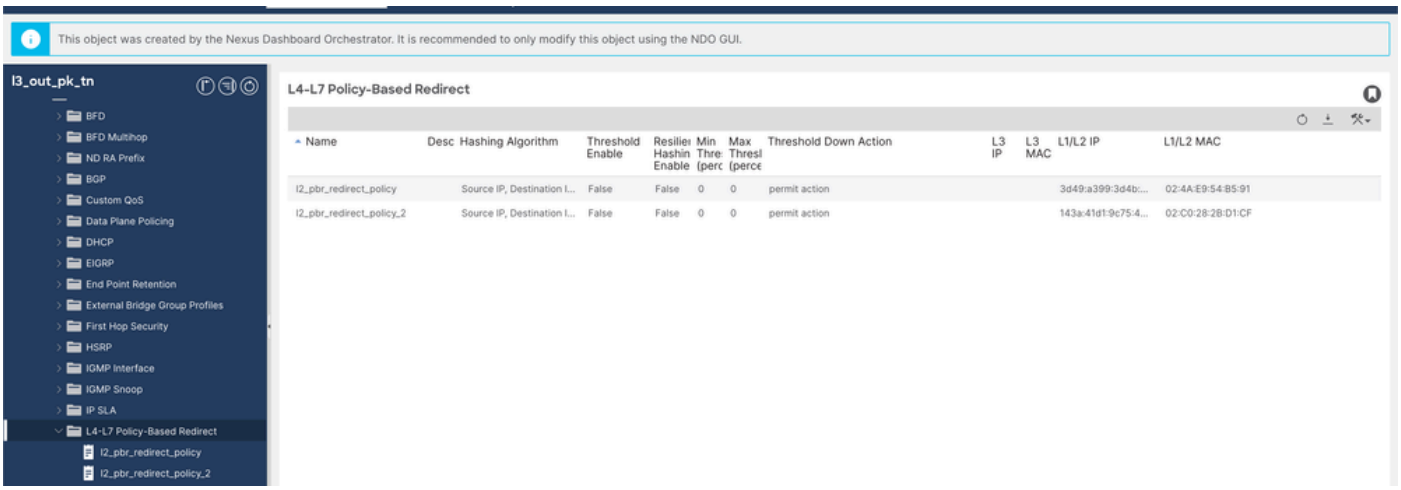
Etapa 4. Configurar o dispositivo L4/L7.

Navegue para Locatário > Serviços > Dispositivos, clique com o botão direito do mouse e crie o dispositivo L4-L7.



Dispositivo L4-L7

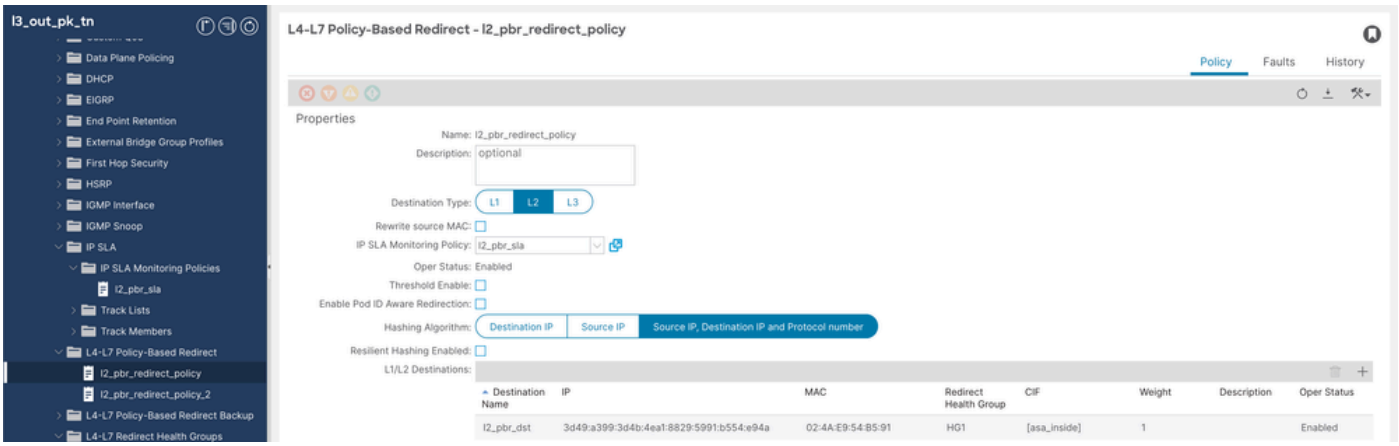
Etapa 5. Validar visão geral do redirecionamento Baseado em Política (você pode verificar isso depois de configurar 5a e 5b).



Política de redirecionamento L4-L7

Etapa 5.1. Configure a política de redirecionamento L4-L7 baseada em política para a interface interna do Adaptive Security Appliance (ASA) (não é necessário especificar MAC ou IP, ele é preenchido pelo próprio APIC).

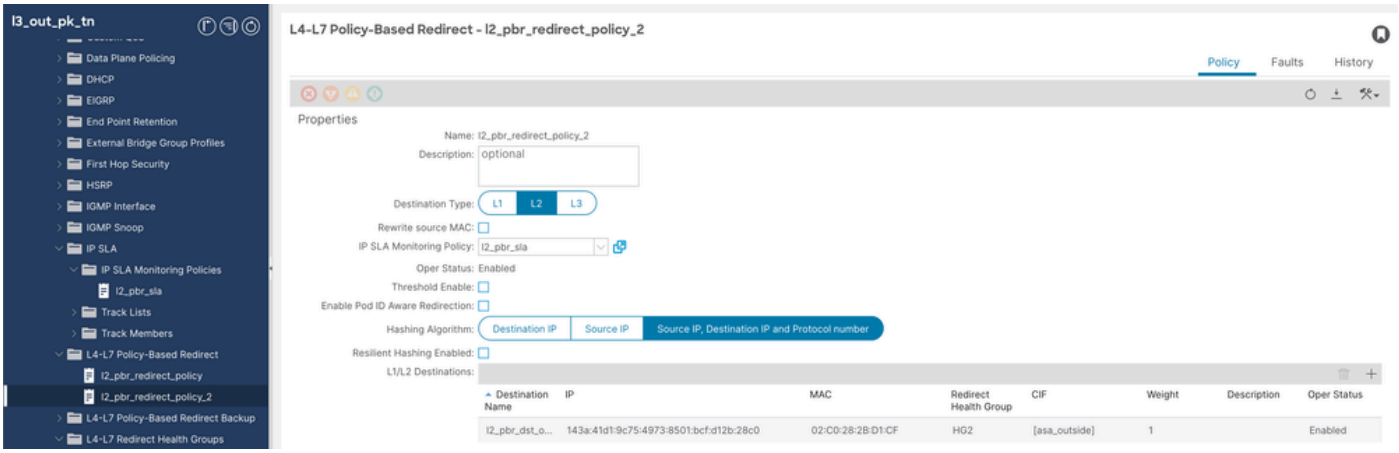
Navegue até Tenant > Policies > Protocol > L4-L7 Policy based redirect e clique com o botão direito do mouse em create policy.



Configuração de política de redirecionamento L4-L7

Etapa 5.2. Configure a política de redirecionamento L4-L7 baseada em política para a interface externa do ASA (não é necessário especificar MAC ou IP, ele é preenchido pelo próprio APIC).

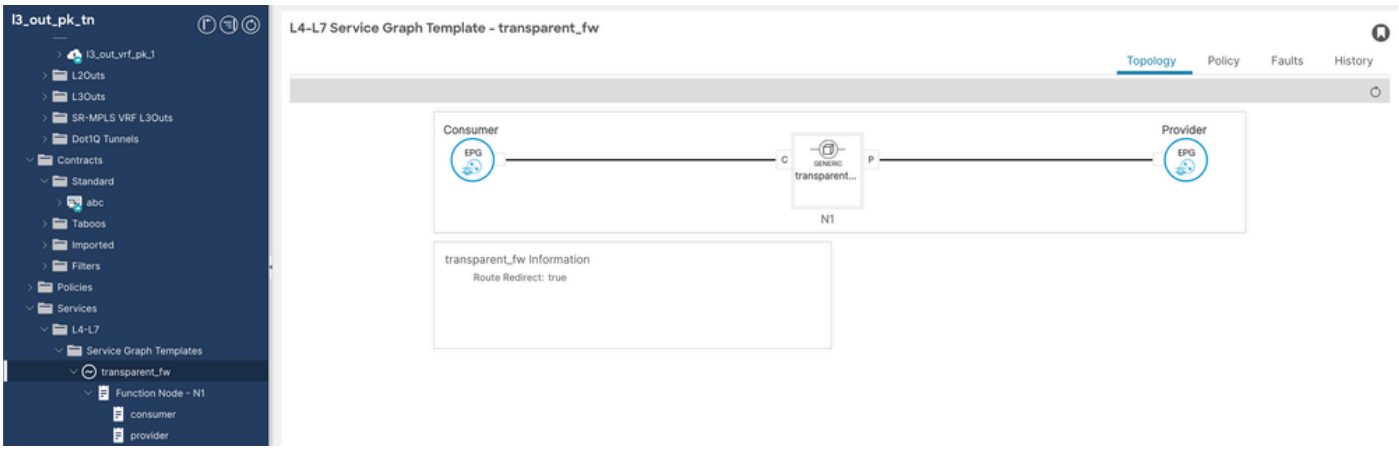
Navegue até Tenant > Policies > Protocol > L4-L7 Policy based redirect e clique com o botão direito do mouse em create policy.



Configuração 2 da política de redirecionamento L4-L7

Etapa 6. Configurar o modelo de gráfico de Serviço.

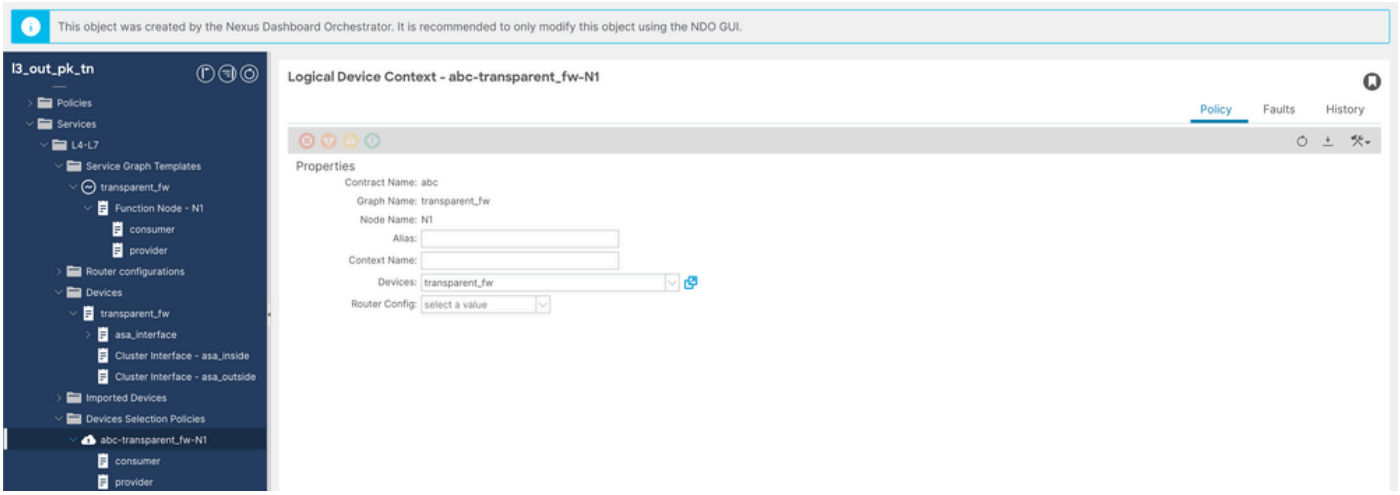
Navegue para Locatário > Serviços > Modelo de gráfico de serviço, clique com o botão direito do mouse e crie o modelo de gráfico de serviço L4-L7.



Configuração do gráfico de serviço

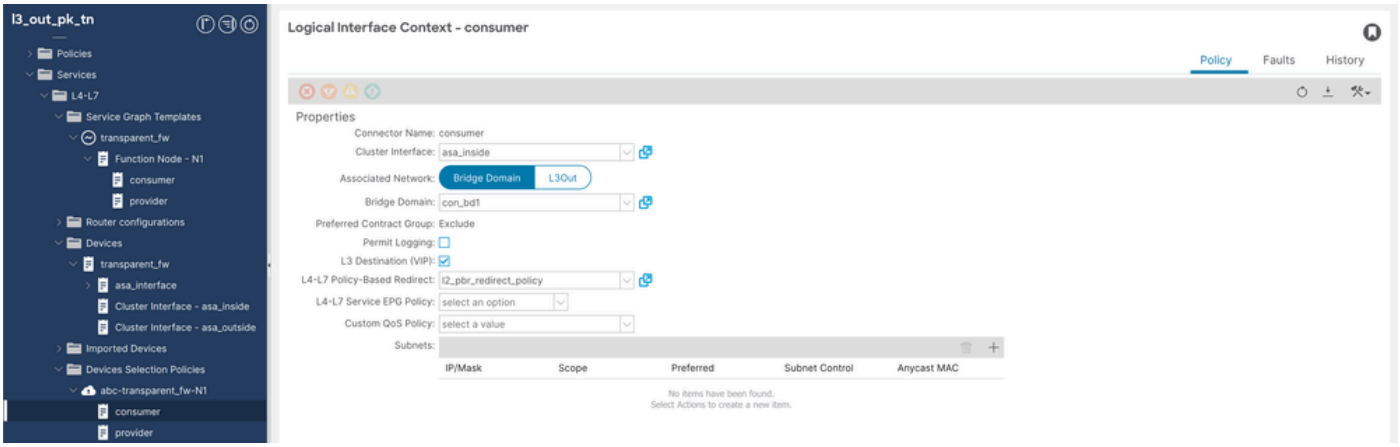
Etapa 7. Configurar a política de seleção de dispositivos.

Navegue para Locatário > Serviços > Política de Seleção de Dispositivo, clique com o botão direito do mouse e crie Política de Seleção de Dispositivo.



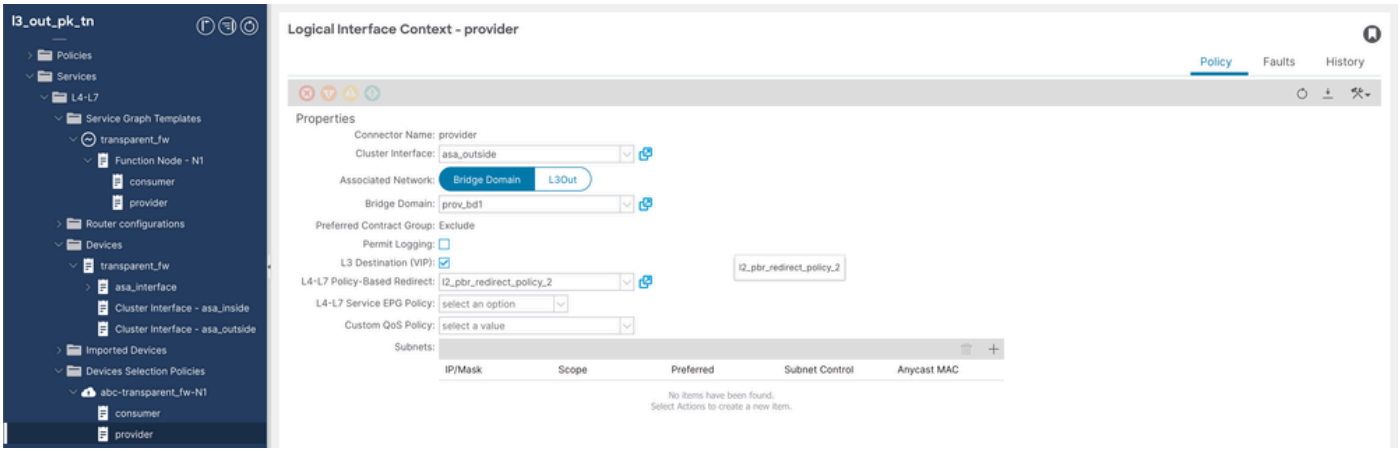
Configuração do gráfico de serviço 2

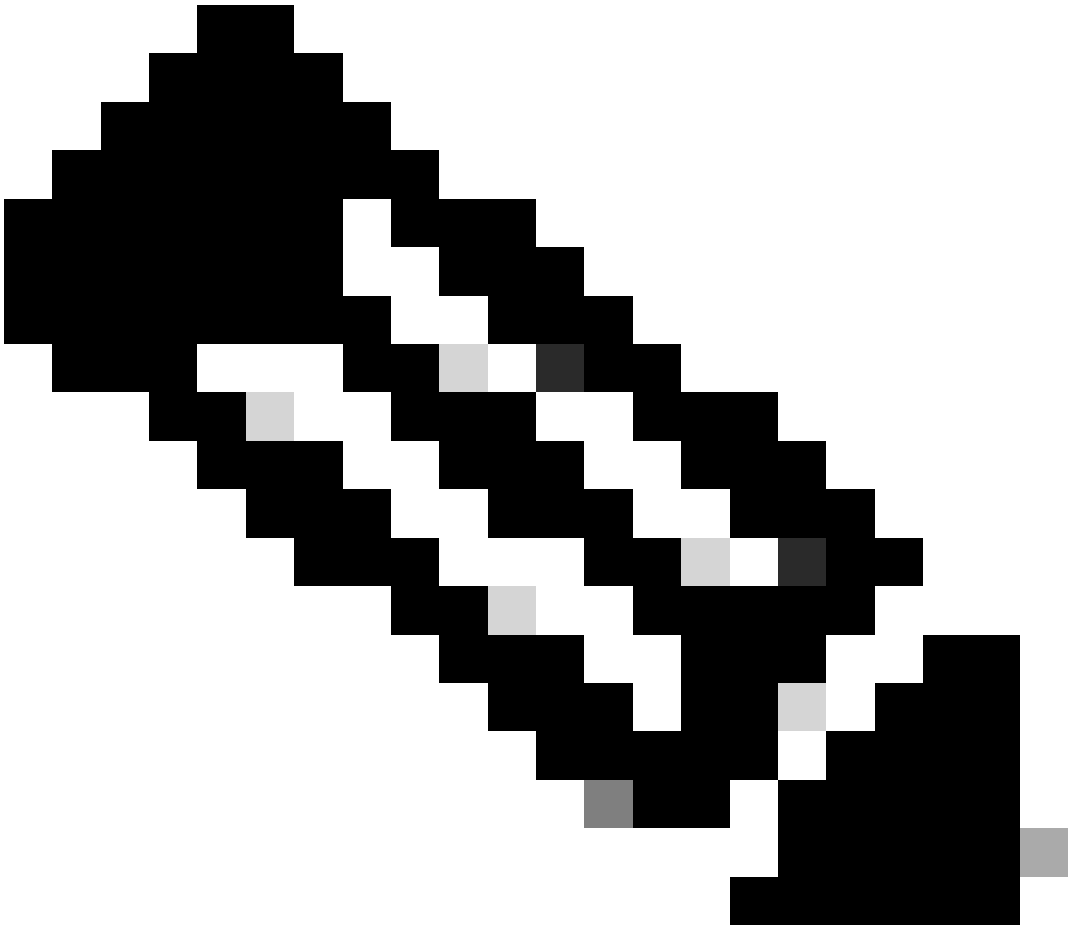
Contexto de Interface Lógica do Consumidor ++



Configuração do Consumidor da Política de Seleção de Dispositivo

Contexto de Interface Lógica do Provedor de ++



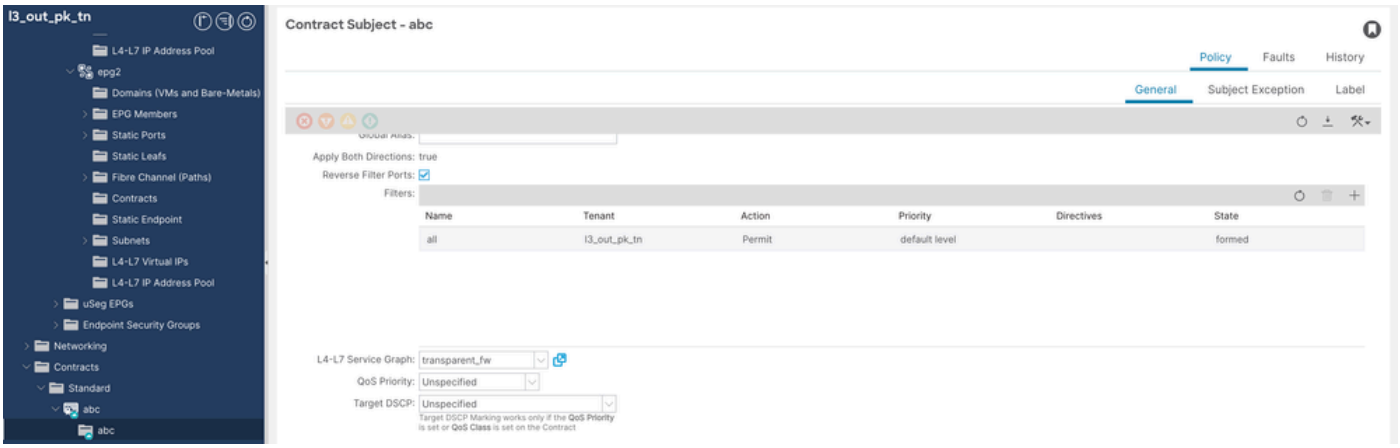


Note: A política de seleção de dispositivos será criada automaticamente caso você use a opção Aplicar gráfico de serviço.

Etapa 8. Aplique o PBR para contratar o sujeito abc.

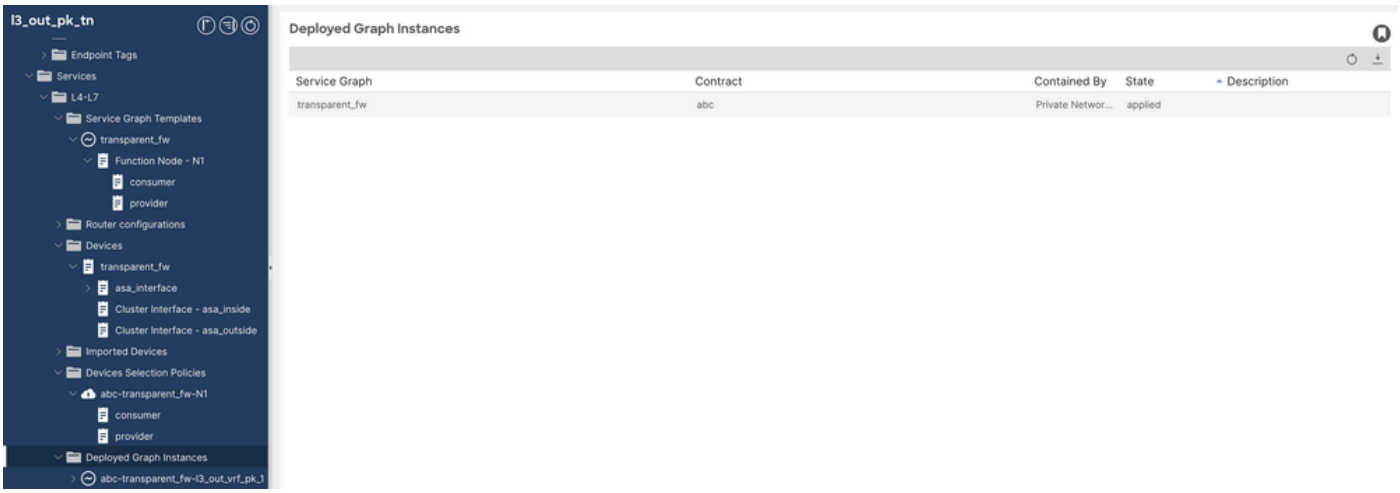
Navegue até Tenant > Contract > Contract Subject > L4-L7 Service Graph > transparent_fw.

Con



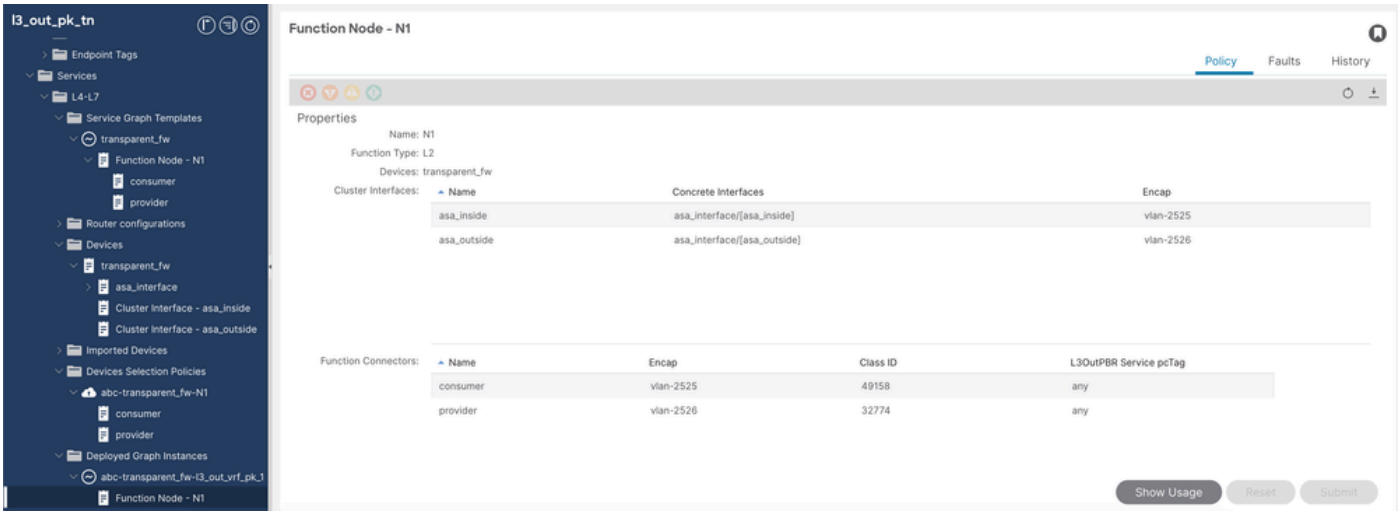
Configuração do contrato

Etapa 9. Se implantado com êxito, valide em Gráfico de instância implantado (procure o estado).



Validação do gráfico de serviço

++ Validar interfaces de cluster, encapsular VLANs e IDs de classe de conector de função.



Validação do gráfico de serviço 2

Validar o tráfego de PBR L2 no ASA

Shell Seguro (SSH) do ponto final de Origem ao ponto final de Destino que você pode ver na entrada da tabela Conn no ASA.

Validação do ASA

Verificar o L2 PBR na folha

1. Programação de VLAN no Nó Folha 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. Política de redirecionamento e regra de zoneamento no nó consumidor (101) e provedor (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-apic100#
```

`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  |
```



```
++ Redirect Policy on Provider Node
bgl-aci07-apic100#
```

`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-apic1oo#
```

fabric 104 show zoning-rule | grep redir

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

Falhas observadas em caso de falha do ping L2

Caso os pings L2 estejam falhando no dispositivo PBR, você observará que o PBR ainda está no estado implantado e as falhas F4203, F2833 e F2911 foram acionadas, informando que o grupo de monitoramento/integridade está inoperante.

Capturando pings L2

Você pode capturar L2Pings usando tcpdump em uma interface para saber se eles foram enviados e recebidos corretamente. Se você vir apenas a transmissão de CPU enviada e não recebida, então as falhas mencionadas anteriormente são esperadas e você deve fazer Troubleshooting adicional no ASA por que elas são descartadas (consulte a seção de configuração do ASA).

<#root>

```
Capturing L2Pings using tcpdump on PBR Node 1O2

bgl-aci07-leaf2#
```

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

```
tcpdump: listening on tahoe0, link-type EN1OMB (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

Fluxo De Tráfego Do Ponto De Extremidade Src Para 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
```

Configuração do ASA

Etapa 1. Configuração da interface.

<#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
!
```

Etapa 2. O aprendizado de MAC deve ser desativado.

<#root>

```
ASA(config)#
```

show run mac-learn

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

PBR:

Etapa 3. Static mac-address-table for 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
```

Etapa 4. Configure a ACL (Access Control List Lista de Controle de Acesso) para passar os pings L2.

<#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
```

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.