Configuration et vérification des fuites VRF VXLAN sur Nexus 9000

Table des matières

Introduction

Ce document décrit comment configurer et vérifier les fuites VRF sur un environnement VXLAN.

Informations générales

Dans un environnement VXLAN (Virtual Extensible LAN), la connexion d'hôtes VXLAN à des hôtes externes à partir du fabric nécessite souvent l'utilisation de périphériques VRF avec fuite et périphérie.

Les fuites VRF sont essentielles pour permettre la communication entre les hôtes VXLAN et les hôtes externes, tout en préservant la segmentation et la sécurité du réseau.

Le périphérique de périphérie sert de passerelle entre le fabric VXLAN et les réseaux externes, jouant un rôle essentiel dans la facilitation de cette communication.

L'importance des fuites de VRF dans ce scénario peut être résumée par les énoncés suivants :

1. Interconnexion avec des réseaux externes : les fuites VRF permettent aux hôtes VXLAN du fabric de communiquer avec des hôtes externes situés à l'extérieur du fabric. Cela permet d'accéder aux ressources, aux services et aux applications hébergés sur des réseaux externes, tels qu'Internet ou d'autres data centers.

2. Segmentation et isolation du réseau : les fuites VRF maintiennent la segmentation et l'isolation du réseau au sein du fabric VXLAN tout en permettant une communication sélective avec les réseaux externes. Cela garantit que les hôtes VXLAN restent isolés les uns des autres en fonction de leurs attributions VRF tout en étant en mesure d’accéder aux ressources externes selon les besoins.

3. Application des politiques : les fuites VRF permettent aux administrateurs d'appliquer des politiques réseau et des contrôles d'accès pour le trafic circulant entre les hôtes VXLAN et les hôtes externes. Cela garantit que les communications utilisent des stratégies de sécurité prédéfinies et empêche tout accès non autorisé aux ressources sensibles.

4. Évolutivité et flexibilité : les fuites VRF améliorent l'évolutivité et la flexibilité des déploiements VXLAN en permettant aux hôtes VXLAN de communiquer de manière transparente avec les hôtes externes. Il permet l'allocation et le partage dynamiques des ressources entre le VXLAN et les réseaux externes, en s'adaptant à l'évolution des besoins du réseau sans perturber les configurations existantes.

Le filtrage des routes dans les fuites VRF (Virtual Routing and Forwarding) est essentiel pour maintenir la sécurité du réseau, optimiser l'efficacité du routage et empêcher les fuites de données non souhaitées. Les fuites VRF permettent la communication entre les réseaux virtuels tout en les maintenant logiquement séparés.

L'importance du filtrage des routes dans les fuites VRF peut être résumée dans les instructions

suivantes :

1. Sécurité : le filtrage des routes garantit que seules des routes spécifiques fuient entre les instances VRF, réduisant ainsi le risque d'accès non autorisé ou de violation de données. En contrôlant les routes autorisées à traverser les frontières VRF, les administrateurs peuvent appliquer des stratégies de sécurité et empêcher l'exposition d'informations sensibles à des entités non autorisées.

2. Isolement : les VRF sont conçus pour assurer la segmentation et l'isolation du réseau, ce qui permet à différents locataires ou services de fonctionner indépendamment au sein de la même infrastructure physique. Le filtrage des routes dans les fuites VRF contribue à maintenir cette isolation en limitant l'étendue de la propagation de la route entre les instances VRF, en empêchant les communications non intentionnelles et les vulnérabilités potentielles de sécurité.

3. Routage optimisé : le filtrage des routes permet aux administrateurs de ne laisser échapper que les routes nécessaires entre les VRF, ce qui optimise l'efficacité du routage et réduit le trafic inutile sur le réseau. En filtrant les routes non pertinentes, les administrateurs peuvent s'assurer que le trafic utilise les chemins les plus efficaces tout en minimisant l'encombrement et la latence.

4. Utilisation des ressources : en filtrant les routes, les administrateurs peuvent contrôler le flux du trafic entre les instances VRF, ce qui optimise l'utilisation des ressources et l'allocation de la bande passante. Cela permet d'éviter l'encombrement du réseau et garantit que les ressources critiques sont disponibles pour les applications ou les services prioritaires.

5. Conformité : le filtrage des routes dans les fuites VRF aide les entreprises à maintenir la conformité aux exigences réglementaires et aux normes du secteur. En limitant les fuites de routes aux seules entités autorisées, les entreprises peuvent démontrer leur conformité aux réglementations en matière de protection des données et garantir l'intégrité des informations sensibles.

6. Contrôle granulaire : le filtrage des routes offre aux administrateurs un contrôle granulaire sur la communication entre les instances VRF, leur permettant de définir des politiques spécifiques en fonction de leurs besoins uniques. Cette flexibilité permet aux entreprises d'adapter leurs configurations réseau aux besoins des différentes applications, utilisateurs ou services.

Conditions préalables

Environnement VXLAN existant avec un routeur périphérique

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Plate-forme NXOS

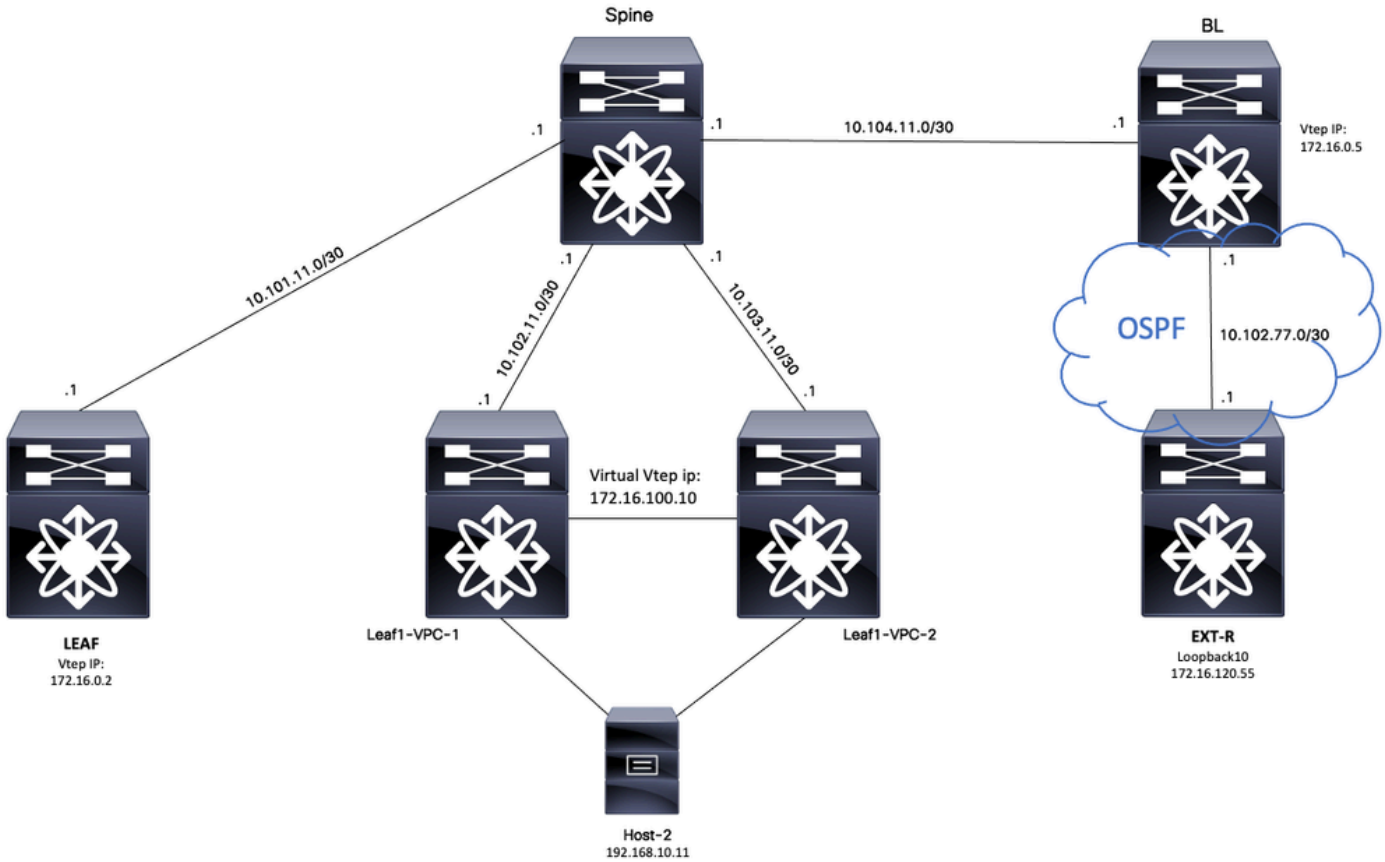
- VXLAN
- VRF
- BGP

Composants utilisés

Nom	Plateforme	Version
HÔTE-2	N9K-C92160YC-X	9.3(6)
Leaf-VPC-1	N9K-C93180YC-EX	9.3(9)
Leaf-VPC-2	N9K-C93108TC-EX	9.3(9)
FEUILLE	N9K-C932D-GX2B	10.2(6)
BL	N9K-C9348D-GX2A	10.2(5)
EXT-R	N9K-C9348D-GX2A	10.2(3)
DOS	N9K-C93108TC-FX3P	10.1(1)

"Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est actif, assurez-vous de comprendre l'impact potentiel de toute commande. »

Diagramme



En considérant BGP comme une application, BGP est l'application qui est utilisée pour effectuer une fuite entre les VRF

VRF par défaut au locataire-VRF

Pour cet exemple, Border VTEP (BL) reçoit 172.16.120.55 du périphérique externe via OSFP dans le VRF par défaut qui va être transmis au VRF du locataire.

Vérifier la table de routage

```
BL# sh ip route 172.16.120.55
IP Route Table for VRF "default"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

172.16.120.55/32, ubest/mbest: 1/0
*via 10.105.100.2, Eth1/41.2, [110/2], 00:00:10, ospf-1, intra
```

Filtrer le routage

Dans NXOS, une route-map est requise comme paramètre pour filtrer et redistribuer les routes, pour cet exemple le préfixe 172.16.120.55/32 va être filtré.

Configurer

	Commande ou action	Objectif
Étape 1	BL# configure terminal Entrez les commandes de configuration, une par ligne. Terminez par CNTL/Z.	Passe en mode de configuration.
Étape 2	BL(config)# ip prefix-list VXLAN-VRF-default-to-Tenant permit 172.16.120.55/32	Créez une liste de préfixes correspondant à l'hôte.
Étape 3	BL(config)# route-map VXLAN-VRF-default-to-Tenant	Créez une route-map.
Étape 4	BL(config-route-map)# match ip address prefix-list VXLAN-VRF-default-to-Tenant	Faites correspondre la liste de préfixes créée à

		l'étape 2.

Importer la route vers BGP

Une fois qu'il a été vérifié que la route existe sur le VRF par défaut, la route doit être importée dans le processus BGP.

Configurer

	Commande ou action	Objectif
Étape 1	BL# configure terminal Entrez les commandes de configuration, une par ligne. Terminez par CNTL/Z.	Passe en mode de configuration.
Étape 2	BL(config)# router bgp 65000	Passe en configuration BGP.
Étape 3	BL(config-router)# address-family ipv4 unicast	Saisissez l'adresse BGP-famili IPV4.
Étape 4	BL(config-router-af)# redistribute ospf 1 route-map VXLAN-VRF-default-to-Tenant	Redistribuez la route du protocole OSPF au protocole BGP à l'aide de la route-map créée à l'étape 3.

Vérifier la table BGP

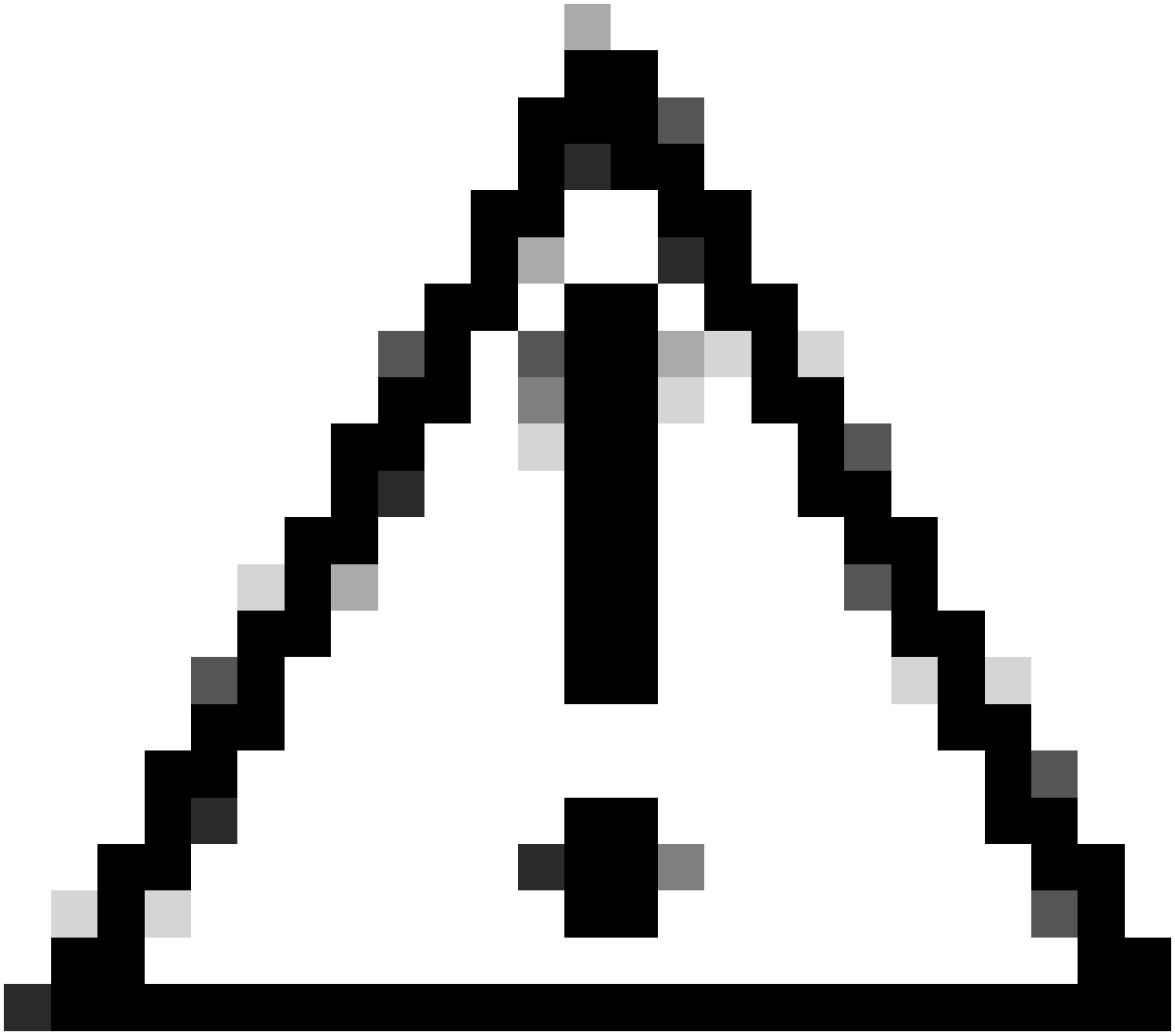
```
BL(config-router-af)# show ip bgp 172.16.120.55
BGP routing table information for VRF default, address family IPv4 Unicast
BGP routing table entry for 172.16.120.55/32, version 16
Paths: (1 available, best #1)
Flags: (0x000002) (high32 00000000) on xmit-list, is not in urib

Advertised path-id 1
Path type: redist, path is valid, is best path, no labeled nexthop
AS-Path: NONE, path locally originated
0.0.0.0 (metric 0) from 0.0.0.0 (172.16.0.5)
Origin incomplete, MED 2, localpref 100, weight 32768
Extcommunity: OSPF RT:0.0.0.0:0:0
```

Importer la route vers le VRF du locataire

Une fois la route importée vers BGP, la route peut maintenant être importée vers le VRF cible (tenant-a).

Configurer

	Commande ou action	Objectif
Étape 1	BL(config)# vrf context tenant-a	Passe en configuration VRF.
Étape 2	BL(config-vrf)# address-family ipv4 unicast	Entre la famille d'adresses IPV4.
Étape 3	BL(config-vrf-af-ipv4)# import vrf default map VXLAN-VRF-default-to-Tenant advertise-vpn	Importer le routage du VRF par défaut vers le VRF du locataire annonçant le VPN



Attention : par défaut, le nombre maximal de préfixes IP pouvant être importés du VRF par défaut dans un VRF autre que le VRF par défaut est de 1 000 routes. Cette valeur peut être modifiée avec la commande sous VRF address-family IPV4: import vrf <nombre de préfixes> default map <nom de la route-map> advertise-vpn.

Étapes récapitulatives

1. configurer le terminal
2. ip prefix-list VXLAN-VRF-default-to-Tenant permit 172.16.120.55/32
3. route-map VXLAN-VRF-default-to-Tenant
4. match ip address prefix-list VXLAN-VRF-default-to-Tenant
5. routeur bgp 65000
6. address-family ipv4 unicast
7. redistribute ospf 1 route-map VXLAN-VRF-default-to-Tenant
8. vrf context tenant-a
9. address-family ipv4 unicast
10. import vrf default map VXLAN-VRF-default-to-Tenant advertise-vpn

Vérifier

Vérifiez que la route est importée vers L2VPN.

```
BL# sh bgp l2vpn evpn 172.16.120.55
BGP routing table information for VRF default, address family L2VPN EVPN
Route Distinguisher: 172.16.0.5:3 (L3VNI 303030)
BGP routing table entry for [5]:[0]:[0]:[32]:[172.16.120.55]/224, version 38
Paths: (1 available, best #1)
Flags: (0x000002) (high32 00000000) on xmit-list, is not in l2rib/evpn
Multipath: Mixed

Advertised path-id 1
Path type: local, path is valid, is best path, no labeled nexthop
Gateway IP: 0.0.0.0
AS-Path: NONE, path locally originated
172.16.0.5 (metric 0) from 0.0.0.0 (172.16.0.5)
Origin incomplete, MED 2, localpref 100, weight 32768
Received label 303030
Extcommunity: RT:65000:303030 ENCAP:8 Router MAC:20cf.ae54.fa3b
OSPF RT:0.0.0.0:0:0

Path-id 1 advertised to peers:
10.104.11.1
```

Vérifier que la route est importée vers le VRF du locataire

```
BL# sh ip route 172.16.120.55 vrf tenant-a
IP Route Table for VRF "tenant-a"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

172.16.120.55/32, ubest/mbest: 1/0
*via 172.16.0.5%default, [200/2], 00:02:47, bgp-65000, internal, tag 65000, segid: 303030 tunnelid: 0xa
```

Locataire-VRF vers VRF par défaut

Pour cet exemple, le VTEP en limite (BL) reçoit la route 192.168.10.11 via le VXLAN sur le locataire-un VRF qui va être transmis au VRF par défaut.

Vérifier la table de routage

```
BL# sh ip route 192.168.10.11 vrf tenant-a
IP Route Table for VRF "tenant-a"
```

```
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

192.168.10.11/32, ubest/mbest: 1/0
*via 172.16.100.10%default, [200/0], 01:15:04, bgp-65000, internal, tag 65000, segid: 303030 tunnelid:
```

Filtrer le routage

Dans NXOS, une route-map est requise en tant que paramètre pour filtrer et redistribuer les routes, pour cet exemple le préfixe 172.16.120.55/32 va être filtré.

Configurer

	Commande ou action	Objectif
Étape 1	BL# configure terminal Entrez les commandes de configuration, une par ligne. Terminez par CNTL/Z.	Passe en mode de configuration.
Étape 2	BL(config)# ip prefix-list VXLAN-VRF-Tenant-to-default permit 192.168.10.11/32	Créez une liste de préfixes correspondant à l'hôte.
Étape 3	BL(config)# route-map VXLAN-VRF-Tenant-to-default	Créez une route-map.
Étape 4	BL(config-route-map)# match ip address prefix-list VXLAN-VRF-Tenant-to-default	Faites correspondre la liste de préfixes créée à l'étape 2.

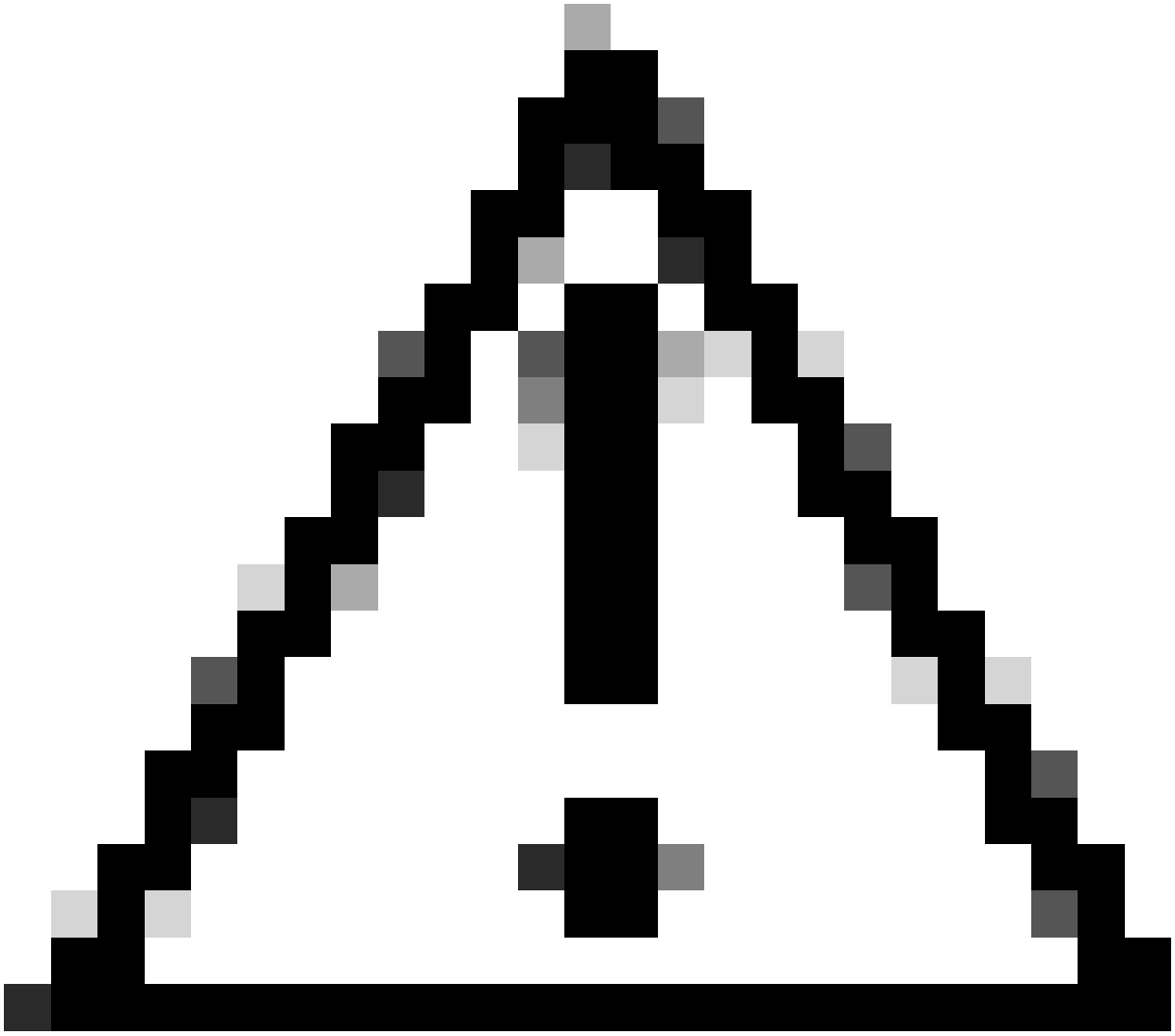
Exporter la route vers le VRF par défaut à partir du locataire-un VRF

Puisque la route est déjà sur le processus L2VPN BGP, elle doit seulement être exportée vers la valeur VRF par défaut.

Configurer

	Commande ou action	Objectif

Étape 1	BL# configure terminal Entrez les commandes de configuration, une par ligne. Terminez par CNTL/Z.	Passe en mode de configuration.
Étape 2	BL(config)# vrf context tenant-a	Passe en configuration VRF.
Étape 3	BL(config-vrf)# address-family ipv4 unicast	Saisissez VRF address-family IPV4.
Étape 4	BL(config-vrf-af-ipv4)# export vrf default map VXLAN-VRF-Tenant-to-default allow-vpn	Exporter la route du VRF du locataire vers le VRF par défaut autorisant le VPN



Attention : par défaut, le nombre maximal de préfixes IP pouvant être exportés du VRF autre que par défaut vers un VRF par défaut est de 1 000 routes. Cette valeur peut être modifiée avec la commande sous VRF address-family IPV4 : export vrf default <number of prefixes> map <route-map name> allow-vpn.

Étapes récapitulatives

1. configurer le terminal
2. ip prefix-list VXLAN-VRF-Tenant-to-default permit 192.168.10.11/32
3. route-map VXLAN-VRF-Tenant-to-default
4. match ip address prefix-list VXLAN-VRF-Tenant-to-default
5. vrf context tenant-a
6. address-family ipv4 unicast
7. export vrf default map VXLAN-VRF-Tenant-to-default allow-vpn

Vérifier

Vérifiez que la route est importée vers la famille d'adresses BGP IPV4 sur le VRF par défaut

```
BL(config-router-vrf-neighbor)# sh ip bgp 192.168.10.11
BGP routing table information for VRF default, address family IPv4 Unicast
BGP routing table entry for 192.168.10.11/32, version 55
Paths: (1 available, best #1)
Flags: (0x8000001a) (high32 00000000) on xmit-list, is in urib, is best urib route, is in HW

Advertised path-id 1
Path type: internal, path is valid, is best path, no labeled nexthop, in rib
Imported from 172.16.0.5:3:192.168.10.11/32 (VRF tenant-a)
Original source: 172.16.100.1:32777:[2]:[0]:[0]:[48]:[0027.e380.6059]:[32]:[192.168.10.11]/272
AS-Path: NONE, path sourced internal to AS
172.16.100.10 (metric 45) from 10.104.11.1 (192.168.0.11)
Origin IGP, MED not set, localpref 100, weight 0
Received label 101010 303030
Extcommunity: RT:65000:101010 RT:65000:303030 SOO:172.16.100.10:0 ENCAP:8
Router MAC:70db.9855.f52f
Originator: 172.16.100.1 Cluster list: 192.168.0.11

Path-id 1 not advertised to any peer
```

Vérifier que la route est importée dans la table de routage VRF par défaut

```
BL(config-router-vrf-neighbor)# show ip route 192.168.10.11
IP Route Table for VRF "default"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

192.168.10.11/32, ubest/mbest: 1/0
*via 172.16.100.10, [200/0], 00:03:51, bgp-65000, internal, tag 65000, segid: 303030 tunnelid: 0xac1064

Tenant-VRF to Default VRF
```

Du locataire-VRF au locataire-VRF

Pour cet exemple, LEAF de nexus reçoit la route 172.16.120.55/32 tenant-a qui va être divulguée à VRF tenant-b

Vérifier la table de routage

```
show ip route 172.16.120.55/32 vrf tenant-a
IP Route Table for VRF "tenant-a"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
```

```
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

172.16.120.55/32, ubest/mbest: 1/0
*via 172.16.0.5%default, [200/2], 4d02h, bgp-65000, internal, tag 65000, segid: 303030 tunnelid: 0xac10
```

Filtrer le routage

Afin de filtrer les routes, deux étapes sont nécessaires, le filtrage entre les VRF est effectué via des cibles de route (RT), RT est conforme par <BGP Process ID>:L3VNI ID> et le filtrage de sous-réseaux spécifiques. Si la deuxième étape n'est pas utilisée, toutes les routes du VRF source seront transmises au VRF de destination.

Identifier la cible de routage

<#root>

```
LEAF# show nve vni
<Snipped>
Interface VNI Multicast-group State Mode Type [BD/VRF] Flags
--------- -------- ----------------- ----- ---- ------------------ -----
nve1 50500 n/a Up CP L3 [tenant-b]
nve1 101010 224.10.10.10 Up CP L2 [10]
nve1 202020 224.10.10.10 Up CP L2 [20]
nve1
```

303030

```
 n/a Up CP L3 [
```

tenant-a

```
]

LEAF# show run bgp | include ignore-case router
router bgp
```

65000

```
router-id 172.16.0.2
```

Pour cet exemple, la cible de route est égale à : 65000:303030 et la route 172.16.120.55/32 va être filtrée.

Configurer

	Commande ou action	Objectif

Étape 1	LEAF# configure terminal Entrez les commandes de configuration, une par ligne. Terminez par CNTL/Z.	Passe en mode de configuration.
Étape 2	LEAF(config)# ip prefix-list filter-tenant-a-to-tenant-b permit 172.16.120.55/32	Créez une liste de préfixes correspondant à l'hôte.
Étape 3	LEAF(config)# route-map tenantA-to-tenantB	Créez une route-map.
Étape 4	LEAF(config-route-map)# match ip address prefix-listfilter-tenant-a-to-tenant-b	Faites correspondre la liste de préfixes créée à l'étape 2.

Importer la route vers le locataire-un VRF à partir du locataire-un VRF

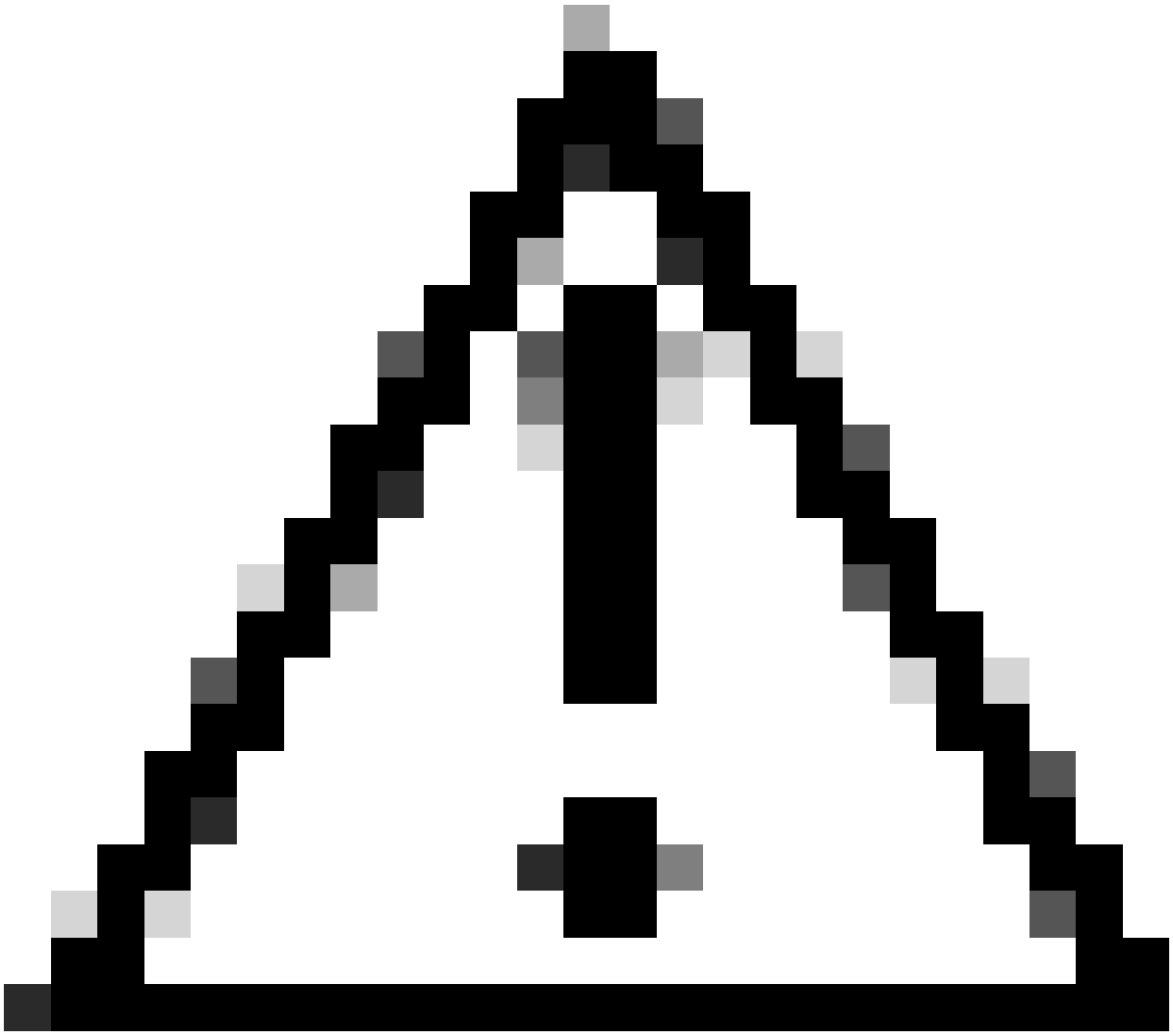
Une fois que RT est identifié et que le filtrage est configuré, la route peut être importée vers le VRF de destination (tenant-b)

Configurer

	Commande ou action	Objectif
Étape 1	LEAF# configure terminal Entrez les commandes de configuration, une par ligne. Terminez par CNTL/Z.	Passe en mode de configuration.
Étape 2	LEAF(config)# vrf context tenant-b	Passe en configuration VRF.
Étape 3	LEAF(config-vrf)# address-family ipv4 unicast	Saisissez VRF address-family IPV4.

Étape 4	LEAF(config-vrf-af-ipv4)# import map tenantA-to-tenantB	Importer la route filtrée avec route-map
Étape 5	LEAF(config-vrf-af-ipv4)# route-target import 65000:303030	Importer la cible de routage
Étape 6	LEAF(config-vrf-af-ipv4)# route-target import 65000:303030 evpn	Importer un evpn cible de routage

---



Attention : le fait de ne pas utiliser de mappage d'importation peut autoriser toutes les routes du VRF d'origine vers le VRF cible. L'utilisation de la carte d'importation peut permettre de contrôler les routes à fuiter.

Étapes récapitulatives

1. configurer le terminal
2. ip prefix-list filter-tenant-a-to-tenant-b permit 172.16.120.55/32
3. route-map tenantA-to-tenantB
4. match ip address prefix-listfilter-tenant-a-to-tenant-b
5. vrf context tenant-b
6. address-family ipv4 unicast
7. importer le mappage tenantA-vers-tenantB
8. route-target import 65000:303030
9. route-target import 65000:303030 evpn

Vérifier

Vérifier que la route est importée vers BGP sur le VRF locataire-b

```
LEAF(config-vrf-af-ipv4)# show ip bgp 172.16.120.55/32 vrf tenant-b
BGP routing table information for VRF tenant-b, address family IPv4 Unicast
BGP routing table entry for 172.16.120.55/32, version 311
Paths: (1 available, best #1)
Flags: (0x8008021a) (high32 00000000) on xmit-list, is in urib, is best urib route, is in HW
vpn: version 456, (0x00000000100002) on xmit-list

Advertised path-id 1, VPN AF advertised path-id 1
Path type: internal, path is valid, is best path, no labeled nexthop, in rib
Imported from 172.16.0.5:3:[5]:[0]:[0]:[32]:[172.16.120.55]/224
AS-Path: NONE, path sourced internal to AS
172.16.0.5 (metric 45) from 10.101.11.1 (192.168.0.11)
Origin incomplete, MED 2, localpref 100, weight 0
Received label 303030
Extcommunity: RT:65000:303030 ENCAP:8 Router MAC:20cf.ae54.fa3b
OSPF RT:0.0.0.0:0:0
Originator: 172.16.0.5 Cluster list: 192.168.0.11

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

VPN AF advertise information:
Path-id 1 not advertised to any peer
```

Vérifier que la route est importée dans la table de routage sur le VRF tenant-b

```
LEAF# show ip route 172.16.120.55/32 vrf tenant-b
IP Route Table for VRF "tenant-b"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>
```

```
172.16.120.55/32, ubest/mbest: 1/0
*via 172.16.0.5%default, [200/2], 00:00:08, bgp-65000, internal, tag 65000, segid: 303030 (Asymmetric)
```

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.