Configurazione e verifica delle perdite VXLAN VRF su Nexus 9000

Sommario

Introduzione

Questo documento descrive come configurare e verificare le perdite VRF in un ambiente VXLAN.

Premesse

In un ambiente VXLAN (Virtual Extensible LAN), la connessione di host VXLAN a host esterni dalla struttura richiede spesso l'uso di dispositivi VRF leaking e Border Leaf.

La perdita di VRF è fondamentale per consentire la comunicazione tra gli host VXLAN e gli host esterni, mantenendo la segmentazione e la sicurezza della rete.

Il dispositivo Border Leaf funge da gateway tra il fabric VXLAN e le reti esterne, svolgendo un ruolo centrale nel facilitare la comunicazione.

L'importanza della perdita di VRF in questo scenario può essere riassunta con le seguenti affermazioni:

1. Interconnessione con reti esterne: la perdita di VRF consente agli host VXLAN all'interno del fabric di comunicare con gli host esterni all'esterno del fabric. In questo modo è possibile accedere a risorse, servizi e applicazioni ospitati su reti esterne, ad esempio Internet o altri centri dati.

2. Segmentazione e isolamento della rete: la perdita di VRF mantiene la segmentazione e l'isolamento della rete all'interno del fabric VXLAN, consentendo al tempo stesso la comunicazione selettiva con le reti esterne. Ciò garantisce che gli host VXLAN rimangano isolati l'uno dall'altro in base alle assegnazioni VRF, pur essendo in grado di accedere alle risorse esterne in base alle esigenze.

3. Applicazione delle policy: la perdita di dati VRF consente agli amministratori di applicare policy di rete e controlli degli accessi per il flusso di traffico tra gli host VXLAN e gli host esterni. Ciò garantisce che la comunicazione utilizzi criteri di sicurezza predefiniti e previene l'accesso non autorizzato alle risorse sensibili.

4. Scalabilità e flessibilità: la perdita di VRF migliora la scalabilità e la flessibilità delle implementazioni VXLAN consentendo agli host VXLAN di comunicare con gli host esterni. Consente l'allocazione e la condivisione dinamica delle risorse tra VXLAN e reti esterne, adattandosi ai requisiti di rete in continua evoluzione senza interrompere le configurazioni esistenti.

Il filtraggio dei percorsi in VRF (Virtual Routing and Forwarding) è fondamentale per mantenere la sicurezza della rete, ottimizzare l'efficienza del routing e prevenire perdite di dati non intenzionali. La perdita di VRF consente la comunicazione tra le reti virtuali, mantenendole logicamente separate.

L'importanza di filtrare le route nelle perdite VRF è importante e può essere riassunta con le

istruzioni seguenti:

1. Sicurezza: il filtraggio delle route garantisce che tra le istanze VRF vengano trapelate solo route specifiche, riducendo il rischio di accessi non autorizzati o violazioni dei dati. Controllando le route autorizzate a superare i limiti VRF, gli amministratori possono applicare policy di sicurezza e impedire l'esposizione di informazioni riservate a entità non autorizzate.

2. Isolamento: i VRF sono progettati per fornire segmentazione e isolamento della rete, consentendo a tenant o reparti diversi di operare in modo indipendente all'interno della stessa infrastruttura fisica. Il filtraggio delle route nella perdita VRF consente di mantenere l'isolamento limitando l'ambito della propagazione delle route tra istanze VRF, impedendo la comunicazione non intenzionale e potenziali vulnerabilità di sicurezza.

3. Optimized Routing: il filtro dei percorsi consente agli amministratori di trafugare in modo selettivo solo i percorsi necessari tra VRF, ottimizzando l'efficienza del routing e riducendo il traffico non necessario attraverso la rete. Filtrando i percorsi irrilevanti, gli amministratori possono garantire che il traffico utilizzi i percorsi più efficienti riducendo al minimo la congestione e la latenza.

4. Utilizzo delle risorse: filtrando le route, gli amministratori possono controllare il flusso di traffico tra le istanze VRF, ottimizzando l'utilizzo delle risorse e l'allocazione della larghezza di banda. In questo modo si evita la congestione della rete e si garantisce la disponibilità di risorse critiche per applicazioni o servizi prioritari.

5. Conformità: il filtraggio delle route in caso di perdita di VRF consente alle organizzazioni di mantenere la conformità ai requisiti normativi e agli standard di settore. Limitando la perdita di percorsi solo alle entità autorizzate, le organizzazioni possono dimostrare la conformità alle normative sulla protezione dei dati e garantire l'integrità delle informazioni sensibili.

6. Controllo granulare: il filtro delle route offre agli amministratori un controllo granulare della comunicazione tra le istanze VRF, consentendo loro di definire policy specifiche in base ai requisiti specifici. Questa flessibilità consente alle organizzazioni di personalizzare le configurazioni di rete per soddisfare le esigenze di applicazioni, utenti o reparti diversi.

Prerequisiti

Ambiente VXLAN esistente con router di confine

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

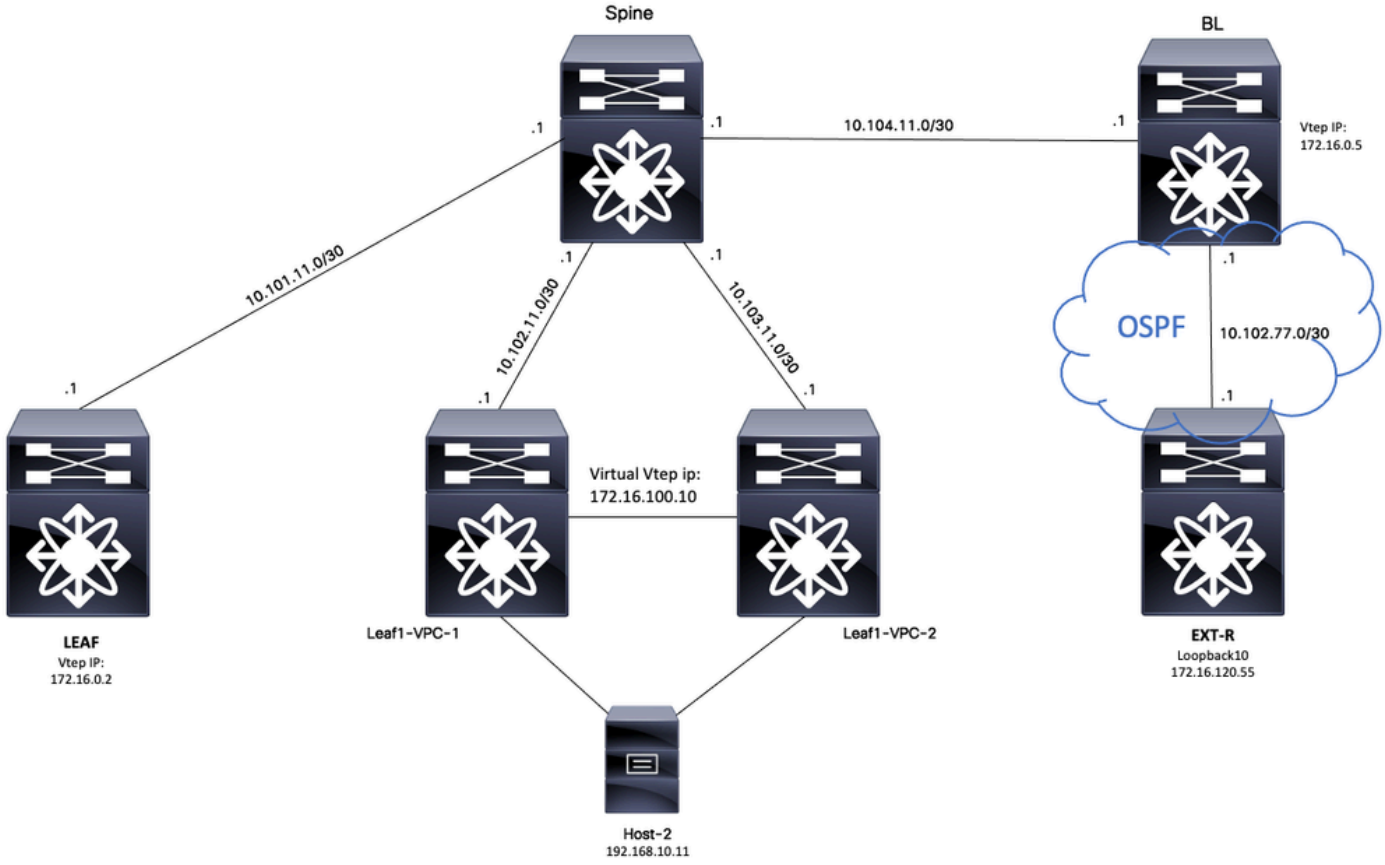
- Piattaforma NXOS
- VXLAN
- VRF
- BGP

Componenti usati

Nome	Piattaforma	Version
HOST-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)
FOGLIA	N9K-C932D-GX2B	10.2(6)
BL	N9K-C9348D-GX2A	10.2(5)
EST-R	N9K-C9348D-GX2A	10.2(3)
DORSO	N9K-C93108TC-FX3P	10.1(1)

"Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi".

Diagramma



Considerando BGP come un'applicazione, BGP è l'applicazione utilizzata per eseguire la perdita tra VRF

VRF predefinito su Tenant-VRF

Per questo esempio, il Border VTEP (BL) riceve la porta 172.16.120.55 da un dispositivo esterno tramite OSFP su un VRF predefinito che andrà perduta sul VRF tenant.

Verifica tabella di routing

```
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
```

Filtra route

In NXOS è necessario specificare una route-map come parametro per filtrare e ridistribuire le route. In questo esempio verrà filtrato il prefisso 172.16.120.55/32.

Configurazione

	Comando o azione	Scopo
Passaggio 1	BL# configurazione terminale Immettere i comandi di configurazione, uno per riga. Termina con CNTL/Z.	Accede alla modalità di configurazione.
Passaggio 2	BL(config)# ip prefix-list VXLAN-VRF-default-to-Tenant permette 172.16.120.55/32	Creare un host corrispondente all'elenco di prefissi.
Passaggio 3	BL(config)# route-map VXLAN-VRF-default-to-Tenant	Creare la mappa del percorso.
Passaggio 4	BL(config-route-map)# corrispondenza prefisso-elenco indirizzi IP VXLAN-VRF-default-to-Tenant	Corrispondenza prefisso-elenco creato nel passaggio 2.

Importa route in BGP

Una volta verificata l'esistenza della route sul VRF predefinito, è necessario importare la route nel processo BGP.

Configurazione

	Comando o azione	Scopo
Passaggio 1	BL# configurazione terminale Immettere i comandi di configurazione, uno per riga. Termina con CNTL/Z.	Accede alla modalità di configurazione.
Passaggio 2	BL(config)# router bgp 6500	Immette la configurazione BGP.
Passaggio 3	BL(config-router)# famiglia di indirizzi ipv4 unicast	Immettere l'indirizzo BGP IPV4 della famiglia di indirizzi.
Passaggio 4	BL(config-router-af)# ridistribuzione ospf 1 route-map VXLAN-VRF-default-to-Tenant	Ridistribuire la route da OSPF a BGP utilizzando la route-map creata nel passaggio 3.

Verifica tabella BGP

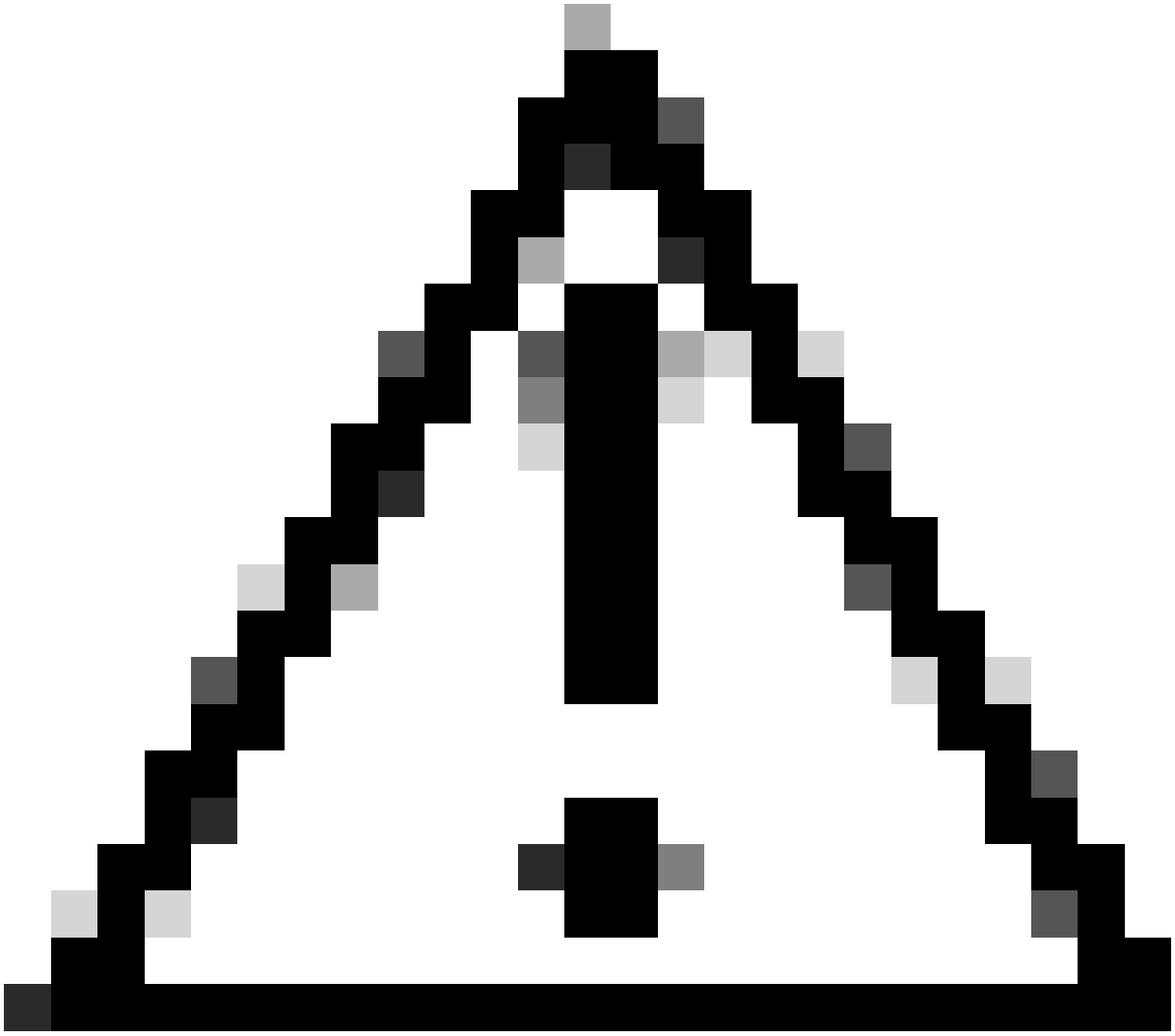
```
BL(config-router-af)# show ip bgp 172.16.120.55
BGP routing table information for VRF default, address family IPv4 Unicast
BGP routing table entry for 172.16.120.55/32, version 16
Paths: (1 available, best #1)
Flags: (0x000002) (high32 00000000) on xmit-list, is not in urib

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
```

Importa route a VRF tenant

Una volta importata la route in BGP, la route può essere importata nel VRF (tenant-a) di destinazione.

Configurazione

	Comando o azione	Scopo
Passaggio 1	BL(config)# vrf context tenant-a	Accede alla configurazione VRF.
Passaggio 2	BL(config-vrf)# famiglia di indirizzi ipv4 unicast	Immette la famiglia di indirizzi IPV4.
Passaggio 3	BL(config-vrf-af-ipv4)# import vrf mappa predefinita VXLAN-VRF-default-to-Tenant annuncio-vpn	Importa route da VRF predefinita a VPN pubblicità VRF tenant



Attenzione: per impostazione predefinita, il numero massimo di prefissi IP che possono essere importati dal VRF predefinito in un VRF non predefinito è 1000 route. Questo valore può essere modificato con il comando in VRF address-family IPV4: import vrf <numero di prefissi> default map <nome-route-map> annuncio-vpn.

Passi di riepilogo

1. configurare il terminale
2. ip prefix-list VXLAN-VRF-default-to-Tenant allow 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. router bgp 6500
6. unicast ipv4 famiglia di indirizzi
7. ridistribuire ospf 1 route-map VXLAN-VRF-default-to-Tenant
8. tenant-a contesto vrf
9. unicast ipv4 famiglia di indirizzi
10. import vrf mappa predefinita VXLAN-VRF-default-to-Tenant annuncio-vpn

Verifica

Verificare che la route sia importata in 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
```

Verificare che la route sia importata nel VRF tenant

```
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
```

Tenant-VRF su VRF predefinito

Nell'esempio, il Border VTEP (BL) riceve la route 192.168.10.11 tramite VXLAN sul tenant-a VRF che verrà trapelata al VRF predefinito.

Verifica tabella di routing

```
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:
```

Filtra route

In NXOS è necessario specificare una route-map come parametro per filtrare e ridistribuire le route. In questo esempio verrà filtrato il prefisso 172.16.120.55/32.

Configurazione

	Comando o azione	Scopo
Passaggio 1	BL# configurazione terminale Immettere i comandi di configurazione, uno per riga. Termina con CNTL/Z.	Accede alla modalità di configurazione.
Passaggio 2	BL(config)# ip prefix-list VXLAN-VRF-Tenant-to-default allow 192.168.10.11/32	Creare un host corrispondente all'elenco di prefissi.
Passaggio 3	BL(config)# route-map VXLAN-VRF-Tenant-to-default	Creare la mappa del percorso.
Passaggio 4	BL(config-route-map)# match ip address prefix-list VXLAN-VRF-Tenant-to-default	Corrispondenza prefisso-elenco creato nel passaggio 2.

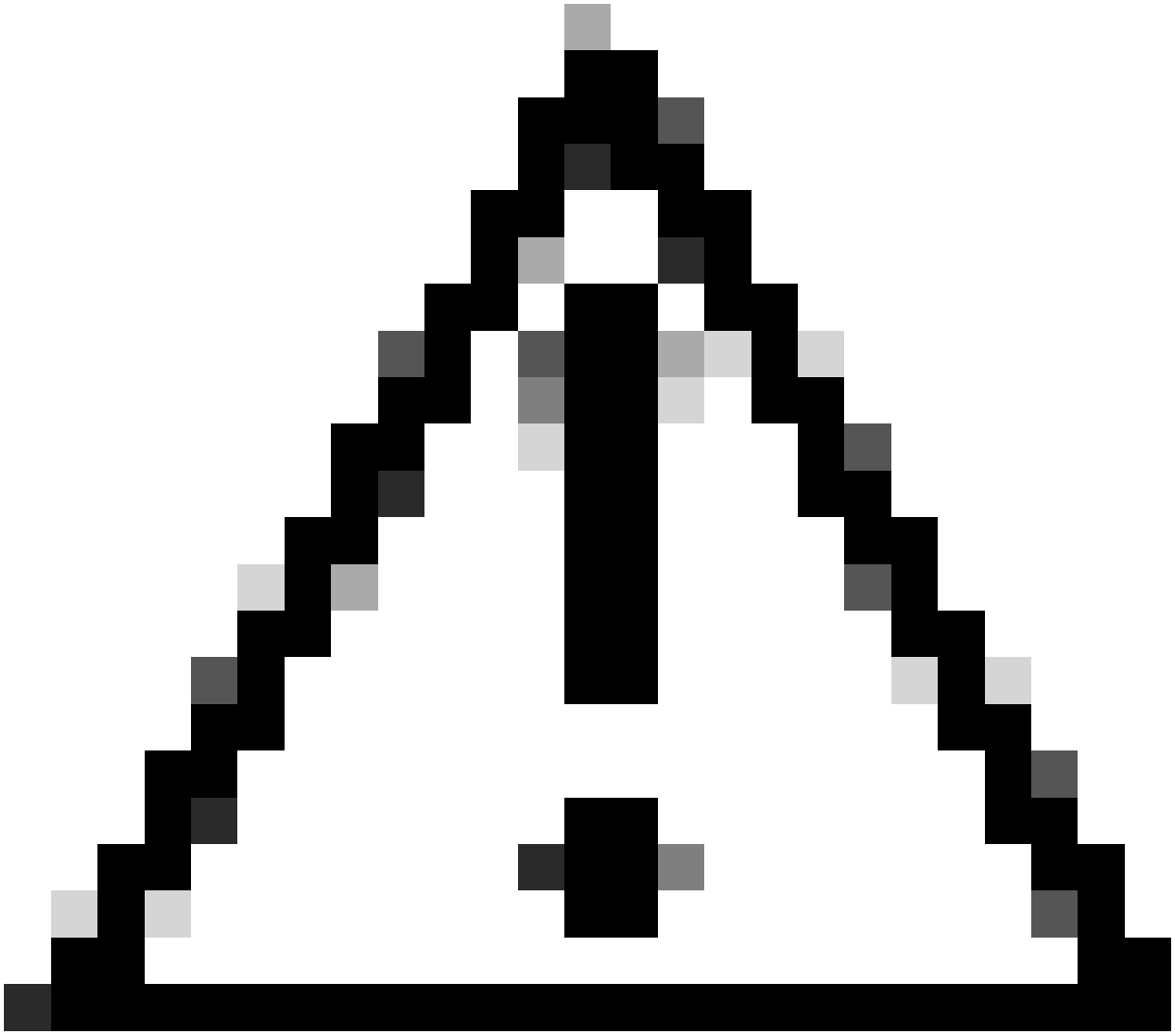
Esporta route al VRF predefinito dal tenant-a VRF

Poiché la route è già nel processo BGP L2VPN, deve essere esportata solo nell'impostazione predefinita VRF.

Configurazione

	Comando o azione	Scopo

Passaggio 1	BL# configurazione terminale Immettere i comandi di configurazione, uno per riga. Termina con CNTL/Z.	Accede alla modalità di configurazione.
Passaggio 2	BL(config)# vrf context tenant-a	Accede alla configurazione VRF.
Passaggio 3	BL(config-vrf)# famiglia di indirizzi ipv4 unicast	Immettere VRF address-family IPV4.
Passaggio 4	BL(config-vrf-af-ipv4)# export vrf mappa predefinita VXLAN-VRF-Tenant-to-default allow-vpn	Esporta route dal VRF tenant al VRF predefinito che consente la VPN



Attenzione: per impostazione predefinita, il numero massimo di prefissi IP che possono essere esportati dal VRF non predefinito in un VRF predefinito è 1000 route. Questo valore può essere modificato con il comando in VRF address-family IPV4: export vrf default <number of prefixes> map <route-map name> allow-vpn.

Passi di riepilogo

1. configurare il terminale
2. ip prefix-list VXLAN-VRF-Tenant-to-default allow 192.168.10.11/32
3. route-map VXLAN-VRF-Tenant-to-default
4. confronto tra prefisso indirizzi IP e elenco VXLAN-VRF-Tenant-to-default
5. tenant-a contesto vrf
6. unicast ipv4 famiglia di indirizzi
7. export vrf default map VXLAN-VRF-Tenant-to-default allow-vpn

Verifica

Verificare che la route sia importata nella famiglia di indirizzi IPV4 BGP sul VRF predefinito

```
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
```

Verificare che la route sia importata nella tabella di routing VRF predefinita

```
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
```

Tenant-VRF su Tenant-VRF

Per questo esempio nexus LEAF riceve la route 172.16.120.55/32 tenant-a che verrà persa in VRF tenant-b

Verifica tabella di routing

```
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
```

Filtra route

Per filtrare le route, sono necessari due passaggi: il filtro tra i VRF viene eseguito mediante il comando Route Targets (RT),il filtro RT viene eseguito in base a <BGP Process ID>:L3VNI ID> e al filtro di subnet specifiche. Se il secondo passaggio non viene utilizzato, tutte le route dal VRF di origine verranno trapelate al VRF di destinazione.

Identifica destinazione ciclo di lavorazione

<#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
```

Per questo esempio, il percorso Target è uguale a: 65000:303030 e il percorso 172.16.120.55/32 verrà filtrato.

Configurazione

	Comando o azione	Scopo

Passaggio 1	LEAF# configura terminale Immettere i comandi di configurazione, uno per riga. Termina con CNTL/Z.	Accede alla modalità di configurazione.
Passaggio 2	LEAF(config)# ip prefix-list filter-tenant-a-tenant-b permetta 172.16.120.55/32	Creare un host corrispondente all'elenco di prefissi.
Passaggio 3	LEAF(config)# route-map tenantA-to-tenantB	Creare la mappa del percorso.
Passaggio 4	LEAF(config-route-map)# match ip address prefix-listfilter-tenant-a-to-tenant-b	Corrispondenza prefisso-elenco creato nel passaggio 2.

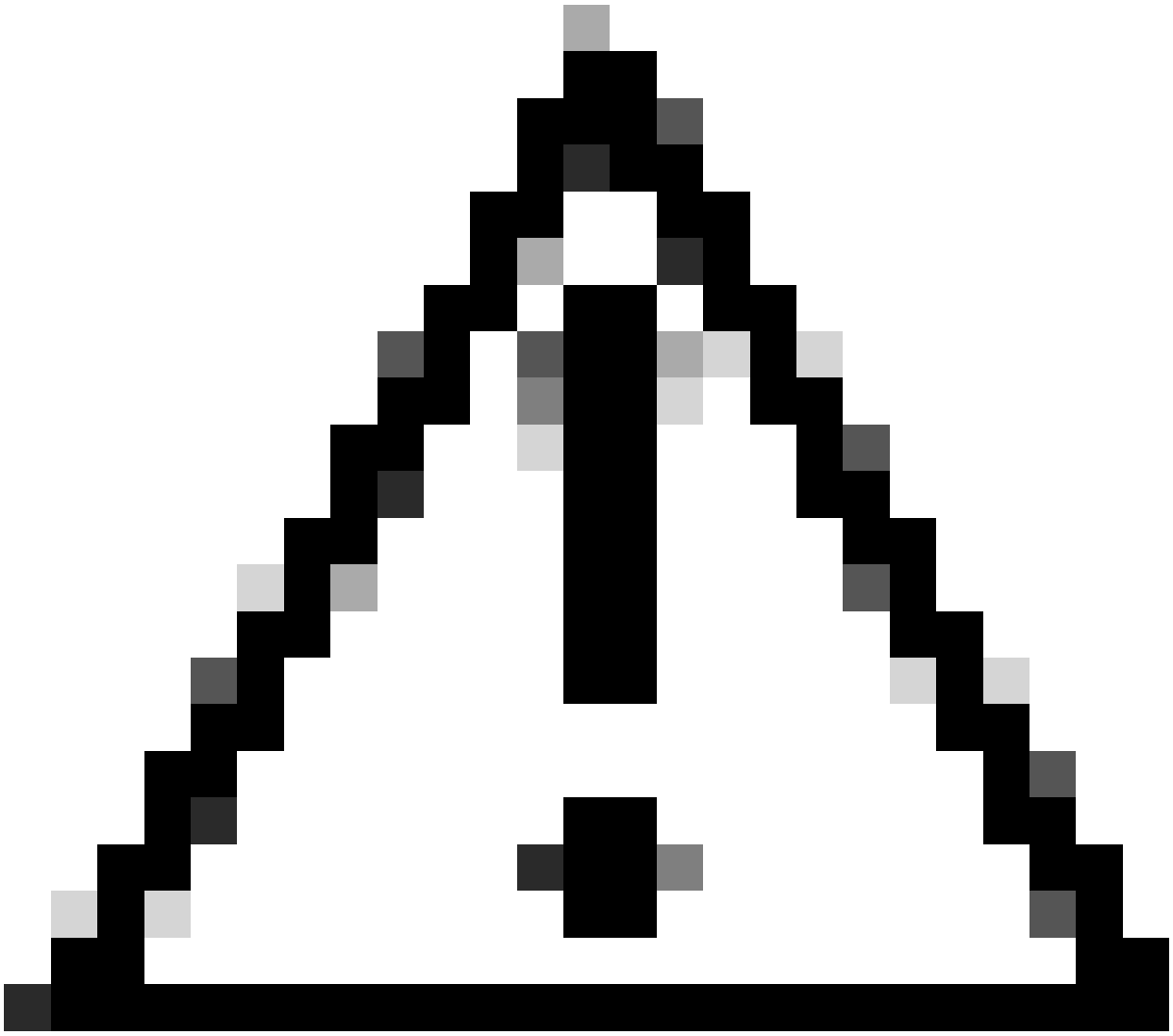
Importa route al tenant-a VRF dal tenant-a VRF

Una volta identificata la tecnologia RT e configurato il filtro, è possibile importare il percorso sul VRF di destinazione (tenant-b)

Configurazione

	Comando o azione	Scopo
Passaggio 1	LEAF# configura terminale Immettere i comandi di configurazione, uno per riga. Termina con CNTL/Z.	Accede alla modalità di configurazione.
Passaggio 2	LEAF(config)# vrf context tenant-b	Accede alla configurazione VRF.
Passaggio 3	LEAF(config-vrf)# famiglia di indirizzi ipv4 unicast	Immettere VRF address-family IPV4.

Passaggio 4	LEAF(config-vrf-af-ipv4)# importa il tenantA-to-tenantB	Importa route filtrata con route-map
Passaggio 5	LEAF(config-vrf-af-ipv4)# importazione route-target 6500:3030	Importa destinazione route
Passaggio 6	LEAF(config-vrf-af-ipv4)# route-target import 6500:303030 evpn	Importa evpn destinazione route



Attenzione: se non si utilizza una mappa di importazione, è possibile che tutte le route dal VRF di origine perdano verso il VRF di destinazione. L'utilizzo della mappa di importazione consente di controllare le route da trafugare.

Passi di riepilogo

1. configurare il terminale
2. autorizzazione ip prefix-list filter-tenant-a-tenant-b 172.16.120.55/32
3. route-map tenantA-tenantB
4. corrispondenza prefisso indirizzo ip-listfilter-tenant-a-tenant-b
5. vrf context tenant-b
6. unicast ipv4 famiglia di indirizzi
7. importa mapping tenantA-tenantB
8. route-target import 6500:303030
9. route-target import 6500:303030 evpn

Verifica

Verificare che la route sia importata in BGP sul tenant-b VRF

```
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
```

Verificare che la route sia importata nella tabella di routing nel 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)
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).