配置和驗證Nexus 9000上的VXLAN VRF洩漏

目錄

簡介

本文檔介紹如何配置和驗證VXLAN環境上的VRF洩漏。

背景資訊

在VXLAN（虛擬可擴充區域網路）環境中，從網狀架構將VXLAN主機連線到外部主機通常需要使用VRF洩漏和邊界枝葉裝置。

VRF洩漏對於實現VXLAN主機與外部主機之間的通訊至關重要，同時保持網路分段和安全性。

Border Leaf裝置充當VXLAN交換矩陣和外部網路之間的網關，在促進此通訊中起著關鍵作用。

在此場景中，VRF洩漏的重要性可透過以下語句進行總結：

1. 與外部網路互聯：VRF洩漏允許交換矩陣內的VXLAN主機與交換矩陣外的外部主機通訊。這樣可以訪問外部網路（如網際網路或其他資料中心）上託管的資源、服務和應用程式。

2. 網路分段和隔離：VRF洩漏在VXLAN交換矩陣內維持網路分段和隔離，同時實現與外部網路的選擇性通訊。這可以確保VXLAN主機根據其VRF分配保持相互隔離，同時仍能根據需要訪問外部資源。

3. 策略實施：VRF洩漏使管理員能夠對VXLAN主機和外部主機之間的流量實施網路策略和訪問控制。這可以確保通訊使用預定義的安全策略，並防止對敏感資源進行未經授權的訪問。

4. 可擴充性和靈活性：VRF洩漏透過允許VXLAN主機與外部主機無縫通訊，增強了VXLAN部署的可擴充性和靈活性。它支援在VXLAN和外部網路之間動態分配和共用資源，適應不斷變化的網路需求，而不會中斷現有配置。

在VRF（虛擬路由和轉發）洩漏中過濾路由對於維護網路安全、最佳化路由效率和防止意外資料洩漏至關重要。VRF洩漏允許虛擬網路之間進行通訊，同時保持它們在邏輯上獨立。

過濾路由在VRF洩漏中的重要性可透過以下語句加以總結：

1. 安全：過濾路由可確保在VRF例項之間僅洩露特定路由，從而降低未經授權訪問或資料洩露的風險。透過控制允許哪些路由透過VRF邊界，管理員可以實施安全策略，並防止敏感資訊暴露給未經授權的實體。

2. 隔離：VRF旨在提供網路分段和隔離，允許不同的租戶或部門在同一物理基礎設施內獨立運行。VRF洩漏中的過濾路由透過限制VRF例項之間的路由傳播範圍，防止意外的通訊和潛在的安全漏洞，從而有助於保持這種隔離。

3. 最佳化路由：透過過濾路由，管理員可以選擇性地僅洩漏VRF之間的必要路由，從而最佳化路由效率並減少網路中不必要的流量。透過過濾掉不相關的路由，管理員可以確保流量使用最有效的路徑，同時最大限度地減少擁塞和延遲。

4. 資源利用率：透過過濾路由，管理員可以控制VRF例項之間的流量傳輸，從而最佳化資源利用率和頻寬分配。這有助於防止網路擁塞，並確保關鍵資源可用於優先順序應用程式或服務。

5. 合規性：在VRF洩漏中過濾路由有助於組織保持合規性要求和行業標準。透過將路由洩漏限制為僅授權實體，組織可以證明遵守了資料保護法規並確保敏感資訊的完整性。

6. 精細控制：過濾路由可為管理員提供對VRF例項之間通訊的精細控制，允許管理員根據自己的獨特需求定義特定策略。這種靈活性使組織能夠定製其網路配置，以滿足不同應用、使用者或部門的需求。

必要條件

使用邊界路由器的現有VXLAN環境

需求

思科建議您瞭解以下主題：

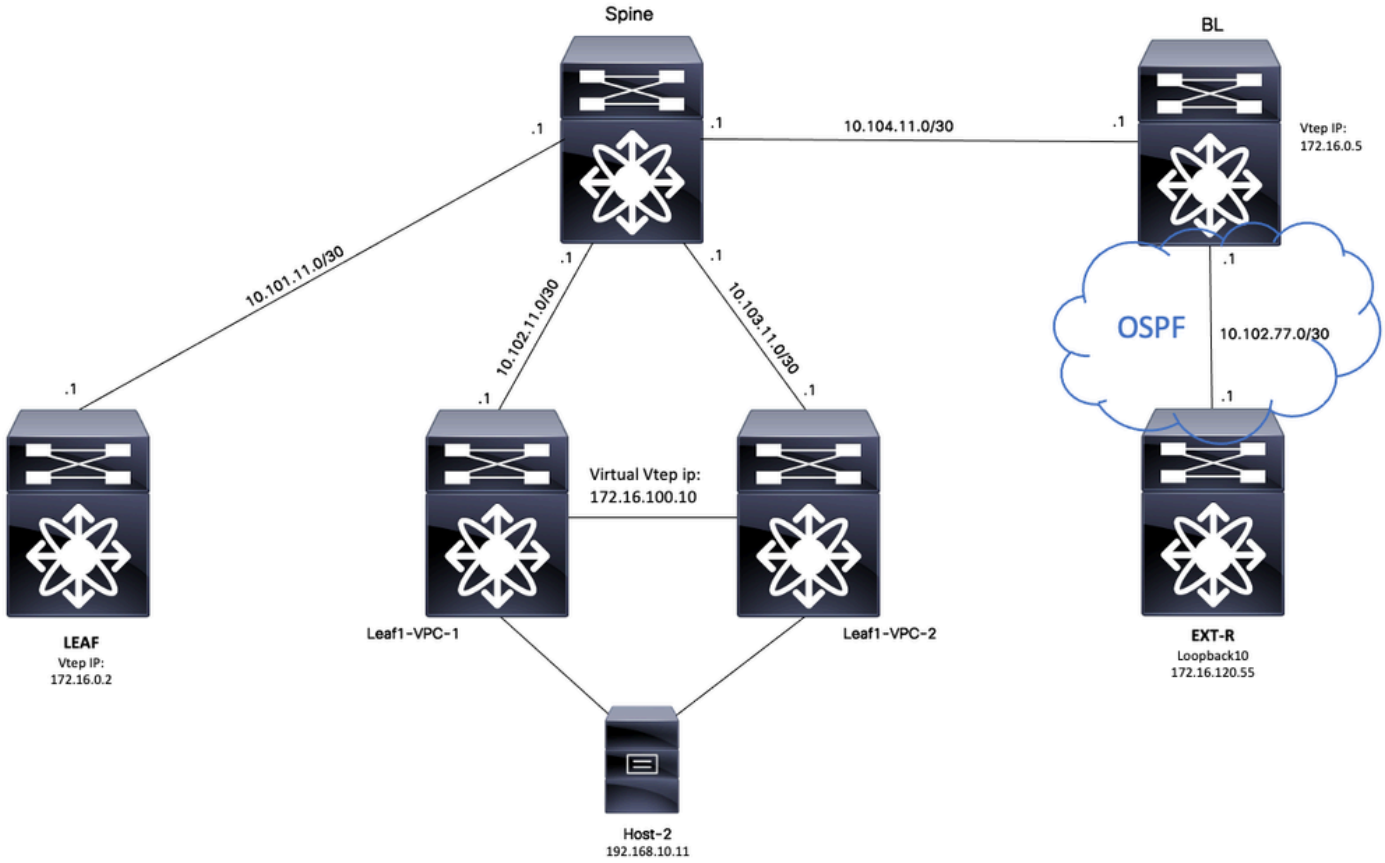
- NXOS平台
- VXLAN
- VRF
- BGP

採用元件

名稱	平台	版本
主機2	N9K-C92160YC-X	9.3(6)
枝葉-VPC-1	N9K-C93180YC-EX	9.3(9)
枝葉-VPC-2	N9K-C93108TC-EX	9.3(9)
分葉	N9K-C9332D-GX2B	10.2(6)
BL	N9K-C9348D-GX2A	10.2(5)
EXT-R	N9K-C9348D-GX2A	10.2(3)
骨幹	N9K-C93108TC-FX3P	10.1(1)

"本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路處於活動狀態，請確保您瞭解所有命令的潛在影響。」

圖表



將BGP視為應用，BGP是用於在VRF之間執行洩漏的應用

預設VRF到租戶VRF

在本示例中，邊界VTEP (BL)透過預設VRF中的OSFP從外部裝置接收172.16.120.55，該VRF將洩漏到租戶VRF。

檢驗路由表

```
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
```

篩選路由

在NXOS中，需要將路由對映用作過濾和重新分配路由的引數，例如，將過濾字首172.16.120.55/32。

設定

	命令或操作	目的
步驟 1	BL#配置終端 輸入配置命令，每行一個。以CNTL/Z結束。	進入配置模式。
步驟 2	BL(config)# ip prefix-list VXLAN-VRF-default-to-Tenant permit 172.16.120.55/32	建立字首清單匹配主機。
步驟 3	BL(config)# route-map VXLAN-VRF-default-to-Tenant	建立路由對映。
步驟 4	BL(config-route-map)# match ip address prefix-list VXLAN-VRF-default-to-Tenant	匹配第2步中建立的字首清單。

將路由導入BGP

一旦驗證預設VRF上存在路由，就必須將路由導入BGP進程。

設定

	命令或操作	目的
步驟 1	BL#配置終端 輸入配置命令，每行一個。以CNTL/Z結束。	進入配置模式。
步驟 2	BL(config)# router bgp 65000	進入BGP配置。
步驟 3	BL(config-router)# address-family ipv4 unicast	輸入BGP address-famili IPV4。
步驟 4	BL(config-router-af)# redistribute ospf 1 route-map VXLAN-VRF-default-to-Tenant	使用步驟3中建立的路由對映將路由從OSPF重分配到BGP。

驗證BGP表

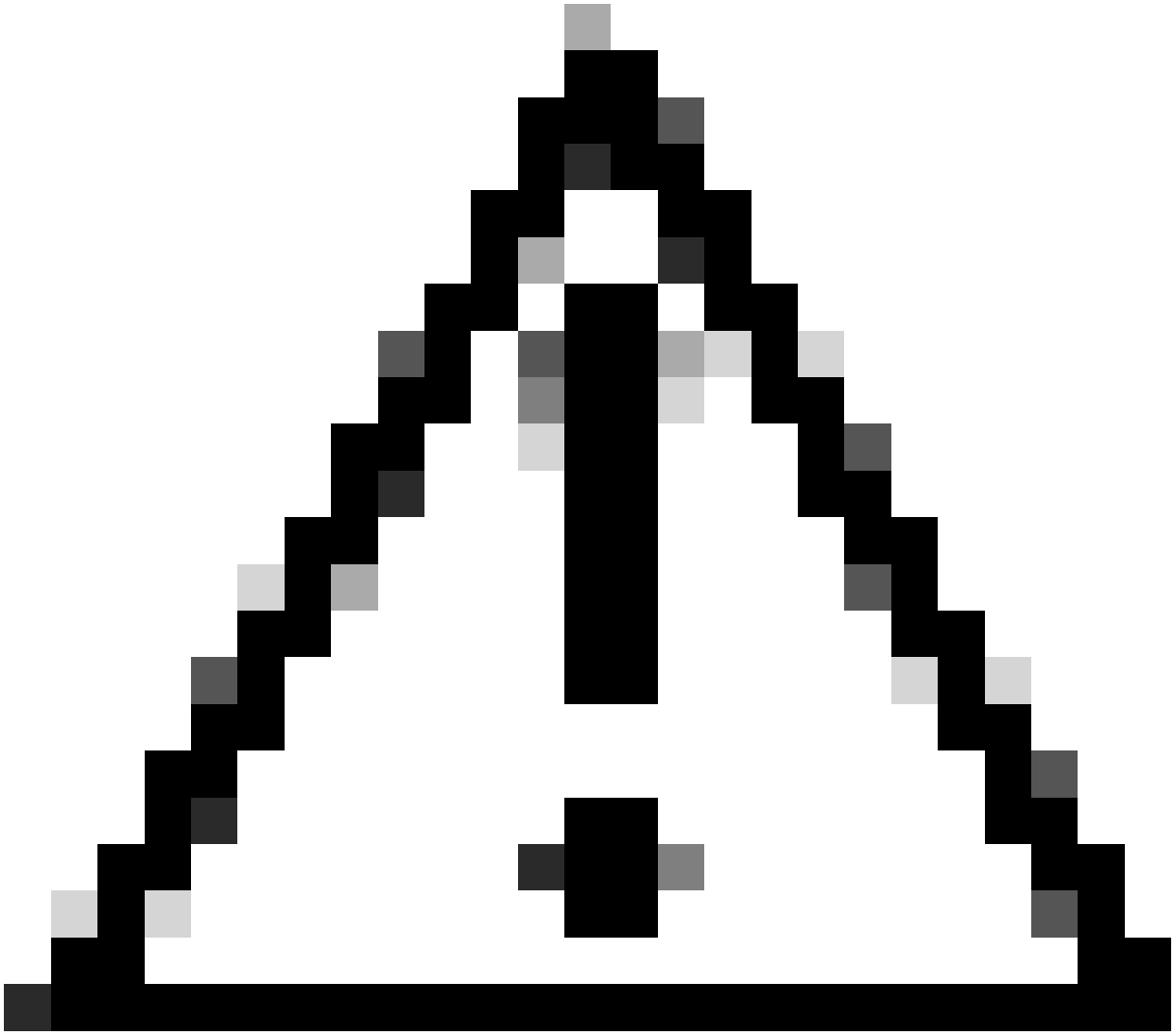
```
BL(config-router-af)# show ip bgp 172.16.120.55
BGP routing table information for VRF default, address family IPv4 Unicast
BGP routing table entry for 172.16.120.55/32, version 16
Paths: (1 available, best #1)
Flags: (0x000002) (high32 00000000) on xmit-list, is not in urib

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
```

將路由導入租戶VRF

一旦路由導入BGP，現在可以將路由導入目標VRF（租戶-a）。

設定

	命令或操作	目的
步驟1	BL(config)# vrf context tenant-a	進入VRF配置。
步驟2	BL(config-vrf)# address-family ipv4 unicast	輸入IPV4地址系列。
步驟3	BL(config-vrf-af-ipv4)# import vrf default map VXLAN-VRF-default-to-Tenant advertise-vpn	從VRF預設路由導入租戶VRF通告VPN



注意：預設情況下，可以從預設VRF導入非預設VRF的IP字首的最大數量為1000個路由。此值可以在VRF地址系列IPV4下使用命令進行更改：import vrf <number of prefixes> default map <route-map name> advertise-vpn。

摘要步驟

1. 配置終端
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. redistribute ospf 1 route-map VXLAN-VRF-default-to-Tenant
8. vrf情景tenant-a
9. address-family ipv4 unicast
10. 導入vrf預設對映VXLAN-VRF-default-to-Tenant advertise-vpn

驗證

檢驗路由是否已導入到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
```

驗證路由是否已導入租戶VRF

```
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
```

租戶-VRF到預設VRF

在本示例中，邊界VTEP (BL)正在透過租戶a VRF上的VXLAN接收將洩漏到預設VRF的路由192.168.10.11。

檢驗路由表

```
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:
```

篩選路由

在NXOS中，需要將路由對映用作過濾和重新分配路由的引數，例如，將過濾字首172.16.120.55/32。

設定

	命令或操作	目的
步驟 1	BL#配置終端 輸入配置命令，每行一個。以CNTL/Z結束。	進入配置模式。
步驟 2	BL(config)# ip prefix-list VXLAN-VRF-租戶到預設許可證 192.168.10.11/32	建立字首清單匹配主機。
步驟 3	BL(config)# route-map VXLAN-VRF-Tenant-to-default	建立路由對映。
步驟 4	BL(config-route-map)# match ip address prefix-list VXLAN-VRF-Tenant-to-default	匹配第2步中建立的字首清單。

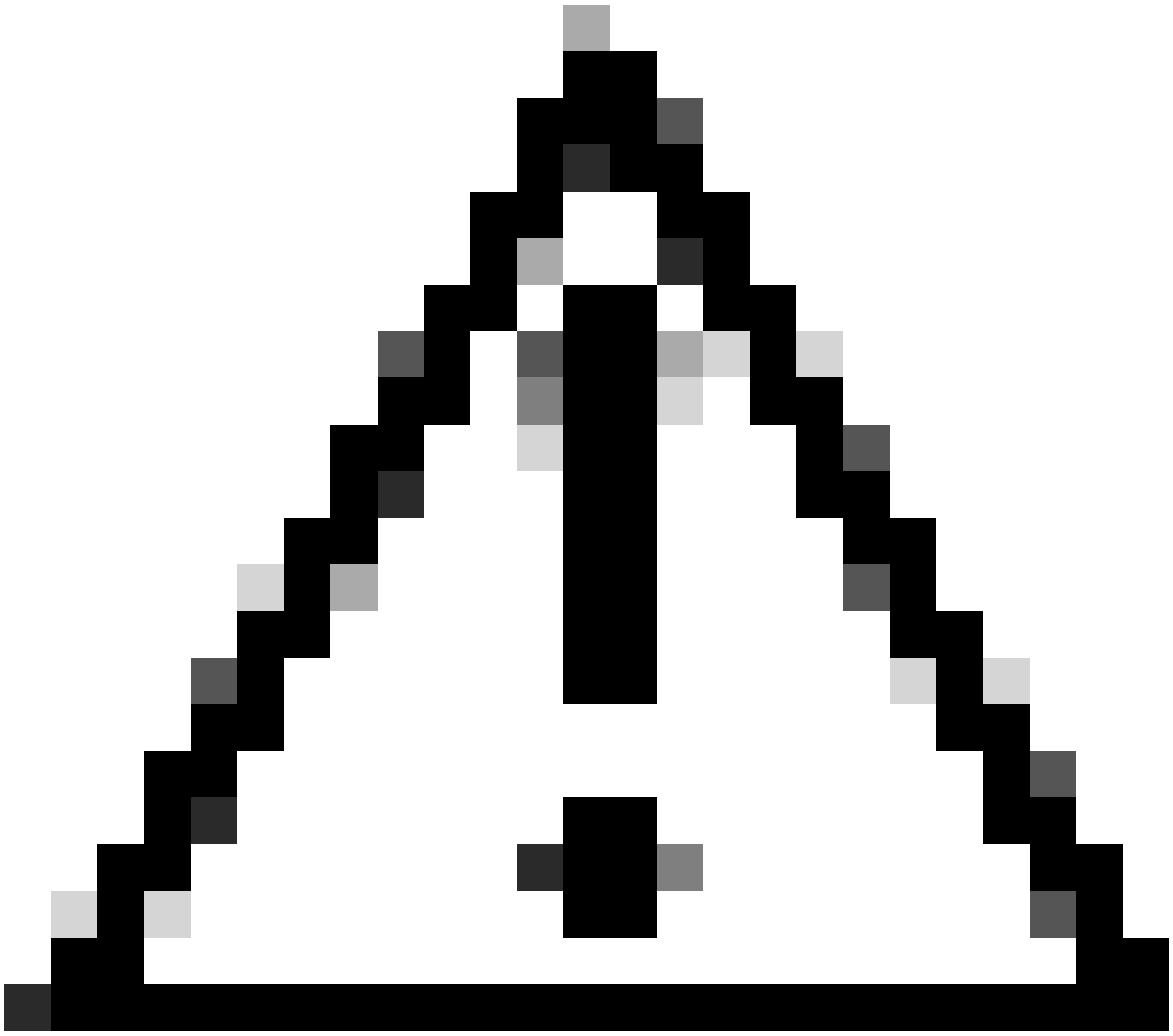
將路由從租戶a VRF導出到預設VRF

由於路由已經在BGP L2VPN進程中，因此只需要將其導出到VRF預設值。

設定

	命令或操作	目的

步驟 1	BL#配置終端 輸入配置命令，每行一個。以CNTL/Z結束。	進入配置模式。
步驟 2	BL(config)# vrf context tenant-a	進入VRF配置。
步驟 3	BL(config-vrf)# address-family ipv4 unicast	輸入VRF地址系列IPV4。
步驟 4	BL(config-vrf-af-ipv4)# export vrf default map VXLAN-VRF-Tenant-to-default allow-vpn	將路由從租戶VRF導出到允許VPN的預設VRF



注意：預設情況下，可以從非預設VRF導出到預設VRF的IP字首的最大數量為1000個路由。此值可在VRF地址系列IPV4下使用命令進行更改：export vrf default <number of prefixes> map <route-map name> allow-vpn。

摘要步驟

1. 配置終端
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情景tenant-a
6. address-family ipv4 unicast
7. 導出vrf預設對映VXLAN-VRF-Tenant-to-default allow-vpn

驗證

驗證是否已將路由導入預設VRF上的BGP IPV4地址系列

```
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
```

驗證是否已將路由導入預設VRF路由表

```
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

租戶-VRF到租戶-VRF

在本示例中，nexus LEAF 正在接收將洩漏到VRF tenant-b的路由172.16.120.55/32 tenant-a

檢驗路由表

```
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
```

篩選路由

為了過濾路由需要兩個步驟，必須在VRF之間進行過濾，方法是檢視路由目標(RT)，RT由<BGP Process ID>：L3VNI ID>和過濾特定子網組成。如果不使用第二步，所有來自源VRF的路由都將洩漏到目標VRF。

確定路由目標

<#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
```

對於此示例，路由目標等於： 65000：303030，並且路由172.16.120.55/32將被過濾。

設定

	命令或操作	目的
步驟 1	LEAF#配置終端 輸入配置命令，每行一個。以CNTL/Z結束。	進入配置模式。
步驟 2	LEAF(config)# ip prefix-list filter-tenant-a-to-tenant-b permit 172.16.120.55/32	建立字首清單匹配主機。
步驟 3	LEAF(config)# route-map tenantA-to-tenantB	建立路由對映。
步驟 4	LEAF(config-route-map)# match ip address prefix-listfilter-tenant-a-to-tenant-b	匹配第2步中建立的字首清單。

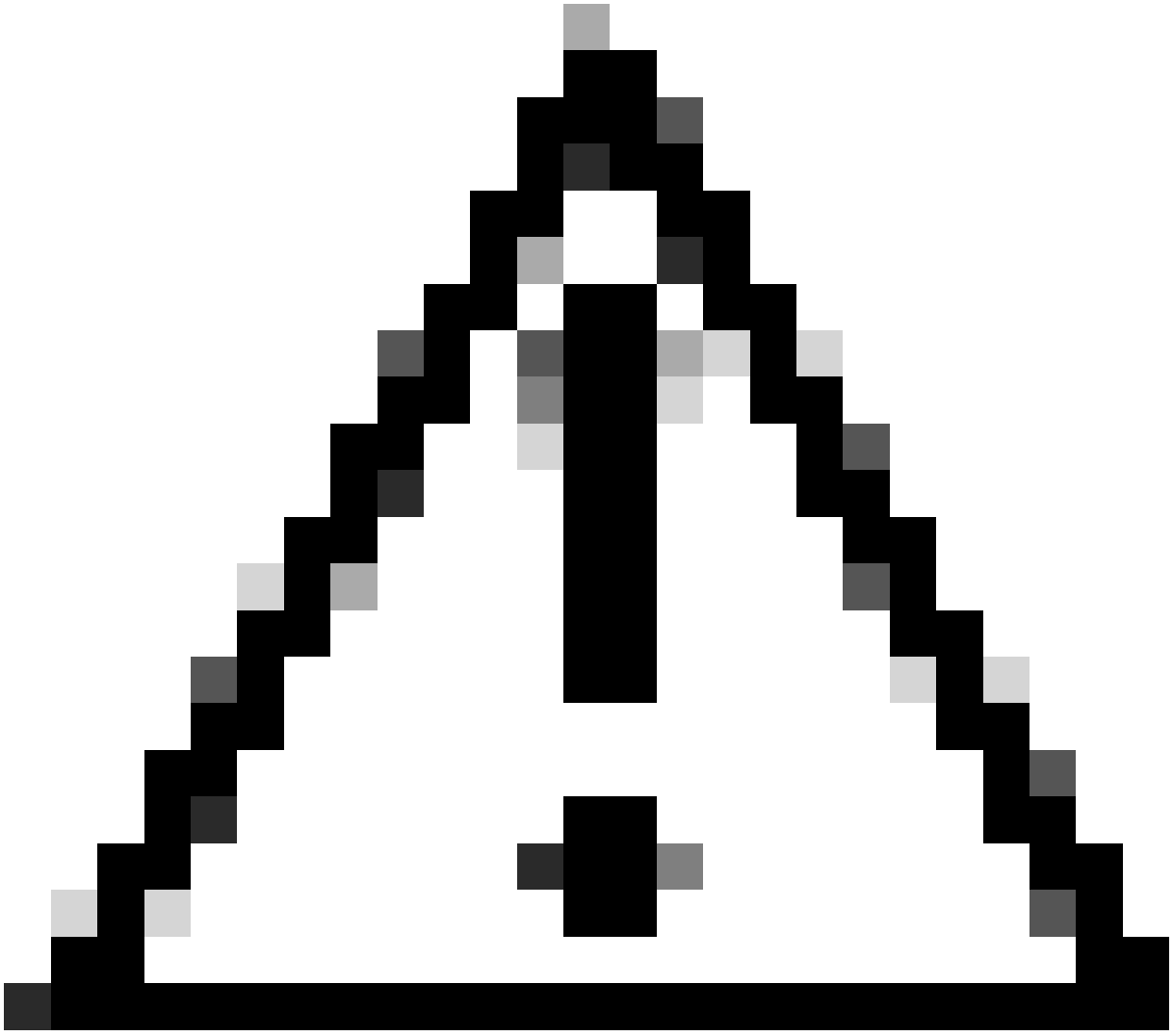
從租戶a VRF導入到租戶a VRF的路由

辨識RT並配置過濾後，可以將路由導入目標VRF（租戶-b）

設定

	命令或操作	目的
步驟 1	LEAF#配置終端 輸入配置命令，每行一個。以CNTL/Z結束。	進入配置模式。
步驟 2	LEAF(config)# vrf context tenant-b	進入VRF配置

		。
步驟 3	LEAF(config-vrf)# address-family ipv4 unicast	輸入VRF地址系列IPV4。
步驟 4	LEAF(config-vrf-af-ipv4)#導入對映tenantA到tenantB	導入使用路由對映過濾的路由
步驟 5	LEAF(config-vrf-af-ipv4)# route-target import 65000：303030	匯入路由目標
步驟 6	LEAF(config-vrf-af-ipv4)# route-target import 65000：303030 evpn	導入路由目標evpn



注意：不使用導入對映可能允許來自源VRF的所有路由洩漏到目標VRF。使用導入對映可以控制要洩漏的路由。

摘要步驟

1. 配置終端
2. ip prefix-list filter-tenant-a-to-tenant-b permit 172.16.120.55/32
3. 路由對映tenantA到tenantB
4. match ip address prefix-listfilter-tenant-a-to-tenant-b
5. vrf情景tenant-b
6. address-family ipv4 unicast
7. 導入對映tenantA到tenantB
8. route-target import 65000：303030
9. route-target import 65000：303030 evpn

驗證

驗證是否已將路由導入租戶b VRF上的BGP

```
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
```

驗證是否已將路由導入租戶b VRF上的路由表

```
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)
```

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。