Configuration et vérification de la configuration du graphique de services de couche 2 avec ASAv

Table des matières

Introduction

Ce document décrit comment configurer et vérifier la configuration du graphique de services de couche 2 dans l'infrastructure axée sur les applications (ACI) de Cisco.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Compréhension du fonctionnement du graphique des services de couche 3 dans l'ACI
- Compréhension de la configuration du groupe de stratégies de terminaux, des domaines de pont et du contrat dans l'ACI
- Comprendre comment configurer (Adaptive Security Applicance Virtual) ASAv comme pare-feu transparent

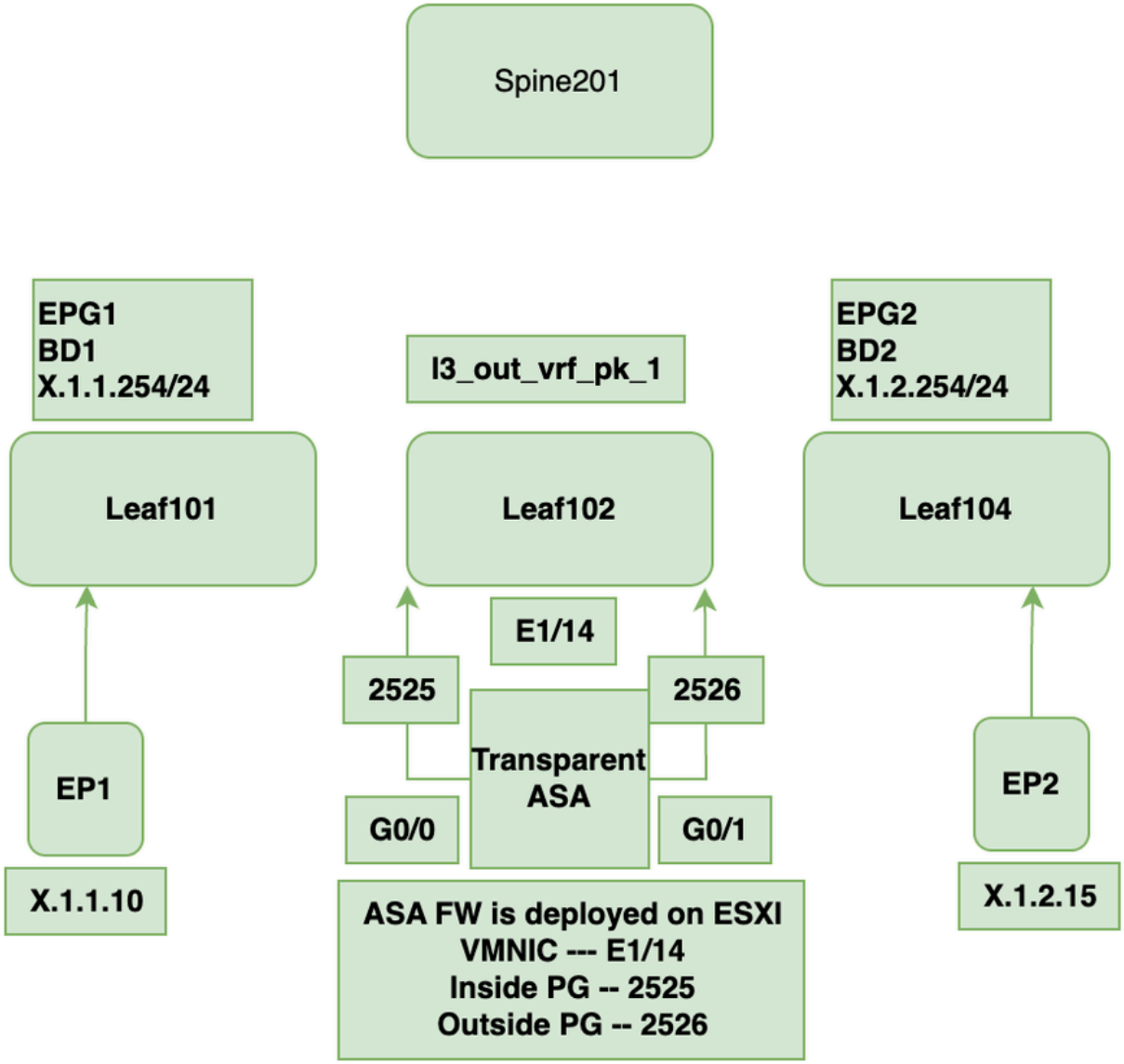
Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version APIC : 6.0 (3g)
- Matériel leaf : N9K-C93180YC-FX
- Logiciel leaf : n9000-16.0 (3g)
- Noeud leaf 101, 102, 103
- ASAv déployé sur le serveur ESXi

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

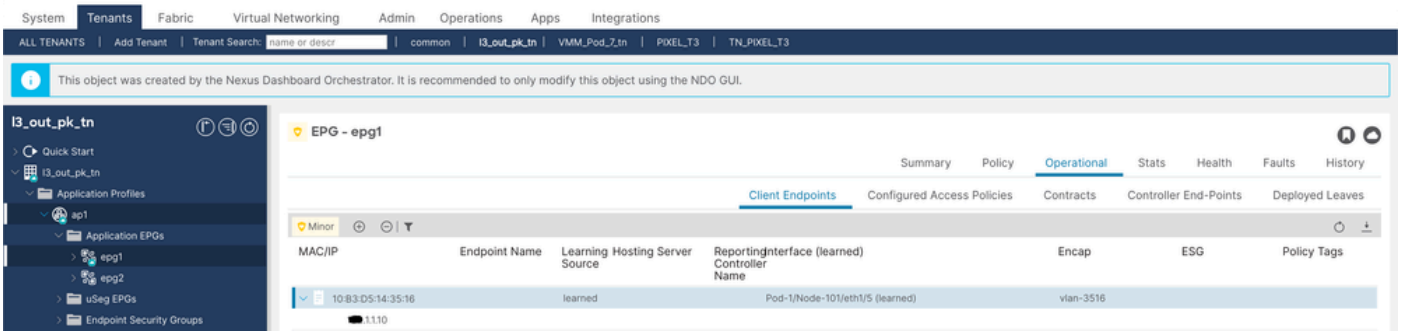
Topologie



Topologie

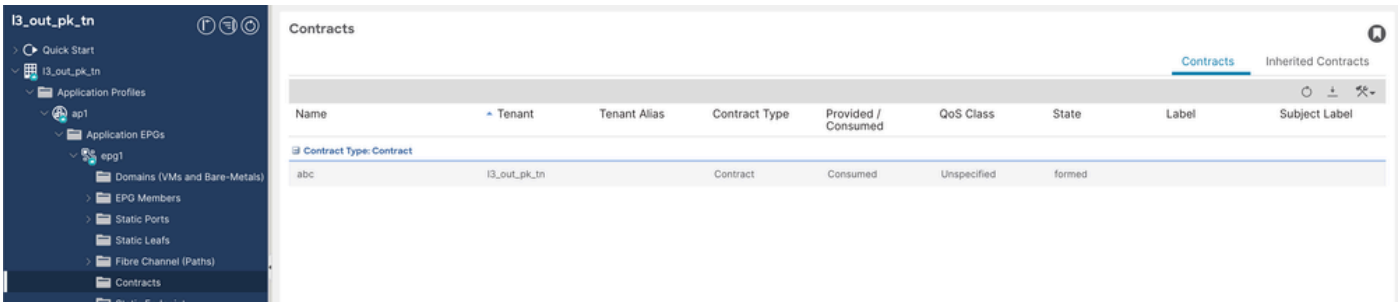
La configuration EPG1 et EPG2 n'est pas présentée dans ce document. Elle doit être configurée avant que la main et le point d'extrémité ne soient appris.

1. Validez le point de terminaison X.1.1.10 haș EPG1 acquis (noeud 101).



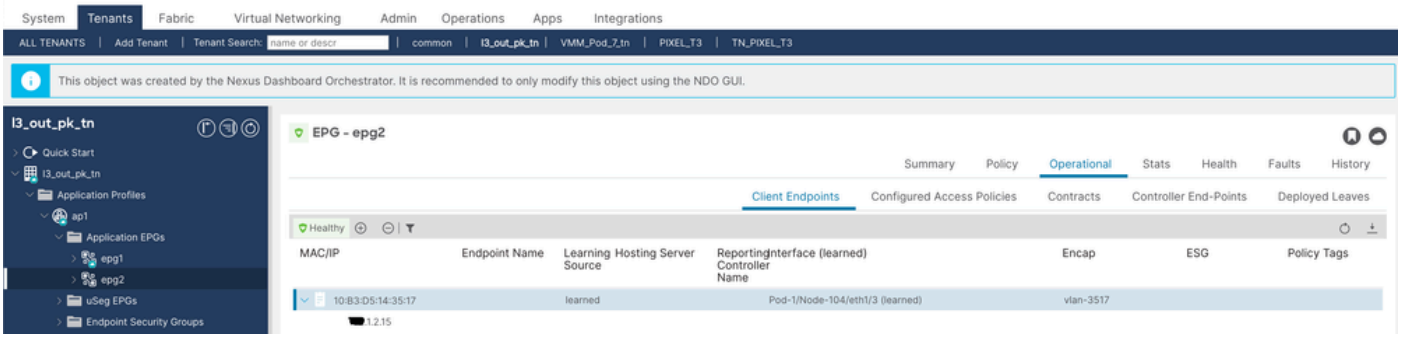
Terminaux clients

2. Le contrat abc est utilisé par EPG1.



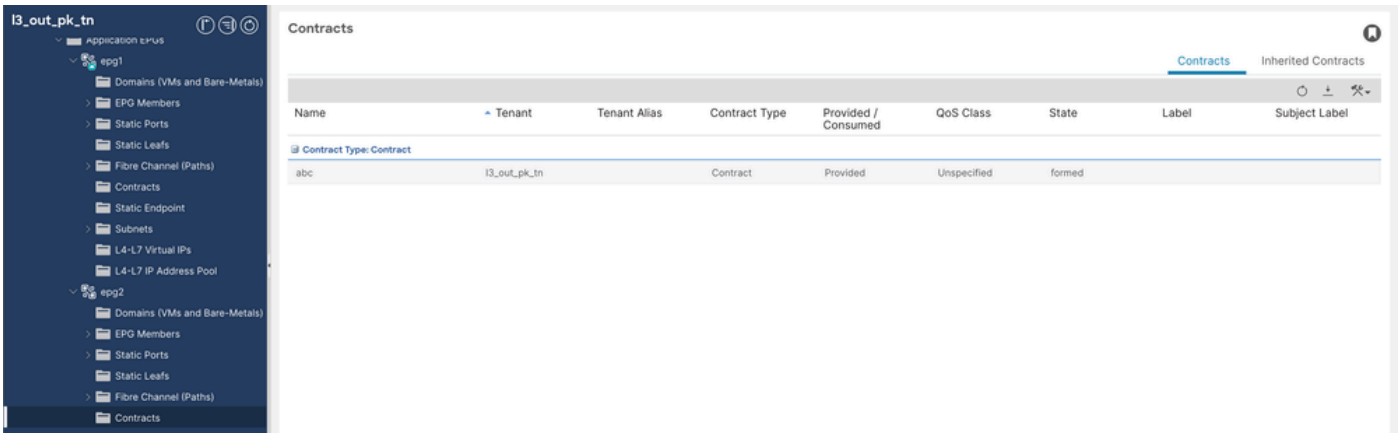
Contrat Consommé

3. Validation du point d’extrémité X.1.2.15 de l’EPG2acquis (noeud 104).



Point de terminaison client

4. Le contrat abc est fourni par EPG2.



Contrat fourni

Pourquoi un graphique des services de couche 2 est-il nécessaire dans l'ACI ?

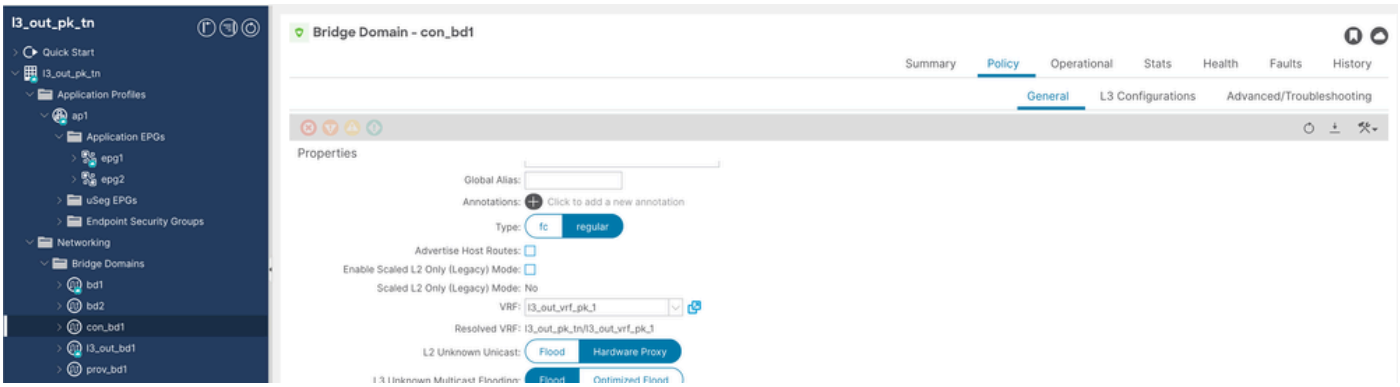
- Dans Cisco ACI, les périphériques de service de couches 4 à 7 peuvent être insérés au niveau de la couche 3 (L3), de la couche 2 (L2) ou de la couche 1 (L1).
- Insertion de service de couche 3 : Le périphérique externe (par exemple, le pare-feu, le système de prévention des intrusions (IPS)) prend les décisions de routage et transfère le trafic en fonction des adresses IP.
- Insertion de service de couche 2 : Le trafic est transféré en fonction des adresses MAC sans implication de routage. Cela est utile pour les pare-feu transparents ou les périphériques IPS.
- Le routage PBR (Policy-Based Routing) de couche 2 est utilisé lors de l'insertion d'un périphérique de service de couche 2, tel qu'un IPS ou un pare-feu transparent dans l'ACI.
- Le mécanisme de transfert de trafic reste le même pour les PBR de couche 3 et de couche 2.
- La différence clé :
    - PBR L3 : Le trafic est redirigé vers une adresse IP (le périphérique participe au routage).
    - PBR L2 : Le trafic est redirigé vers une adresse MAC (le périphérique fonctionne au niveau de la couche 2).
- Dans le PBR de couche 2, les adresses MAC sont liées de manière statique aux interfaces leaf afin de garantir un transfert de trafic approprié.

Pour plus d'informations sur les cas d'utilisation de PBR L1/L2 actif/en veille ou actif/actif, reportez-vous au Livre blanc PBR.

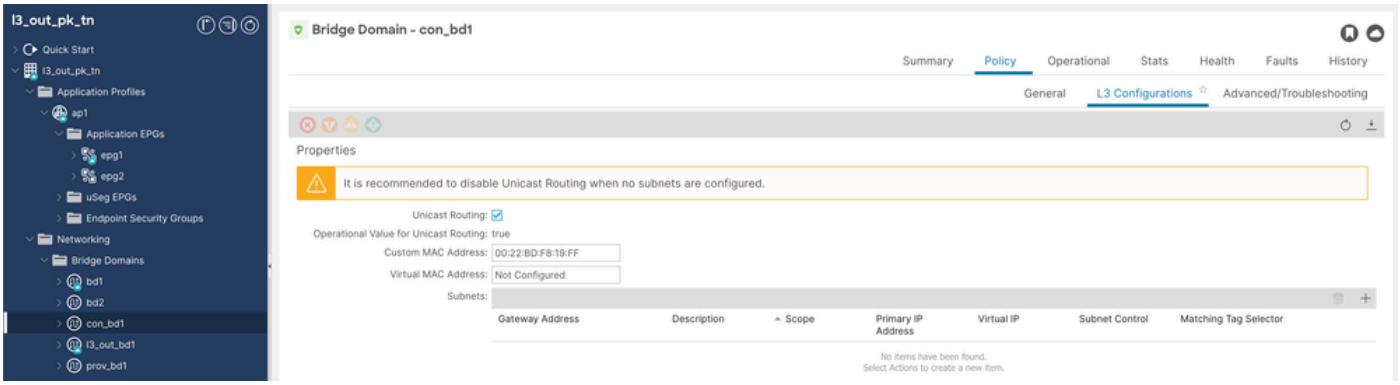
Graphique de configuration du service L2

Étape 1 : configuration de la bd du consommateur nommée con-bd1

Le routage de monodiffusion doit être activé, la monodiffusion inconnue de couche 2 doit être définie sur le proxy matériel et aucun sous-réseau n'est requis pour les domaines de pont (BD) con et prov.

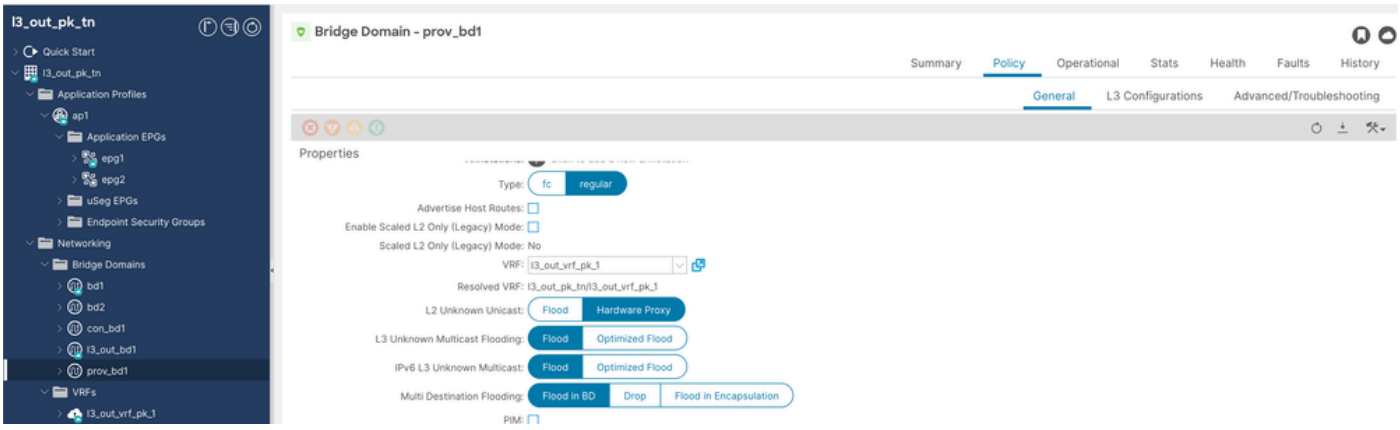


Config. Cons BD

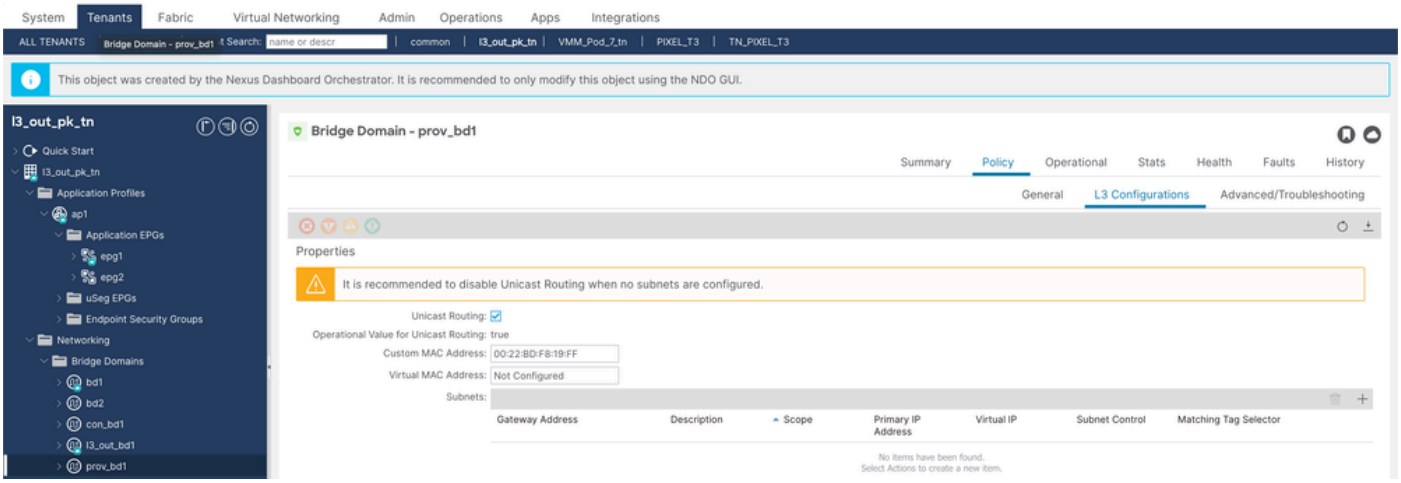


Contre BD Config 2

Étape 2 : configuration du bd du fournisseur sous le nom prov-bd1



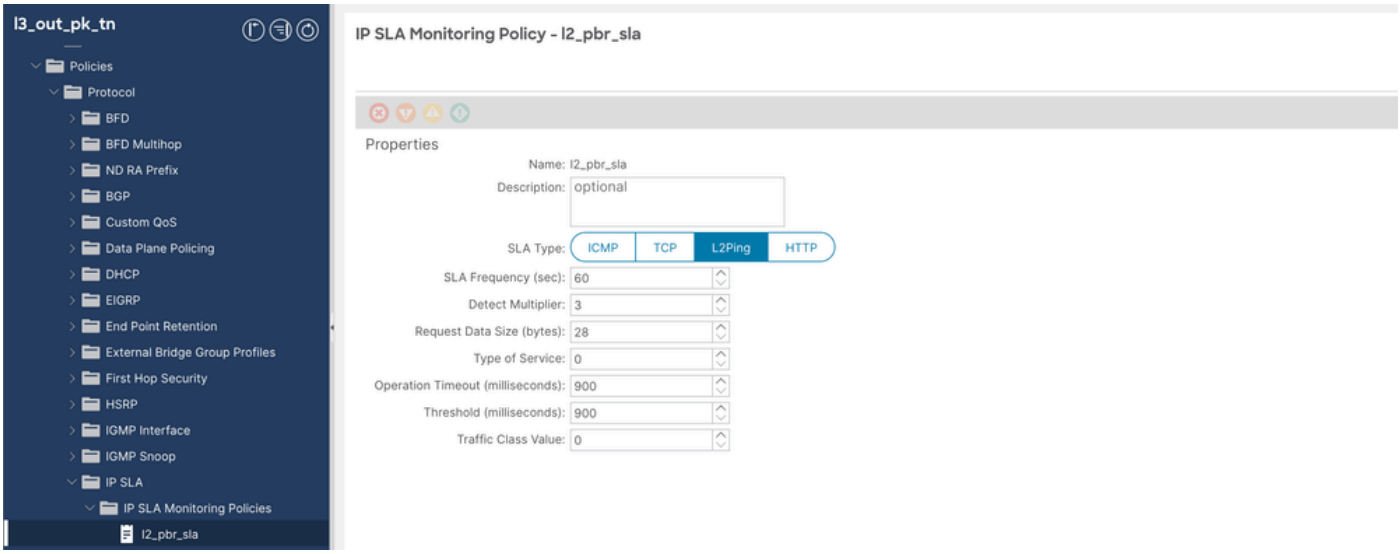
Config BD Prov



Prov BD Config 2

Étape 3 : configuration de la politique d'accord de niveau de service IP avec le type d'accord L2Ping

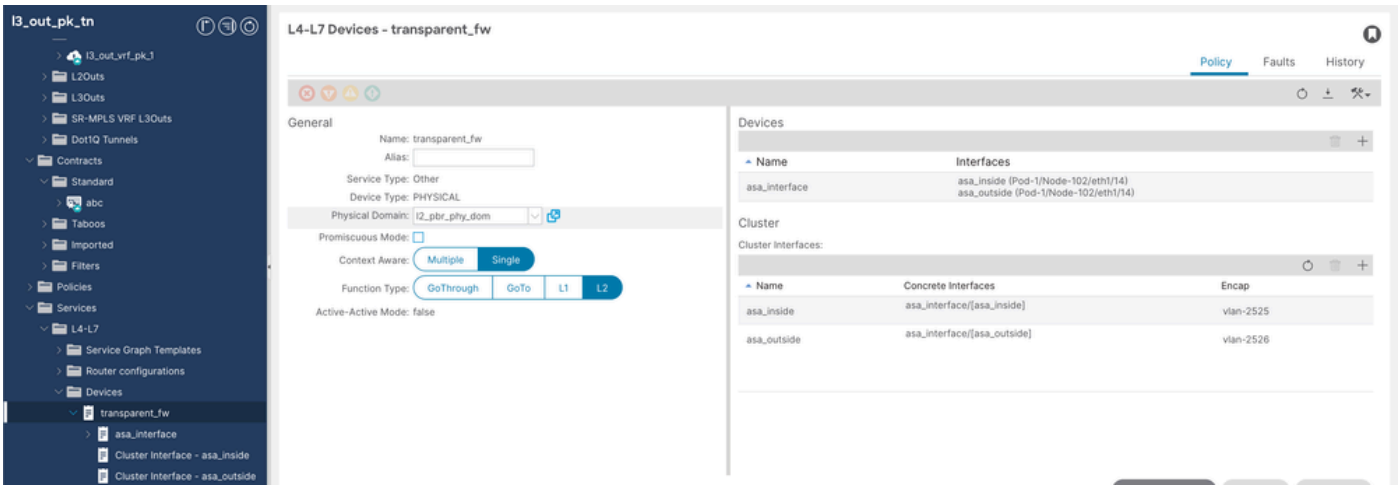
Accédez àTenant > Stratégies > Protocole > IP SLA > Stratégies de surveillance IP SLA, puis cliquez avec le bouton droit sur et créez une stratégie.



Politique IP SLA

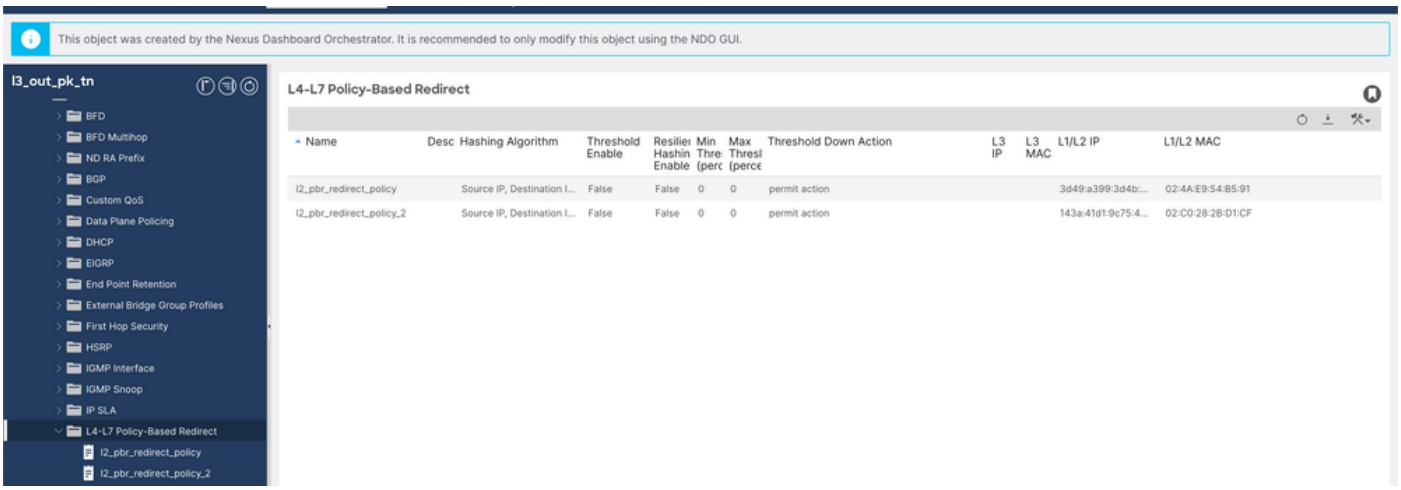
Étape 4 : configuration du périphérique L4/L7

Accédez à Tenant > Services > Devices, puis cliquez avec le bouton droit et créez un périphérique L4-L7.



Périphérique L4-L7

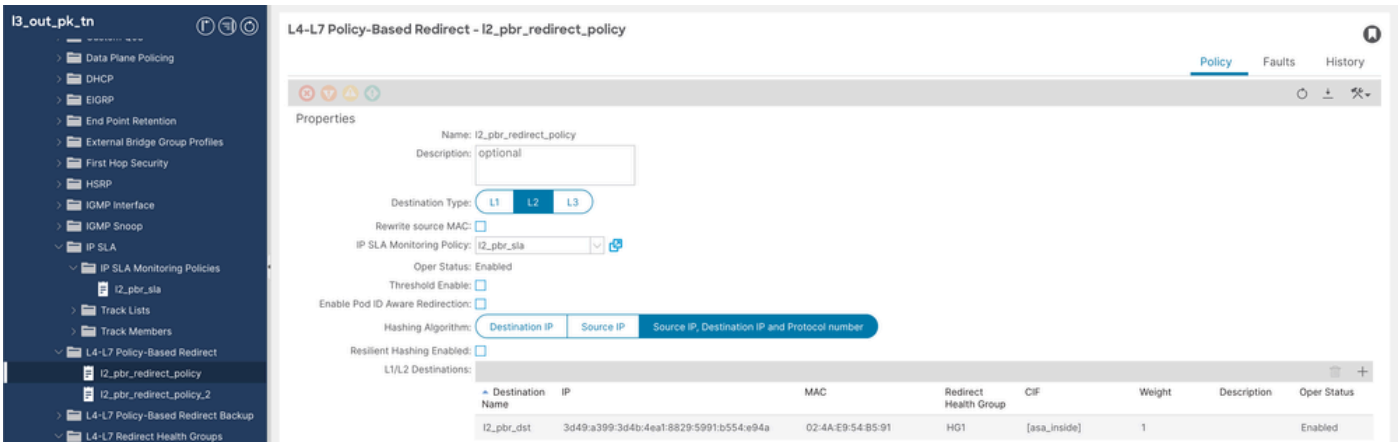
Étape 5 : validation de la présentation de la redirection basée sur les stratégies (vous pouvez vérifier cette option après avoir configuré les interfaces 5a et 5b)



Politique de redirection C4-C7

Étape 5.1. Configuration de la stratégie de redirection basée sur les stratégies L4-L7 pour l'interface interne ASA (Adaptive Security Appliance) (il n'est pas nécessaire de spécifier MAC ou IP, il est rempli par le contrôleur APIC lui-même)

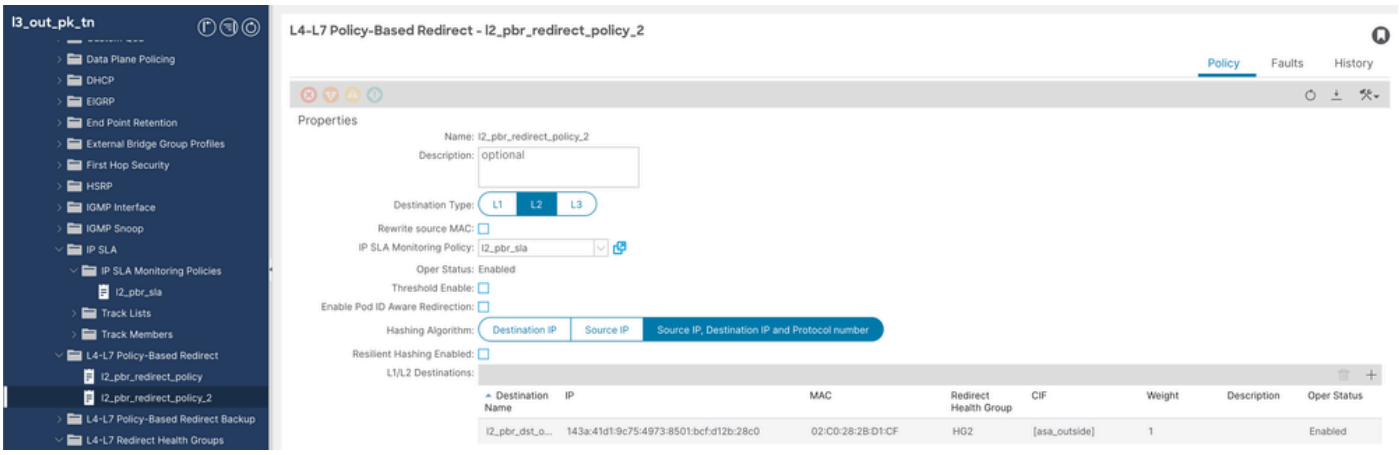
Naviguez jusqu'à Tenant > Politiques > Protocole > Redirection basée sur les politiques L4-L7, puis cliquez avec le bouton droit et créez une politique.



Configuration de la stratégie de redirection C4-C7

Étape 5.2. Configuration de la stratégie de redirection basée sur les stratégies L4-L7 pour l'interface externe ASA (il n'est pas nécessaire de spécifier MAC ou IP, elle est remplie par le contrôleur APIC lui-même)

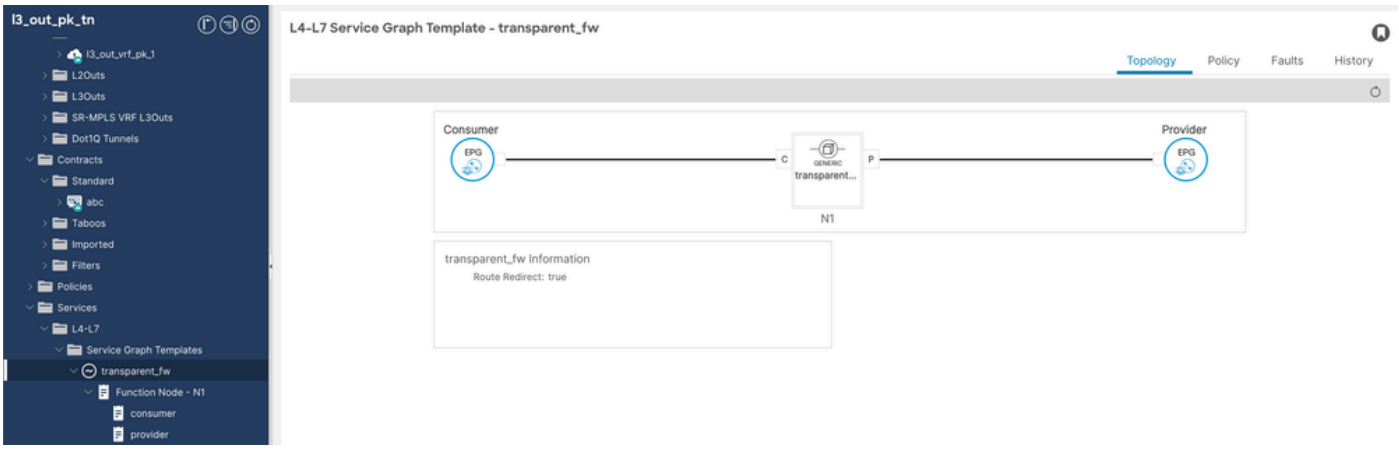
Naviguez jusqu'à Tenant > Politiques > Protocole > Redirection basée sur les politiques L4-L7, puis cliquez avec le bouton droit et créez une politique.



Config. de stratégie de redirection C4-C7 2

Étape 6 : configuration du modèle de graphique de service

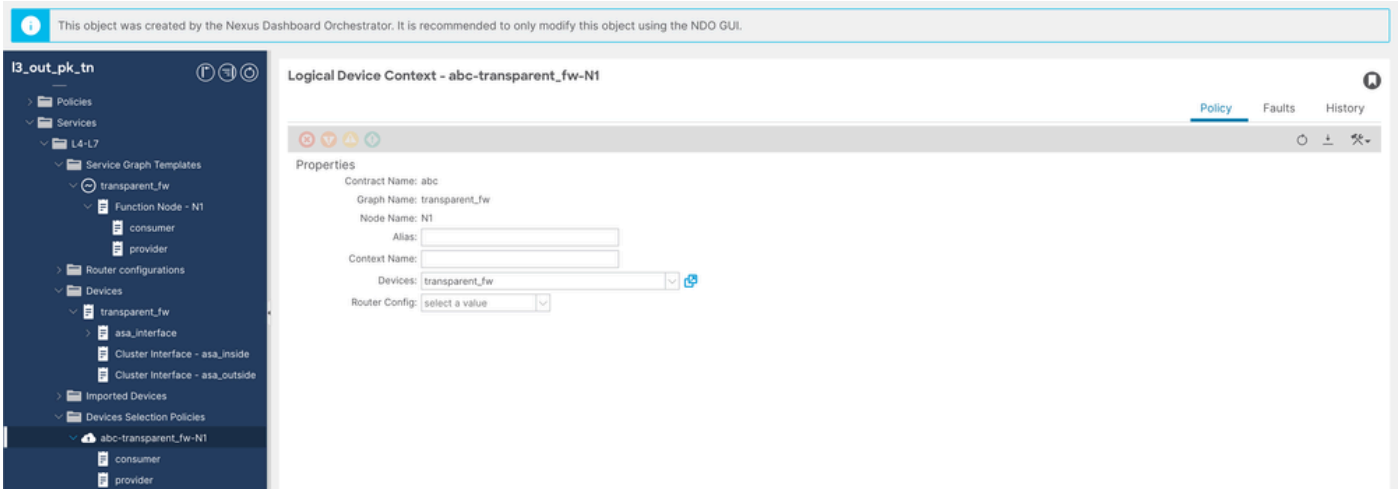
Accédez à Locataire > Services > Modèle de graphique de service, puis cliquez avec le bouton droit et créez un modèle de graphique de service de couches 4 à 7.



Configuration du graphique de services

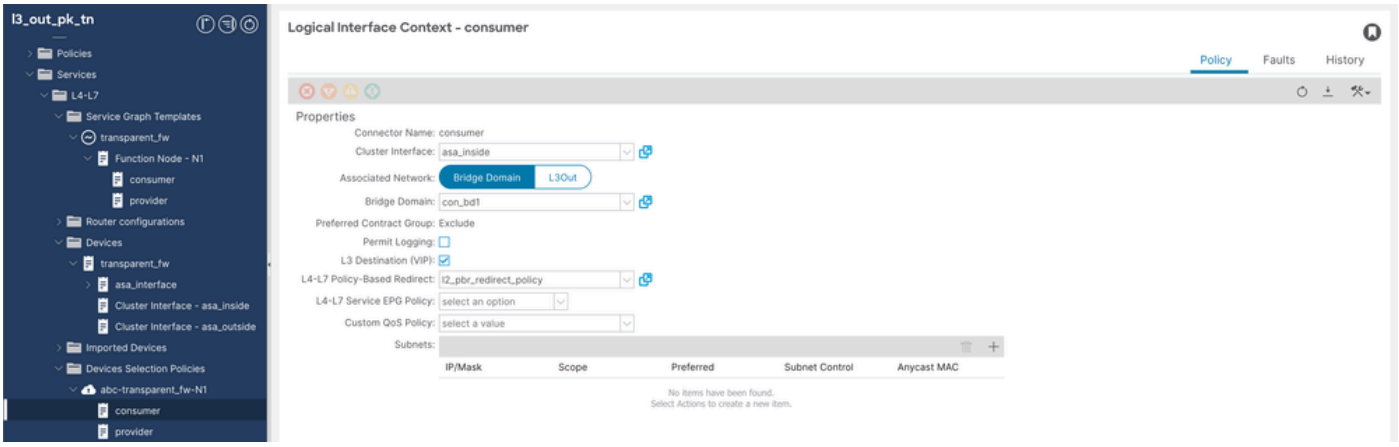
Étape 7 : configuration de la stratégie de sélection des périphériques

Accédez à Tenant > Services > Device Selection Policy, puis cliquez avec le bouton droit et créez Device Selection Policy.



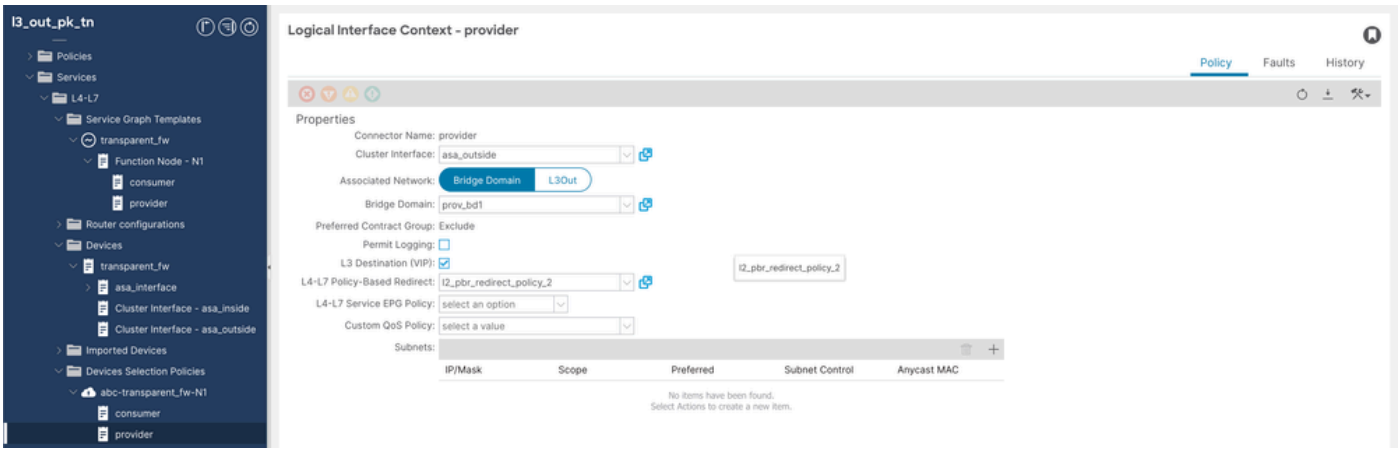
Configuration du graphique de services 2

++ Contexte de l'interface logique grand public



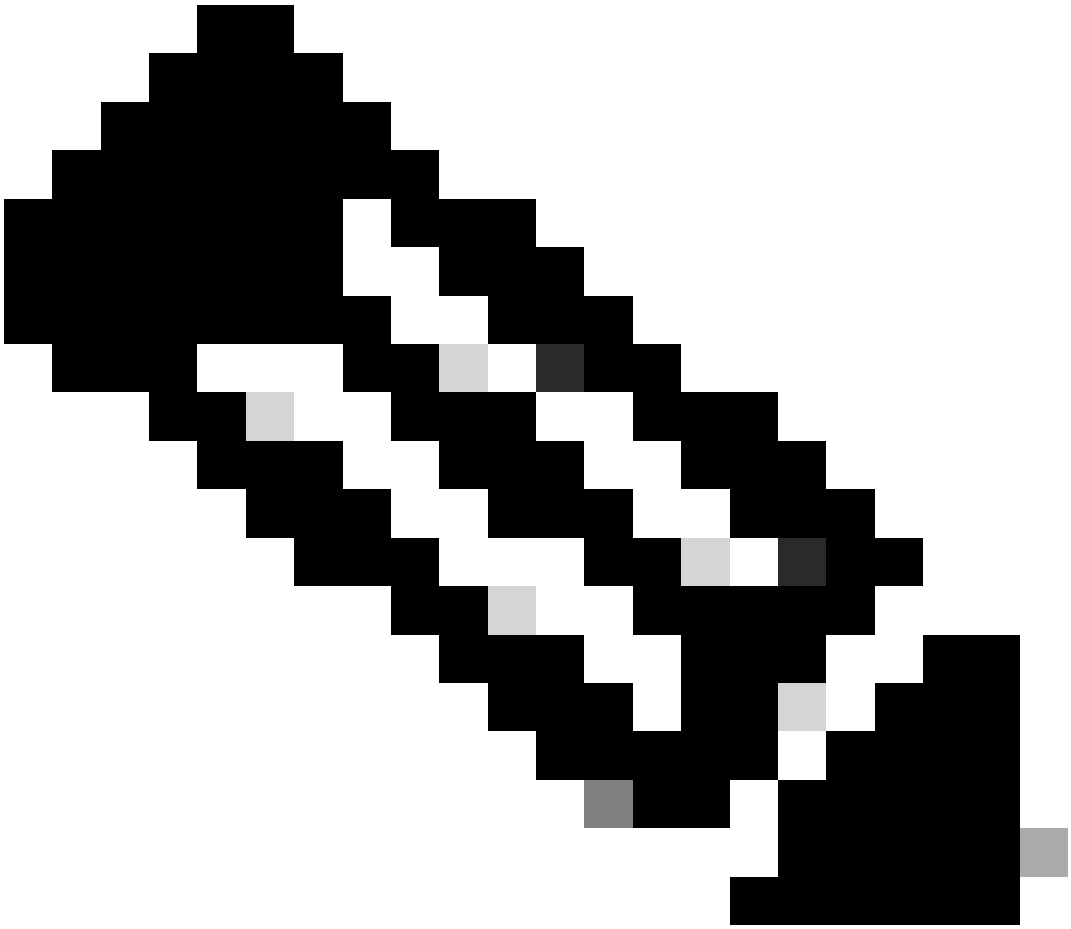
Config. consommateur de stratégie de sélection de périphérique

++ Contexte de l’interface logique du fournisseur



Configuration du fournisseur de stratégie de sélection de périphérique

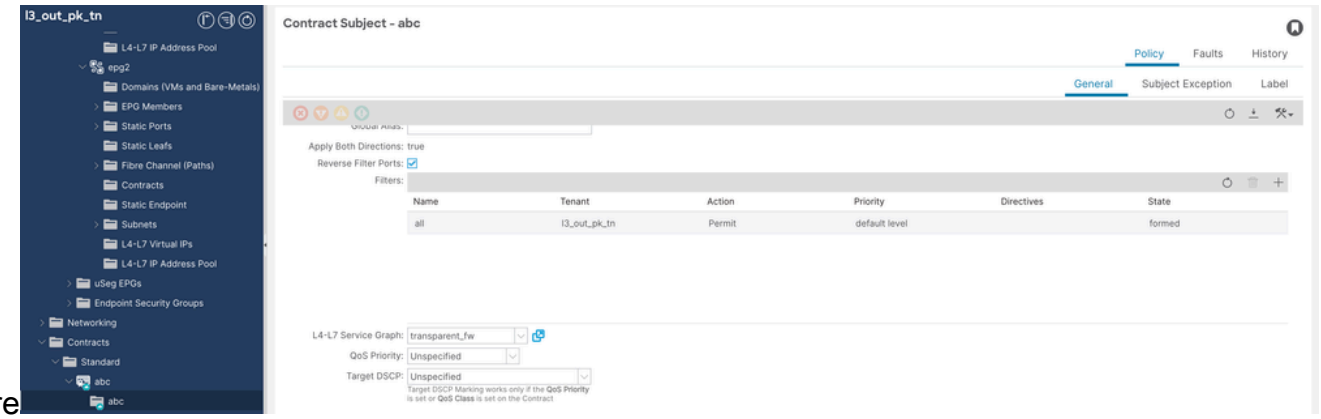
---



Remarque : Stratégie de sélection de périphérique si elle doit être créée automatiquement au cas où vous utiliseriez l'option Appliquer le graphique des services.

Étape 8. Appliquez PBR afin de contracter un sujet abc.

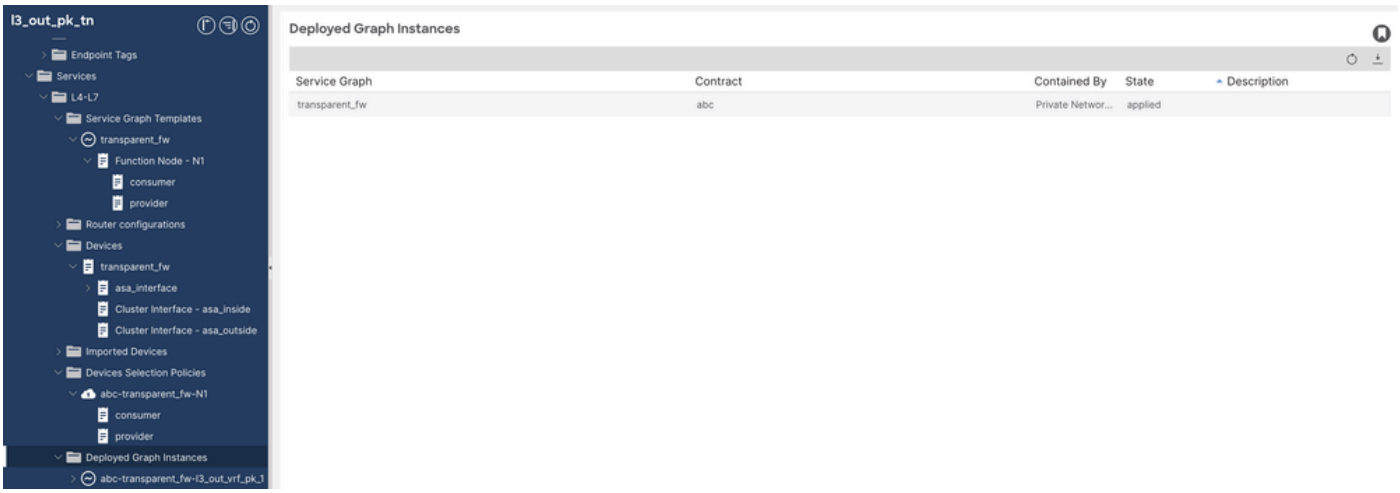
Accédez à Tenant > Contract > Contract Subject > L4-L7 Service Graph > transparent_fw.



Contre

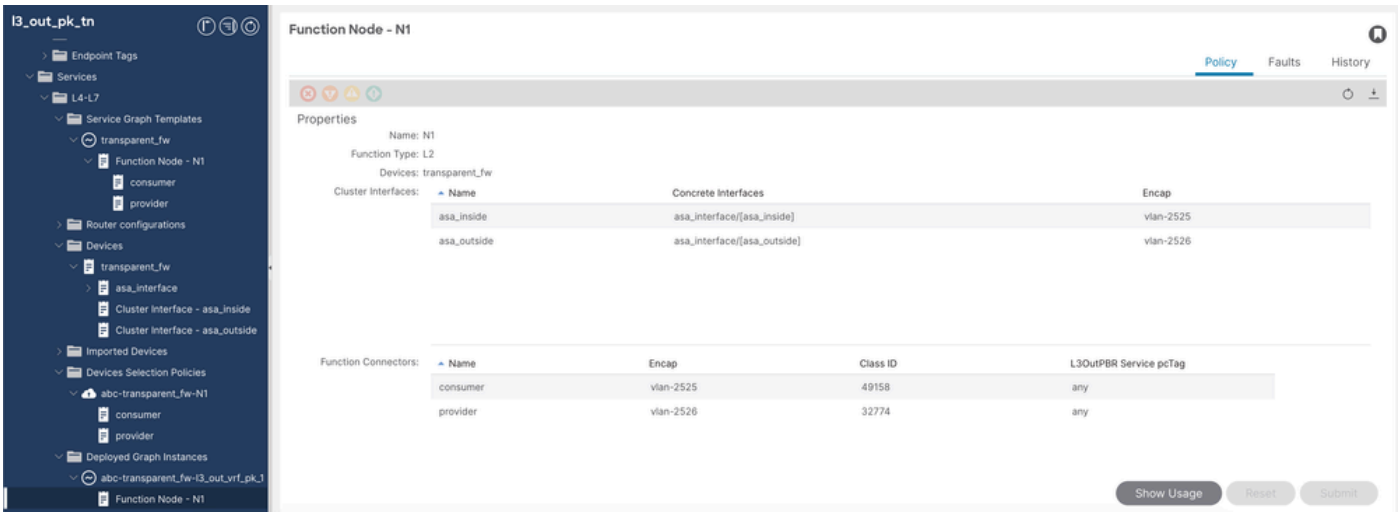
Configuration du contrat

Étape 9. Si le déploiement a réussi, validez sous Graphique d'instance déployée (recherchez l'état).



Validation du graphique de services

++ Valider les interfaces de cluster, encapsuler les VLAN et les ID de classe de connecteur de fonction.



Validation du graphique de services 2

Valider le trafic PBR L2 sur ASA

Secure Shell (SSH) du point de terminaison Src au point de terminaison dst que vous pouvez voir dans l'entrée de table Conn sur ASA.

Validation ASA

Vérification de L2 PBR sur Leaf

1. Programmation VLAN sur le noeud leaf 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. Politique de redirection et règle de zonage sur le noeud consommateur (101) et fournisseur (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 |  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
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 |  T
================================================================================================================
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  |
```

Erreurs détectées en cas d'échec de L2Ping

Si les requêtes ping L2 échouent sur le périphérique PBR, vous constaterez que le PBR est toujours à l'état déployé et que les défaillances F4203, F2833 et F2911 sont surélevées, indiquant que le groupe de suivi/d'intégrité est inactif.

Capture des requêtes ping L2

Vous pouvez capturer des L2Pings à l'aide de tcpdump sur l'interface tahoe afin de savoir s'ils sont correctement envoyés et reçus. Si vous ne voyez que la transmission CPU envoyée et non reçue, alors les erreurs mentionnées précédemment sont attendues et vous devez dépanner plus avant sur ASA pourquoi elles sont abandonnées (référez-vous à la section de configuration 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

Flux de trafic de Src à Dst Endpoint

<#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
```

Configuration ASA

Étape 1 : configuration de l’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
!
```

Étape 2. L'apprentissage MAC doit être désactivé.

<#root>

```
ASA(config)#
```

show run mac-learn

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

PBR :

Étape 3. Table d'adresses MAC statiques pour 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
```

Étape 4 : configuration de la liste de contrôle d'accès (ACL) afin de transmettre les requêtes ping 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
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.