Dépannage du transfert externe ACI

Contenu

Introduction

Ce document décrit les étapes à suivre pour comprendre et dépanner un L3out dans l'ACI

Informations générales

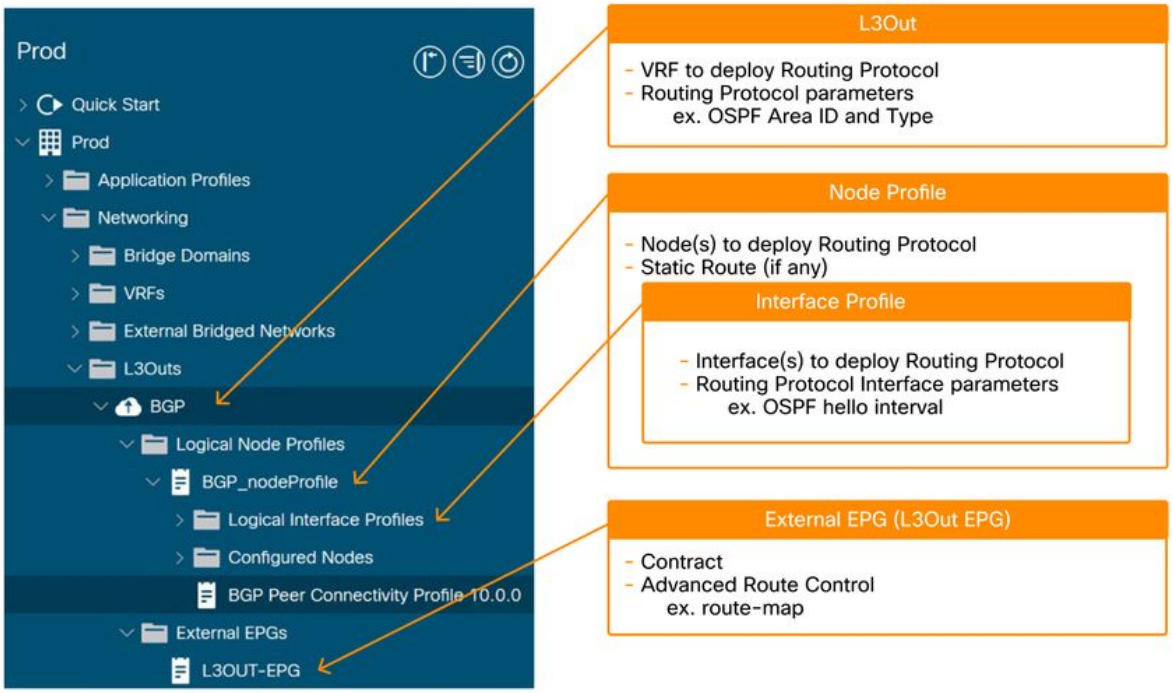
Le contenu de ce document a été extrait du livre Troubleshooting Cisco Application Centric Infrastructure, Second Edition, en particulier **External Forwarding - Overview, External Forwarding - Adjacencies, External Forwarding - Route advertisement, External Forwarding - Contract et L3out** et **External Forwarding - Share L3out**.

Aperçu

Composants L3Out

L'image suivante illustre les principaux blocs de construction requis pour configurer un L3 externe (L3Out).

Principaux composants d'une L3Out



1. Racine de L3Out : Sélectionnez un protocole de routage à déployer (tel qu'OSPF, BGP).Sélectionnez un VRF pour déployer le protocole de routage.Sélectionnez un domaine L3Out pour définir les interfaces Leaf et le VLAN disponibles pour L3Out.
2. Profil de noeud : Sélectionnez des commutateurs Leaf pour déployer le protocole de routage. Ces commutateurs sont généralement appelés « commutateurs de périphérie » (BL).Configurez l'ID de routeur (RID) pour le protocole de routage sur chaque noeud leaf périphérique. Contrairement à un routeur normal, l'ACI n'attribue pas automatiquement l'ID de routeur en fonction d'une adresse IP sur le commutateur.Configurez une route statique.
3. Profil d'interface : Configurez les interfaces leaf pour exécuter le protocole de routage. Type d'interface (SVI, port routé, sous-interface), ID d'interface et adresses IP, etc.Sélectionnez une stratégie pour les paramètres de protocole de routage au niveau de

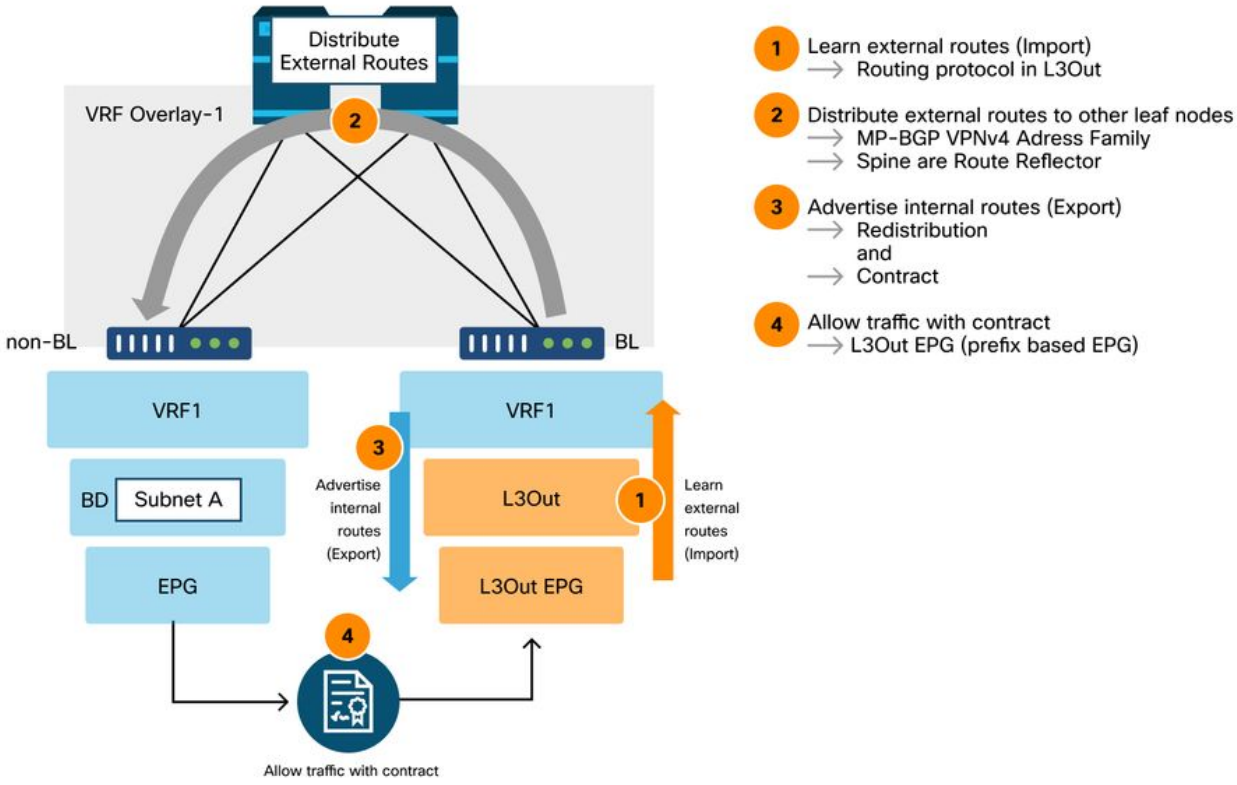
l'interface (tels que l'intervalle Hello).

4. EPG externe (L3Out EPG) : Un « EPG externe » est une exigence difficile pour déployer toutes les politiques liées à L3Out, telles que les adresses IP ou les interfaces SVI pour établir des voisins. Les détails sur l'utilisation des groupes de terminaux externes seront traités ultérieurement.

Routage externe

Le schéma suivant illustre l'opération de haut niveau impliquée pour le routage externe.

Flux de routage externe de haut niveau



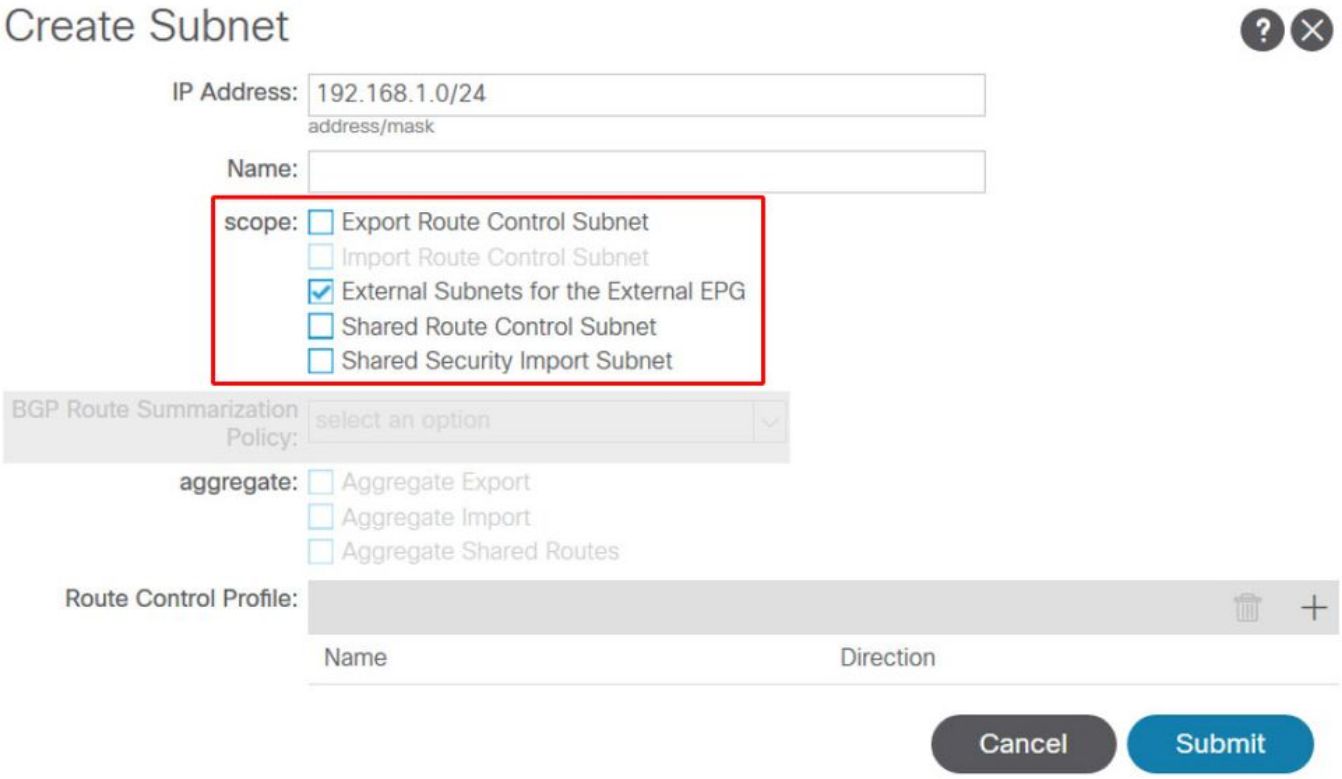
1. Le ou les BL établiront des contiguïtés de protocole de routage avec des routeurs externes.
2. Les préfixes de route sont reçus des routeurs externes et sont injectés dans MP-BGP comme chemin de la famille d'adresses VPNv4. Au minimum, deux noeuds spine doivent être configurés comme réflecteurs de route BGP pour refléter les routes externes vers tous les noeuds leaf.
3. Les préfixes internes (sous-réseaux BD) et/ou les préfixes reçus d'autres L3Out doivent être explicitement redistribués dans le protocole de routage pour être annoncés au routeur externe.
4. Application de la sécurité : un L3Out contient au moins un EPG L3Out. Un contrat doit être utilisé ou fourni sur l'EPG L3Out (également appelé l3extInstP à partir du nom de classe) pour autoriser le trafic entrant/sortant de L3Out.

Options de configuration de L3Out EPG

Dans la section L3Out EPG, les sous-réseaux peuvent être définis avec une série d'options «

Scope » et « Aggregate » comme illustré ci-dessous :

Un sous-réseau L3Out en cours de définition incluant la définition « scope »



Options d'étendue :

- **Exporter le sous-réseau de contrôle de routage :** cette étendue consiste à annoncer (exporter) un sous-réseau de l'ACI vers l'extérieur via L3Out. Bien qu'il s'agisse principalement du routage de transit, il peut également être utilisé pour annoncer un sous-réseau BD comme décrit dans la section « Annonce de sous-réseau BD ACI ».
- **Import Route Control Subnet :** cette étendue traite de l'apprentissage (importation) d'un sous-réseau externe à partir de L3Out. Par défaut, cette portée est désactivée, par conséquent elle est grisée, et un noeud terminal (BL) apprend toutes les routes à partir d'un protocole de routage. Cette portée peut être activée lorsqu'elle doit limiter les routes externes apprises via OSPF et BGP. Cette fonctionnalité n'est pas prise en charge pour EIGRP. Pour utiliser cette étendue, l'application 'Import Route Control Enforcement' doit d'abord être activée sur une L3Out donnée.
- **Sous-réseaux externes pour l'EPG externe (import-security) :** cette étendue est utilisée pour autoriser les paquets avec le sous-réseau configuré en provenance ou à destination de L3Out avec un contrat. Il classe un paquet dans l'EPG L3Out configuré en fonction du sous-réseau, de sorte qu'un contrat sur l'EPG L3Out puisse être appliqué au paquet. Cette étendue est une correspondance de préfixe la plus longue au lieu d'une correspondance exacte comme les autres étendues de la table de routage. Si 10.0.0.0/16 est configuré avec « Sous-réseaux externes pour l'EPG externe » dans L3Out EPG A, tous les paquets avec IP dans ce sous-réseau, tels que 10.0.1.1, seront classés dans l'EPG A L3Out pour utiliser un contrat sur celui-ci. Cela ne signifie pas que la portée « Sous-réseaux externes pour l'EPG externe » installe une route 10.0.0.0/16 dans une table de routage. Il crée une table interne différente pour mapper un sous-réseau à un EPG (pcTag) uniquement pour un contrat. Il n'a aucun effet sur

le comportement des protocoles de routage. Cette étendue doit être configurée sur un L3Out qui apprend le sous-réseau.
- **Sous-réseau de contrôle de route partagé :** cette étendue permet de transmettre un sous-réseau externe à un autre VRF. L'ACI utilise le protocole MP-BGP et la cible de route pour transmettre une route externe d'un VRF à un autre. Cette étendue crée une liste de préfixes avec le sous-réseau, qui est utilisée comme filtre pour exporter/importer des routes avec une cible de route dans MP-BGP. Cette étendue doit être configurée sur un L3Out qui apprend le sous-réseau dans le VRF d'origine.
- **Sous-réseau d'importation de sécurité partagée :** cette étendue est utilisée pour autoriser les paquets avec le sous-réseau configuré lorsque les paquets se déplacent sur des VRF avec une L3Out. Une route dans une table de routage est transmise à un autre VRF avec le sous-réseau de contrôle de route partagé comme mentionné ci-dessus. Cependant, un autre VRF doit encore savoir à quel EPG la route ayant fuité doit appartenir. Le sous-réseau d'importation de sécurité partagée informe un autre VRF de l'EPG L3Out auquel appartient la route ayant fui. Par conséquent, cette portée ne peut être utilisée que lorsque 'Sous-réseaux externes pour l'EPG externe' est également utilisé, sinon le VRF d'origine ne sait pas à quel EPG L3Out le sous-réseau appartient. Cette étendue est également la plus longue correspondance de préfixe.

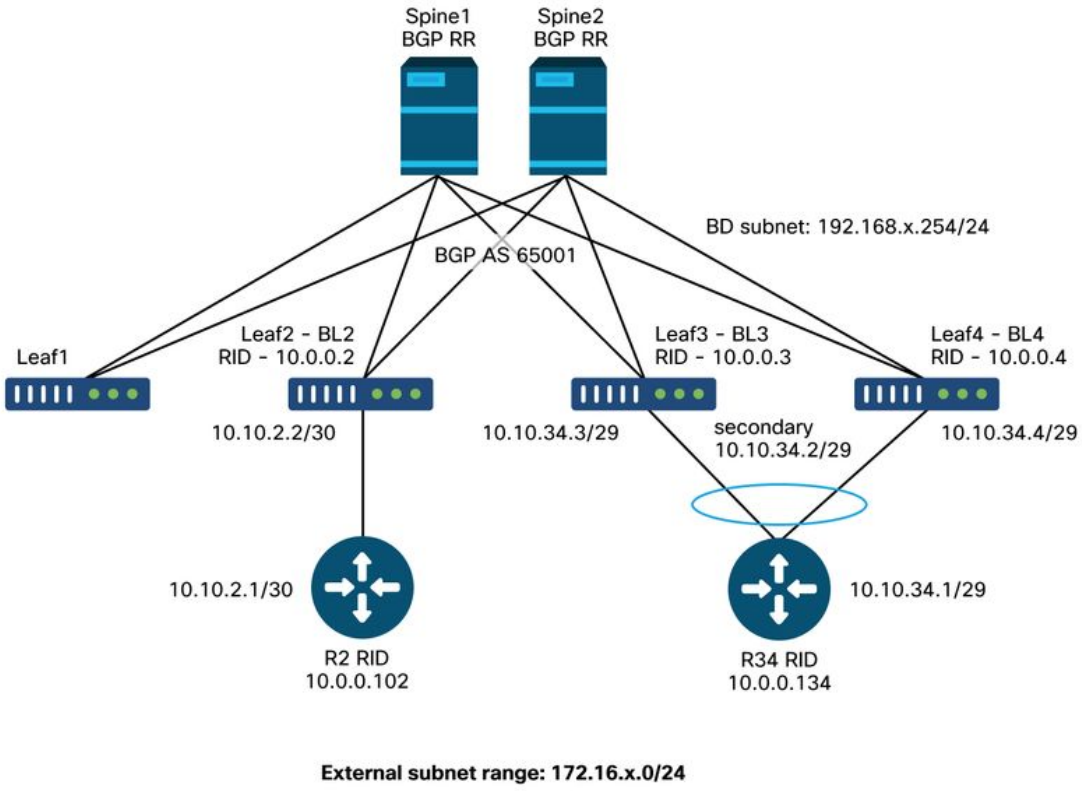
Options d'agrégation :

- **Aggregate Export :** cette option ne peut être utilisée que pour 0.0.0.0/0 avec 'Export Route Control Subnet'. Lorsque 'Export Route Control Subnet' et 'Aggregate Export' sont tous deux activés pour 0.0.0.0/0 ; il crée une liste de préfixes avec '0.0.0.0/0 le 32' qui correspond à n'importe quel sous-réseau. Par conséquent, cette option peut être utilisée lorsqu'une L3Out doit annoncer (exporter) des routes vers l'extérieur. Lorsqu'une agrégation plus granulaire est requise, une carte de routage/profil avec une liste de préfixes explicite peut être utilisée.
- **Aggregate Import :** cette option ne peut être utilisée que pour 0.0.0.0/0 avec « Import Route Control Subnet ». Lorsque 'Import Route Control Subnet' et 'Aggregate Import' sont activés pour 0.0.0.0/0, il crée une liste de préfixes avec '0.0.0.0/0 le 32' qui correspond à tous les sous-réseaux. Par conséquent, cette option peut être utilisée lorsqu'une L3Out doit apprendre (importer) n'importe quelle route depuis l'extérieur. Cependant, la même chose peut être accomplie en désactivant 'Import Route Control Enforcement' qui est la valeur par défaut. Lorsqu'une agrégation plus granulaire est requise, une carte de routage/profil avec une liste de préfixes explicite peut être utilisée.
- **Aggregate Shared Routes :** cette option peut être utilisée pour tous les sous-réseaux avec « Shared Route Control Subnet ». Lorsque 'Shared Route Control Subnet' et 'Aggregate Shared Routes' sont activés pour 10.0.0.0/8, par exemple, il crée une liste de préfixes avec '10.0.0.0/8 le 32' qui correspond à 10.0.0.0/8, 10.1.0.0/16 et ainsi de suite.

Topologie L3Out utilisée dans cette section

La topologie suivante sera utilisée dans cette section :

Topologie L3Out



Contiguïtés

Cette section explique comment dépanner et vérifier les contiguïtés de protocole de routage sur les interfaces L3Out.

Voici quelques paramètres à vérifier qui seront applicables à tous les protocoles de routage externe ACI :

- **ID de routeur :** dans l'ACI, chaque L3Out doit utiliser le même ID de routeur dans le même VRF sur le même leaf, même si les protocoles de routage sont différents. En outre, une seule de ces sorties L3 sur le même noeud leaf peut créer un bouclage avec l'ID de routeur, qui est généralement BGP.
- **MTU :** bien que la condition matérielle de MTU ne concerne que la contiguïté OSPF, il est recommandé de faire correspondre MTU pour tous les protocoles de routage afin de garantir que les paquets jumbo utilisés pour l'échange/les mises à jour de route peuvent être transmis sans fragmentation, car la plupart des trames du plan de contrôle seront envoyées avec le bit DF (ne pas fragmenter) défini, qui abandonnera la trame si sa taille dépasse la MTU maximale de l'interface.
- **MP-BGP Router Reflector :** sans cela, le processus BGP ne démarrera pas sur les noeuds leaf. Bien que cela ne soit pas nécessaire pour OSPF ou EIGRP simplement pour établir un voisin, il est toujours nécessaire pour les BL de distribuer des routes externes à d'autres noeuds leaf.
- **Défauts :** veillez toujours à vérifier les défauts pendant et après la configuration.

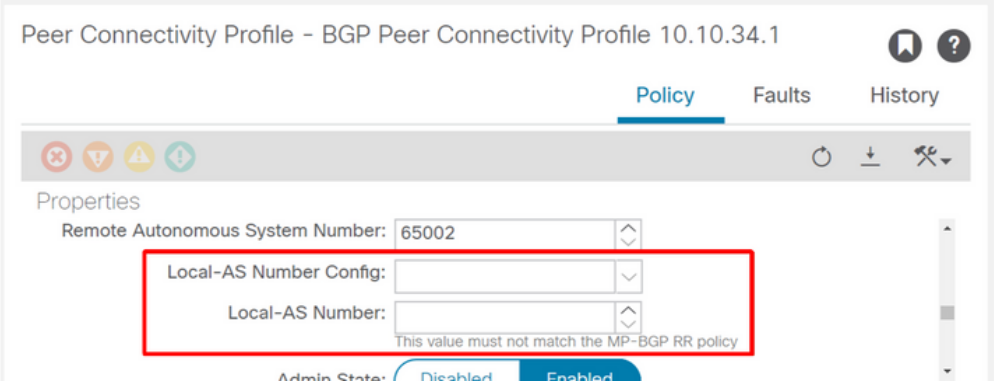
BGP

Cette section utilise un exemple d'appairage eBGP entre le bouclage sur BL3, BL4 et R34 à partir de la topologie dans la section Overview. Le SA BGP sur R34 est 65002.

Vérifiez les critères suivants lors de l'établissement d'une contiguïté BGP.

- Numéro BGP AS local (côté ACI BL).

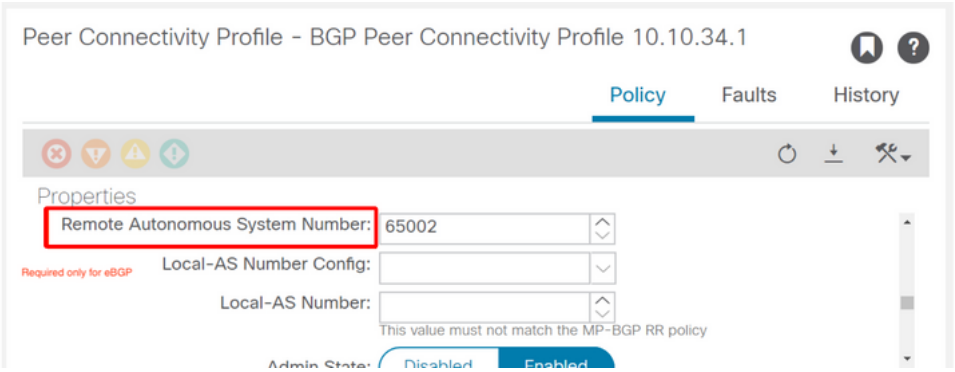
Profil de connectivité homologue — Local-AS



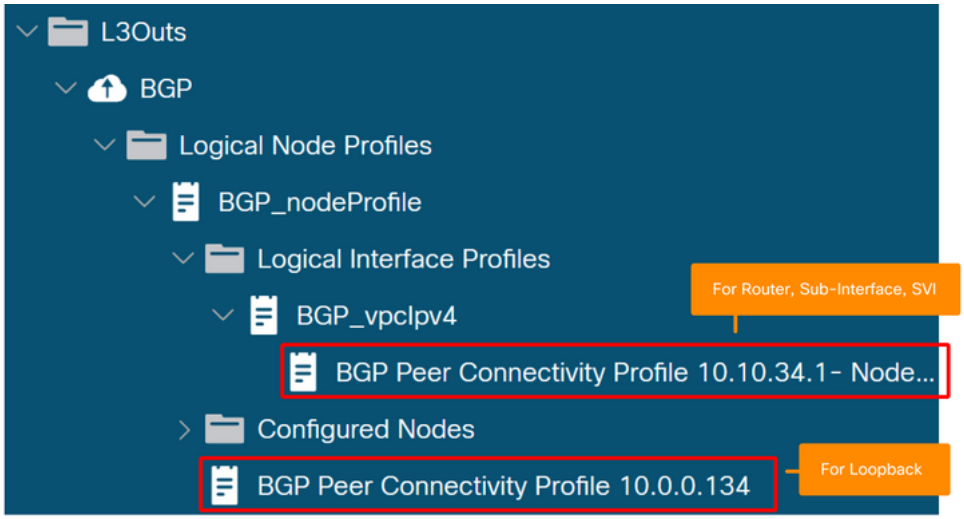
Le numéro de système autonome BGP d'un utilisateur L3Out sera automatiquement le même que le système autonome BGP pour l'infra-MP-BGP qui est configuré dans la stratégie BGP Route Reflector. La configuration « AS local » dans le profil de connectivité d'homologue BGP n'est pas requise, sauf si l'on doit dissimuler le AS BGP ACI au monde extérieur. Cela signifie que les routeurs externes doivent pointer vers le système autonome BGP configuré dans le réflecteur de route BGP.

REMARQUE : le scénario dans lequel la configuration du système autonome local est requise est identique à la commande autonome NX-OS « local-as ».

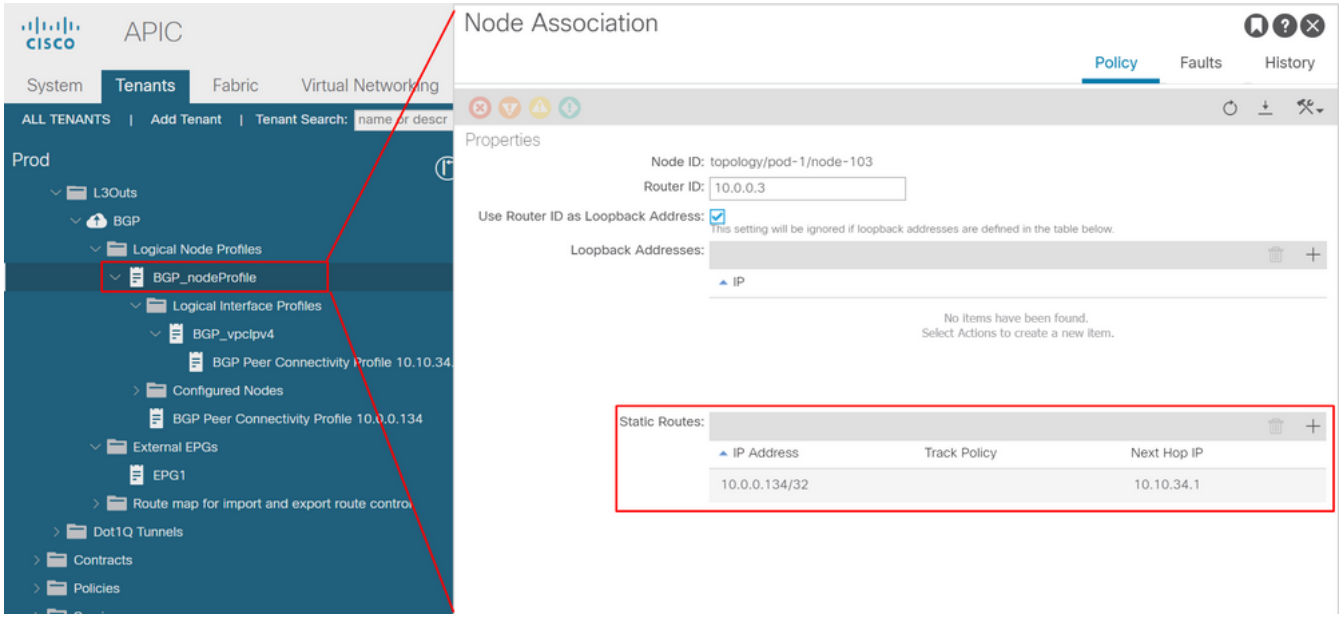
- Numéro de système autonome BGP distant (côté externe) **Profil de connectivité homologue - AS distant**



Le numéro de système autonome BGP distant est requis uniquement pour eBGP lorsque le système autonome BGP du voisin est différent du système autonome BGP ACI.IP source pour la session homologue BGP.**L3Out — Profil de connectivité homologue BGP**



L'ACI prend en charge l'approvisionnement d'une session BGP depuis l'interface de bouclage au-dessus d'un type d'interface ACI L3Out typique (routée, sous-interface, SVI).Lorsqu'une session BGP doit provenir d'un bouclage, configurez le profil de connectivité des homologues BGP sous le profil de **noeud** logique.Lorsque la session BGP doit être originaire d'une interface routée/sous-interface/SVI, configurez le profil de connectivité d'homologue BGP sous le profil d'**interface** logique.Accessibilité IP des homologues BGP.**Profil de noeud logique — Association de noeud**



Lorsque les adresses IP de l'homologue BGP sont des boucles, assurez-vous que le BL et le routeur externe sont accessibles à l'adresse IP de l'homologue. Les routes statiques ou OSPF peuvent être utilisées pour atteindre les IP homologues.**Vérification CLI BGP (eBGP avec exemple de bouclage)**Les résultats CLI des étapes suivantes sont collectés à partir de BL3 dans la section Topologie de la présentation.**1. Vérifiez si la session BGP est établie**'State/PfxRcd' dans le résultat CLI suivant signifie que la session BGP est établie.

```
f2-leaf3# show bgp ipv4 unicast summary vrf Prod:VRF1
BGP summary information for VRF Prod:VRF1, address family IPv4 Unicast
BGP router identifier 10.0.0.3, local AS number 65001
```

```
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.0.0.134      4 65002      10      10       10    0    0 00:06:39 0
```

Si le 'State/PfxRcd' indique Inactif ou Actif, les paquets BGP ne sont pas encore échangés avec l'homologue. Dans un tel scénario, vérifiez les points suivants et passez à l'étape suivante.

- Assurez-vous que le routeur externe pointe correctement vers le système autonome BGP ACI (numéro de système autonome local 65001).
- Assurez-vous que le profil de connectivité d'homologue BGP ACI spécifie l'adresse IP de voisinage correcte à partir de laquelle le routeur externe approvisionne la session BGP (10.0.0.134).
- Assurez-vous que le profil de connectivité des homologues BGP ACI spécifie le bon AS voisin du routeur externe (Remote Autonomous System Number dans l'interface utilisateur graphique, qui apparaît dans l'interface de ligne de commande sous le nom AS 65002).

2. Vérifiez les détails du voisin BGP (profil de connectivité homologue BGP)

La commande suivante montre les paramètres qui sont essentiels pour l'établissement du voisin BGP.

- Adresse IP du voisin : 10.0.0.134 .
- AS BGP voisin : AS distant 65002.
- Source IP : Utilisation de loopback3 comme source de mise à jour.
- Saut multiple eBGP : L'homologue BGP externe peut se trouver à 2 sauts.

```
f2-leaf3# show bgp ipv4 unicast neighbors vrf Prod:VRF1
BGP neighbor is 10.0.0.134,  remote AS 65002, ebgp link,  Peer index 1
 BGP version 4, remote router ID 10.0.0.134
 BGP state = Established, up for 00:11:18
 Using loopback3 as update source for this peer
 External BGP peer might be upto 2 hops away

...

  For address family: IPv4 Unicast
...
Inbound route-map configured is permit-all, handle obtained
Outbound route-map configured is exp-l3out-BGP-peer-3047424, handle obtained
Last End-of-RIB received 00:00:01 after session start
Local host: 10.0.0.3, Local port: 34873
 Foreign host: 10.0.0.134, Foreign port: 179
 fd = 64
```

Une fois que l'homologue BGP est établi correctement, 'Local host' et 'Foreign host' apparaissent au bas de la sortie.

3. Vérifiez l'accessibilité IP pour l'homologue BGP

```
f2-leaf3# show ip route vrf Prod:VRF1
10.0.0.3/32, ubest/mbest: 2/0, attached, direct
   *via 10.0.0.3, lo3, [0/0], 02:41:46, local, local
   *via 10.0.0.3, lo3, [0/0], 02:41:46, direct
10.0.0.134/32, ubest/mbest: 1/0
   *via 10.10.34.1, vlan27, [1/0], 02:41:46, static    <--- neighbor IP reachability via static
route
```

```
10.10.34.0/29, ubest/mbest: 2/0, attached, direct
   *via 10.10.34.3, vlan27, [0/0], 02:41:46, direct
   *via 10.10.34.2, vlan27, [0/0], 02:41:46, direct
10.10.34.2/32, ubest/mbest: 1/0, attached
   *via 10.10.34.2, vlan27, [0/0], 02:41:46, local, local
10.10.34.3/32, ubest/mbest: 1/0, attached
   *via 10.10.34.3, vlan27, [0/0], 02:41:46, local, local
```

Assurez-vous que la commande ping vers l'IP voisine fonctionne à partir de l'IP source du BGP ACI.

```
f2-leaf3# iping 10.0.0.134 -V Prod:VRF1 -S 10.0.0.3
PING 10.0.0.134 (10.0.0.134) from 10.0.0.3: 56 data bytes
64 bytes from 10.0.0.134: icmp_seq=0 ttl=255 time=0.571 ms
64 bytes from 10.0.0.134: icmp_seq=1 ttl=255 time=0.662 ms
```

4. Vérifiez la même chose sur le routeur externe

Voici un exemple de configuration sur le routeur externe (autonome NX-OS).

```
router bgp 65002
 vrf f2-bgp
   router-id 10.0.0.134
   neighbor 10.0.0.3
     remote-as 65001
     update-source loopback134
     ebgp-multihop 2
     address-family ipv4 unicast
   neighbor 10.0.0.4
     remote-as 65001
     update-source loopback134
     ebgp-multihop 2
     address-family ipv4 unicast

interface loopback134
 vrf member f2-bgp
 ip address 10.0.0.134/32

interface Vlan2501
 no shutdown
 vrf member f2-bgp
 ip address 10.10.34.1/29

vrf context f2-bgp
 ip route 10.0.0.0/29 10.10.34.2
```

5. Étape supplémentaire — tcpdump

Sur les noeuds leaf ACI, l'outil tcpdump peut analyser l'interface CPU « kpm_inb » pour confirmer si les paquets de protocole ont atteint le CPU leaf. Utilisez le port L4 179 (BGP) comme filtre.

```
f2-leaf3# tcpdump -ni kpm_inb port 179
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on kpm_inb, link-type EN10MB (Ethernet), capture size 65535 bytes
20:36:58.292903 IP 10.0.0.134.179 > 10.0.0.3.34873: Flags [P.], seq 3775831990:3775832009, ack
807595300, win 3650, length 19: BGP, length: 19
```

```
20:36:58.292962 IP 10.0.0.3.34873 > 10.0.0.134.179: Flags [.], ack 19, win 6945, length 0
20:36:58.430418 IP 10.0.0.3.34873 > 10.0.0.134.179: Flags [P.], seq 1:20, ack 19, win 6945,
length 19: BGP, length: 19
20:36:58.430534 IP 10.0.0.134.179 > 10.0.0.3.34873: Flags [.], ack 20, win 3650, length 0
```

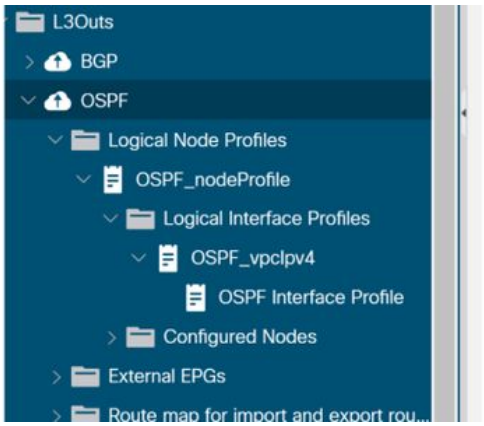
OSPF

Cette section utilise un exemple de voisinage OSPF entre BL3, BL4 et R34 de la section Topologie dans Vue d'ensemble avec l'ID de zone OSPF 1 (NSSA).

Voici les critères courants pour vérifier l'établissement de la contiguïté OSPF.

- ID et type de zone OSPF

L3Out — OSPF Interface Profile — ID et type de zone



Comme tout périphérique de routage, l'ID de zone OSPF et le type doivent correspondre sur les deux voisins. Certaines limitations spécifiques à l'ACI sur les configurations d'ID de zone OSPF incluent :

- Un L3Out ne peut avoir qu'un seul ID de zone OSPF.
- Deux sorties L3 peuvent utiliser le même ID de zone OSPF dans le même VRF uniquement lorsqu'elles se trouvent sur deux noeuds leaf différents.

Bien que l'ID OSPF n'ait pas besoin d'être backbone 0, dans le cas du routage de transit, il est requis entre deux sorties L3 OSPF sur le même leaf ; l'un d'eux doit utiliser la zone OSPF 0, car tout échange de route entre les zones OSPF doit passer par la zone OSPF 0.

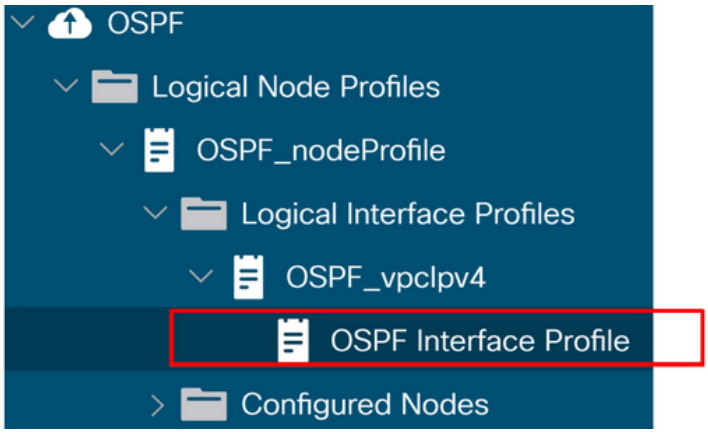
- MTU

Profil d'interface logique - SVI

Le MTU par défaut sur l'ACI est de 9 000 octets, au lieu de 1 500 octets, ce qui est généralement le MTU par défaut utilisé sur les périphériques de routage traditionnels. Vérifiez que le MTU correspond au périphérique externe. Lorsque l'établissement du voisin OSPF échoue en raison de MTU, il est bloqué à EXCHANGE/DROTHER.

- Masque de sous-réseau IP. OSPF exige que l'adresse IP voisine utilise le même masque de sous-réseau.
- Profil d'interface OSPF.

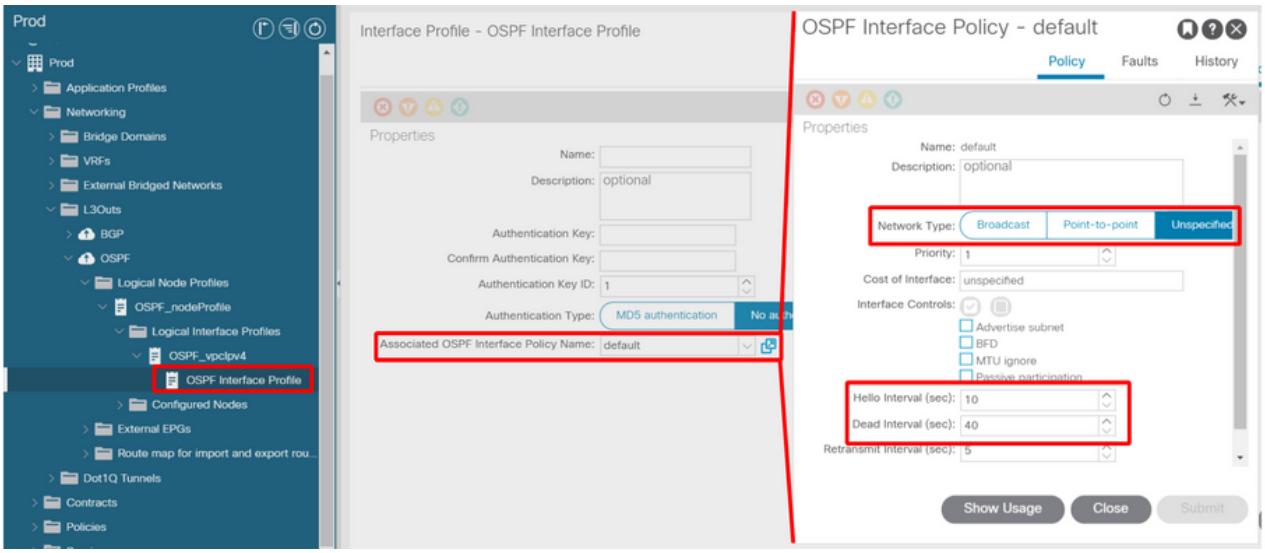
Profil d'interface OSPF



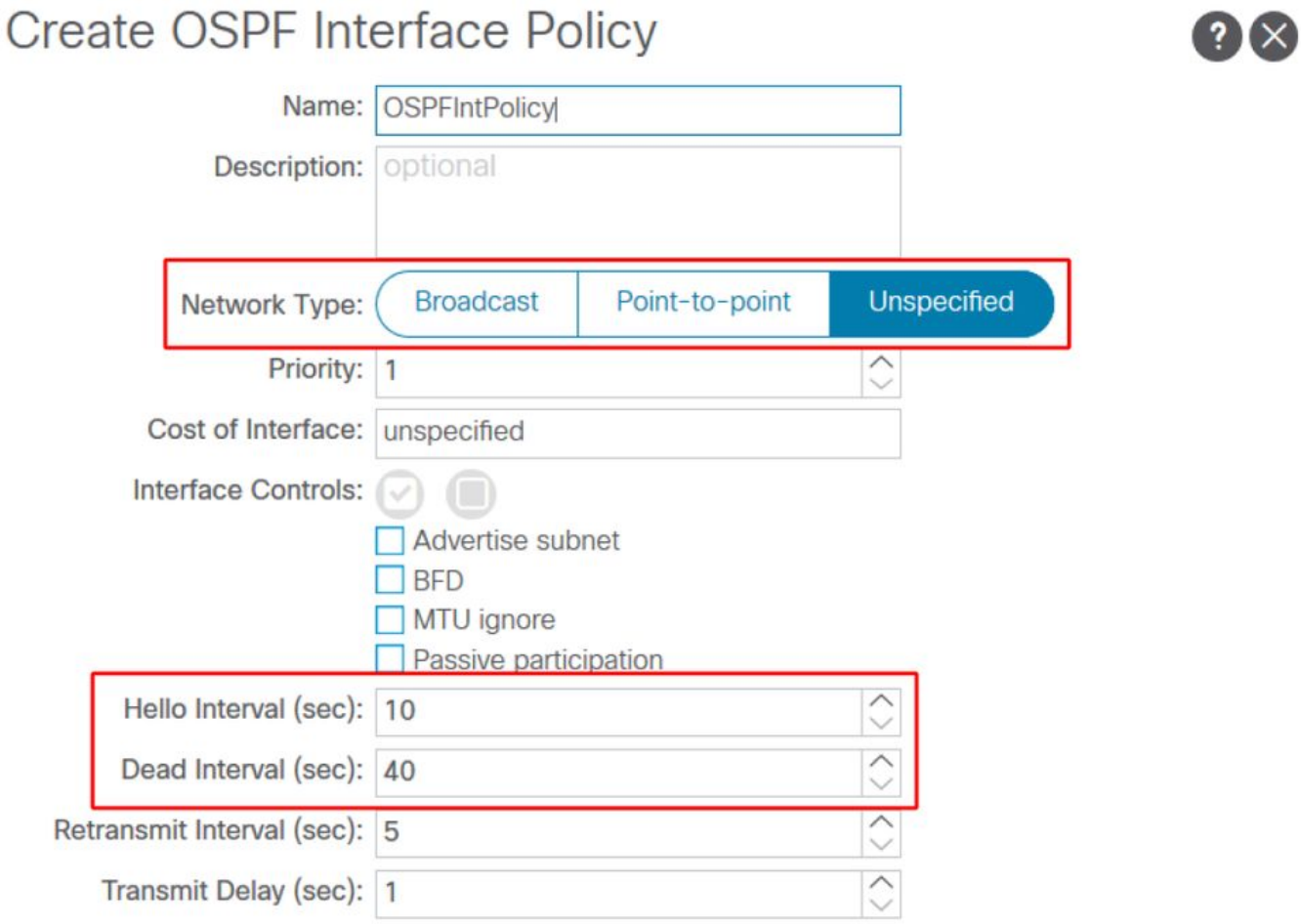
Cela équivaut à « ip router ospf <tag> area <area id> » dans une configuration NX-OS autonome pour activer OSPF sur l'interface. Sans cela, les interfaces leaf ne rejoignent pas OSPF.

- OSPF Hello / Dead Timer, type de réseau

Profil d'interface OSPF : minuteur Hello / Dead et type de réseau



Détails de la stratégie d'interface OSPF



OSPF nécessite que les minuteurs Hello et Dead correspondent sur chaque périphérique voisin. Elles sont configurées dans le profil d'interface OSPF.

Vérifiez que le type de réseau de l'interface OSPF correspond au périphérique externe. Lorsque le périphérique externe utilise le type Point-to-Point, l'ACI doit également configurer explicitement le type Point-to-Point. Ils sont également configurés dans le profil d'interface OSPF.

Vérification CLI OSPF

Les sorties CLI des étapes suivantes sont collectées à partir de BL3 dans la section « Topologie » de la section « Présentation ».

1. Vérifiez l'état du voisin OSPF

Si l'état est FULL dans l'interface de ligne de commande suivante, le voisin OSPF est établi correctement. Sinon, passez à l'étape suivante pour vérifier les paramètres.

```
f2-leaf3# show ip ospf neighbors vrf Prod:VRF2
OSPF Process ID default VRF Prod:VRF2
Total number of neighbors: 2
Neighbor ID     Pri State            Up Time  Address         Interface
10.0.0.4          1 FULL/DR          00:47:30 10.10.34.4      Vlan28      <--- neighbor with BL4
10.0.0.134        1 FULL/DROTHER     00:00:21 10.10.34.1      Vlan28      <--- neighbor with R34
```

Dans l'ACI, les BL forment des voisins OSPF les uns avec les autres au-dessus des routeurs externes lorsqu'ils utilisent le même ID de VLAN avec une SVI. En effet, l'ACI dispose d'un

domaine d'inondation interne appelé L3Out BD (ou External BD) pour chaque ID de VLAN dans les interfaces SVI L3Out. Notez que l'ID de VLAN 28 est un VLAN interne appelé PI-VLAN (Platform-Independent VLAN) au lieu du VLAN réel (Access Encap VLAN) utilisé sur le câble. Utilisez la commande suivante pour vérifier le VLAN access encap ('vlan-2502').

```
f2-leaf3# show vlan id 28 extended
 VLAN Name                             Encap            Ports
 ---- -------------------------------- ---------------- ------------------------
 28   Prod:VRF2:l3out-OSPF:vlan-2502   vxlan-14942176,  Eth1/13, Po1
                                       vlan-2502
```

On pourrait obtenir le même résultat via l'ID VLAN d'encapsulation d'accès également.

```
f2-leaf3# show vlan encap-id 2502 extended
 VLAN Name                             Encap            Ports
 ---- -------------------------------- ---------------- ------------------------
 28   Prod:VRF2:l3out-OSPF:vlan-2502   vxlan-14942176,  Eth1/13, Po1
                                       vlan-2502
```

2. Vérifiez la zone OSPF

Vérifiez que l'ID et le type de zone OSPF sont identiques aux voisins. Si le profil d'interface OSPF est manquant, l'interface ne se connecte pas à OSPF et ne s'affiche pas dans le résultat de l'interface de ligne de commande OSPF.

```
f2-leaf3# show ip ospf interface brief vrf Prod:VRF2
OSPF Process ID default VRF Prod:VRF2
Total number of interface: 1
Interface               ID     Area            Cost   State    Neighbors Status
Vlan28                  94     0.0.0.1         4      BDR      2         up
f2-leaf3# show ip ospf vrf Prod:VRF2
Routing Process default with ID 10.0.0.3 VRF Prod:VRF2
...
  Area (0.0.0.1)
       Area has existed for 00:59:14
       Interfaces in this area: 1 Active interfaces: 1
       Passive interfaces: 0  Loopback interfaces: 0
       This area is a NSSA area
       Perform type-7/type-5 LSA translation
       SPF calculation has run 10 times
        Last SPF ran for 0.001175s
       Area ranges are
       Area-filter in 'exp-ctx-proto-3112960'
       Area-filter out 'permit-all'
       Number of LSAs: 4, checksum sum 0x0
```

3. Vérifiez les détails de l'interface OSPF

Assurez-vous que les paramètres de niveau interface répondent aux exigences de l'établissement du voisin OSPF, telles que le sous-réseau IP, le type de réseau, le minuteur Hello/Dead. Notez l'ID de VLAN pour spécifier que l'interface SVI est PI-VLAN (vlan28)

```
f2-leaf3# show ip ospf interface vrf Prod:VRF2
Vlan28 is up, line protocol is up
```

```
   IP address 10.10.34.3/29, Process ID default VRF Prod:VRF2, area 0.0.0.1
   Enabled by interface configuration
   State BDR, Network type BROADCAST, cost 4
   Index 94, Transmit delay 1 sec, Router Priority 1
   Designated Router ID: 10.0.0.4, address: 10.10.34.4
   Backup Designated Router ID: 10.0.0.3, address: 10.10.34.3
   2 Neighbors, flooding to 2, adjacent with 2
   Timer intervals: Hello 10, Dead 40, Wait 40, Retransmit 5
     Hello timer due in 0.000000
   No authentication
   Number of opaque link LSAs: 0, checksum sum 0

f2-leaf3# show interface vlan28
Vlan28 is up, line protocol is up, autostate disabled
  Hardware EtherSVI, address is  0022.bdf8.19ff
  Internet Address is 10.10.34.3/29
  MTU 9000 bytes, BW 10000000 Kbit, DLY 1 usec
```

4. Vérifiez l’accessibilité IP au voisin

Bien que les paquets Hello OSPF soient des paquets de multidiffusion locale de liaison, les paquets DBD OSPF requis pour le premier échange LSDB OSPF sont en monodiffusion. Par conséquent, l'accessibilité de monodiffusion doit également être vérifiée pour l'établissement de voisinage OSPF.

```
f2-leaf3# iping 10.10.34.1 -V Prod:VRF2
PING 10.10.34.1 (10.10.34.1) from 10.10.34.3: 56 data bytes
64 bytes from 10.10.34.1: icmp_seq=0 ttl=255 time=0.66 ms
64 bytes from 10.10.34.1: icmp_seq=1 ttl=255 time=0.653 ms
```

5. Vérifiez la même chose sur le routeur externe

Voici des exemples de configurations sur le routeur externe (NX-OS autonome)

```
router ospf 1
    vrf f2-ospf
    router-id 10.0.0.134
    area 0.0.0.1 nssa

interface Vlan2502
    no shutdown
    mtu 9000
    vrf member f2-ospf
    ip address 10.10.34.1/29
    ip router ospf 1 area 0.0.0.1
```

Assurez-vous de vérifier également le MTU sur l'interface physique.

6. Étape supplémentaire — tcpdump

Sur les noeuds leaf ACI, l'utilisateur peut exécuter tcpdump sur l'interface CPU « kpm_inb » pour vérifier si les paquets de protocole ont atteint le CPU leaf. Bien qu’il existe plusieurs filtres pour OSPF, le numéro de protocole IP est le filtre le plus complet.

- Numéro de protocole IP : proto 89 (IPv4) ou ip6 proto 0x59 (IPv6)
- Adresse IP du voisin : hôte <ip>

- Adresse IP Mcast locale de liaison OSPF : hôte 224.0.0.5 ou hôte 224.0.0.6

```
f2-leaf3# tcpdump -ni kpm_inb proto 89
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on kpm_inb, link-type EN10MB (Ethernet), capture size 65535 bytes
22:28:38.231356 IP 10.10.34.4 > 224.0.0.5: OSPFv2, Hello, length 52
22:28:42.673810 IP 10.10.34.3 > 224.0.0.5: OSPFv2, Hello, length 52
22:28:44.767616 IP 10.10.34.1 > 224.0.0.5: OSPFv2, Hello, length 52
22:28:44.769092 IP 10.10.34.3 > 10.10.34.1: OSPFv2, Database Description, length 32
22:28:44.769803 IP 10.10.34.1 > 10.10.34.3: OSPFv2, Database Description, length 32
22:28:44.775376 IP 10.10.34.3 > 10.10.34.1: OSPFv2, Database Description, length 112
22:28:44.780959 IP 10.10.34.1 > 10.10.34.3: OSPFv2, LS-Request, length 36
22:28:44.781376 IP 10.10.34.3 > 10.10.34.1: OSPFv2, LS-Update, length 64
22:28:44.790931 IP 10.10.34.1 > 224.0.0.6: OSPFv2, LS-Update, length 64
```

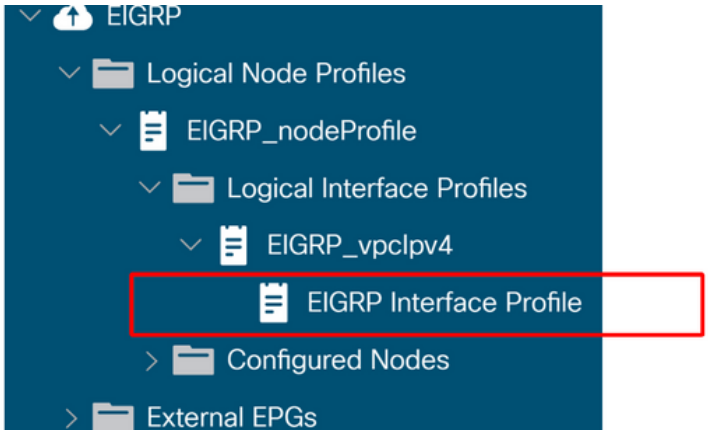
EIGRP

Cette section utilise un exemple de voisinage EIGRP entre BL3, BL4 et R34 de la topologie de la section « Vue d'ensemble » avec le système autonome EIGRP 10.

Voici les critères communs pour l'établissement de contiguïté EIGRP.

- AS EIGRP : Un AS EIGRP est attribué à un L3Out. Cela doit correspondre au périphérique externe.
- Profil d'interface EIGRP.

Profil d'interface EIGRP



Cela équivaut à la configuration « ip router eigrp <as> » sur un périphérique NX-OS autonome. Sans cela, les interfaces leaf ne rejoignent pas EIGRP.

- MTU

Bien que cela ne doive pas correspondre pour établir simplement le voisinage EIGRP, la topologie EIGRP échange des paquets peut devenir plus grande que la MTU maximale autorisée sur les interfaces entre les homologues, et comme ces paquets ne sont pas autorisés à être fragmentés, ils sont abandonnés et par conséquent le voisinage EIGRP va basculer.

Vérification de la CLI EIGRP

Les sorties CLI des étapes suivantes sont collectées à partir de BL3 dans la topologie de la

section « Overview ».

1. Vérifiez l’état du voisin EIGRP

```
f2-leaf3# show ip eigrp neighbors vrf Prod:VRF3
EIGRP neighbors for process 10 VRF Prod:VRF3
H   Address                 Interface       Hold  Uptime  SRTT   RTO  Q  Seq
                                           (sec)         (ms)       Cnt Num
0   10.10.34.4              vlan29          14   00:12:58  1    50    0   6    <--- neighbor
with BL4
1   10.10.34.1              vlan29          13   00:08:44  2    50    0   4    <--- neighbor
with R34
```

Dans l'ACI, les BL forment un voisinage EIGRP les uns avec les autres au-dessus des routeurs externes lorsqu'ils utilisent le même ID de VLAN avec SVI. En effet, une infrastructure ACI possède un domaine d'inondation interne appelé L3Out BD (ou External BD) pour chaque ID de VLAN dans les interfaces SVI L3Out.

Notez que l'ID de VLAN 29 est un VLAN interne appelé PI-VLAN (Platform-Independent VLAN) au lieu du VLAN réel (Access Encap VLAN) utilisé sur le câble. Utilisez la commande suivante pour vérifier le VLAN access encap (vlan-2503).

```
f2-leaf3# show vlan id 29 extended
 VLAN Name                            Encap            Ports
 ---- ------------------------------- ---------------- -----------------------
 29   Prod:VRF3:l3out-EIGRP:vlan-2503  vxlan-15237052,  Eth1/13, Po1
                                       vlan-2503
```

On pourrait obtenir le même résultat via l'ID VLAN d'encapsulation d'accès également.

```
f2-leaf3# show vlan encap-id 2503 extended
 VLAN Name                            Encap            Ports
 ---- ------------------------------- ---------------- -----------------------
 29   Prod:VRF3:l3out-EIGRP:vlan-2503  vxlan-15237052,  Eth1/13, Po1
                                       vlan-2503
```

2. Vérifiez les détails de l’interface EIGRP

Assurez-vous que le protocole EIGRP fonctionne sur l’interface attendue. Si ce n'est pas le cas, vérifiez Logical Interface Profile et EIGRP Interface Profile.

```
f2-leaf3# show ip eigrp interfaces vrf Prod:VRF3
EIGRP interfaces for process 10 VRF Prod:VRF3
                        Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface        Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
vlan29             2        0/0         1       0/0         50             0
  Hello interval is 5 sec
  Holdtime interval is 15 sec
  Next xmit serial: 0
  Un/reliable mcasts: 0/2     Un/reliable ucasts: 5/10
  Mcast exceptions: 0    CR packets: 0    ACKs suppressed: 2
  Retransmissions sent: 2    Out-of-sequence rcvd: 0
  Classic/wide metric peers: 2/0
```

```
f2-leaf3# show int vlan 29
Vlan29 is up, line protocol is up, autostate disabled
  Hardware EtherSVI, address is  0022.bdf8.19ff
  Internet Address is 10.10.34.3/29
  MTU 9000 bytes, BW 10000000 Kbit, DLY 1 usec
```

3. Vérifiez la même chose sur le routeur externe

L'exemple suivant illustre la configuration sur le routeur externe (NX-OS autonome).

```
router eigrp 10
 vrf f2-eigrp

interface Vlan2503
 no shutdown
 vrf member f2-eigrp
 ip address 10.10.34.1/29
 ip router eigrp 10
```

4. Étape supplémentaire — tcpdump

Sur les noeuds leaf ACI, l'utilisateur peut exécuter tcpdump sur l'interface CPU « kpm_inb » pour confirmer si les paquets de protocole ont atteint le CPU du leaf. Utilisez le protocole IP numéro 88 (EIGRP) comme filtre.

```
f2-leaf3# tcpdump -ni kpm_inb proto 88
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on kpm_inb, link-type EN10MB (Ethernet), capture size 65535 bytes
23:29:43.725676 IP 10.10.34.3 > 224.0.0.10: EIGRP Hello, length: 40
23:29:43.726271 IP 10.10.34.4 > 224.0.0.10: EIGRP Hello, length: 40
23:29:43.728178 IP 10.10.34.1 > 224.0.0.10: EIGRP Hello, length: 40
23:29:45.729114 IP 10.10.34.1 > 10.10.34.3: EIGRP Update, length: 20
23:29:48.316895 IP 10.10.34.3 > 224.0.0.10: EIGRP Hello, length: 40
```

Annonce de route

Cette section porte sur la vérification et le dépannage de l'annonce de route dans l'ACI. Plus précisément, il examine des exemples impliquant :

- Annonce de sous-réseau de domaines Bridge.
- Annonce de route de transit.
- Importer et exporter le contrôle de routage.

Cette section traite des fuites de route en ce qui concerne les sorties L3 partagées dans les sections suivantes.

Workflow d'annonce de routage de domaine Bridge

Avant d'examiner le dépannage courant, l'utilisateur doit se familiariser avec le fonctionnement supposé de l'annonce de domaine Bridge.

L'annonce BD, lorsque le BD et L3Out sont dans le même VRF, implique :

- Avoir une relation contractuelle entre L3Out et l'EPG interne.
- Association de L3Out au domaine Bridge.
- Sélection de « Annonce externe » sur le sous-réseau BD.

En outre, il est également possible de contrôler l'annonce de domaine de pont à l'aide de profils de routage d'exportation, ce qui évite d'avoir à associer le L3Out. Cependant, vous devez toujours sélectionner « Annoncer en externe ». Il s'agit d'un cas d'utilisation moins courant, il ne sera donc pas discuté ici.

La relation contractuelle entre L3Out et l'EPG est nécessaire pour que la route statique omniprésente BD soit poussée vers le BL. L'annonce de route réelle est gérée par la redistribution de la route statique dans le protocole externe. Enfin, les route-maps de redistribution ne seront installées que dans les L3Out qui sont associés au BD. De cette manière, la route n'est pas annoncée sur toutes les sorties L3.

Dans ce cas, le sous-réseau BD est 192.168.1.0/24 et il doit être annoncé via OSPF L3Out.

Avant d'appliquer le contrat entre le L3Out et l'EPG interne

```
leaf103# show ip route 192.168.1.0/24 vrf Prod:Vrf1
IP Route Table for VRF "Prod:Vrf1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%' in via output denotes VRF
Route not found
```

Notez que la route BD n'est pas encore présente sur le BL.

Après l'application du contrat entre le L3Out et l'EPG interne

Àce stade, aucune autre configuration n'a été effectuée. L3Out n'est pas encore associé au BD et l'indicateur 'Annoncer en externe' n'est pas défini.

```
leaf103# show ip route 10.0.1.0/24 vrf Prod:Vrf1
IP Route Table for VRF "Prod:Vrf1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%' in via output denotes VRF
192.168.1.0/24, ubest/mbest: 1/0, attached, direct, pervasive
   *via 10.0.120.34%overlay-1, [1/0], 00:00:08, static, tag 4294967294
        recursive next hop: 10.0.120.34/32%overlay-1
```

Notez que la route de sous-réseau BD (indiquée par l'indicateur omniprésent) est désormais déployée sur la liste de contrôle d'accès. Notez toutefois que la route est étiquetée. Cette valeur de balise est une valeur implicite attribuée aux routes BD avant d'être configurée avec 'Annoncer en externe'. Tous les protocoles externes refusent la redistribution de cette balise.

Après avoir sélectionné « Annoncer en externe » sur le sous-réseau BD

L3Out n'a toujours pas été associé au BD. Cependant, notez que la balise a été effacée.

```
leaf103# show ip route 192.168.1.0/24 vrf Prod:Vrf1
IP Route Table for VRF "Prod:Vrf1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%' in via output denotes VRF
192.168.1.0/24, ubest/mbest: 1/0, attached, direct, pervasive *via 10.0.120.34%overlay-1, [1/0],
00:00:06, static recursive next hop: 10.0.120.34/32%overlay-1
```

Àce stade, la route n'est toujours pas annoncée de manière externe, car il n'y a pas de route-map et de prefix-list correspondant à ce préfixe pour la redistribution dans le protocole externe. Vous pouvez le vérifier à l'aide des commandes suivantes :

```
leaf103# show ip ospf vrf Prod:Vrf1
Routing Process default with ID 10.0.0.3 VRF Prod:Vrf1
Stateful High Availability enabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
Table-map using route-map exp-ctx-2392068-deny-external-tag
Redistributing External Routes from
  static route-map exp-ctx-st-2392068
  direct route-map exp-ctx-st-2392068
  bgp route-map exp-ctx-proto-2392068
  eigrp route-map exp-ctx-proto-2392068
  coop route-map exp-ctx-st-2392068
```

La route BD est programmée en tant que route statique. Vérifiez donc la route-map de redistribution statique en exécutant « show route-map <route-map name> » puis « show ip prefix-list <name> » sur toutes les listes de préfixes présentes dans la route-map. Effectuez cette opération à l'étape suivante.

Après association de L3Out à la BD

Comme mentionné précédemment, cette étape aboutit à la liste de préfixes qui correspond au sous-réseau BD installé dans la route-map de redistribution statique vers protocole externe.

```
leaf103# show route-map exp-ctx-st-2392068
route-map exp-ctx-st-2392068, deny, sequence 1
 Match clauses:
   tag: 4294967294
 Set clauses:

...
route-map exp-ctx-st-2392068, permit, sequence 15803
 Match clauses:
   ip address prefix-lists: IPv4-st16390-2392068-exc-int-inferred-export-dst
   ipv6 address prefix-lists: IPv6-deny-all
 Set clauses:
   tag 0
```

Vérifiez la liste de préfixes :

```
leaf103# show ip prefix-list IPv4-st16390-2392068-exc-int-inferred-export-dst
ip prefix-list IPv4-st16390-2392068-exc-int-inferred-export-dst: 1 entries
```

```
  seq 1 permit 192.168.1.1/24
```

Le sous-réseau BD est mis en correspondance pour être redistribué dans OSPF.

Àce stade, le workflow de configuration et de vérification est terminé pour l'annonce du sous-réseau BD à partir de L3Out. Passé ce point, la vérification serait spécifique au protocole. Par exemple :

- Pour le protocole EIGRP, vérifiez que la route est installée dans la table topologique avec la commande « show ip eigrp topology vrf **<name>** »
- Pour OSPF, vérifiez que la route est installée dans la table de base de données en tant que LSA externe avec « show ip ospf database vrf **<name>** »
- Pour BGP, vérifiez que la route se trouve dans le RIB BGP avec « show bgp ipv4 unicast vrf **<name>** »

Annonce de route BGP

Pour BGP, toutes les routes statiques sont implicitement autorisées pour la redistribution. La route-map qui correspond au sous-réseau BD est appliquée au niveau du voisin BGP.

```
leaf103# show bgp ipv4 unicast neighbor 10.0.0.134 vrf Prod:Vrf1 | grep Outbound
 Outbound route-map configured is exp-l3out-BGP-peer-2392068, handle obtained
```

Dans l'exemple ci-dessus, 10.0.0.134 est le voisin BGP configuré dans L3Out.

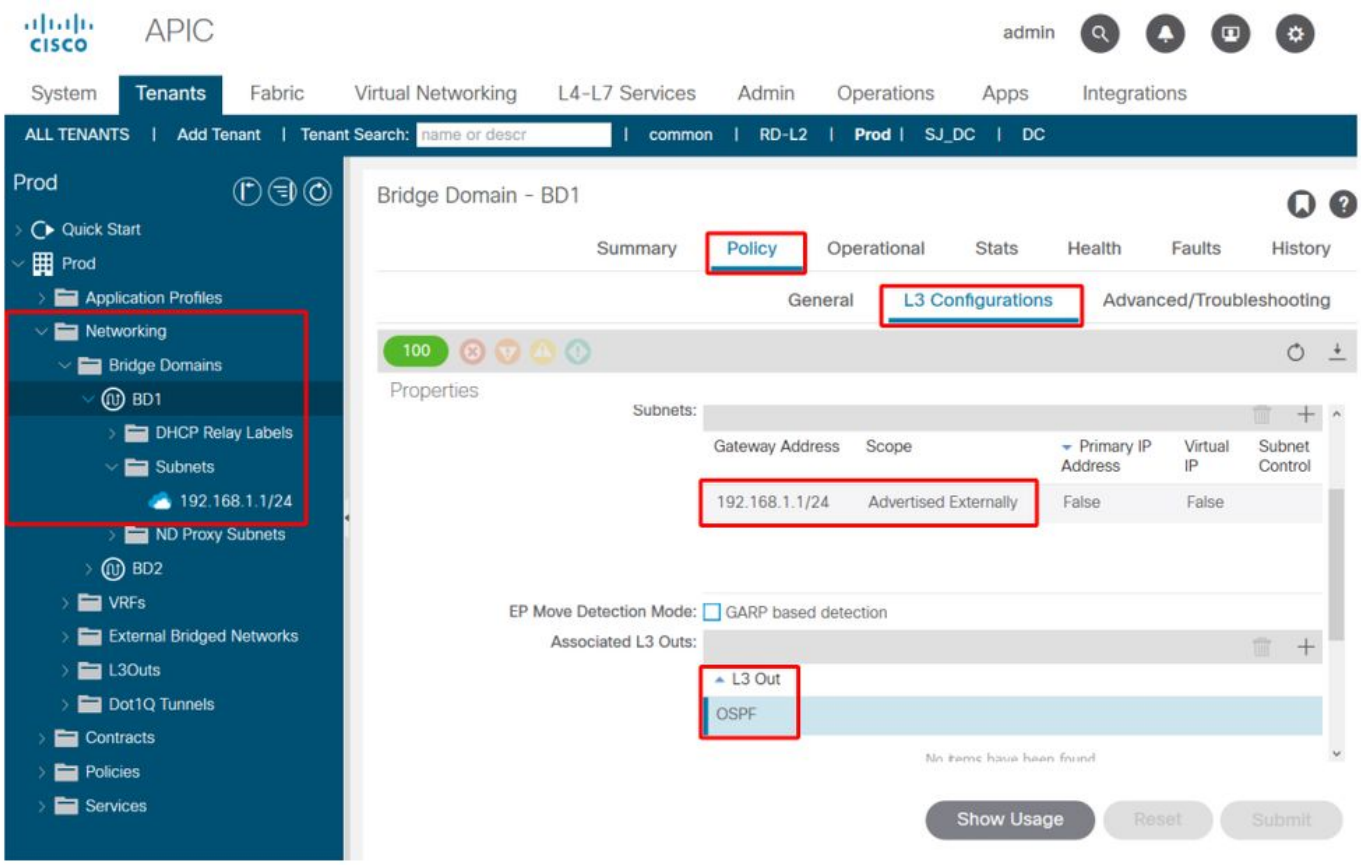
Annonce de route EIGRP

Comme le protocole OSPF, une route-map est utilisée pour contrôler la redistribution statique vers EIGRP. De cette façon, seuls les sous-réseaux associés à L3Out et définis sur 'Advertise Externally' doivent être redistribués. Ceci peut être vérifié avec cette commande :

```
leaf103# show ip eigrp vrf Prod:Vrf1
IP-EIGRP AS 100 ID 10.0.0.3 VRF Prod:Vrf1
 Process-tag: default
 Instance Number: 1
 Status: running
 Authentication mode: none
 Authentication key-chain: none
 Metric weights: K1=1 K2=0 K3=1 K4=0 K5=0
 metric version: 32bit
 IP proto: 88 Multicast group: 224.0.0.10
 Int distance: 90 Ext distance: 170
 Max paths: 8
 Active Interval: 3 minute(s)
 Number of EIGRP interfaces: 1 (0 loopbacks)
 Number of EIGRP passive interfaces: 0
 Number of EIGRP peers: 2
 Redistributing:
   static route-map exp-ctx-st-2392068
   ospf-default route-map exp-ctx-proto-2392068
   direct route-map exp-ctx-st-2392068
   coop route-map exp-ctx-st-2392068
   bgp-65001 route-map exp-ctx-proto-2392068
```

La configuration finale du BD est présentée ci-dessous.

Configuration de Bridge Domain L3



Scénario de dépannage d'annonce de route de domaine Bridge

Dans ce cas, le symptôme typique serait normalement qu'un sous-réseau BD configuré n'est pas annoncé à partir d'un L3Out. Suivez le workflow précédent pour comprendre quel composant est cassé.

Commencez par la configuration avant d'obtenir un niveau trop bas en vérifiant les éléments suivants :

- Existe-t-il un contrat entre l'EPG et L3Out ?
- L3Out est-il associé au BD ?
- Le sous-réseau BD est-il configuré pour annoncer en externe ?
- La contiguïté de protocole externe est-elle activée ?

Cause possible: BD non déployé

Ce cas serait applicable dans deux scénarios différents, tels que :

- L'EPG interne utilise l'intégration VMM avec l'option On Demand et aucun terminal de VM n'a été connecté au groupe de ports pour l'EPG.
- L'EPG interne a été créé mais aucune liaison de chemin statique n'a été configurée ou l'interface sur laquelle le chemin statique est configuré est désactivée.

Dans les deux cas, le BD ne serait pas déployé et, par conséquent, la route statique BD ne serait pas poussée vers le BL. La solution consiste ici à déployer certaines ressources actives dans un

EPG qui est lié à ce BD afin que le sous-réseau soit déployé.

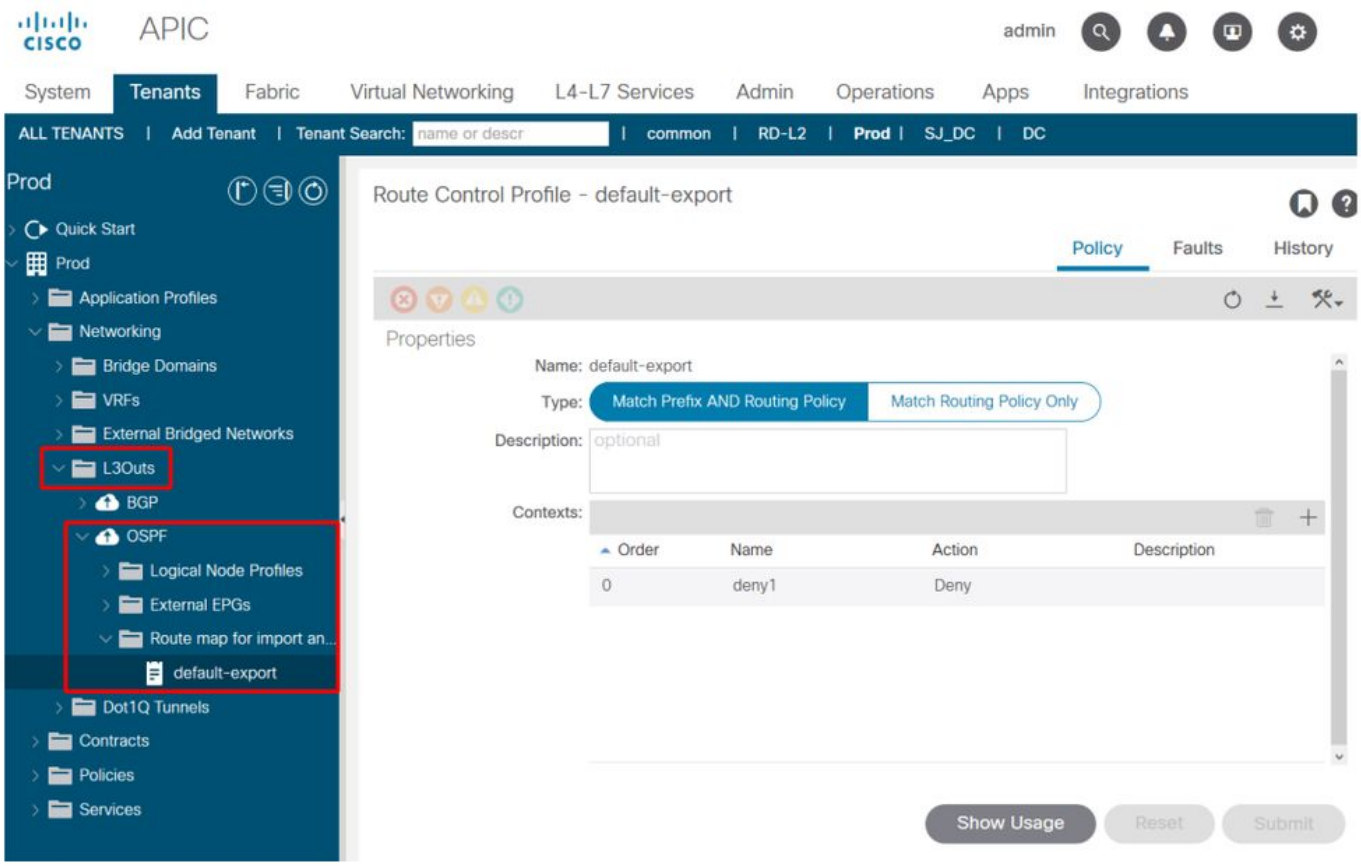
Cause possible: OSPF L3Out est configuré comme « Stub » ou « NSSA » sans redistribution

Lorsque le protocole OSPF est utilisé comme protocole L3Out, les règles OSPF de base doivent toujours être respectées. Les zones d'extrémité n'autorisent pas les LSA redistribuées, mais peuvent annoncer une route par défaut à la place. Les zones NSSA autorisent les chemins redistribués, mais vous devez sélectionner l'option Envoyer les LSA redistribuées dans la zone NSSA dans L3Out. Ou NSSA peut également annoncer une route par défaut à la place en désactivant 'Originate Summary LSA' ainsi qui est un scénario typique où 'Send Redistribute LSA's into NSSA Area' serait désactivé.

Cause possible: Route-Profile 'Default-Export' avec une action 'Deny' configurée sous L3Out

Lorsque des profils de routage sont configurés sous une L3Out avec les noms « default-export » ou « default-import », ils sont implicitement appliqués à L3Out. En outre, si le profil de route d'exportation par défaut est défini sur une action de refus et configuré en tant que 'Préfixe de correspondance et stratégie de routage', les sous-réseaux BD doivent être annoncés à partir de cette L3Out et seraient implicitement refusés :

Profil de routage de refus d'exportation par défaut



Les correspondances de préfixe dans le profil de routage d'exportation par défaut n'incluent pas implicitement les sous-réseaux BD si l'option 'Correspondance de la politique de routage uniquement' est sélectionnée.

Workflow d'importation de route externe

Cette section explique comment l'ACI apprend les routes externes via une L3Out et les distribue aux noeuds leaf internes. Elle couvre également les cas d'utilisation de transit et de fuite de route dans les sections ultérieures

Comme dans la section précédente, l'utilisateur doit être conscient de ce qui se passe à un niveau supérieur.

Par défaut, toutes les routes apprises via le protocole externe sont redistribuées dans le processus BGP de fabric interne. Cela est vrai quels que soient les sous-réseaux configurés sous l'EPG externe et les indicateurs sélectionnés. Il y a deux exemples où ce n'est pas vrai.

- Si l'option « Application du contrôle de route » au niveau supérieur de la stratégie L3Out est définie sur « Importer ». Dans ce cas, le modèle d'importation de route passerait d'un modèle de liste de blocage (ne spécifiez que ce qui ne devrait pas être autorisé) à un modèle de liste d'autorisation (tout est implicitement refusé sauf s'il est configuré autrement).
- Si le protocole externe est EIGRP ou OSPF et qu'un profil de routage d'interfuite utilisé ne correspond pas aux routes externes.

Pour qu'une route externe soit distribuée à un noeud terminal interne, les événements suivants doivent se produire :

- La route doit être apprise sur le BL à partir du routeur externe. Pour être un candidat à la redistribution dans le processus MP-BGP de fabric, la route doit être installée dans la table de routage plutôt que simplement dans le RIB de protocole.
- La route doit être autorisée à être redistribuée ou annoncée dans le processus BGP interne. Cela devrait toujours se produire sauf si l'application du contrôle de route d'importation ou un profil de route d'interfuite est utilisé.
- Une politique de réflecteur de route BGP doit être configurée et appliquée à un groupe de politiques de pod qui est appliqué au profil de pod. Si cela n'est pas appliqué, le processus BGP ne s'initialisera pas sur les commutateurs.

Si l'EPG/BD interne se trouve dans le même VRF que l'interface L3Out, les trois étapes ci-dessus sont tout ce qui est nécessaire pour que l'EPG/BD interne utilise des routes externes.

La route est installée dans la table de routage BL

Dans ce cas, la route externe qui doit être apprise sur les BL 103 et 104 est 172.16.20.1/32.

```
leaf103# show ip route 172.16.20.1 vrf Prod:Vrf1
IP Route Table for VRF "Prod:Vrf1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%' in via output denotes VRF

172.16.20.1/32, ubest/mbest: 1/0
    *via 10.10.34.3, vlan347, [110/20], 00:06:29, ospf-default, type-2
```

Il est évident qu'elle est installée dans la table de routage comme étant apprise via OSPF. Si ce n'est pas le cas, vérifiez le protocole individuel et assurez-vous que les contiguïtés sont actives. La route est redistribuée dans BGP La route-map de redistribution peut être vérifiée, après vérification que ni l'application 'Import' ni les profils de route d'interfuite ne sont utilisés, en regardant la route-map utilisée pour le protocole externe à la redistribution BGP. Reportez-vous à

la commande suivante :

```
leaf103# show bgp process vrf Prod:Vrf1

Information regarding configured VRFs:

BGP Information for VRF Prod:Vrf1
VRF Type                        : System
VRF Id                          : 85
VRF state                       : UP
VRF configured                  : yes
VRF refcount                    : 1
VRF VNID                        : 2392068
Router-ID                       : 10.0.0.3
Configured Router-ID            : 10.0.0.3
Confed-ID                       : 0
Cluster-ID                      : 0.0.0.0
MSITE Cluster-ID                : 0.0.0.0
No. of configured peers         : 1
No. of pending config peers     : 0
No. of established peers        : 1
VRF RD                          : 101:2392068
VRF EVPN RD                     : 101:2392068
...
    Redistribution
        direct, route-map permit-all
        static, route-map imp-ctx-bgp-st-interleak-2392068
        ospf, route-map permit-all
        coop, route-map exp-ctx-st-2392068
        eigrp, route-map permit-all
```

Ici, il est évident que la route-map « permit-all » est utilisée pour la redistribution OSPF vers BGP. Il s'agit de la configuration par défaut. De là, BL peut être vérifié et la route locale provenant de BGP vérifiée :

```
a-leaf101# show bgp ipv4 unicast 172.16.20.1/32 vrf Prod:Vrf1
BGP routing table information for VRF Prod:Vrf1, address family IPv4 Unicast
BGP routing table entry for 172.16.20.1/32, version 25 dest ptr 0xa6f25ad0
Paths: (2 available, best #2)
Flags: (0x80c0002 00000000) on xmit-list, is not in urib, exported
  vpn: version 16316, (0x100002) on xmit-list
Multipath: eBGP iBGP


  Advertised path-id 1, VPN AF advertised path-id 1
  Path type: redist 0x408 0x1 ref 0 adv path ref 2, path is valid, is best path
  AS-Path: NONE, path locally originated
    0.0.0.0 (metric 0) from 0.0.0.0 (10.0.0.3)
      Origin incomplete, MED 20, localpref 100, weight 32768
      Extcommunity:
          RT:65001:2392068
          VNID:2392068
          COST:pre-bestpath:162:110

  VRF advertise information:
  Path-id 1 not advertised to any peer

  VPN AF advertise information:
  Path-id 1 advertised to peers:
    10.0.64.64         10.0.72.66
```

```
  Path-id 2 not advertised to any peer
```

Dans le résultat ci-dessus, le 0.0.0.0/0 indique qu'il provient localement. La liste des homologues annoncés est constituée des noeuds spine du fabric qui agissent en tant que réflecteurs de route.

Vérifier la route sur le leaf interne

Le BL doit l'annoncer aux noeuds spine via la famille d'adresses BGP VPNv4. Les noeuds spine doivent l'annoncer à tous les noeuds leaf avec le VRF déployé (vrai de l'exemple de non-fuite de route). Sur l'un de ces noeuds leaf, exécutez « show bgp vpnv4 unicast <route> vrf overlay-1 » pour vérifier qu'il se trouve dans VPNv4

Utilisez la commande ci-dessous pour vérifier la route sur le leaf interne.

```
leaf101# show ip route 172.16.20.1 vrf Prod:Vrf1
IP Route Table for VRF "Prod:Vrf1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%' in via output denotes VRF

172.16.20.1/32, ubest/mbest: 2/0
    *via 10.0.72.64%overlay-1, [200/20], 00:21:24, bgp-65001, internal, tag 65001
         recursive next hop: 10.0.72.64/32%overlay-1
    *via 10.0.72.67%overlay-1, [200/20], 00:21:24, bgp-65001, internal, tag 65001
         recursive next hop: 10.0.72.67/32%overlay-1
```

Dans le résultat ci-dessus, la route est apprise via BGP et les sauts suivants doivent être les TEP physiques (PTEP) des BL.

```
leaf101# acidiag fnvread
      ID   Pod ID                 Name    Serial Number         IP Address    Role        State
LastUpdMsgId
-------------------------------------------------------------------------------------------
--------------
     103        1            a-leaf101      FDO20160TPS      10.0.72.67/32    leaf
active   0
     104        1            a-leaf103      FDO20160TQ0      10.0.72.64/32    leaf
active   0
```

Scénario de dépannage de route externe

Dans ce scénario, le leaf interne (101) ne reçoit pas de route externe.

Comme toujours, vérifiez d'abord les bases. Assurez-vous que :

- Les contiguïtés de protocole de routage sont actives sur les listes de contrôle d’accès.
- Une politique de réflecteur de route BGP est appliquée au groupe de politiques Pod et au profil Pod.

Si les critères ci-dessus sont corrects, vous trouverez ci-dessous des exemples plus avancés de

ce qui pourrait être à l'origine du problème.

Cause possible: VRF non déployé sur le leaf interne

Dans ce cas, le problème serait qu'il n'y a pas d'EPG avec des ressources déployées sur le leaf interne où la route externe est attendue. Cela peut être dû à des liaisons de chemins statiques configurées uniquement sur les interfaces hors service ou à la présence d'EPG intégrés VMM en mode à la demande, sans pièces jointes dynamiques détectées.

Étant donné que le VRF L3Out n'est pas déployé sur le leaf interne (vérifiez avec « show vrf » sur le leaf interne), le leaf interne n'importera pas la route BGP depuis VPNv4.

Pour résoudre ce problème, l'utilisateur doit déployer des ressources dans le VRF L3Out sur le leaf interne.

Cause possible: L'application de routage d'importation est utilisée

Comme mentionné précédemment, lorsque l'application du contrôle de route d'importation est activée, L3Out accepte uniquement les routes externes qui sont explicitement autorisées. Généralement, la fonctionnalité est implémentée sous la forme d'une table-map. Une table-map se trouve entre le RIB de protocole et la table de routage réelle, de sorte qu'elle affecte uniquement ce qui se trouve dans la table de routage.

Dans la sortie ci-dessous, le contrôle de route d'importation est activé, mais il n'y a pas de routes explicitement autorisées. Notez que la LSA se trouve dans la base de données OSPF, mais pas dans la table de routage de la BL :

```
leaf103# vsh -c "show ip ospf database external 172.16.20.1 vrf Prod:Vrf1"
        OSPF Router with ID (10.0.0.3) (Process ID default VRF Prod:Vrf1)

                Type-5 AS External Link States

Link ID         ADV Router      Age         Seq#       Checksum Tag
172.16.20.1     10.0.0.134      455         0x80000003 0xb9a0    0


leaf103# show ip route 172.16.20.1 vrf Prod:Vrf1
IP Route Table for VRF "Prod:Vrf1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%' in via output denotes VRF

Route not found
```

Voici la table-map qui est maintenant installée et qui provoque ce comportement :

```
leaf103# show ip ospf vrf Prod:Vrf1

 Routing Process default with ID 10.0.0.3 VRF Prod:Vrf1
 Stateful High Availability enabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Table-map using route-map exp-ctx-2392068-deny-external-tag
 Redistributing External Routes from..
```

```
leaf103# show route-map exp-ctx-2392068-deny-external-tag
route-map exp-ctx-2392068-deny-external-tag, deny, sequence 1
  Match clauses:
    tag: 4294967295
  Set clauses:
route-map exp-ctx-2392068-deny-external-tag, deny, sequence 19999
  Match clauses:
    ospf-area: 0.0.0.100
  Set clauses:
```

Tout apprentissage dans la zone 100, qui est la zone configurée sur cette L3Out, est implicitement refusé par cette table-map afin qu'il ne soit pas installé dans la table de routage.

Pour résoudre ce problème, l'utilisateur doit définir le sous-réseau sur l'EPG externe avec l'indicateur « Import Route Control Subnet » ou créer un profil d'importation de route correspondant aux préfixes à installer.

- Notez que l'application des importations n'est pas prise en charge pour EIGRP.
- Notez également que pour BGP, l'application d'importation est implémentée en tant que route-map entrante appliquée au voisin BGP. Consultez la sous-section « Annonce de route BGP » pour plus de détails sur la façon de vérifier cela.

Cause possible: un profil de fuite intermédiaire est utilisé

Les Interleak Route-Profiles sont utilisés pour les sorties L3 EIGRP et OSPF et sont destinés à permettre le contrôle de ce qui est redistribué de l'IGP dans BGP, ainsi qu'à permettre l'application d'une stratégie telle que la définition des attributs BGP.

Sans un profil de routage d'interfuite, toutes les routes sont implicitement importées dans BGP.

Sans profil de routage d'interfuite :

```
leaf103# show bgp process vrf Prod:Vrf1

Information regarding configured VRFs:

BGP Information for VRF Prod:Vrf1
VRF Type                        : System
VRF Id                          : 85
VRF state                       : UP
VRF configured                  : yes
VRF refcount                    : 1
VRF VNID                        : 2392068
Router-ID                       : 10.0.0.3
Configured Router-ID            : 10.0.0.3
Confed-ID                       : 0
Cluster-ID                      : 0.0.0.0
MSITE Cluster-ID                : 0.0.0.0
No. of configured peers         : 1
No. of pending config peers     : 0
No. of established peers        : 1
VRF RD                          : 101:2392068
VRF EVPN RD                     : 101:2392068

...
    Peers      Active-peers    Routes     Paths      Networks   Aggregates
    1          1               7          11         0          0
```

```
    Redistribution
        direct, route-map permit-all
        static, route-map imp-ctx-bgp-st-interleak-2392068
        ospf, route-map permit-all
        coop, route-map exp-ctx-st-2392068
        eigrp, route-map permit-all
```

Avec un profil de routage d'interfuite :

```
a-leaf103# show bgp process vrf Prod:Vrf1

Information regarding configured VRFs:

BGP Information for VRF Prod:Vrf1
VRF Type                        : System
VRF Id                          : 85
VRF state                       : UP
VRF configured                  : yes
VRF refcount                    : 1
VRF VNID                        : 2392068
Router-ID                       : 10.0.0.3
Configured Router-ID            : 10.0.0.3
Confed-ID                       : 0
Cluster-ID                      : 0.0.0.0
MSITE Cluster-ID                : 0.0.0.0
No. of configured peers         : 1
No. of pending config peers     : 0
No. of established peers        : 1
VRF RD                          : 101:2392068
VRF EVPN RD                     : 101:2392068

...

    Redistribution
        direct, route-map permit-all
        static, route-map imp-ctx-bgp-st-interleak-2392068
        ospf, route-map imp-ctx-proto-interleak-2392068
        coop, route-map exp-ctx-st-2392068
        eigrp, route-map permit-all
```

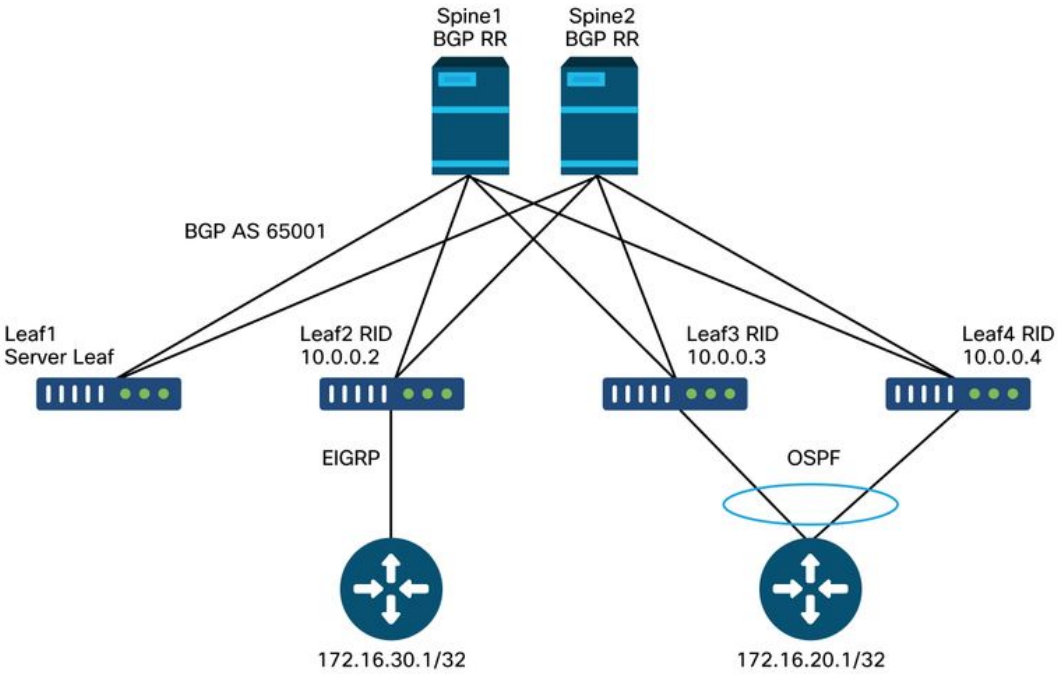
La route-map mise en surbrillance ci-dessus n'autoriserait que ce qui correspond explicitement dans le profil de fuite inter-réseau configuré. Si la route externe ne correspond pas, elle ne sera pas redistribuée dans BGP.

Workflow d'annonce de route de transit

Cette section explique comment les routes d'une L3Out sont annoncées à une autre L3Out. Cela couvrirait également le scénario dans lequel les routes statiques qui sont configurées directement sur une L3Out doivent être annoncées. Elle ne traite pas de chaque protocole spécifique, mais de la manière dont il est mis en oeuvre dans l'ACI. Il ne sera pas utilisé dans le routage de transit inter-VRF pour le moment.

Ce scénario utilise la topologie suivante :

Topologie de routage de transit



Le flux de haut niveau de la manière dont 172.16.20.1 serait appris à partir du protocole OSPF, puis annoncé dans le protocole EIGRP, et les vérifications de l'ensemble du processus et des scénarios de dépannage sont abordés ci-dessous.

Pour que la route 172.16.20.1 soit annoncée dans le protocole EIGRP, l'une des options suivantes doit être configurée :

- Le sous-réseau à annoncer a pu être défini sur l'EIGRP L3Out avec l'indicateur « Export Route-Control Subnet ». Comme indiqué dans la section Vue d'ensemble, cet indicateur est principalement utilisé pour le routage de transit et définit les sous-réseaux qui doivent être annoncés à partir de cette L3Out.
- Configurez 0.0.0.0/0 et sélectionnez « Aggregate Export » et « Export Route Control Subnet ». Ceci crée une route-map pour la redistribution dans le protocole externe qui correspond à 0.0.0.0/0 et tous les préfixes qui sont plus spécifiques (ce qui est une correspondance effective avec tout). Notez que lorsque 0.0.0.0/0 est utilisé avec « Aggregate Export », les routes statiques ne seront pas mises en correspondance pour la redistribution. Cela permet d'empêcher la publicité par inadvertance de routes BD qui ne devraient pas être annoncées.
- Enfin, il est possible de créer un profil de route d'exportation qui correspond aux préfixes à annoncer. L'utilisation de cette méthode pourrait configurer l'option « Aggregate » avec des préfixes autres que 0.0.0.0/0.

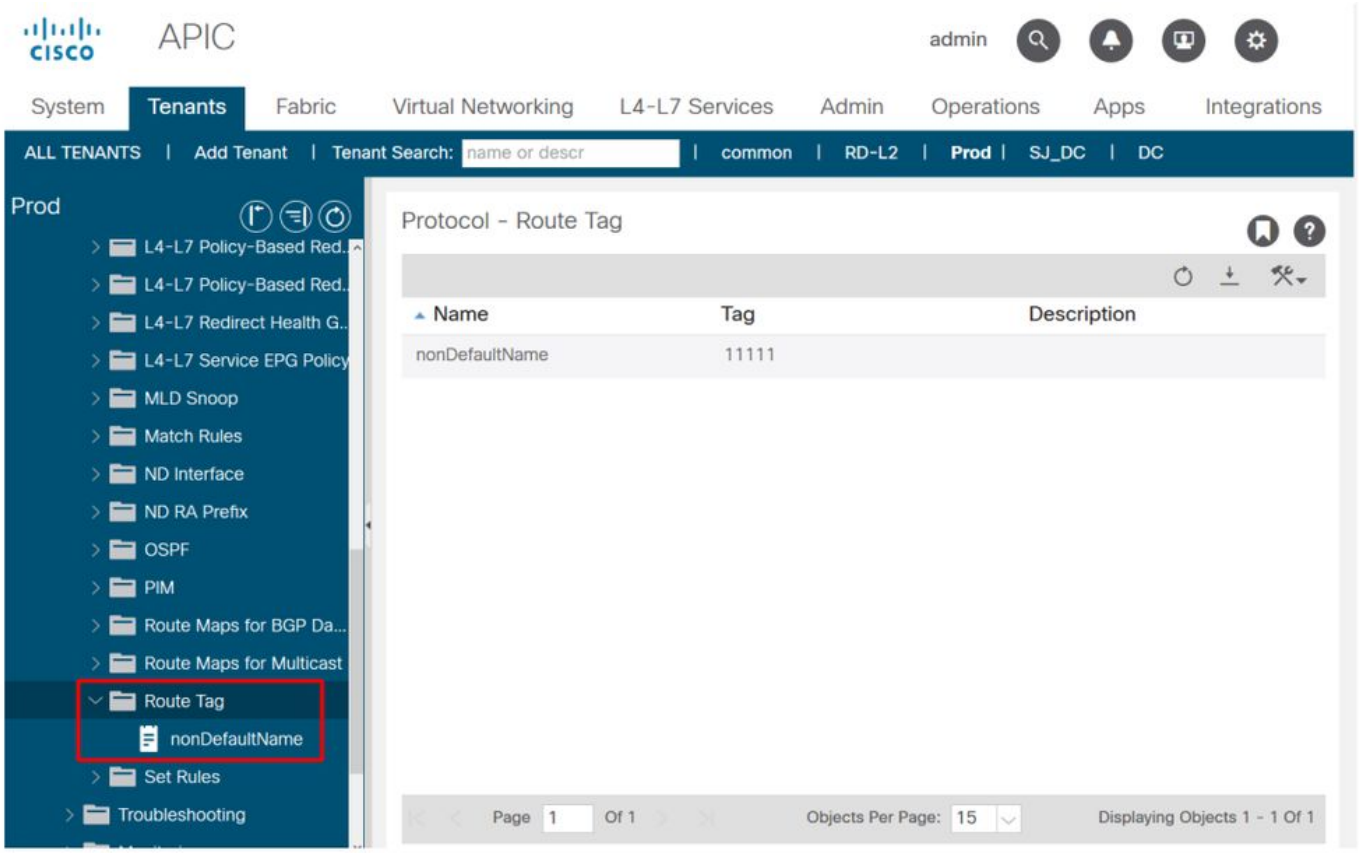
Les configurations ci-dessus entraîneraient l'annonce de la route de transit, mais une stratégie de sécurité doit toujours être en place pour permettre au trafic du plan de données de circuler. Comme pour toute communication EPG à EPG, un contrat doit être en place avant que le trafic soit autorisé.

> Notez que les sous-réseaux externes dupliqués avec le « Sous-réseau externe pour EPG externe » ne peuvent pas être configurés dans le même VRF. Une fois configurés, les sous-réseaux doivent être plus spécifiques que 0.0.0.0. Il est important de configurer « Sous-réseau externe pour EPG externe » uniquement pour l'interface L3Out où la route est reçue.

Ne configurez pas ce paramètre sur l'interface L3Out qui doit annoncer cette route.

Il est également important de comprendre que toutes les routes de transit sont étiquetées avec une étiquette VRF spécifique. Par défaut, cette balise est 4294967295. La stratégie Balise de routage est configurée sous 'Client > Mise en réseau > Protocoles > Balise de routage :

Politique de balise de route



Cette stratégie de balise de routage est ensuite appliquée au VRF. L'objectif de cette balise est essentiellement d'empêcher les boucles. Cette étiquette de route est appliquée lorsque la route de transit est annoncée à nouveau à partir d'une L3Out. Si ces routes sont alors reçues en retour avec la même étiquette de route, alors la route est abandonnée.

Vérifiez que la route est présente sur le BL récepteur via OSPF

Comme dans la dernière section, vérifiez d'abord que la liste de contrôle d'accès qui doit initialement recevoir la route correcte.

```
leaf103# show ip route 172.16.20.1 vrf Prod:Vrf1
IP Route Table for VRF "Prod:Vrf1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%' in via output denotes VRF

172.16.20.1/32, ubest/mbest: 1/0
    *via 10.10.34.3, vlan347, [110/20], 01:25:30, ospf-default, type-2
```

Pour l'instant, supposons que l'annonce L3Out se trouve sur un BL différent (comme dans la topologie) (les scénarios ultérieurs discuteront de son emplacement sur le même BL).

Vérifiez que la route est présente dans BGP sur le BL OSPF récepteur

Pour que la route OSPF soit annoncée au routeur EIGRP externe, elle doit être annoncée dans BGP sur la liste de contrôle d'accès OSPF réceptrice.

```
leaf103# show bgp ipv4 unicast 172.16.20.1/32 vrf Prod:Vrf1
BGP routing table information for VRF Prod:Vrf1, address family IPv4 Unicast
BGP routing table entry for 172.16.20.1/32, version 30 dest ptr 0xa6f25ad0
Paths: (2 available, best #1)
Flags: (0x80c0002 00000000) on xmit-list, is not in urib, exported
  vpn: version 17206, (0x100002) on xmit-list
Multipath: eBGP iBGP

  Advertised path-id 1, VPN AF advertised path-id 1
  Path type: redist 0x408 0x1 ref 0 adv path ref 2, path is valid, is best path
  AS-Path: NONE, path locally originated
    0.0.0.0 (metric 0) from 0.0.0.0 (10.0.0.3)
      Origin incomplete, MED 20, localpref 100, weight 32768
      Extcommunity:
          RT:65001:2392068
          VNID:2392068
          COST:pre-bestpath:162:110

  VRF advertise information:

  Path-id 1 not advertised to any peer

  VPN AF advertise information:
  Path-id 1 advertised to peers:
    10.0.64.64         10.0.72.66
  Path-id 2 not advertised to any peer
```

La route est en BGP.

Vérifiez sur la liste de contrôle d'accès EIGRP que doit annoncer la route qu'elle est installée

```
leaf102# show ip route 172.16.20.1 vrf Prod:Vrf1
IP Route Table for VRF "Prod:Vrf1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%' in via output denotes VRF

172.16.20.1/32, ubest/mbest: 2/0
    *via 10.0.72.67%overlay-1, [200/20], 00:56:46, bgp-65001, internal, tag 65001
         recursive next hop: 10.0.72.67/32%overlay-1
    *via 10.0.72.64%overlay-1, [200/20], 00:56:46, bgp-65001, internal, tag 65001
         recursive next hop: 10.0.72.64/32%overlay-1
```

Il est installé dans la table de routage avec des sauts suivants superposés pointant vers les noeuds leaf de bordure d'origine.

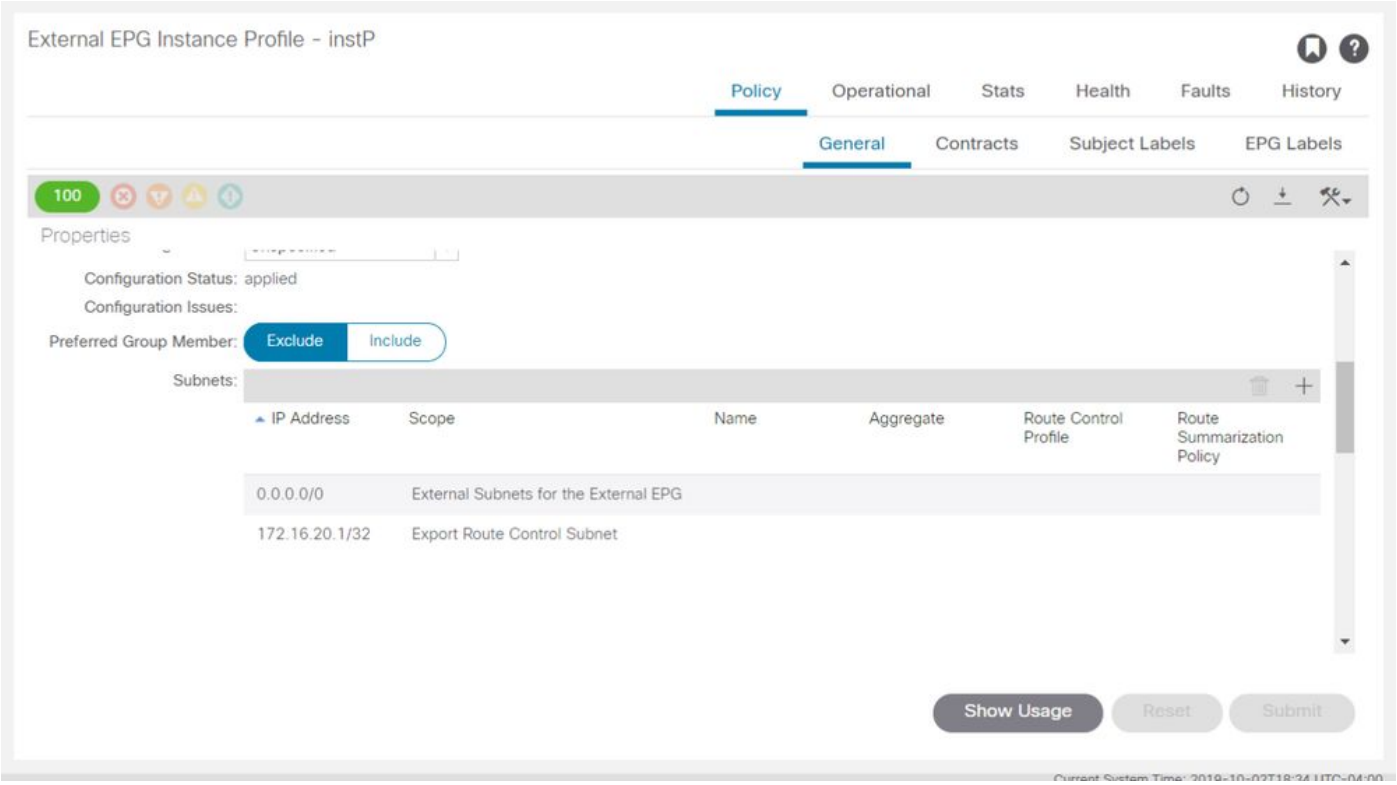
```
leaf102# acidiag fnvread

      ID   Pod ID                 Name    Serial Number         IP Address    Role        State
LastUpdMsgId
--------------------------------------------------------------------------------------------
```

```
--------------
     103        1            a-leaf101      FDO20160TPS      10.0.72.67/32    leaf
active   0
     104        1            a-leaf103      FDO20160TQ0      10.0.72.64/32    leaf
active   0
```

Vérifiez que la route est annoncée sur la liste de contrôle d'accès

La route sera annoncée par BL 102 suite à la définition de l'indicateur « Export Route Control Subnet » sur le sous-réseau configuré :

Exporter le contrôle de routage



Utilisez la commande suivante pour afficher la route-map créée à la suite de cet indicateur « Export Route Control » :

```
leaf102# show ip eigrp vrf Prod:Vrf1
IP-EIGRP AS 101 ID 10.0.0.2 VRF Prod:Vrf1
  Process-tag: default
  Instance Number: 1
  Status: running
  Authentication mode: none
  Authentication key-chain: none
  Metric weights: K1=1 K2=0 K3=1 K4=0 K5=0
  metric version: 32bit
  IP proto: 88 Multicast group: 224.0.0.10
  Int distance: 90 Ext distance: 170
  Max paths: 8
  Active Interval: 3 minute(s)
  Number of EIGRP interfaces: 1 (0 loopbacks)
  Number of EIGRP passive interfaces: 0
  Number of EIGRP peers: 1
  Redistributing:
    static route-map exp-ctx-st-2392068
```

```
    ospf-default route-map exp-ctx-proto-2392068
    direct route-map exp-ctx-st-2392068
    coop route-map exp-ctx-st-2392068
    bgp-65001 route-map exp-ctx-proto-2392068
```

Pour rechercher la 'redistribution BGP > EIGRP', consultez la route-map. Cependant, la route-map elle-même doit être identique, que le protocole source soit OSPF, EIGRP ou BGP. Les routes statiques seront contrôlées avec une route-map différente.

```
leaf102# show route-map exp-ctx-proto-2392068
route-map exp-ctx-proto-2392068, permit, sequence 15801
  Match clauses:
    ip address prefix-lists: IPv4-proto32771-2392068-exc-ext-inferred-export-dst
    ipv6 address prefix-lists: IPv6-deny-all
  Set clauses:
    tag 4294967295

a-leaf102# show ip prefix-list IPv4-proto32771-2392068-exc-ext-inferred-export-dst
ip prefix-list IPv4-proto32771-2392068-exc-ext-inferred-export-dst: 1 entries
   seq 1 permit 172.16.20.1/32
```

Dans le résultat ci-dessus, la balise VRF est définie sur ce préfixe pour la prévention des boucles et le sous-réseau configuré avec le contrôle de route d'exportation est explicitement mis en correspondance.

Routage de transit lors de la réception et de la publicité BL sont les mêmes

Comme nous l'avons vu précédemment, lorsque les BL de réception et d'annonce sont différents, la route doit être annoncée via le fabric à l'aide du protocole BGP. Lorsque les BL sont identiques, la redistribution ou l'annonce peut être effectuée directement entre les protocoles sur le leaf.

Vous trouverez ci-dessous de brèves descriptions de la mise en oeuvre :

- **Routage de transit entre deux sorties L3 OSPF sur le même leaf : l'**annonce de route est contrôlée via un 'filtre de zone' appliqué au niveau du processus OSPF. Une L3Out dans la zone 0 doit être déployée sur le leaf puisque les routes sont annoncées entre les zones plutôt que par redistribution. Utilisez « show ip ospf vrf <name> » pour afficher la liste de filtres. Affichez le contenu du filtre à l'aide de la commande « show route-map <nom du filtre> ».
- **Routage de transit entre les sorties L3 OSPF et EIGRP sur le même noeud leaf : l'**annonce de route est contrôlée via des route-maps de redistribution qui peuvent être vues avec « show ip ospf » et « show ip eigrp ». Notez que si plusieurs L3Out OSPF existent sur la même BL, la seule façon de redistribuer dans un seul de ces L3Out OSPF est si l'autre est un Stub ou NSSA avec **'Send redistribute LSAs into NSSA area' désactivé afin** qu'il n'autorise aucune LSA externe.
- **Routage de transit entre OSPF ou EIGRP et BGP sur la même feuille :** l'annonce de route dans l'IGP est contrôlée via la redistribution route-maps. L'annonce de route dans BGP est contrôlée via une route-map sortante appliquée directement au voisin bgp que la route doit être envoyée. Ceci peut être vérifié avec « show bgp ipv4 unicast neighbor <adresse du voisin> vrf <nom> | grep Outbound'.
- **Routage de transit entre deux l3Out BGP sur le même leaf :** Toute annonce est contrôlée via des route-maps appliquées directement au voisin bgp auquel la route doit être envoyée. Ceci

peut être vérifié avec « show bgp ipv4 unicast neighbor <adresse du voisin> vrf <nom> | grep Outbound'.

Scénarios de dépannage du routage de transit #1 : Route de transit non annoncée

Ce scénario de dépannage implique que les routes qui doivent être apprises par une L3Out ne sont pas envoyées par l'autre L3Out.

Comme toujours, vérifiez les bases avant d'examiner tout ce qui concerne l'ACI.

- Les contiguïtés de protocole sont-elles activées ?
- La route, que l'ACI doit annoncer, est-elle apprise d'un protocole externe ?
- Pour BGP, le chemin est-il abandonné en raison d'un attribut BGP ? (as-path, etc.).
- La couche 3 sortante réceptrice l'a-t-elle dans la base de données OSPF, la table topologique EIGRP ou la table BGP ?
- Une stratégie de réflecteur de route BGP est-elle appliquée au groupe de stratégies Pod appliqué au profil Pod ?

Si toutes les vérifications de protocole de base sont configurées correctement, voici quelques autres causes courantes d'une route de transit qui n'est pas annoncée.

Cause possible: Aucune zone OSPF 0

Si la topologie affectée implique deux sorties L3 OSP sur la même feuille de périphérie, alors il doit y avoir une zone 0 pour que les routes soient annoncées d'une zone à une autre. Consultez la puce « Routage de transit entre deux sorties L3 OSPF sur la même feuille » ci-dessus pour plus de détails.

Cause possible: La zone OSPF est stub ou NSSA

Cela se produirait si l'OSPF L3Out est configuré avec une zone Stub ou NSSA qui n'est pas configurée pour annoncer les LSA externes. Avec OSPF, les LSA externes ne sont jamais annoncées dans les zones de stub. Ils sont annoncés dans les zones NSSA si l'option « Envoyer les LSA redistribuées dans la zone NSSA » est sélectionnée.

Scénarios de dépannage du routage de transit #2 : Route de transit non reçue

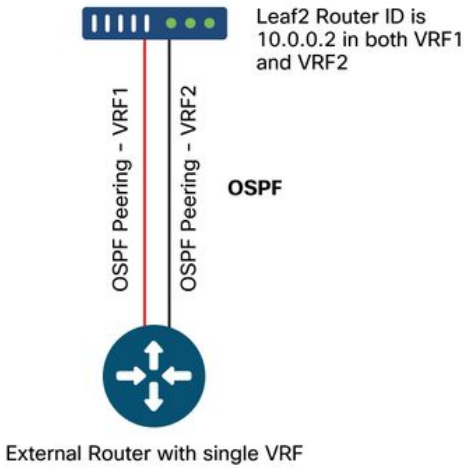
Dans ce scénario, le problème est que certaines routes annoncées par une L3Out ACI ne sont pas reçues en retour dans une autre L3Out. Ce scénario peut être applicable si les sorties L3 se trouvent dans deux fabrics séparés et sont connectées par des routeurs externes ou si les sorties L3 se trouvent dans des VRF différents et que les routes sont transmises entre les VRF par un routeur externe.

Cause possible: BL est configuré avec le même ID de routeur dans plusieurs VRF

Du point de vue de la configuration, un ID de routeur ne peut pas être dupliqué dans le même VRF. Cependant, il est généralement acceptable d'utiliser le même ID de routeur dans différents VRF tant que les deux VRF ne sont pas attachés aux mêmes domaines de protocole de routage.

Examinez la topologie suivante :

Routeur externe avec VRF unique - Route de transit non reçue



Le problème ici serait que le leaf ACI voit des LSA avec son propre ID de routeur en cours de réception, ce qui a pour conséquence qu'elles ne sont pas installées dans la base de données OSPF.

En outre, si la même configuration était observée avec les paires VPC, les LSA seraient ajoutées et supprimées en permanence sur certains routeurs. Par exemple, le routeur verrait les LSA provenant de son homologue VPC avec VRF et les LSA provenant du même noeud (avec le même ID de routeur) provenant de l'autre VRF.

Pour résoudre ce problème, l'utilisateur doit s'assurer qu'un noeud aura un ID de routeur différent et unique dans chaque VRF dans lequel il a un L3Out.

Cause possible: Routes d'un L3Out dans un fabric ACI reçues sur un autre fabric avec la même étiquette VRF

La route-tag par défaut dans l'ACI est toujours la même, sauf si elle est modifiée. Si des routes sont annoncées d'un L3Out dans un fabric VRF ou ACI à un autre L3Out dans un autre fabric VRF ou ACI sans modifier les balises VRF par défaut, les routes sont abandonnées par les BL récepteurs.

La solution à ce scénario consiste simplement à utiliser une politique de balise de route unique pour chaque VRF dans l'ACI.

Scénarios de dépannage de routage de transit #3 — Annonce inattendue de routes de transit

Ce scénario se produit lorsque des routes de transit sont annoncées à partir d'une L3Out où elles ne sont pas destinées à être annoncées.

Cause possible: utilisation de 0.0.0.0/0 avec « Aggregate Export »

Lorsqu'un sous-réseau externe est configuré en tant que 0.0.0.0/0 avec « Export Route Control Subnet » et « Aggregate Export », le résultat est qu'une correspondance de tous les mappages de route de redistribution est installée. Dans ce cas, toutes les routes sur le BL qui ont été apprises via OSPF, EIGRP ou BGP sont annoncées sur le L3Out où ceci est configuré.

Voici la route-map déployée sur le noeud leaf à la suite de l'exportation d'agrégat :

```
leaf102# show ip eigrp vrf Prod:Vrf1
IP-EIGRP AS 101 ID 10.0.0.2 VRF Prod:Vrf1
 Process-tag: default
 Instance Number: 1
 Status: running
 Authentication mode: none
 Authentication key-chain: none
 Metric weights: K1=1 K2=0 K3=1 K4=0 K5=0
 metric version: 32bit
 IP proto: 88 Multicast group: 224.0.0.10
 Int distance: 90 Ext distance: 170
 Max paths: 8
 Active Interval: 3 minute(s)
 Number of EIGRP interfaces: 1 (0 loopbacks)
 Number of EIGRP passive interfaces: 0
 Number of EIGRP peers: 1
 Redistributing:
   static route-map exp-ctx-st-2392068
   ospf-default route-map exp-ctx-proto-2392068
   direct route-map exp-ctx-st-2392068
   coop route-map exp-ctx-st-2392068
   bgp-65001 route-map exp-ctx-proto-2392068
 Tablemap: route-map exp-ctx-2392068-deny-external-tag , filter-configured
 Graceful-Restart: Enabled
 Stub-Routing: Disabled
 NSF converge time limit/expiries: 120/0
 NSF route-hold time limit/expiries: 240/0
 NSF signal time limit/expiries: 20/0
 Redistributed max-prefix: Disabled
 selfAdvRtTag: 4294967295
leaf102# show route-map exp-ctx-proto-2392068
route-map exp-ctx-proto-2392068, permit, sequence 19801
 Match clauses:
   ip address prefix-lists: IPv4-proto32771-2392068-agg-ext-inferred-export-dst
   ipv6 address prefix-lists: IPv6-deny-all
 Set clauses:
   tag 4294967295



leaf102# show ip prefix-list IPv4-proto32771-2392068-agg-ext-inferred-export-dst
    ip prefix-list IPv4-proto32771-2392068-agg-ext-inferred-export-dst: 1 entries
seq 1 permit 0.0.0.0/0 le 32
```

Il s'agit de la première cause de boucles de routage impliquant un environnement ACI.

Contrat et L3Out

EPG basé sur préfixe sur L3Out

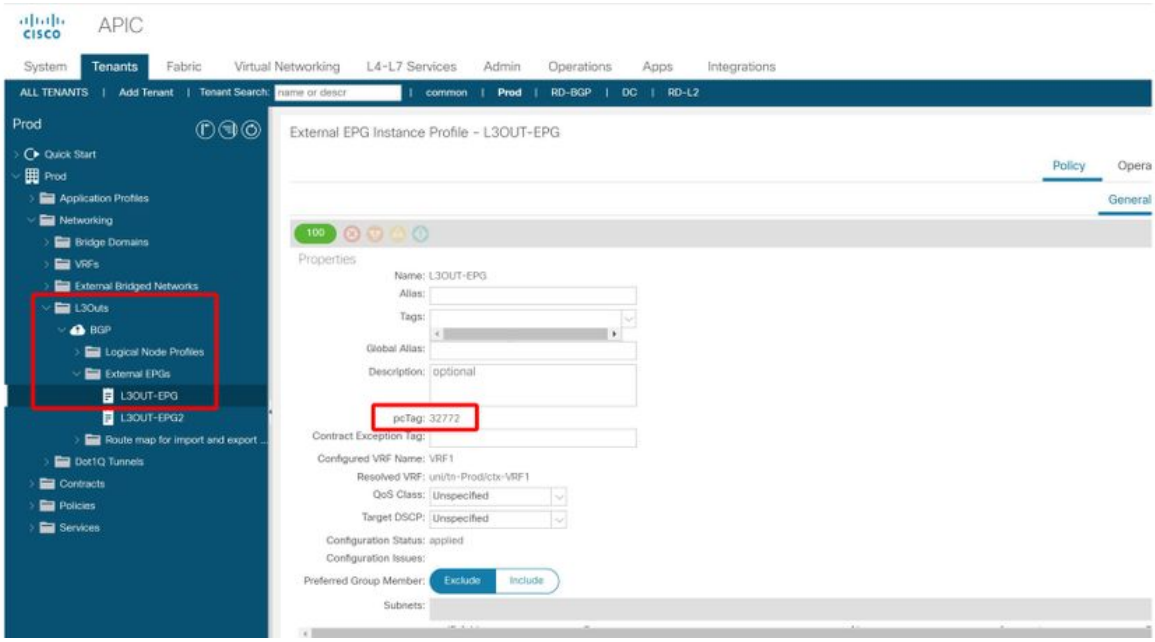
Dans un EPG interne (non-L3Out), les contrats sont appliqués après dérivation du pcTag de la source et du pcTag de l'EPG de destination. L'encapsulation VLAN/VXLAN du paquet reçu sur le port de liaison descendante est utilisée pour piloter ce pcTag en classant le paquet dans l'EPG. À chaque fois qu'il apprend une adresse MAC ou une adresse IP, il apprend avec son encapsulation d'accès et l'EPG pcTag associé. Pour plus de détails sur pcTag et l'application du contrat,

reportez-vous au chapitre « Politiques de sécurité ».

Les sorties L3out dirigent également un pcTag à l'aide de son EPG L3Out (EPG externe) situé sous 'Tenant > Networking > L3OUT > Networks > L3OUT-EPG'. Cependant, les sorties L3 ne dépendent pas des VLAN et des interfaces pour classer les paquets comme tels. La classification est plutôt basée sur le préfixe/sous-réseau source selon la méthode de « plus longue correspondance de préfixe ». Par conséquent, un EPG L3Out peut être appelé un **EPG basé sur** un **préfixe**. Une fois qu'un paquet est classé dans une L3Out basée sur un sous-réseau, il suit un modèle d'application de stratégie similaire à un EPG normal.

Le schéma suivant indique où se trouve le pcTag d'un EPG L3Out donné dans l'interface utilisateur graphique.

Emplacement du pcTag pour un L3Out



L'utilisateur est chargé de définir la table EPG basée sur les préfixes. Pour ce faire, utilisez la portée de sous-réseau « Sous-réseau externe pour EPG externe ». Chaque ensemble de sous-réseaux avec cette étendue ajoute une entrée dans une table LPM (Longest Prefix Match) statique. Ce sous-réseau pointe vers la valeur pcTag qui sera utilisée pour toute adresse IP appartenant à ce préfixe.

La table LPM des sous-réseaux EPG basés sur des préfixes peut être vérifiée sur les commutateurs Leaf à l'aide de la commande suivante :

```
vsh -c 'show system internal policy-mgr prefix'
```

Remarques:

- Les entrées de la table LPM sont étendues au VNID VRF. La recherche est effectuée par vrf_vnid/src pcTag/dst pcTag.
- Chaque entrée pointe vers un pcTag unique. Par conséquent, deux EPG L3Out ne peuvent pas utiliser le même sous-réseau avec la même longueur de masque dans le même VRF.
- Le sous-réseau 0.0.0.0/0 utilise toujours un pcTag 15 spécial. En tant que tel, il peut être dupliqué, mais il ne doit être effectué qu'avec une compréhension complète des implications

de l’application des politiques.
- Cette table est utilisée dans les deux sens. De L3Out à Leaf Local Endpoint, le pcTag source est dérivé à l'aide de cette table.De Leaf Local Endpoint à L3Out, le pcTag de destination est dérivé à l'aide de cette table.
- Si le VRF a le paramètre d'application « Ingress » pour « Policy Control Enforcement Direction », alors la table de préfixe LPM sera présente sur les BL L3Out ainsi que sur tous les commutateurs Leaf dans le VRF qui ont un contrat avec l'L3Out.

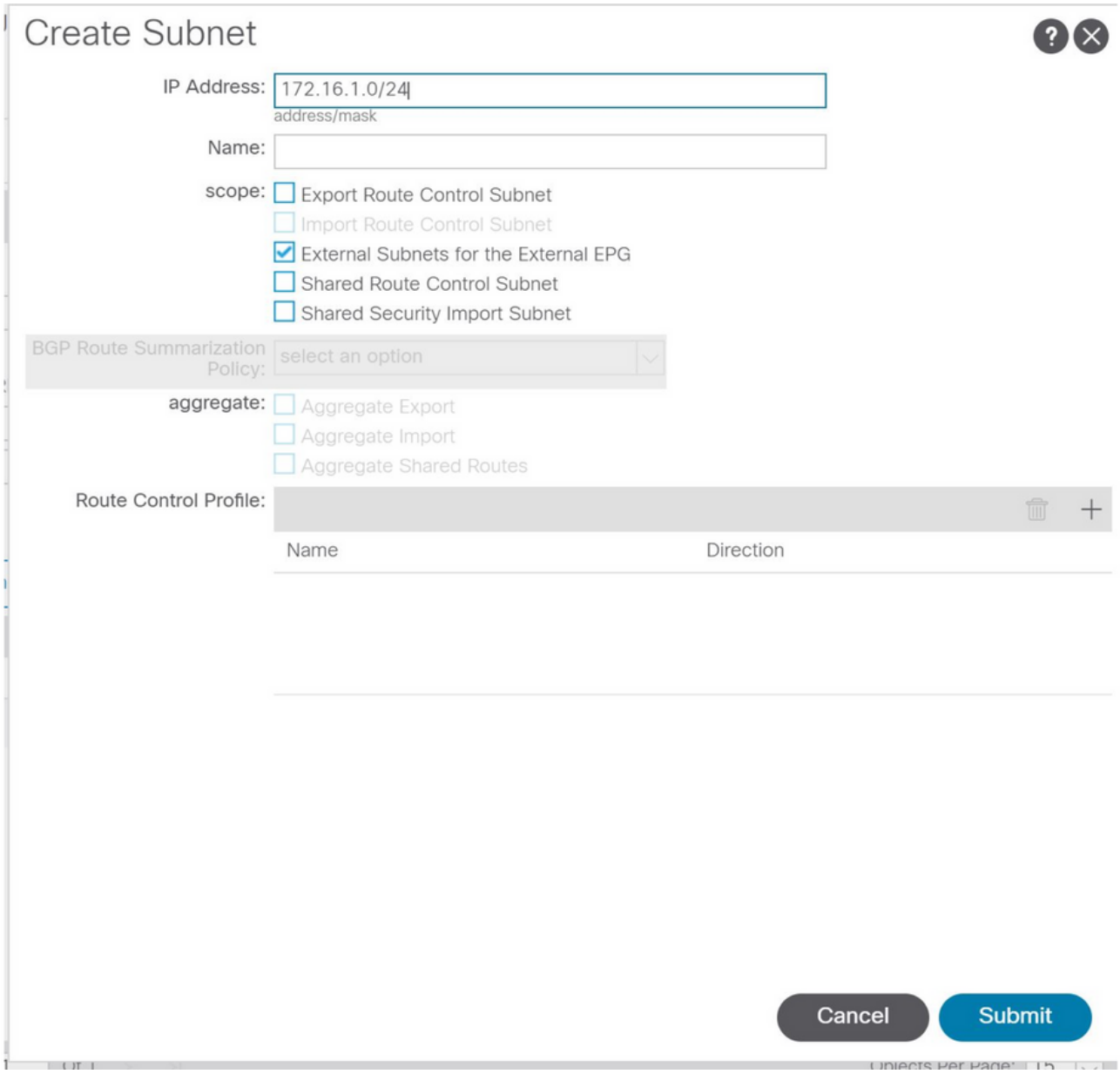
Exemple 1 : L3Out unique avec préfixe spécifique

Scénario: Un seul BGP L3Out dans vrf Prod:VRF1 avec un L3Out EPG. Le préfixe 172.16.1.0/24 étant reçu d'une source externe, il doit être classé dans l'EPG L3Out.

```
bdsol-aci32-leaf3# show ip route 172.16.1.0  vrf Prod:VRF1
IP Route Table for VRF "Prod:VRF1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%' in via output denotes VRF

172.16.1.0/24, ubest/mbest: 1/0
    *via 10.0.0.134%Prod:VRF1, [20/0], 00:56:14, bgp-132, external, tag 65002
         recursive next hop: 10.0.0.134/32%Prod:VRF1
```

Ajoutez d’abord le sous-réseau à la table de préfixes.

Sous-réseau avec étendue « Sous-réseaux externes pour le groupe de terminaux externe »



Vérifiez la programmation de la liste de préfixes sur les commutateurs Leaf qui ont le VRF de L3Out :

```
bdsol-aci32-leaf3# vsh -c ' show system internal  policy-mgr prefix ' |  egrep "Prod|==|Addr"
Vrf-Vni VRF-Id Table-Id Table-State  VRF-Name                     Addr
Class Shared Remote Complete
======= ======  =========== =======  ============================
================================ ====== ====== ====== ========
2097154 35     0x23          Up     Prod:VRF1
0.0.0.0/0   15      True   True   False
2097154 35     0x23          Up     Prod:VRF1
172.16.1.0/24  32772   True   True   False
```

Le pcTag de l'EPG L3Out est 32772 dans la portée VRF 2097154.

Exemple 2 : L3Out unique avec plusieurs préfixes

En développant l'exemple précédent, dans ce scénario, L3Out reçoit plusieurs préfixes. Bien que la saisie de chaque préfixe soit fonctionnelle, une autre option (selon la conception prévue) consiste à accepter tous les préfixes reçus sur L3Out.

Pour ce faire, utilisez le préfixe « 0.0.0.0/0' ».

Subnet - 0.0.0.0/0

Policy | Faults | History

Properties

IP Address: 0.0.0.0/0
address/mask

Scope:
- [ ] Export Route Control Subnet
- [ ] Import Route Control Subnet
- [x] External Subnets for the External EPG
- [ ] Shared Route Control Subnet
- [ ] Shared Security Import Subnet

Aggregate:
- [ ] Aggregate Export
- [ ] Aggregate Import
- [ ] Aggregate Shared Routes

BGP Route Summarization Policy: select an option

Route Control Profile:

Name	Direction

No items have been found.
Select Actions to create a new item.

Il en résulte l'entrée de table de préfixe policy-mgr suivante :

```
bdsol-aci32-leaf3# vsh -c ' show system internal  policy-mgr prefix ' |  egrep "Prod|==|Addr"
Vrf-Vni VRF-Id Table-Id Table-State  VRF-Name                     Addr
Class Shared Remote Complete
======= ======  =========== =======  ============================
================================ ====== ====== ====== ========
2097154 35     0x23          Up     Prod:VRF1
0.0.0.0/0   15      True   True   False
2097154 35     0x23          Up     Prod:VRF1
172.16.1.0/24  32772   True   True   False
```

> Notez que le pcTag attribué à 0.0.0.0/0 utilise la valeur 15, et non 32772. pcTag 15 est un pcTag système réservé qui est utilisé uniquement avec 0.0.0.0/0 qui agit comme un caractère générique pour correspondre à tous les préfixes sur un L3Out.

Si le VRF a un seul L3Out avec un seul L3Out EPG utilisant le 0.0.0.0/0, alors le préfixe de politique reste unique et est l'approche la plus facile pour tout attraper.

Exemple 3a : Plusieurs EPG L3Out dans un VRF

Dans ce scénario, il existe plusieurs EPG L3Out dans le même VRF.

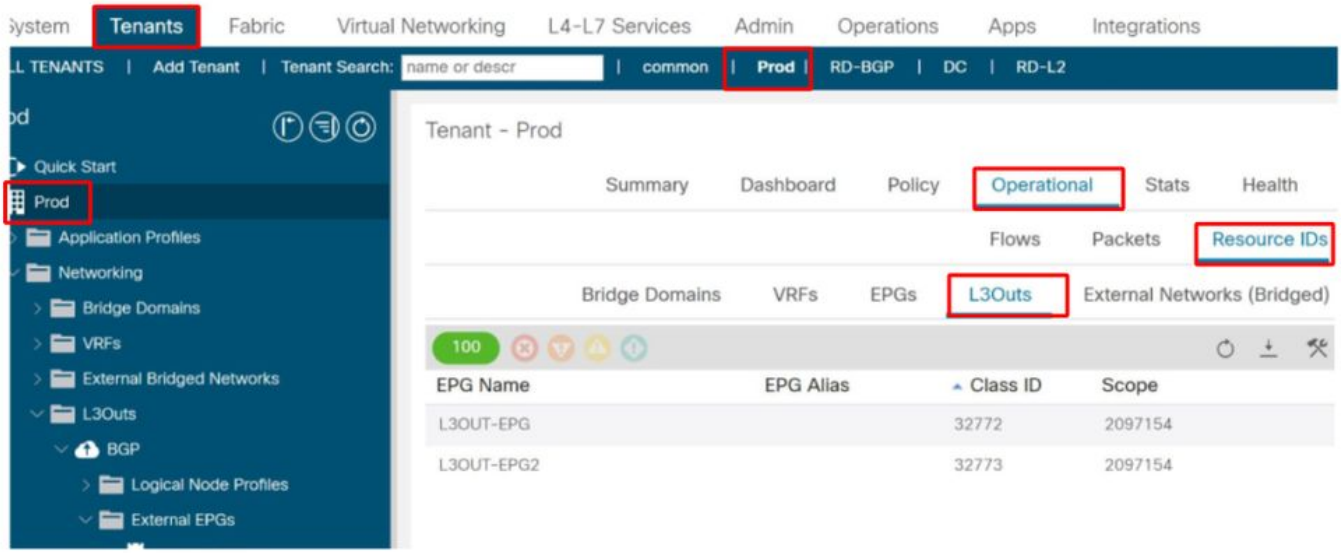
Note: D'un point de vue EPG basé sur le préfixe, les deux configurations suivantes donneront lieu à des entrées de table de préfixe LPM policy-mgr équivalentes :

1. Deux sorties L3Out avec un EPG L3Out chacune.
2. Un L3Out avec deux EPG L3Out

Dans les deux scénarios, le nombre total d'EPG L3Out est de 2. Cela signifie que chacun aura son propre pcTag et ses sous-réseaux associés.

Tous les pcTags d'un EPG L3Out donné peuvent être affichés dans l'interface utilisateur graphique à 'Tenant > Opérationnel > ID de ressource > L3Out'

Vérification de L3Out pcTag



Dans ce scénario, le fabric ACI reçoit plusieurs préfixes des routeurs externes et la définition EPG L3Out est la suivante :

- 172.16.1.0/24 attribué à L3OUT-EPG.
- 172.16.2.0/24 attribué à L3OUT-EPG2.
- 172.16.0.0/16 attribué à L3OUT-EPG (pour intercepter le préfixe 172.16.3.0/24).

Pour correspondre à cela, la configuration sera définie comme suit :

- L3OUT-EPG comporte les sous-réseaux 172.16.1.0/24 et 172.16.0.0/16 avec la portée « Sous-réseau externe pour l'EPG externe ».
- L3OUT-EPG2 possède le sous-réseau 172.16.2.0/24 avec la portée « Sous-réseau externe pour l'EPG externe ».

Les entrées de la table de préfixes résultantes seront :

```
bdsol-aci32-leaf3# vsh -c 'show system internal  policy-mgr prefix' |  egrep "Prod|==|Addr"
Vrf-Vni VRF-Id Table-Id Table-State  VRF-Name                    Addr
Class Shared Remote Complete
======= ======  =========== =======  ============================
================================ ====== ====== ====== ========
2097154 35     0x23          Up     Prod:VRF1
0.0.0.0/0   15      True   True   False
2097154 35     0x23          Up     Prod:VRF1
172.16.1.0/24  32772   True   True   False
2097154 35     0x23          Up     Prod:VRF1
172.16.0.0/16  32772   True   True   False
2097154 35     0x23          Up     Prod:VRF1
172.16.2.0/24  32773   True   True   False
```

172.16.2.0/24 est attribué à pcTag 32773 (L3OUT-EPG2) et 172.16.0.0/16 est attribué à 32772 (L3OUT-EPG).

Dans ce scénario, l'entrée pour 172.16.1.0/24 est redondante car le super-réseau /16 est attribué au même EPG.

Plusieurs EPG L3Out sont utiles lorsque l'objectif est d'appliquer différents contrats à des groupes de préfixes au sein d'un seul EPG L3Out. L'exemple suivant illustre comment les contrats entrent en jeu avec plusieurs EPG L3Out.

Exemple 3b : plusieurs EPG L3Out avec différents contrats

Ce scénario contient la configuration suivante :

- Contrat ICMP autorisant uniquement le protocole ICMP.
- Le contrat HTTP autorise uniquement le port de destination TCP 80.
- EPG1 (pcTag 32770) fournit le contrat HTTP utilisé par L3OUT-EPG (pcTag 32772).
- EPG2 (pcTag 32771) fournit le contrat ICMP utilisé par L3OUT-EPG2 (pcTag 32773).

Les préfixes policymgr de l'exemple précédent seront utilisés :

- 172.16.1.0/24 dans L3OUT-EPG doit autoriser HTTP vers EPG1
- 172.16.2.0/24 dans L3OUT-EPG2 doit autoriser ICMP à EPG2

policy-mgr prefix et zoning-rules :

```
bdsol-aci32-leaf3# vsh -c ' show system internal  policy-mgr prefix ' |  egrep "Prod|==|Addr"
Vrf-Vni VRF-Id Table-Id Table-State  VRF-Name                   Addr
Class Shared Remote Complete
======= ======  =========== =======  ============================
================================ ====== ====== ====== ========
2097154 35     0x23          Up     Prod:VRF1
0.0.0.0/0   15      True   True   False
2097154 35     0x23          Up     Prod:VRF1
172.16.1.0/24  32772   True   True   False
2097154 35     0x23          Up     Prod:VRF1
172.16.0.0/16  32772   True   True   False
2097154 35     0x23          Up     Prod:VRF1
172.16.2.0/24  32773   True   True   False


bdsol-aci32-leaf3# show zoning-rule scope 2097154
+---------+--------+--------+----------+----------------+---------+---------+------+----------+-
---------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  | Name |  Action  |
Priority       |
+---------+--------+--------+----------+----------------+---------+---------+------+----------+-
---------------------+
|   4326  |   0    |   0    | implicit |    uni-dir     | enabled | 2097154 |      | deny,log |
any_any_any(21)    |
|   4335  |   0    | 16387  | implicit |    uni-dir     | enabled | 2097154 |      |  permit  |
any_dest_any(16)   |
|   4334  |   0    |   0    | implarp  |    uni-dir     | enabled | 2097154 |      |  permit  |
any_any_filter(17)  |
|   4333  |   0    |   15   | implicit |    uni-dir     | enabled | 2097154 |      | deny,log |
any_vrf_any_deny(22) |
|   4332  |   0    | 16386  | implicit |    uni-dir     | enabled | 2097154 |      |  permit  |
any_dest_any(16)   |
|   4342  | 32771  | 32773  |    5     | uni-dir-ignore | enabled | 2097154 | ICMP |  permit  |
fully_qual(7)     |
|   4343  | 32773  | 32771  |    5     |     bi-dir     | enabled | 2097154 | ICMP |  permit  |
fully_qual(7)     |
|   4340  | 32770  | 32772  |    38    |    uni-dir     | enabled | 2097154 | HTTP |  permit  |
fully_qual(7)     |
|   4338  | 32772  | 32770  |    37    |    uni-dir     | enabled | 2097154 | HTTP |  permit  |
fully_qual(7)     |
+---------+--------+--------+----------+----------------+---------+---------+------+----------+-
---------------------+
```

Validation du chemin de données avec fTriage — flux autorisé par la stratégie

Avec un flux ICMP entre 172.16.2.1 sur le réseau externe et 192.168.3.1 dans EPG2, fTriage peut être utilisé pour intercepter et analyser le flux. Dans ce cas, démarrez fTriage sur les commutateurs Leaf 103 et 104 car le trafic peut entrer dans l'un ou l'autre :

```
admin@apic1:~> ftriage route -ii LEAF:103,104 -sip 172.16.2.1 -dip 192.168.3.1
fTriage Status: {"dbgFtriage": {"attributes": {"operState": "InProgress", "pid": "14454",
"apicId": "1", "id": "0"}}}
Starting ftriage
Log file name for the current run is: ftlog_2019-10-02-22-30-41-871.txt
2019-10-02 22:30:41,874 INFO     /controller/bin/ftriage route -ii LEAF:103,104 -sip 172.16.2.1
-dip 192.168.3.1
2019-10-02 22:31:28,868 INFO     ftriage:     main:1165 Invoking ftriage with default password
and default username: apic#fallback\\admin
2019-10-02 22:32:15,076 INFO     ftriage:     main:839  L3 packet Seen on bdsol-aci32-leaf3
```

```
Ingress: Eth1/12 (Po1) Egress: Eth1/12 (Po1) Vnid: 11365
2019-10-02 22:32:15,295 INFO     ftriage:     main:242  ingress encap string vlan-2551
2019-10-02 22:32:17,839 INFO     ftriage:     main:271  Building ingress BD(s), Ctx
2019-10-02 22:32:20,583 INFO     ftriage:     main:294  Ingress BD(s) Prod:VRF1:l3out-BGP:vlan-
2551
2019-10-02 22:32:20,584 INFO     ftriage:     main:301  Ingress Ctx: Prod:VRF1
2019-10-02 22:32:20,693 INFO     ftriage:   pktrec:490  bdsol-aci32-leaf3: Collecting transient
losses snapshot for LC module: 1
2019-10-02 22:32:38,933 INFO     ftriage:     nxos:1404 bdsol-aci32-leaf3: nxos matching rule
id:4343 scope:34 filter:5
2019-10-02 22:32:39,931 INFO     ftriage:     main:522  Computed egress encap string vlan-2502
2019-10-02 22:32:39,933 INFO     ftriage:     main:313  Building egress BD(s), Ctx
2019-10-02 22:32:41,796 INFO     ftriage:     main:331  Egress Ctx Prod:VRF1
2019-10-02 22:32:41,796 INFO     ftriage:     main:332  Egress BD(s): Prod:BD2
2019-10-02 22:32:48,636 INFO     ftriage:     main:933  SIP 172.16.2.1 DIP 192.168.3.1
2019-10-02 22:32:48,637 INFO     ftriage:  unicast:973  bdsol-aci32-leaf3: <- is ingress node
2019-10-02 22:32:51,257 INFO     ftriage:  unicast:1202 bdsol-aci32-leaf3: Dst EP is local
2019-10-02 22:32:54,129 INFO     ftriage:     misc:657  bdsol-aci32-leaf3: EP if(Po1) same as
egr if(Po1)
2019-10-02 22:32:55,348 INFO     ftriage:     misc:657  bdsol-aci32-leaf3:
DMAC(00:22:BD:F8:19:FF) same as RMAC(00:22:BD:F8:19:FF)
2019-10-02 22:32:55,349 INFO     ftriage:     misc:659  bdsol-aci32-leaf3: L3 packet getting
routed/bounced in SUG
2019-10-02 22:32:55,596 INFO     ftriage:     misc:657  bdsol-aci32-leaf3: Dst IP is present in
SUG L3 tbl
2019-10-02 22:32:55,896 INFO     ftriage:     misc:657  bdsol-aci32-leaf3: RW seg_id:11365 in
SUG same as EP segid:11365
2019-10-02 22:33:02,150 INFO     ftriage:     main:961  Packet is Exiting fabric with peer-
device: bdsol-aci32-n3k-3 and peer-port: Ethernet1/16
```

fTriage confirme l'impact de la règle de zonage sur la règle ICMP de L3OUT_EPG2 à EPG :

```
2019-10-02 22:32:38,933 INFO     ftriage:     nxos:1404 bdsol-aci32-leaf3: nxos matching rule
id:4343 scope:34 filter:5
```

Validation du chemin de données à l'aide de fTriage — flux non autorisé par la stratégie

Avec le trafic ICMP provenant de 172.16.1.1 (L3OUT-EPG) vers 192.168.3.1 (EPG2), attendez-vous à une perte de stratégie.

```
admin@apic1:~> ftriage route -ii LEAF:103,104 -sip 172.16.1.1 -dip 192.168.3.1
fTriage Status: {"dbgFtriage": {"attributes": {"operState": "InProgress", "pid": "15139",
"apicId": "1", "id": "0"}}}
Starting ftriage
Log file name for the current run is: ftlog_2019-10-02-22-39-15-050.txt
2019-10-02 22:39:15,056 INFO     /controller/bin/ftriage route -ii LEAF:103,104 -sip 172.16.1.1
-dip 192.168.3.1
2019-10-02 22:40:03,523 INFO     ftriage:     main:1165 Invoking ftriage with default password
and default username: apic#fallback\\admin
2019-10-02 22:40:43,338 ERROR    ftriage:  unicast:234  bdsol-aci32-leaf3: L3 packet getting fwd
dropped, checking drop reason
2019-10-02 22:40:43,339 ERROR    ftriage:  unicast:234  bdsol-aci32-leaf3: L3 packet getting fwd
dropped, checking drop reason
SECURITY_GROUP_DENY              condition setcast:236  bdsol-aci32-leaf3: Drop reason -
SECURITY_GROUP_DENY              condition set
2019-10-02 22:40:43,340 INFO     ftriage:  unicast:252  bdsol-aci32-leaf3: policy drop flow
sclass:32772 dclass:32771 sg_label:34 proto:1
2019-10-02 22:40:43,340 INFO     ftriage:     main:681  : Ftriage Completed with hunch: None
fTriage Status: {"dbgFtriage": {"attributes": {"operState": "Idle", "pid": "0", "apicId": "0",
"id": "0"}}}
```

fTriage confirme que le paquet est abandonné avec la raison SECURITY_GROUP_DENY (abandon de stratégie) et que le pcTag source dérivé est 32772 et le pcTag de destination est 32771. En vérifiant cela par rapport aux règles de zonage, il n'y a clairement aucune entrée entre ces EPG.

```
bdsol-aci32-leaf3# show zoning-rule  scope 2097154 src-epg 32772 dst-epg 32771
+---------+--------+--------+----------+-----+--------+-------+------+--------+----------+
| Rule ID | SrcEPG | DstEPG | FilterID | Dir | operSt | Scope | Name | Action | Priority |
+---------+--------+--------+----------+-----+--------+-------+------+--------+----------+
+---------+--------+--------+----------+-----+--------+-------+------+--------+----------+
```

Exemple 4 : Plusieurs sorties L3 avec plusieurs préfixes

Le scénario est configuré de la même manière que dans l'exemple 3 (définitions EPG L3Out et L3Out), mais le réseau défini sur les deux EPG L3Out est 0.0.0.0/0.

La configuration du contrat est la suivante :

- Contrat ICMP1 autorisant ICMP.
- Contrat ICMP2 autorisant le protocole ICMP.
- EPG1 (pcTag 32770) fournit un contrat ICMP1 qui est utilisé par L3OUT-EPG (pcTag 32772).
- EPG2 (pcTag 32771) fournit un contrat ICMP2 qui est utilisé par L3OUT-EPG2 (pcTag 32773).

Cette configuration peut sembler idéale dans le cas où le réseau externe annonce de nombreux préfixes, mais il existe au moins deux blocs de préfixes qui suivent des modèles de flux autorisés différents. Dans cet exemple, un préfixe ne doit autoriser que le protocole ICMP1 et l'autre ne doit autoriser que le protocole ICMP2.

Malgré l'utilisation de '0.0.0.0/0' deux fois dans le même VRF, un seul préfixe est programmé dans la table de préfixe policy-mgr :

```
bdsol-aci32-leaf3# vsh -c ' show system internal  policy-mgr prefix ' |  egrep "Prod|==|Addr"
Vrf-Vni VRF-Id Table-Id Table-State  VRF-Name                  Addr
Class Shared Remote Complete
======= ======  =========== =======  ============================
================================ ====== ====== ====== ========
2097154 35     0x23          Up     Prod:VRF1
```

Deux flux sont réexaminés ci-dessous. Selon la configuration du contrat ci-dessus, les éléments suivants sont attendus :

1. Les adresses 172.16.2.1 (L3OUT-EPG2) à 192.168.3.1 (EPG2) **doivent** être autorisées par ICMP2
2. Les versions 172.16.2.1 (L3OUT-EPG2) à 192.168.1.1 (EPG1) **ne doivent pas** être autorisées, car aucun contrat n'existe entre EPG1 et L3OUT-EPG2

Validation du chemin de données à l'aide de fTriage — flux autorisé par la stratégie

Exécutez fTriage avec un flux ICMP de 172.16.2.1 (L3OUT-EPG2) à 192.168.3.1 (EPG2 — pcTag

32771).

```
Starting ftriage
Log file name for the current run is: ftlog_2019-10-02-23-11-14-298.txt
2019-10-02 23:11:14,302 INFO     /controller/bin/ftriage route -ii LEAF:103,104 -sip 172.16.2.1
-dip 192.168.3.1
2019-10-02 23:12:00,887 INFO     ftriage:     main:1165 Invoking ftriage with default password
and default username: apic#fallback\\admin
2019-10-02 23:12:44,565 INFO     ftriage:     main:839  L3 packet Seen on bdsol-aci32-leaf3
Ingress: Eth1/12 (Po1) Egress: Eth1/12 (Po1) Vnid: 11365
2019-10-02 23:12:44,782 INFO     ftriage:     main:242  ingress encap string vlan-2551
2019-10-02 23:12:47,260 INFO     ftriage:     main:271  Building ingress BD(s), Ctx
2019-10-02 23:12:50,041 INFO     ftriage:     main:294  Ingress BD(s) Prod:VRF1:l3out-BGP:vlan-
2551
2019-10-02 23:12:50,042 INFO     ftriage:     main:301  Ingress Ctx: Prod:VRF1
2019-10-02 23:12:50,151 INFO     ftriage:   pktrec:490  bdsol-aci32-leaf3: Collecting transient
losses snapshot for LC module: 1
2019-10-02 23:13:08,595 INFO     ftriage:     nxos:1404 bdsol-aci32-leaf3: nxos matching rule
id:4336 scope:34 filter:5
2019-10-02 23:13:09,608 INFO     ftriage:     main:522  Computed egress encap string vlan-2502
2019-10-02 23:13:09,609 INFO     ftriage:     main:313  Building egress BD(s), Ctx
2019-10-02 23:13:11,449 INFO     ftriage:     main:331  Egress Ctx Prod:VRF1
2019-10-02 23:13:11,449 INFO     ftriage:     main:332  Egress BD(s): Prod:BD2
2019-10-02 23:13:18,383 INFO     ftriage:     main:933  SIP 172.16.2.1 DIP 192.168.3.1
2019-10-02 23:13:18,384 INFO     ftriage:  unicast:973  bdsol-aci32-leaf3: <- is ingress node
2019-10-02 23:13:21,078 INFO     ftriage:  unicast:1202 bdsol-aci32-leaf3: Dst EP is local
2019-10-02 23:13:23,926 INFO     ftriage:     misc:657  bdsol-aci32-leaf3: EP if(Po1) same as
egr if(Po1)
2019-10-02 23:13:25,216 INFO     ftriage:     misc:657  bdsol-aci32-leaf3:
DMAC(00:22:BD:F8:19:FF) same as RMAC(00:22:BD:F8:19:FF)
2019-10-02 23:13:25,217 INFO     ftriage:     misc:659  bdsol-aci32-leaf3: L3 packet getting
routed/bounced in SUG
2019-10-02 23:13:25,465 INFO     ftriage:     misc:657  bdsol-aci32-leaf3: Dst IP is present in
SUG L3 tbl
2019-10-02 23:13:25,757 INFO     ftriage:     misc:657  bdsol-aci32-leaf3: RW seg_id:11365 in
SUG same as EP segid:11365
2019-10-02 23:13:32,235 INFO     ftriage:     main:961  Packet is Exiting fabric with peer-
device: bdsol-aci32-n3k-3 and peer-port: Ethernet1/16
```

Ce flux est autorisé (comme prévu) par la règle de zonage 4336.

Validation du chemin de données à l'aide de fTriage — flux non autorisé par la stratégie

Exécutez fTriage avec un flux ICMP de 172.16.2.1 (L3OUT-EPG2) à 192.168.1.1 (EPG1 — pcTag 32770) :

```
admin@apic1:~> ftriage route -ii LEAF:103,104 -sip 172.16.2.1 -dip 192.168.1.1
fTriage Status: {"dbgFtriage": {"attributes": {"operState": "InProgress", "pid": "31500",
"apicId": "1", "id": "0"}}}
Starting ftriage
Log file name for the current run is: ftlog_2019-10-02-23-53-03-478.txt
2019-10-02 23:53:03,482 INFO     /controller/bin/ftriage route -ii LEAF:103,104 -sip 172.16.2.1
-dip 192.168.1.1
2019-10-02 23:53:50,014 INFO     ftriage:     main:1165 Invoking ftriage with default password
and default username: apic#fallback\\admin
2019-10-02 23:54:39,199 INFO     ftriage:     main:839  L3 packet Seen on bdsol-aci32-leaf3
Ingress: Eth1/12 (Po1) Egress: Eth1/12 (Po1) Vnid: 11364
2019-10-02 23:54:39,417 INFO     ftriage:     main:242  ingress encap string vlan-2551
```

```
2019-10-02 23:54:41,962 INFO     ftriage:     main:271  Building ingress BD(s), Ctx
2019-10-02 23:54:44,765 INFO     ftriage:     main:294  Ingress BD(s) Prod:VRF1:l3out-BGP:vlan-
2551
2019-10-02 23:54:44,766 INFO     ftriage:     main:301  Ingress Ctx: Prod:VRF1
2019-10-02 23:54:44,875 INFO     ftriage:   pktrec:490  bdsol-aci32-leaf3: Collecting transient
losses snapshot for LC module: 1
2019-10-02 23:55:02,905 INFO     ftriage:     nxos:1404 bdsol-aci32-leaf3: nxos matching rule
id:4341 scope:34 filter:5
2019-10-02 23:55:04,525 INFO     ftriage:     main:522  Computed egress encap string vlan-2501
2019-10-02 23:55:04,526 INFO     ftriage:     main:313  Building egress BD(s), Ctx
2019-10-02 23:55:06,390 INFO     ftriage:     main:331  Egress Ctx Prod:VRF1
2019-10-02 23:55:06,390 INFO     ftriage:     main:332  Egress BD(s): Prod:BD1
2019-10-02 23:55:13,571 INFO     ftriage:     main:933  SIP 172.16.2.1 DIP 192.168.1.1
2019-10-02 23:55:13,572 INFO     ftriage:  unicast:973  bdsol-aci32-leaf3: <- is ingress node
2019-10-02 23:55:16,159 INFO     ftriage:  unicast:1202 bdsol-aci32-leaf3: Dst EP is local
2019-10-02 23:55:18,949 INFO     ftriage:     misc:657  bdsol-aci32-leaf3: EP if(Po1) same as
egr if(Po1)
2019-10-02 23:55:20,126 INFO     ftriage:     misc:657  bdsol-aci32-leaf3:
DMAC(00:22:BD:F8:19:FF) same as RMAC(00:22:BD:F8:19:FF)
2019-10-02 23:55:20,126 INFO     ftriage:     misc:659  bdsol-aci32-leaf3: L3 packet getting
routed/bounced in SUG
2019-10-02 23:55:20,395 INFO     ftriage:     misc:657  bdsol-aci32-leaf3: Dst IP is present in
SUG L3 tbl
2019-10-02 23:55:20,687 INFO     ftriage:     misc:657  bdsol-aci32-leaf3: RW seg_id:11364 in
SUG same as EP segid:11364
2019-10-02 23:55:26,982 INFO     ftriage:     main:961  Packet is Exiting fabric with peer-
device: bdsol-aci32-n3k-3 and peer-port: Ethernet1/16
```

Ce flux est autorisé (inattendu) par la règle de zonage 4341. Les règles de zonage doivent maintenant être analysées pour comprendre pourquoi.

Validation du chemin de données — règles de zonage

Les règles de zonage correspondant aux 2 derniers tests sont les suivantes :

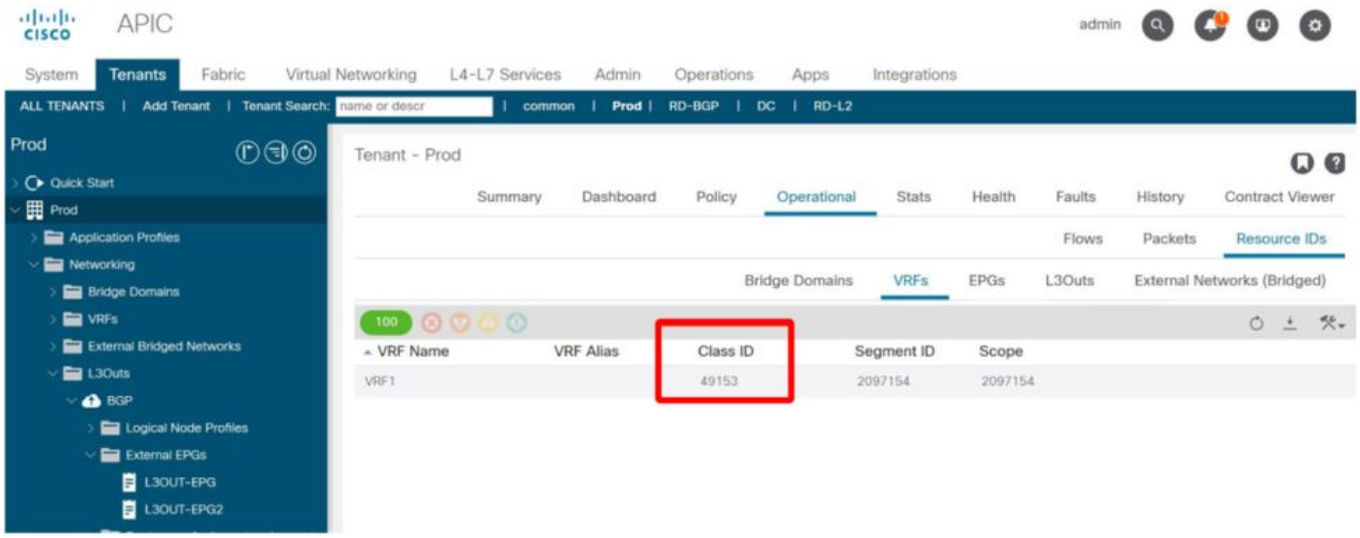
- Attendu : le flux atteint la ligne de règle de zonage 4336 (contrat ICMP2).
- Inattendu : le flux atteint la ligne de règle de zonage 4341 (contrat ICMP1).

```
+---------+--------+--------+----------+---------+---------+---------+-------+----------+-------
---------------+
| Rule ID | SrcEPG | DstEPG | FilterID |   Dir   |  operSt |  Scope  |  Name |  Action  |
Priority       |
+---------+--------+--------+----------+---------+---------+---------+-------+----------+-------
---------------+
|   4326  |   0    |   0    | implicit | uni-dir | enabled | 2097154 |       | deny,log |
any_any_any(21)    |
|   4335  |   0    | 16387  | implicit | uni-dir | enabled | 2097154 |       |  permit  |
any_dest_any(16)   |
|   4334  |   0    |   0    | implarp  | uni-dir | enabled | 2097154 |       |  permit  |
any_any_filter(17)  |
|   4333  |   0    |   15   | implicit | uni-dir | enabled | 2097154 |       | deny,log |
any_vrf_any_deny(22) |
|   4332  |   0    | 16386  | implicit | uni-dir | enabled | 2097154 |       |  permit  |
any_dest_any(16)   |
|   4339  | 32770  |   15   |    5     | uni-dir | enabled | 2097154 | ICMP2 |  permit  |
fully_qual(7)     |
|   4341  | 49153  | 32770  |    5     | uni-dir | enabled | 2097154 | ICMP2 |  permit  |
fully_qual(7)     |
|   4337  | 32771  |   15   |    5     | uni-dir | enabled | 2097154 | ICMP1 |  permit  |
```

```
fully_qual(7)     |
|   4336  | 49153  | 32771  |    5     | uni-dir | enabled | 2097154 | ICMP1 |  permit  |
fully_qual(7)     |
+---------+--------+--------+----------+---------+---------+---------+-------+----------+-------
--------------+
```

Les deux flux dérivent le pcTag src de 49153. Il s'agit du pcTag du VRF. Ceci peut être vérifié dans l'interface utilisateur :

Vérification du pcTag du VRF



Ce qui suit se produit lorsque le préfixe 0.0.0.0/0 est utilisé avec un L3Out :

- Le trafic d'un EPG interne vers un EPG L3Out avec 0.0.0.0/0 dérive une balise pcTag de destination de 15.
- Le trafic provenant d'un EPG L3Out avec 0.0.0.0/0 vers un EPG interne ACI dérivera un pcTag source du VRF (49153).

Le script contract_parser donne une vue globale des règles de zonage :

```
bdsol-aci32-leaf3# contract_parser.py --vrf Prod:VRF1
Key:
[prio:RuleId] [vrf:{str}] action protocol src-epg [src-l4] dst-epg [dst-l4]
[flags][contract:{str}] [hit=count]
[7:4339] [vrf:Prod:VRF1] permit ip icmp tn-Prod/ap-App/epg-EPG1(32770) pfx-0.0.0.0/0(15)
[contract:uni/tn-Prod/brc-ICMP2] [hit=0]
[7:4337] [vrf:Prod:VRF1] permit ip icmp tn-Prod/ap-App/epg-EPG2(32771) pfx-0.0.0.0/0(15)
[contract:uni/tn-Prod/brc-ICMP] [hit=0]
[7:4341] [vrf:Prod:VRF1] permit ip icmp tn-Prod/vrf-VRF1(49153) tn-Prod/ap-App/epg-EPG1(32770)
[contract:uni/tn-Prod/brc-ICMP2] [hit=270]
[7:4336] [vrf:Prod:VRF1] permit ip icmp tn-Prod/vrf-VRF1(49153) tn-Prod/ap-App/epg-EPG2(32771)
[contract:uni/tn-Prod/brc-ICMP] [hit=0]
```

Confirmation de pcTag utilisé par le paquet à l'aide de l'application ELAM Assistant

L'application ELAM Assistant fournit une autre méthode pour confirmer la source et la destination pcTag des flux de trafic en direct.

La capture d'écran ci-dessous montre le résultat d'ELAM pour le trafic entre pcTag 32771 et

pcTag 49153.

Sortie de l'application ELAM Assistant pour src 32771 à dst 49153

Packet Forwarding Information

Forward Result	
Destination Type	To a local port
Destination Logical Port	Po1
Destination Physical Port	eth1/12
Sent to SUP/CPU instead	no
SUP Redirect Reason (SUP code)	NONE

Contract	
Destination EPG pcTag (dclass)	32771 (Prod:App:EPG2)
Source EPG pcTag (sclass)	49153 (Prod:VRF1:l3out-BGP:vlan-2551)

Conclusion

L'utilisation de 0.0.0.0/0 doit être suivie avec attention dans un VRF, car chaque L3Out utilisant ce sous-réseau héritera des contrats appliqués à chaque L3Out l'utilisant. Cela entraînera probablement des flux de permis non planifiés.

Partagé L3Out

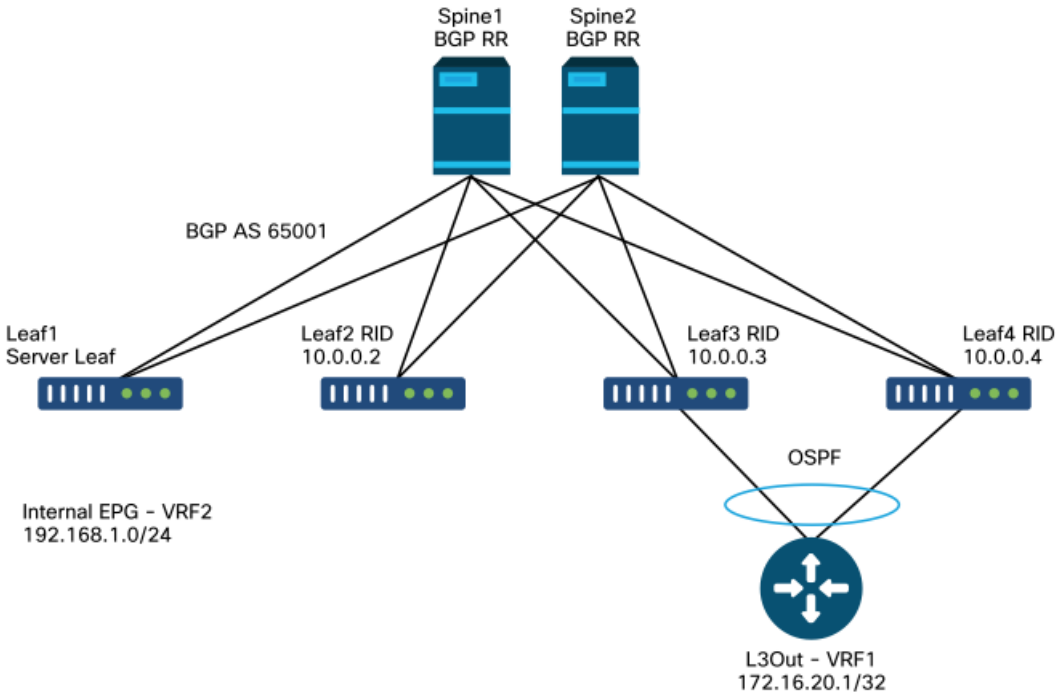
Aperçu

Cette section traite du dépannage de l’annonce de route dans les configurations L3Out partagées. Le terme « L3Out partagé » fait référence au scénario dans lequel une L3Out se trouve dans un VRF, mais un EPG interne ayant un contrat avec la L3Out se trouve dans un autre VRF. Avec les sorties L3 partagées, la fuite de route est effectuée en interne vers le fabric ACI.

Cette section ne traite pas en détail du dépannage des stratégies de sécurité. Pour cela, reportez-vous au chapitre « Security Policies » de ce manuel. Cette section ne traite pas en détail de la classification des préfixes de stratégie externe à des fins de sécurité. Reportez-vous à la section « Contract and L3Out » du chapitre « external forwarding ».

Cette section utilise la topologie suivante pour nos exemples.

Topologie L3Out partagée



Àun niveau élevé, les configurations suivantes doivent être en place pour qu'un L3Out partagé fonctionne :

- Un sous-réseau L3Out doit être configuré avec l'étendue « Sous-réseau de contrôle de route partagé » pour laisser passer des routes externes dans des VRF internes. L'option « Aggregate Shared » peut également être sélectionnée pour laisser passer toutes les routes qui sont plus spécifiques que le sous-réseau configuré.
- Un sous-réseau L3Out doit être configuré avec l'étendue « Sous-réseau d'importation de sécurité partagé » pour programmer les stratégies de sécurité nécessaires pour permettre la communication via ce sous-réseau L3Out.
- Le sous-réseau BD interne doit être défini sur « Partagé entre les VRF » et « Annoncer en externe » pour programmer le sous-réseau BD dans le VRF externe et l'annoncer.
- Un contrat d'étendue 'locataire' ou 'global' doit être configuré entre l'EPG interne et l'EPG externe de l'interface L3Out partagée.

La section suivante traite en détail de la manière dont les routes divulguées sont annoncées et apprises dans l'ACI.

Workflow L3Out partagé — apprentissage des routes externes

Cette section décrit le chemin d'une route externe apprise telle qu'elle est annoncée dans le fabric.

Route externe telle qu'elle apparaît sur la feuille de bordure

Cette commande affiche la route externe apprise à partir du protocole OSPF :

```
leaf103# show ip route 172.16.20.1/32 vrf Prod:Vrf1
IP Route Table for VRF "Prod:Vrf1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%' in via output denotes VRF

172.16.20.1/32, ubest/mbest: 1/0
    *via 10.10.34.3, vlan347, [110/20], 03:59:59, ospf-default, type-2
```

Ensuite, la route doit être importée dans BGP. Par défaut, toutes les routes externes doivent être importées dans BGP.

Vérifications BGP sur le leaf de bordure

La route doit faire partie de la famille d'adresses BGP VPNv4 avec une route cible à distribuer dans le fabric. La route-target est une communauté étendue BGP exportée par le VRF externe et importée par tous les VRF internes qui doivent recevoir le chemin.

Vérifiez ensuite la route-target exportée par le VRF externe sur la liste de contrôle d'accès.

```
leaf103# show bgp process vrf Prod:Vrf1

Information regarding configured VRFs:

BGP Information for VRF Prod:Vrf1
VRF Type                        : System
VRF Id                          : 85
VRF state                       : UP
VRF configured                  : yes
VRF refcount                    : 1
VRF VNID                        : 2392068
Router-ID                       : 10.0.0.3
Configured Router-ID            : 10.0.0.3
Confed-ID                       : 0
Cluster-ID                      : 0.0.0.0
MSITE Cluster-ID                : 0.0.0.0
No. of configured peers         : 1
No. of pending config peers     : 0
No. of established peers        : 0
VRF RD                          : 101:2392068
VRF EVPN RD                     : 101:2392068

...

    Wait for IGP convergence is not configured
    Export RT list:
        65001:2392068
    Import RT list:
        65001:2392068
    Label mode: per-prefix
```

Le résultat ci-dessus montre que tous les chemins annoncés depuis le VRF externe vers VPNv4 doivent recevoir une route-target de 65001:2392068.

Vérifiez ensuite le chemin bgp :

```
leaf103# show bgp ipv4 unicast 172.16.20.1/32 vrf Prod:Vrf1
BGP routing table information for VRF Prod:Vrf1, address family IPv4 Unicast
BGP routing table entry for 172.16.20.1/32, version 30 dest ptr 0xa6f25ad0
Paths: (2 available, best #1)
Flags: (0x80c0002 00000000) on xmit-list, is not in urib, exported
  vpn: version 17206, (0x100002) on xmit-list
Multipath: eBGP iBGP

  Advertised path-id 1, VPN AF advertised path-id 1
  Path type: redist 0x408 0x1 ref 0 adv path ref 2, path is valid, is best path
  AS-Path: NONE, path locally originated
    0.0.0.0 (metric 0) from 0.0.0.0 (10.0.0.3)
      Origin incomplete, MED 20, localpref 100, weight 32768
      Extcommunity:
          RT:65001:2392068
          VNID:2392068
          COST:pre-bestpath:162:110

  VRF advertise information:
  Path-id 1 not advertised to any peer

  VPN AF advertise information:
  Path-id 1 advertised to peers:
    10.0.64.64         10.0.72.66
  Path-id 2 not advertised to any peer
```

Le résultat ci-dessus montre que le chemin a la route-target correcte. Le chemin VPNv4 peut également être vérifié à l'aide de la commande « show bgp vpnv4 unicast 172.16.20.1 vrf overlay-1 ».

Vérifications sur le serveur leaf

Pour que le leaf EPG interne installe la route BL annoncée, il doit importer la route-target (mentionnée ci-dessus) dans le VRF interne. Le processus BGP du VRF interne peut être vérifié pour valider ceci :

```
leaf101# show bgp process vrf Prod:Vrf2

Information regarding configured VRFs:

BGP Information for VRF Prod:Vrf2
VRF Type                        : System
VRF Id                          : 54
VRF state                       : UP
VRF configured                  : yes
VRF refcount                    : 0
VRF VNID                        : 2916352
Router-ID                       : 192.168.1.1
Configured Router-ID            : 0.0.0.0
Confed-ID                       : 0
Cluster-ID                      : 0.0.0.0
MSITE Cluster-ID                : 0.0.0.0
No. of configured peers         : 0
No. of pending config peers     : 0
No. of established peers        : 0
VRF RD                          : 102:2916352
VRF EVPN RD                     : 102:2916352
...
    Wait for IGP convergence is not configured
```

```
    Import route-map 2916352-shared-svc-leak
    Export RT list:
        65001:2916352
    Import RT list:
        65001:2392068
        65001:2916352
```

Le résultat ci-dessus montre le VRF interne qui importe la route-target exportée par le VRF externe. De plus, il y a un 'Import Route-Map' qui est référencé. La route-map d'importation inclut les préfixes spécifiques qui sont définis dans le L3Out partagé avec l'indicateur 'Sous-réseau de contrôle de route partagé'.

Le contenu de la route-map peut être vérifié pour s'assurer qu'il inclut le préfixe externe :

```
leaf101# show route-map 2916352-shared-svc-leak
route-map 2916352-shared-svc-leak, deny, sequence 1
 Match clauses:
   pervasive: 2
 Set clauses:
route-map 2916352-shared-svc-leak, permit, sequence 2
 Match clauses:
   extcommunity  (extcommunity-list filter): 2916352-shared-svc-leak
 Set clauses:
route-map 2916352-shared-svc-leak, permit, sequence 1000
 Match clauses:
   ip address prefix-lists: IPv4-2392068-16387-5511-2916352-shared-svc-leak
   ipv6 address prefix-lists: IPv6-deny-all
 Set clauses:
a-leaf101# show ip prefix-list IPv4-2392068-16387-5511-2916352-shared-svc-leak
ip prefix-list IPv4-2392068-16387-5511-2916352-shared-svc-leak: 1 entries
  seq 1 permit 172.16.20.1/32
```

Le résultat ci-dessus montre la route-map d'importation qui inclut le sous-réseau à importer.

Les vérifications finales incluent la vérification que la route est dans la table BGP et qu'elle est installée dans la table de routage.

Table BGP sur le serveur leaf :

```
leaf101# show bgp ipv4 unicast 172.16.20.1/32 vrf Prod:Vrf2
BGP routing table information for VRF Prod:Vrf2, address family IPv4 Unicast
BGP routing table entry for 172.16.20.1/32, version 3 dest ptr 0xa763add0
Paths: (2 available, best #1)
Flags: (0x08001a 00000000) on xmit-list, is in urib, is best urib route, is in HW
  vpn: version 10987, (0x100002) on xmit-list
Multipath: eBGP iBGP

  Advertised path-id 1, VPN AF advertised path-id 1
  Path type: internal 0xc0000018 0x40 ref 56506 adv path ref 2, path is valid, is best path
             Imported from 10.0.72.64:5:172.16.20.1/32
  AS-Path: NONE, path sourced internal to AS
    10.0.72.64 (metric 3) from 10.0.64.64 (192.168.1.102)
      Origin incomplete, MED 20, localpref 100, weight 0
      Received label 0
      Received path-id 1
      Extcommunity:
          RT:65001:2392068
          VNID:2392068
```

```
          COST:pre-bestpath:162:110
      Originator: 10.0.72.64 Cluster list: 192.168.1.102
```

La route est importée dans la table BGP VRF interne et a la route-target attendue.

Les routes installées peuvent être vérifiées :

```
leaf101# vsh -c "show ip route 172.16.20.1/32 detail vrf Prod:Vrf2"
IP Route Table for VRF "Prod:Vrf2"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%' in via output denotes VRF
172.16.20.1/32, ubest/mbest: 2/0
   *via 10.0.72.64%overlay-1, [200/20], 01:00:51, bgp-65001, internal, tag 65001 (mpls-vpn)
        MPLS[0]: Label=0 E=0 TTL=0 S=0 (VPN)
        client-specific data: 548
        recursive next hop: 10.0.72.64/32%overlay-1
        extended route information: BGP origin AS 65001 BGP peer AS 65001 rw-vnid: 0x248004
table-id: 0x36 rw-mac: 0
   *via 10.0.72.67%overlay-1, [200/20], 01:00:51, bgp-65001, internal, tag 65001 (mpls-vpn)
        MPLS[0]: Label=0 E=0 TTL=0 S=0 (VPN)
        client-specific data: 54a
        recursive next hop: 10.0.72.67/32%overlay-1
        extended route information: BGP origin AS 65001 BGP peer AS 65001 rw-vnid: 0x248004
table-id: 0x36 rw-mac: 0
```

Le résultat ci-dessus utilise une commande 'vsh -c' spécifique pour obtenir le résultat 'detail'. L'indicateur « detail » inclut le VNID VXLAN de réécriture. Il s'agit du VNID VXLAN du VRF externe. Lorsque le BL reçoit le trafic du plan de données avec ce VNID, il sait qu'il doit prendre la décision de transfert dans le VRF externe.

La valeur rw-vnid est au format hexadécimal, donc la conversion au format décimal permet d'obtenir le VNID VRF de 2392068. Recherchez le VRF correspondant à l'aide de la commande « show system internal epm vrf all » | grep 2392068' sur la feuille. Une recherche globale peut être effectuée sur un APIC à l'aide de la commande 'moquery -c fvCtx -f 'fv.Ctx.seg=="2392068"'.

L'IP du tronçon suivant doit également pointer vers les PTEP BL et le '%overlay-1' indique que la recherche de route pour le tronçon suivant se trouve dans le VRF de superposition.

Workflow L3Out partagé - annonce des routes internes

Comme dans les sections précédentes, l'annonce de sous-réseaux BD internes à partir d'une L3Out partagée est gérée par les éléments suivants :

- Le sous-réseau BD (VRF interne) est installé sur le BL (VRF externe) en tant que route statique. Ce déploiement de route statique est le résultat de la relation contractuelle entre l'EPG interne et L3Out.
- La route statique est redistribuée dans le protocole externe lorsque la portée « Annoncée de manière externe » est définie sur le sous-réseau BD.

Vérification de la route statique BD sur le BL

```
leaf103# vsh -c "show ip route 192.168.1.0 detail vrf Prod:Vrf1"
IP Route Table for VRF "Prod:Vrf1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%' in via output denotes VRF

192.168.1.0/24, ubest/mbest: 1/0, attached, direct, pervasive
    *via 10.0.120.34%overlay-1, [1/0], 00:55:27, static, tag 4294967292
         recursive next hop: 10.0.120.34/32%overlay-1
         vrf crossing information:  VNID:0x2c8000 ClassId:0 Flush#:0
```

Notez que dans le résultat ci-dessus, le VNID du VRF interne est défini pour la réécriture. Le tronçon suivant est également défini sur l'adresse proxy-v4-anycast.

La route ci-dessus est annoncée en externe via les mêmes route-maps que celles présentées dans la section « Annonce de route ».

Si un sous-réseau BD est défini sur 'Annoncer en externe', il est redistribué dans **chaque protocole externe de L3Out** avec lequel l'EPG interne a une relation contractuelle.

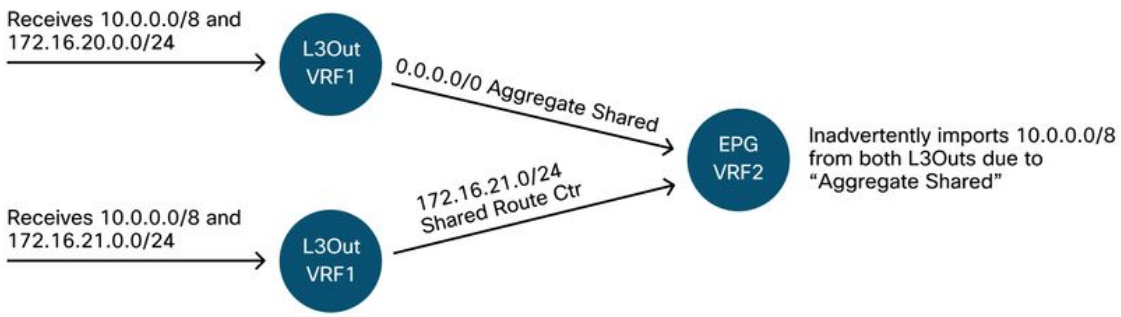
Scénario de dépannage L3Out partagé : fuite de route inattendue

Ce scénario comporte plusieurs sorties L3Out dans le VRF externe et un EPG interne reçoit une route d'une sortie L3Out où le réseau n'**est pas** défini avec les options d'étendue « partagée ».

Utilisation de « Aggregate Shared »

Examinez la figure suivante :

Fuite de route inattendue



Le import-map BGP avec la liste de préfixes programmée à partir des indicateurs **'Shared Route Control Subnet'** est appliqué au niveau VRF. Si un L3Out dans VRF1 possède un sous-réseau avec le sous-réseau de contrôle de route partagé, toutes les routes reçues sur les L3Out dans VRF1 qui correspondent à ce sous-réseau de contrôle de route partagé seront importées dans VRF2.

La conception ci-dessus peut entraîner des flux de trafic inattendus. S'il n'y a aucun contrat entre l'EPG interne et l'EPG L3Out publicitaire inattendue, alors il y aura des pertes de trafic.

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.