Konfigurieren und Überprüfen der VXLAN-VRF-Leaking auf dem Nexus 9000

Inhalt

- Einleitung
- Hintergrundinformationen
- Voraussetzungen
- Anforderungen
- Verwendete Komponenten
- Diagramm
- Standard-VRF zu Tenant-VRF
  - Routing-Tabelle überprüfen
  - Filterroute
    - Konfigurieren
  - Route in BGP importieren
    - Konfigurieren
    - BGP-Tabelle überprüfen
  - Route in Tenant-VRF importieren
    - Konfigurieren
  - Zusammenfassende Schritte
  - Überprüfung
    - Überprüfen Sie, ob die Route in L2VPN importiert wurde.
    - Überprüfen des Imports der Route in die Tenant-VRF-Instanz
- Tenant-VRF zu Standard-VRF
  - Routing-Tabelle überprüfen
  - Filterroute
    - Konfigurieren
  - Exportieren der Route von einer Tenant-VRF-Instanz in eine Standard-VRF-Instanz
    - Konfigurieren
  - Zusammenfassende Schritte
  - Überprüfung
    - Überprüfen des Imports der Route in die BGP IPV4-Adressfamilie bei Standard-VRF
    - Überprüfen, ob die Route in die Standard-VRF-Routing-Tabelle importiert wurde
- Tenant-VRF zu Tenant-VRF
  - Routing-Tabelle überprüfen
  - Filterroute
    - Route Target identifizieren
    - Konfigurieren
  - Route zu Tenant-a-VRF von Tenant-a-VRF importieren
    - Konfigurieren
  - Zusammenfassende Schritte
  - Überprüfung
    - Überprüfen des Imports der Route in das BGP bei Tenant-b-VRF

Überprüfen des Imports der Route in die Routing-Tabelle auf Tenant-b-VRF

Einleitung

In diesem Dokument wird beschrieben, wie VRF-Lecks in einer VXLAN-Umgebung konfiguriert und verifiziert werden.

Hintergrundinformationen

In einer VXLAN-Umgebung (Virtual Extensible LAN) ist für die Verbindung von VXLAN-Hosts mit externen Hosts aus der Fabric häufig die Verwendung von VRF Leaking- und Border Leaf-Geräten erforderlich.

VRF-Leaking ist für die Kommunikation zwischen VXLAN-Hosts und externen Hosts unter Beibehaltung der Netzwerksegmentierung und -sicherheit von entscheidender Bedeutung.

Das Border Leaf-Gerät dient als Gateway zwischen der VXLAN-Struktur und externen Netzwerken und spielt eine zentrale Rolle bei der Vereinfachung dieser Kommunikation.

Die Bedeutung von VRF-Leaking in diesem Szenario kann mit den folgenden Aussagen zusammengefasst werden:

1. Verbindung mit externen Netzwerken: VRF-Leaking ermöglicht VXLAN-Hosts innerhalb der Fabric die Kommunikation mit externen Hosts außerhalb der Fabric. Dies ermöglicht den Zugriff auf Ressourcen, Services und Anwendungen, die in externen Netzwerken wie dem Internet oder anderen Rechenzentren gehostet werden.

2. Netzwerksegmentierung und -isolierung: VRF-Leaking gewährleistet die Netzwerksegmentierung und -isolierung innerhalb der VXLAN-Fabric und ermöglicht gleichzeitig eine selektive Kommunikation mit externen Netzwerken. Auf diese Weise wird sichergestellt, dass VXLAN-Hosts basierend auf ihren VRF-Zuweisungen voneinander isoliert bleiben und weiterhin nach Bedarf auf externe Ressourcen zugreifen können.

3. Richtliniendurchsetzung: Mithilfe von VRF-Leaking können Administratoren Netzwerkrichtlinien und Zugriffskontrollen für den Datenverkehr zwischen VXLAN-Hosts und externen Hosts durchsetzen. So wird sichergestellt, dass bei der Kommunikation vordefinierte Sicherheitsrichtlinien verwendet werden und dass kein unbefugter Zugriff auf vertrauliche Ressourcen möglich ist.

4. Skalierbarkeit und Flexibilität: VRF-Leaking verbessert die Skalierbarkeit und Flexibilität von VXLAN-Bereitstellungen, da VXLAN-Hosts nahtlos mit externen Hosts kommunizieren können. Sie ermöglicht die dynamische Zuweisung und gemeinsame Nutzung von Ressourcen zwischen VXLAN und externen Netzwerken und kann so an sich ändernde Netzwerkanforderungen angepasst werden, ohne vorhandene Konfigurationen zu unterbrechen.

Die Filterung von Routen im VRF (Virtual Routing and Forwarding) ist für die Aufrechterhaltung der Netzwerksicherheit, die Optimierung der Routing-Effizienz und die Vermeidung

unbeabsichtigter Datenlecks von entscheidender Bedeutung. VRF Leaking ermöglicht die Kommunikation zwischen virtuellen Netzwerken, wobei diese logisch getrennt bleiben.

Die Bedeutung der Filterung von Routen bei VRF-Leaking ist wichtig und kann mit den folgenden Aussagen zusammengefasst werden:

1. Sicherheit: Durch das Filtern von Routen wird sichergestellt, dass nur bestimmte Routen zwischen VRF-Instanzen weitergeleitet werden, wodurch das Risiko von nicht autorisierten Zugriffen oder Datensicherheitsverletzungen reduziert wird. Durch die Festlegung, welche Routen VRF-Grenzen überschreiten dürfen, können Administratoren Sicherheitsrichtlinien durchsetzen und verhindern, dass vertrauliche Informationen unbefugten Personen zugänglich gemacht werden.

2. Isolierung: VRFs sind auf Netzwerksegmentierung und -isolierung ausgelegt, sodass verschiedene Tenants oder Abteilungen unabhängig innerhalb derselben physischen Infrastruktur agieren können. Die Filterung von Routen in VRF-Leaking hilft, diese Isolierung aufrechtzuerhalten, indem der Umfang der Routenpropagierung zwischen VRF-Instanzen begrenzt wird, sodass unbeabsichtigte Kommunikation und potenzielle Sicherheitslücken vermieden werden.

3. Optimiertes Routing: Durch das Filtern von Routen können Administratoren selektiv nur die erforderlichen Routen zwischen VRFs weiterleiten, wodurch die Routing-Effizienz optimiert und unnötiger Datenverkehr im Netzwerk reduziert wird. Durch das Herausfiltern irrelevanter Routen können Administratoren sicherstellen, dass der Datenverkehr die effizientesten Pfade nutzt, und gleichzeitig Engpässe und Latenzen minimieren.

4. Ressourcennutzung: Durch das Filtern von Routen können Administratoren den Datenverkehrsfluss zwischen VRF-Instanzen steuern und so die Ressourcennutzung und die Bandbreitenzuweisung optimieren. Dies trägt zur Vermeidung von Netzwerküberlastungen bei und stellt sicher, dass wichtige Ressourcen für vorrangige Anwendungen oder Services zur Verfügung stehen.

5. Compliance: Durch das Filtern von Routen in VRF-Leaking können Unternehmen die Einhaltung gesetzlicher Vorschriften und Branchenstandards gewährleisten. Indem sie das Versickern von Routen auf autorisierte Einheiten beschränken, können Organisationen die Einhaltung von Datenschutzbestimmungen nachweisen und die Integrität sensibler Informationen sicherstellen.

6. Präzise Kontrolle: Die Filterung von Routen bietet Administratoren eine präzise Kontrolle über die Kommunikation zwischen VRF-Instanzen, sodass sie spezifische Richtlinien auf Basis ihrer individuellen Anforderungen definieren können. Dank dieser Flexibilität können Unternehmen ihre Netzwerkkonfigurationen an die Anforderungen verschiedener Anwendungen, Benutzer oder Abteilungen anpassen.

Voraussetzungen

Bestehende VXLAN-Umgebung mit Border Router

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

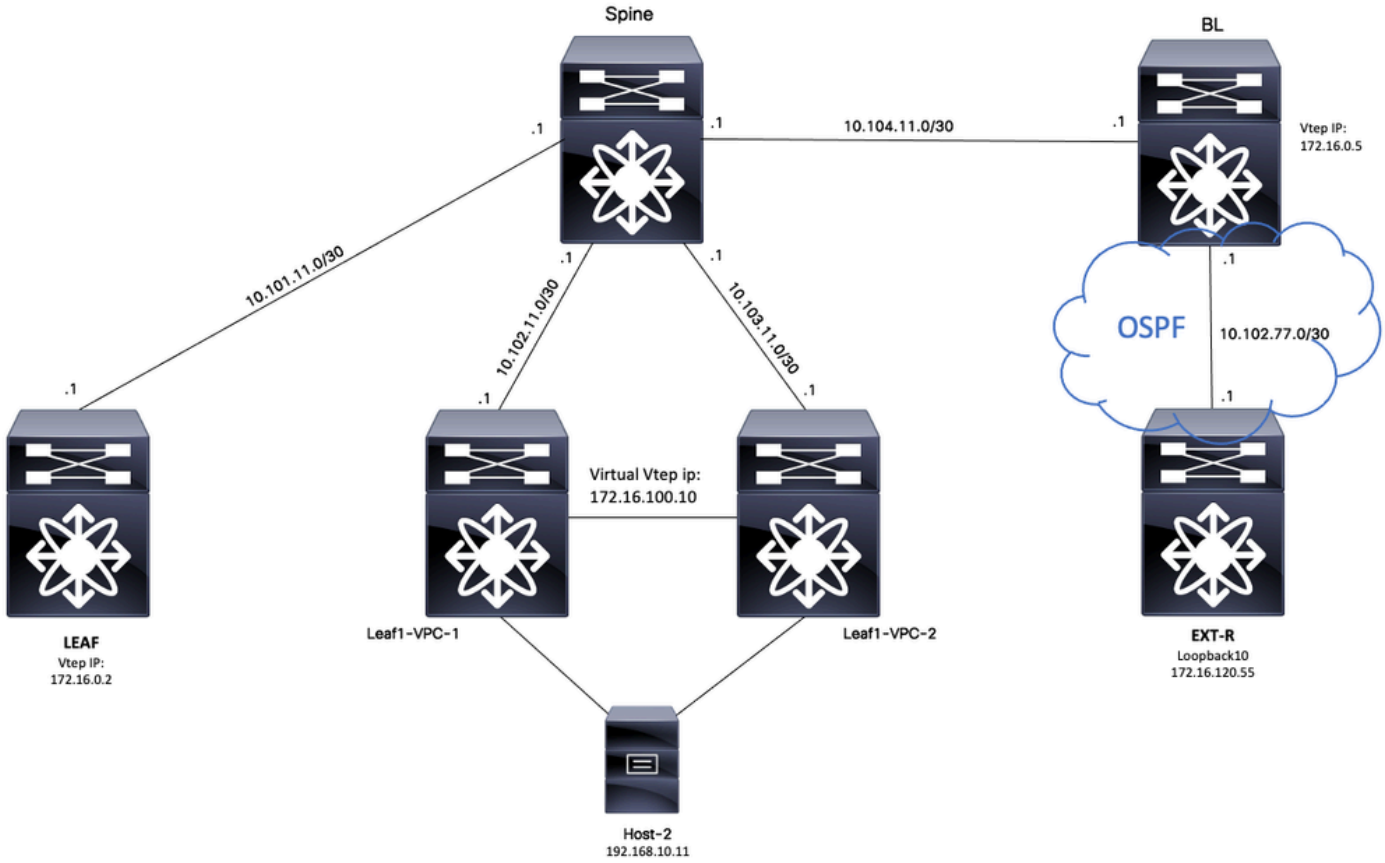
- NXOS-Plattform
- VXLAN
- VRF
- BGP

Verwendete Komponenten

Name	Plattform	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)
BLATT	N9K-C9332D-GX2B	10.2(6)
BL	N9K-C9348D-GX2A	10.2(5)
EXT-R	N9K-C9348D-GX2A	10.2(3)
WIRBELSÄULE	N9K-C93108TC-FX3P	10.1(1)

"Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen aller Befehle verstehen."

Diagramm



BGP wird als Anwendung verwendet, um Lecks zwischen VRFs zu erzeugen.

Standard-VRF zu Tenant-VRF

In diesem Beispiel empfängt Border VTEP (BL) 172.16.120.55 von einem externen Gerät über OSFP in der Standard-VRF-Instanz, die an das Tenant-VRF weitergeleitet wird.

Routing-Tabelle überprüfen

```
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
```

Filterroute

In NX-OS ist eine Routing-Map als Parameter zum Filtern und Neuverteilen von Routen erforderlich. In diesem Beispiel wird das Präfix 172.16.120.55/32 gefiltert.

Konfigurieren

	Befehl oder Aktion	Zweck
Schritt 1	BL# konfigurierbares Terminal Geben Sie die Konfigurationsbefehle ein, einen pro Zeile. Beenden Sie mit STRG+Z.	Wechselt in den Konfigurationsmodus.
Schritt 2	BL(config)# ip prefix-list VXLAN-VRF-default-to-Tenant permit 172.16.120.55/32	Präfixliste für passenden Host erstellen.
Schritt 3	BL(config)# route-map VXLAN-VRF-default-to-Tenant	Routenplan erstellen.
Schritt 4	BL(config-route-map)# match ip address prefix-list VXLAN-VRF-default-to-Tenant	Übereinstimmung mit der in Schritt 2 erstellten Präfixliste

Route in BGP importieren

Nachdem überprüft wurde, ob die Route in der Standard-VRF-Instanz vorhanden ist, muss die Route in den BGP-Prozess importiert werden.

Konfigurieren

	Befehl oder Aktion	Zweck
Schritt 1	BL# konfigurierbares Terminal Geben Sie die Konfigurationsbefehle ein, einen pro Zeile. Beenden Sie mit STRG+Z.	Wechselt in den Konfigurationsmodus.
Schritt 2	BL(config)# Router BGP 65000	Wechselt in die BGP-Konfiguration
Schritt 3	BL(config-router)# address-family-IPv4 Unicast	Geben Sie BGP-address-family IPV4 ein.
Schritt 4	BL(config-router-af)# ospf 1 route-map	Verteilen Sie die Route vom

	VXLAN-VRF-default-to-Tenant neu verteilen	OSPF zum BGP mithilfe der in Schritt 3 erstellten Route-Map neu.

BGP-Tabelle überprüfen

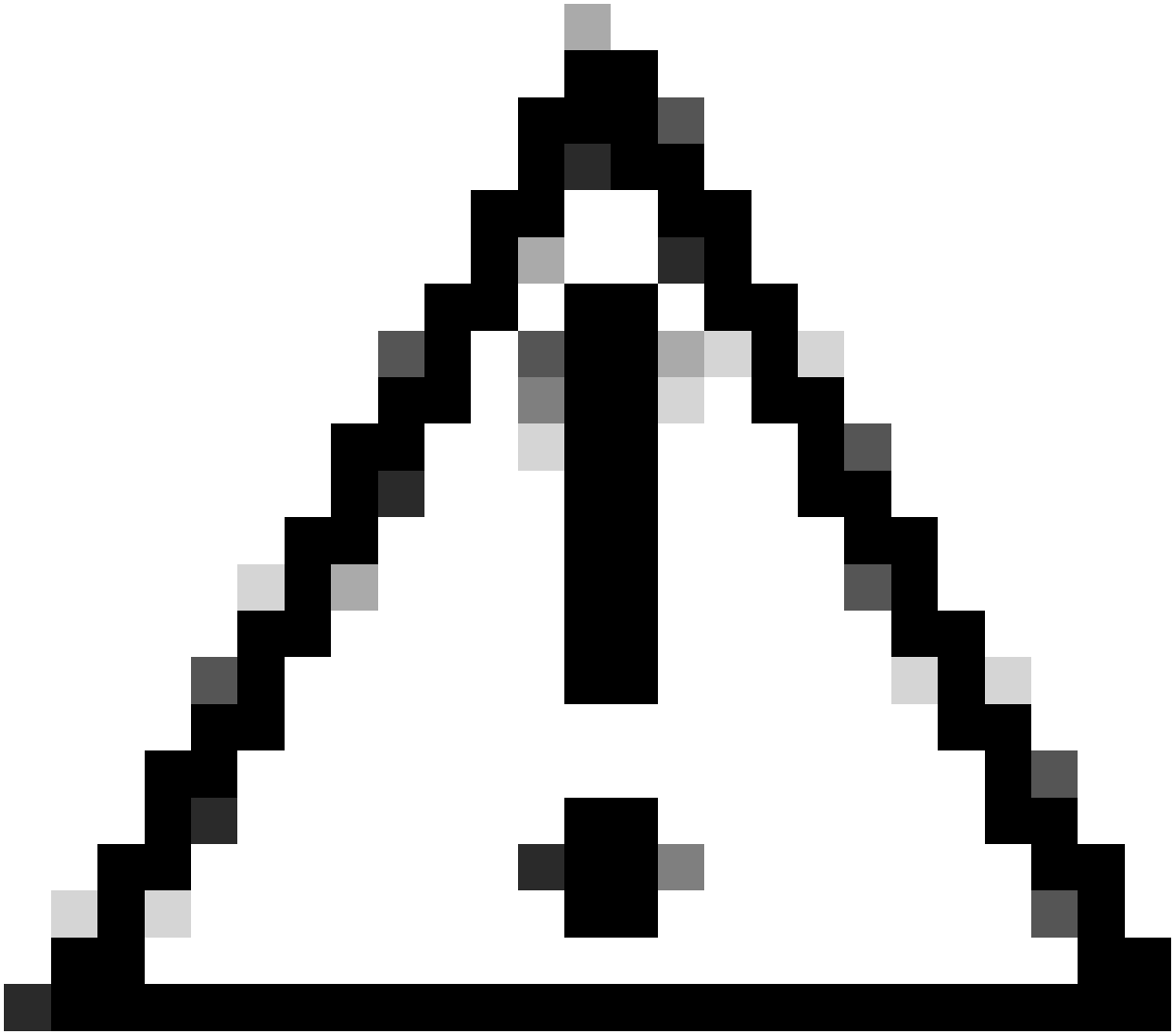
```
BL(config-router-af)# show ip bgp 172.16.120.55
BGP routing table information for VRF default, address family IPv4 Unicast
BGP routing table entry for 172.16.120.55/32, version 16
Paths: (1 available, best #1)
Flags: (0x000002) (high32 00000000) on xmit-list, is not in urib

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
```

Route in Tenant-VRF importieren

Nach dem Import des Routings in das BGP kann das Routing jetzt in die Ziel-VRF (Tenant-a) importiert werden.

Konfigurieren

	Befehl oder Aktion	Zweck
Schritt 1	BL(config)# VRF-Kontext-Tenant-a	Zur VRF-Konfiguration
Schritt 2	BL(config-vrf)# address-family-IPv4-Unicast	Wechselt in die IPv4-Adressfamilie.
Schritt 3	BL(config-vrf-af-ipv4)# import vrf default map VXLAN-VRF-default-to-Tenant advertise-vpn	Importieren der Route vom VRF-Standard zum VPN mit Tenant-VRF-Werbung



Achtung: Standardmäßig können maximal 1000 Routen von IP-Präfixen aus dem Standard-VRF in eine Nicht-Standard-VRF importiert werden. Dieser Wert kann mithilfe des Befehls unter VRF-Adressfamilie IPV4 geändert werden: import vrf <Anzahl der Präfixe> default map <route-map name> advertise-vpn.

Zusammenfassende Schritte

1. Konfigurationsterminal
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. Router BGP 65000
6. address-family-IPv4-Unicast
7. Neuverteilung von OSPF 1-Route-Map-VXLAN-VRF-Default-to-Tenant
8. VRF-Kontext-Tenant-a
9. address-family-IPv4-Unicast
10. Importieren der VRF-Standardzuordnung VXLAN-VRF-default-to-Tenant advertise-vpn

Überprüfung

Überprüfen Sie, ob die Route in L2VPN importiert wurde.

```
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
```

Überprüfen des Imports der Route in die Tenant-VRF-Instanz

```
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 zu Standard-VRF

In diesem Beispiel empfängt Border VTEP (BL) die Route 192.168.10.11 über VXLAN auf Tenant-A-VRF, das an die Standard-VRF-Instanz weitergeleitet wird.

Routing-Tabelle überprüfen

```
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:
```

Filterroute

In NX-OS ist eine Routing-Map als Parameter zum Filtern und Neuverteilen von Routen erforderlich. In diesem Beispiel wird das Präfix 172.16.120.55/32 gefiltert.

Konfigurieren

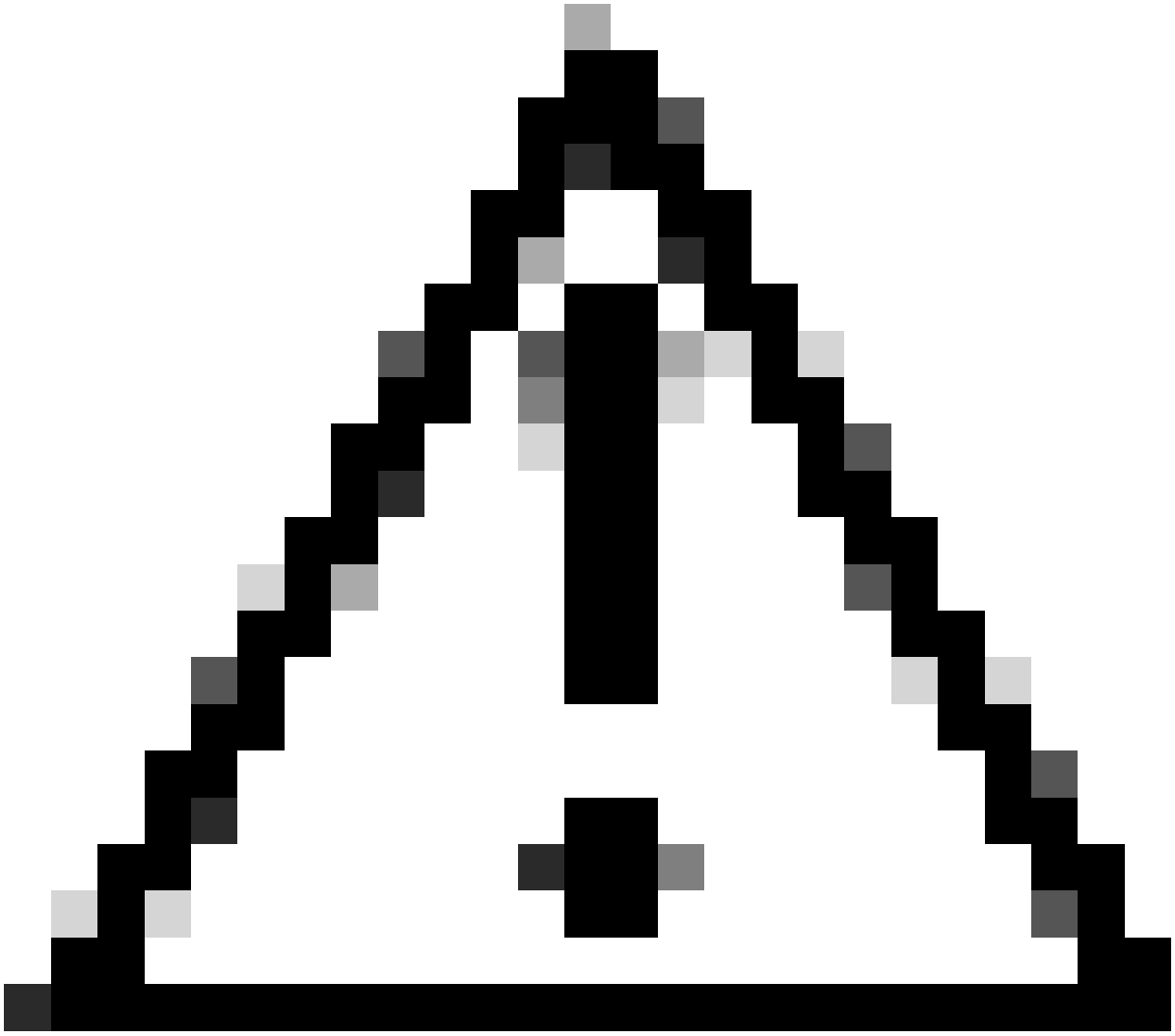
	Befehl oder Aktion	Zweck
Schritt 1	BL# konfigurierbares Terminal Geben Sie die Konfigurationsbefehle ein, einen pro Zeile. Beenden Sie mit STRG+Z.	Wechselt in den Konfigurationsmodus.
Schritt 2	BL(config)# ip prefix-list VXLAN-VRF-Tenant-to-default permit 192.168.10.11/32	Präfixliste für passenden Host erstellen.
Schritt 3	BL(config)# route-map VXLAN-VRF-Tenant-to-default	Routenplan erstellen.
Schritt 4	BL(config-route-map)# match ip address prefix-list VXLAN-VRF-Tenant-to-default	Übereinstimmung mit der in Schritt 2 erstellten Präfixliste

Exportieren der Route von einer Tenant-VRF-Instanz in eine Standard-VRF-Instanz

Da sich die Route bereits im BGP L2VPN-Prozess befindet, muss sie nur in die VRF-Standardeinstellung exportiert werden.

Konfigurieren

	Befehl oder Aktion	Zweck
Schritt 1	BL# konfigurierbares Terminal Geben Sie die Konfigurationsbefehle ein, einen pro Zeile. Beenden Sie mit STRG+Z.	Wechselt in den Konfigurationsmodus.
Schritt 2	BL(config)# VRF-Kontext-Tenant-a	Zur VRF-Konfiguration
Schritt 3	BL(config-vrf)# address-family-IPv4-Unicast	Geben Sie VRF-Adressfamilie IPV4 ein.
Schritt 4	BL(config-vrf-af-ipv4)# export vrf default map VXLAN-VRF-Tenant-to-default allow-vpn	Exportieren der Route von Tenant-VRF zu Standard-VRF mit VPN-Zulassung



Achtung: Standardmäßig können maximal 1.000 IP-Präfixe aus der nicht standardmäßigen VRF-Instanz in eine Standard-VRF-Instanz exportiert werden. Dieser Wert kann mithilfe des Befehls unter VRF-Adressfamilie IPV4 geändert werden: export vrf default <Anzahl der Präfixe> map <route-map name> allow-vpn.

Zusammenfassende Schritte

1. Konfigurationsterminal
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-Kontext-Tenant-a
6. address-family-IPv4-Unicast
7. export vrf default map VXLAN-VRF-Tenant-to-default allow-vpn

Überprüfung

Überprüfen des Imports der Route in die BGP IPV4-Adressfamilie bei Standard-VRF

```
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
```

Überprüfen, ob die Route in die Standard-VRF-Routing-Tabelle importiert wurde

```
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 zu Tenant-VRF

In diesem Beispiel empfängt der Nexus LEAF die Route 172.16.120.55/32, die an den VRF-Tenant b weitergeleitet wird.

Routing-Tabelle überprüfen

```
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
```

Filterroute

Zum Filtern von Routen sind zwei Schritte erforderlich. Die Filterung zwischen VRFs erfolgt über Route Targets (RT). Das RT wird durch <BGP-Prozess-ID>:L3VNI-ID> konform und filtert spezifische Subnetze. Wenn der zweite Schritt nicht verwendet wird, werden alle Routen von der Quell-VRF-Instanz an die Ziel-VRF-Instanz weitergeleitet.

Route Target identifizieren

<#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
```

In diesem Beispiel entspricht das Routenziel 65000:303030, und die Route 172.16.120.55/32 wird gefiltert.

Konfigurieren

	Befehl oder Aktion	Zweck

Schritt 1	LEAF# configure terminal Geben Sie die Konfigurationsbefehle ein, einen pro Zeile. Beenden Sie mit STRG+Z.	Wechselt in den Konfigurationsmodus.
Schritt 2	LEAF(config)# ip prefix-list filter-tenant-a-to-tenant-b permit 172.16.120.55/32	Präfixliste für passenden Host erstellen.
Schritt 3	LEAF(config)# route-map tenantA-to-tenantB	Routenplan erstellen.
Schritt 4	LEAF(config-route-map)# match ip address prefix-listFilter-Tenant-a-to-Tenant-b	Übereinstimmung mit der in Schritt 2 erstellten Präfixliste

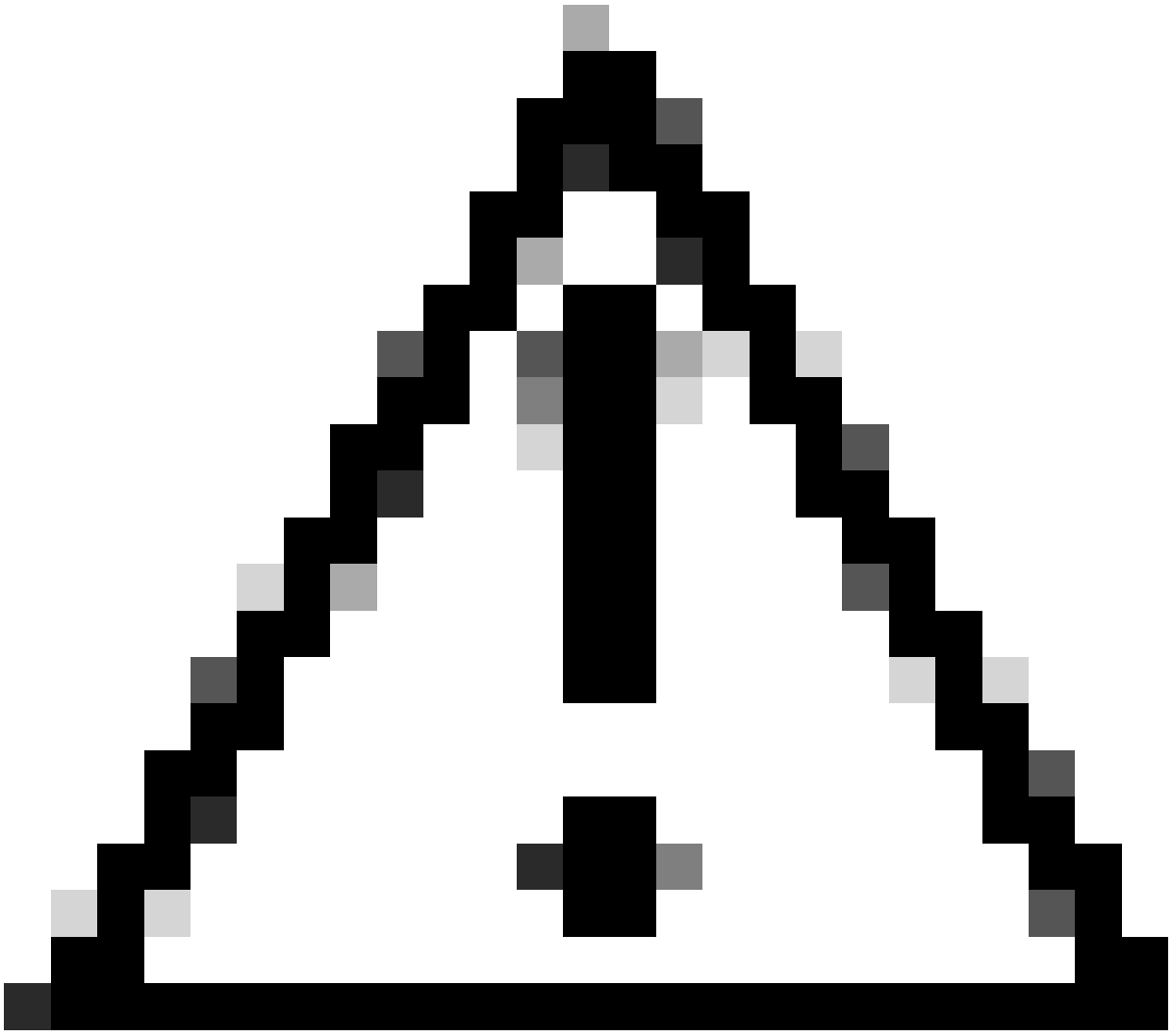
Route zu Tenant-a-VRF von Tenant-a-VRF importieren

Nachdem das RT identifiziert und die Filterung konfiguriert wurde, kann die Route in die Ziel-VRF-Instanz importiert werden (Tenant-b).

Konfigurieren

	Befehl oder Aktion	Zweck
Schritt 1	LEAF# configure terminal Geben Sie die Konfigurationsbefehle ein, einen pro Zeile. Beenden Sie mit STRG+Z.	Wechselt in den Konfigurationsmodus.
Schritt 2	LEAF(config)# vrf context tenant-b	Zur VRF-Konfiguration
Schritt 3	LEAF(config-vrf)# address-family-IPv4-Unicast	Geben Sie VRF-Adressfamilie IPV4 ein.
Schritt 4	LEAF(config-vrf-af-ipv4)# import map tenantA-to-tenantB	Route mit Routenübersicht gefiltert importieren
Schritt 5	LEAF(config-vrf-af-ipv4)# route-target import 65000:303030	Route Target

		importieren
Schritt 6	LEAF(config-vrf-af-ipv4)# route-target import 65000:303030 evpn	Route Target-EVPN importieren



Achtung: Wenn keine Import-Map verwendet wird, können alle Routen von der Ursprungs-VRF-Instanz an die Ziel-VRF-Instanz weitergeleitet werden. Durch die Verwendung von Import-Karten können die zu verlöschenden Routen kontrolliert werden.

Zusammenfassende Schritte

1. Konfigurationsterminal
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-Kontext-Tenant-b
6. address-family-IPv4-Unicast
7. Tenant-ImportzuordnungA-zu-TenantB
8. route-target import 65000:303030
9. route-target import 65000:303030 evpn

Überprüfung

Überprüfen des Imports der Route in das BGP bei 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
```

Überprüfen des Imports der Route in die Routing-Tabelle auf Tenant-b-VRF

```
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)
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.