# Configurar e verificar vazamento de VRF de VXLAN no Nexus 9000

## Contents

# Introdução

Este documento descreve como configurar e verificar o vazamento de VRF em um ambiente VXLAN.

# Informações de Apoio

Em um ambiente VXLAN (Virtual Extensible LAN), a conexão de hosts VXLAN a hosts externos da malha geralmente exige o uso de vazamento de VRF e dispositivos de folha de borda.

O vazamento de VRF é crucial para permitir a comunicação entre hosts VXLAN e hosts externos, mantendo a segmentação e a segurança da rede.

O dispositivo Border Leaf serve como um gateway entre a estrutura VXLAN e as redes externas, desempenhando um papel fundamental na facilitação dessa comunicação.

A importância do vazamento de VRF neste cenário pode ser resumida com as próximas afirmações:

1. Interconexão com redes externas: o vazamento de VRF permite que os hosts VXLAN dentro da malha se comuniquem com os hosts externos fora da malha. Isso permite acesso a recursos, serviços e aplicativos hospedados em redes externas, como a Internet ou outros data centers.

2. Segmentação e isolamento de rede: o vazamento de VRF mantém a segmentação e o isolamento de rede dentro da estrutura de VXLAN enquanto permite a comunicação seletiva com redes externas. Isso garante que os hosts de VXLAN permaneçam isolados uns dos outros com base em suas atribuições de VRF, enquanto ainda podem acessar recursos externos conforme necessário.

3. Aplicação de políticas: o vazamento de VRF permite que os administradores apliquem políticas de rede e controles de acesso para o fluxo de tráfego entre hosts VXLAN e hosts externos. Isso garante que a comunicação use políticas de segurança predefinidas e evite o acesso não autorizado a recursos confidenciais.

4. Escalabilidade e flexibilidade: vazamento de VRF melhora a escalabilidade e a flexibilidade das implantações de VXLAN, permitindo que os hosts de VXLAN se comuniquem perfeitamente com os hosts externos. Ele permite a alocação e o compartilhamento dinâmicos de recursos entre VXLAN e redes externas, adaptando-se aos requisitos de rede em constante mudança sem interromper as configurações existentes.

A filtragem de rotas no vazamento VRF (Virtual Routing and Forwarding, roteamento e encaminhamento virtual) é crucial para manter a segurança da rede, otimizar a eficiência do roteamento e evitar o vazamento não intencional de dados. O vazamento de VRF permite a comunicação entre redes virtuais enquanto as mantém separadas logicamente.

A importância da filtragem de rotas no vazamento de VRF é importante e pode ser resumida com as próximas instruções:

1. Segurança: a filtragem de rotas garante que apenas rotas específicas vazem entre instâncias de VRF, reduzindo o risco de acesso não autorizado ou violações de dados. Ao controlar quais rotas têm permissão para cruzar os limites do VRF, os administradores podem aplicar políticas de segurança e evitar que informações confidenciais sejam expostas a entidades não autorizadas.

2. Isolamento: os VRFs são projetados para fornecer segmentação e isolamento de rede, permitindo que diferentes usuários ou departamentos operem de forma independente dentro da mesma infraestrutura física. A filtragem de rotas no vazamento de VRF ajuda a manter esse isolamento, limitando o escopo da propagação de rota entre instâncias de VRF, evitando comunicação não intencional e possíveis vulnerabilidades de segurança.

3. Roteamento otimizado: a filtragem de rotas permite que os administradores vazem seletivamente apenas as rotas necessárias entre VRFs, otimizando a eficiência do roteamento e reduzindo o tráfego desnecessário na rede. Filtrando rotas irrelevantes, os administradores podem garantir que o tráfego use os caminhos mais eficientes, minimizando o congestionamento e a latência.

4. Utilização de recursos: filtrando rotas, os administradores podem controlar o fluxo de tráfego entre instâncias de VRF, otimizando a utilização de recursos e a alocação de largura de banda. Isso ajuda a evitar o congestionamento da rede e garante que recursos críticos estejam disponíveis para aplicativos ou serviços prioritários.

5. Conformidade: as rotas de filtragem no vazamento de VRF ajudam as empresas a manter a conformidade com os requisitos normativos e os padrões do setor. Restringindo o vazamento de rotas somente a entidades autorizadas, as organizações podem demonstrar conformidade com as normas de proteção de dados e garantir a integridade das informações confidenciais.

6. Controle granular: as rotas de filtragem fornecem aos administradores controle granular sobre a comunicação entre instâncias de VRF, permitindo que eles definam políticas específicas com base em seus requisitos exclusivos. Essa flexibilidade permite que as organizações adaptem suas configurações de rede para atender às necessidades de diferentes aplicativos, usuários ou departamentos.

# Pré-requisitos

Ambiente VXLAN existente com um roteador de borda

# Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Plataforma NXOS

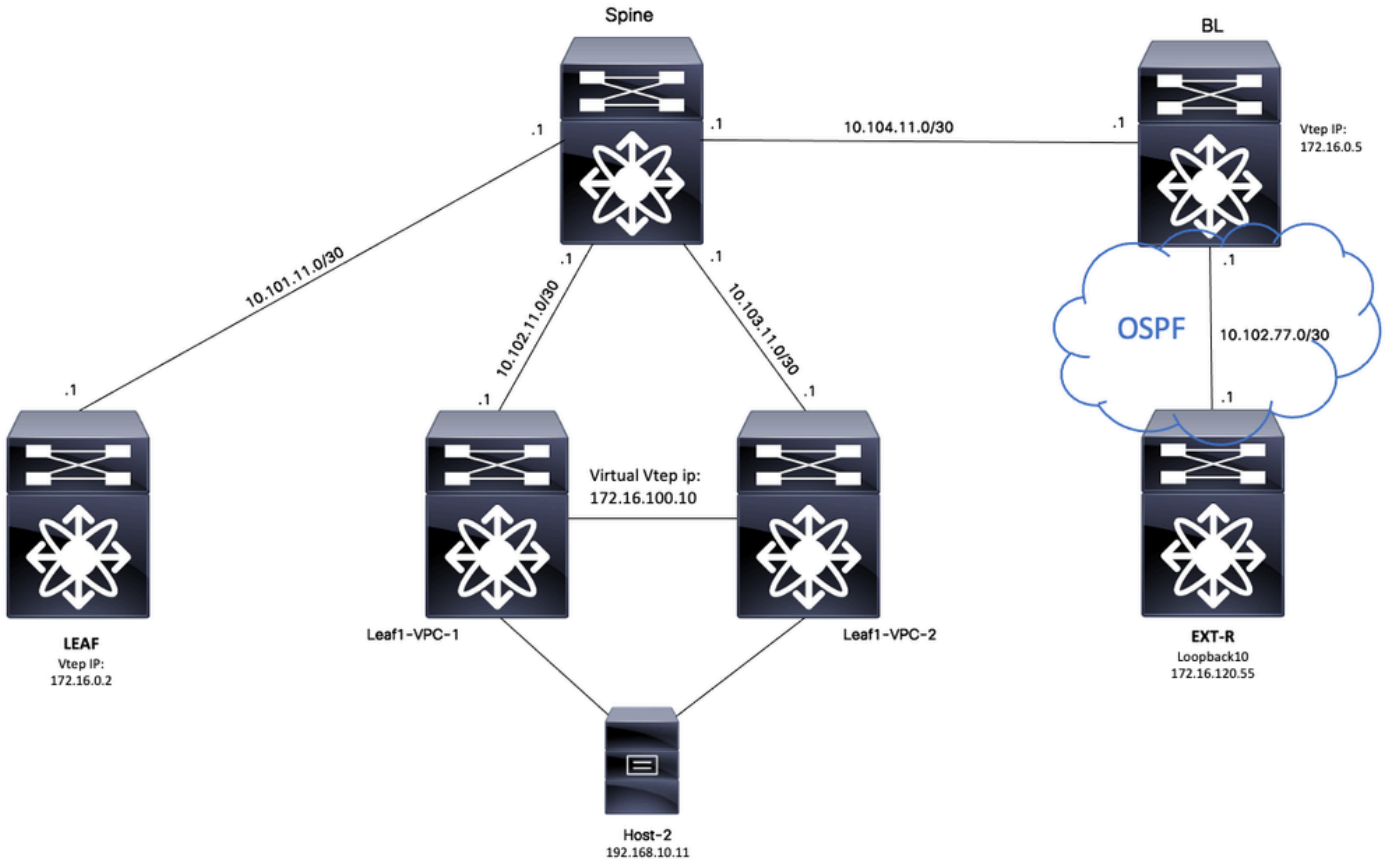
- VXLAN
- VRF
- BGP

## Componentes Utilizados

| Nome | Platform | Versão |
|---|---|---|
| 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) |
| FOLHA | N9K-C9332D-GX2B | 10.2(6) |
| BL | N9K-C9348D-GX2A | 10.2(5) |
| EXT-R | N9K-C9348D-GX2A | 10.2(3) |
| COLUNA | N9K-C93108TC-FX3P | 10.1(1) |

"As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que você compreende o impacto potencial de qualquer comando."

## Diagrama



Considerando o BGP como um aplicativo, o BGP é o aplicativo usado para executar vazamento entre VRFs

# VRF padrão para usuário-VRF

Para este exemplo, o VTEP de borda (BL) está recebendo 172.16.120.55 do dispositivo externo via OSFP no VRF padrão que será vazado para o VRF do usuário.

## Verificar a tabela de roteamento

```
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
```

## Filtrar rota

No NXOS, um mapa de rota é necessário como um parâmetro para filtrar e redistribuir rotas, para este exemplo, o prefixo 172.16.120.55/32 será filtrado.

Configurar

| | Comando ou Ação | Propósito |
|---|---|---|
| Passo 1 | BL# configure terminal<br><br>Enter configuration commands, one per line. Finalize com CNTL/Z. | Entra no modo de configuração. |
| Passo 2 | BL(config)# ip prefix-list VXLAN-VRF-default-to-Tenant permit 172.16.120.55/32 | Crie uma lista de prefixos que corresponda ao host. |
| Etapa 3 | BL(config)# route-map VXLAN-VRF-default-to-Tenant | Crie um mapa de rotas. |
| Passo 4 | BL(config-route-map)# match ip address prefix-list VXLAN-VRF-default-to-Tenant | Faça a correspondência da lista de prefixos criada na |

| | | |
|---|---|---|
| | | etapa 2. |

## Importar rota para BGP

Uma vez verificado que a rota existe no VRF padrão, a rota deve ser importada para o processo BGP.

Configurar

| | Comando ou Ação | Propósito |
|---|---|---|
| Passo 1 | BL# configure terminal<br>Enter configuration commands, one per line. Finalize com CNTL/Z. | Entra no modo de configuração. |
| Passo 2 | BL(config)# router bgp 65000 | Entra na configuração do BGP. |
| Etapa 3 | BL(config-router)# address-family ipv4 unicast | Digite BGP address-family IPV4. |
| Passo 4 | BL(config-router-af)# redistribute ospf 1 route-map VXLAN-VRF-default-to-Tenant | Redistribua a rota do OSPF para o BGP usando o mapa de rota criado na etapa 3. |

Verificar tabela BGP

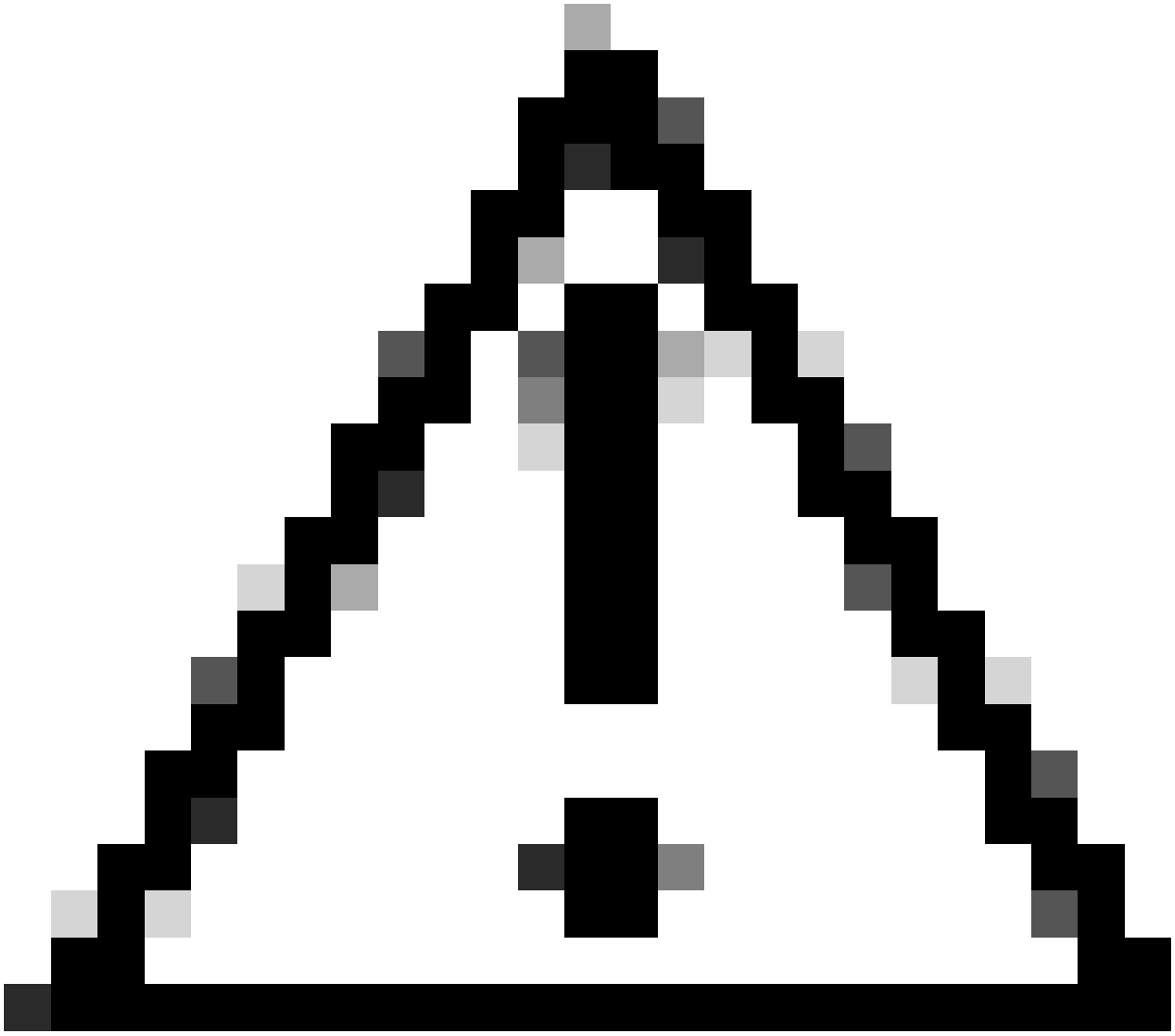
```
BL(config-router-af)# show ip bgp 172.16.120.55
BGP routing table information for VRF default, address family IPv4 Unicast
BGP routing table entry for 172.16.120.55/32, version 16
Paths: (1 available, best #1)
Flags: (0x000002) (high32 00000000) on xmit-list, is not in urib

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
```

## Importar rota para VRF de Locatário

Uma vez que a rota é importada para o BGP, a rota agora pode ser importada para o VRF de destino (locatário-a).

Configurar

| | Comando ou Ação | Propósito |
|---|---|---|
| Passo 1 | BL(config)# vrf context tenant-a | Entra na configuração do VRF. |
| Passo 2 | BL(config-vrf)# address-family ipv4 unicast | Insere a família de endereços IPV4. |
| Etapa 3 | BL(config-vrf-af-ipv4)# import vrf default map VXLAN-VRF-default-to-Tenant advertise-vpn | Importar rota do VRF padrão para o VRF do usuário anunciando VPN |



Cuidado: por padrão, o número máximo de prefixos IP que podem ser importados do VRF padrão para um VRF não padrão é de 1000 rotas. Esse valor pode ser alterado com o comando em VRF address-family IPV4: import vrf <number of prefixes> default map <route-map name> advertise-vpn.

## Etapas de resumo

1. configure 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. router 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

### Verificar

Verifique se a rota é importada para 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
```

Verifique se a rota é importada para o VRF do usuário

```
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
```

## VRF de Locatário para VRF Padrão

Para este exemplo, o VTEP de borda (BL) está recebendo a rota 192.168.10.11 via VXLAN em um VRF de locatário que será vazado para o VRF padrão.

### Verificar a tabela de roteamento

```
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:
```

## Filtrar rota

No NXOS, um mapa de rota é necessário como um parâmetro para filtrar e redistribuir rotas, para este exemplo, o prefixo 172.16.120.55/32 será filtrado.

Configurar

| | Comando ou Ação | Propósito |
|---|---|---|
| Passo 1 | BL# configure terminal<br>Enter configuration commands, one per line. Finalize com CNTL/Z. | Entra no modo de configuração. |
| Passo 2 | BL(config)# ip prefix-list VXLAN-VRF-Tenant-to-default permit 192.168.10.11/32 | Crie uma lista de prefixos que corresponda ao host. |
| Etapa 3 | BL(config)# route-map VXLAN-VRF-Tenant-to-default | Crie um mapa de rotas. |
| Passo 4 | BL(config-route-map)# match ip address prefix-list VXLAN-VRF-Tenant-to-default | Faça a correspondência da lista de prefixos criada na etapa 2. |

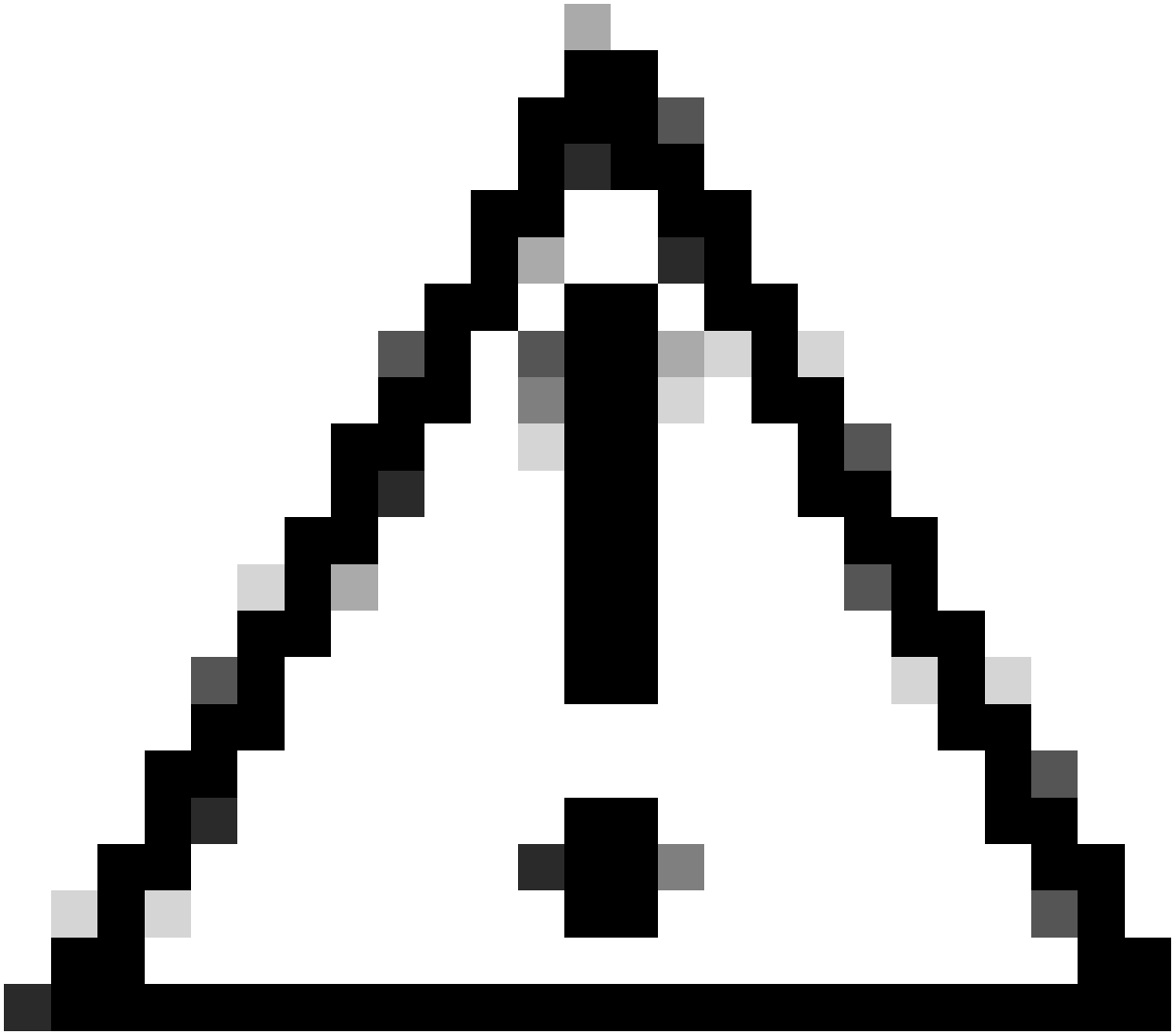
## Exportar rota para VRF padrão do usuário-um VRF

Como a rota já está no processo BGP L2VPN, ela só precisa ser exportada para o padrão VRF.

Configurar

| | Comando ou Ação | Propósito |
|---|---|---|

| | | |
|---|---|---|
| Passo 1 | BL# configure terminal<br><br>Enter configuration commands, one per line. Finalize com CNTL/Z. | Entra no modo de configuração. |
| Passo 2 | BL(config)# vrf context tenant-a | Entra na configuração do VRF. |
| Etapa 3 | BL(config-vrf)# address-family ipv4 unicast | Digite VRF address-family IPV4. |
| Passo 4 | BL(config-vrf-af-ipv4)# export vrf default map VXLAN-VRF-Tenant-to-default allow-vpn | Exportar a rota do VRF de Locatário para o VRF padrão permitindo VPN |



Cuidado: por padrão, o número máximo de prefixos IP que podem ser exportados do VRF não padrão para um VRF padrão é de 1000 rotas. Esse valor pode ser alterado com o comando em VRF address-family IPV4: export vrf default <number of prefixes> map <route-map name> allow-vpn.

## Etapas de resumo

1. configure 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

## Verificar

Verifique se a rota é importada para a família de endereços BGP IPV4 no VRF padrão

```
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
```

Verifique se a rota é importada para a tabela de roteamento VRF padrão

```
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
```

# VRF de Locatário para VRF de Locatário

Para este exemplo, o Nexus LEAF está recebendo a rota 172.16.120.55/32 locatário-a que será vazada para o locatário-b do VRF

## Verificar a tabela de roteamento

```
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
```

## Filtrar rota

Para filtrar as rotas, são necessárias duas etapas: a filtragem entre VRFs é realizada exibindo Destinos de Rota (RT - Route Targets), o RT é compatível com <BGP Process ID>:L3VNI ID> e filtrando sub-redes específicas. Se a segunda etapa não for usada, todas as rotas do VRF de origem serão vazadas para o VRF de destino.

### Identificar Destino da Rota

**<#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
```

Para este exemplo, o destino de rota é igual a: 65000:303030 e a rota 172.16.120.55/32 será filtrada.

### Configurar

| | Comando ou Ação | Propósito |
|---|---|---|

| | | |
|---|---|---|
| Passo 1 | LEAF#configure terminal<br>Enter configuration commands, one per line. Finalize com CNTL/Z. | Entra no modo de configuração. |
| Passo 2 | LEAF(config)# ip prefix-list filter-tenant-a-to-tenant-b permit 172.16.120.55/32 | Crie uma lista de prefixos que corresponda ao host. |
| Etapa 3 | LEAF(config)# route-map tenantA-to-tenantB | Crie um mapa de rotas. |
| Passo 4 | LEAF(config-route-map)# match ip address prefix-listfilter-tenant-a-to-tenant-b | Faça a correspondência da lista de prefixos criada na etapa 2. |

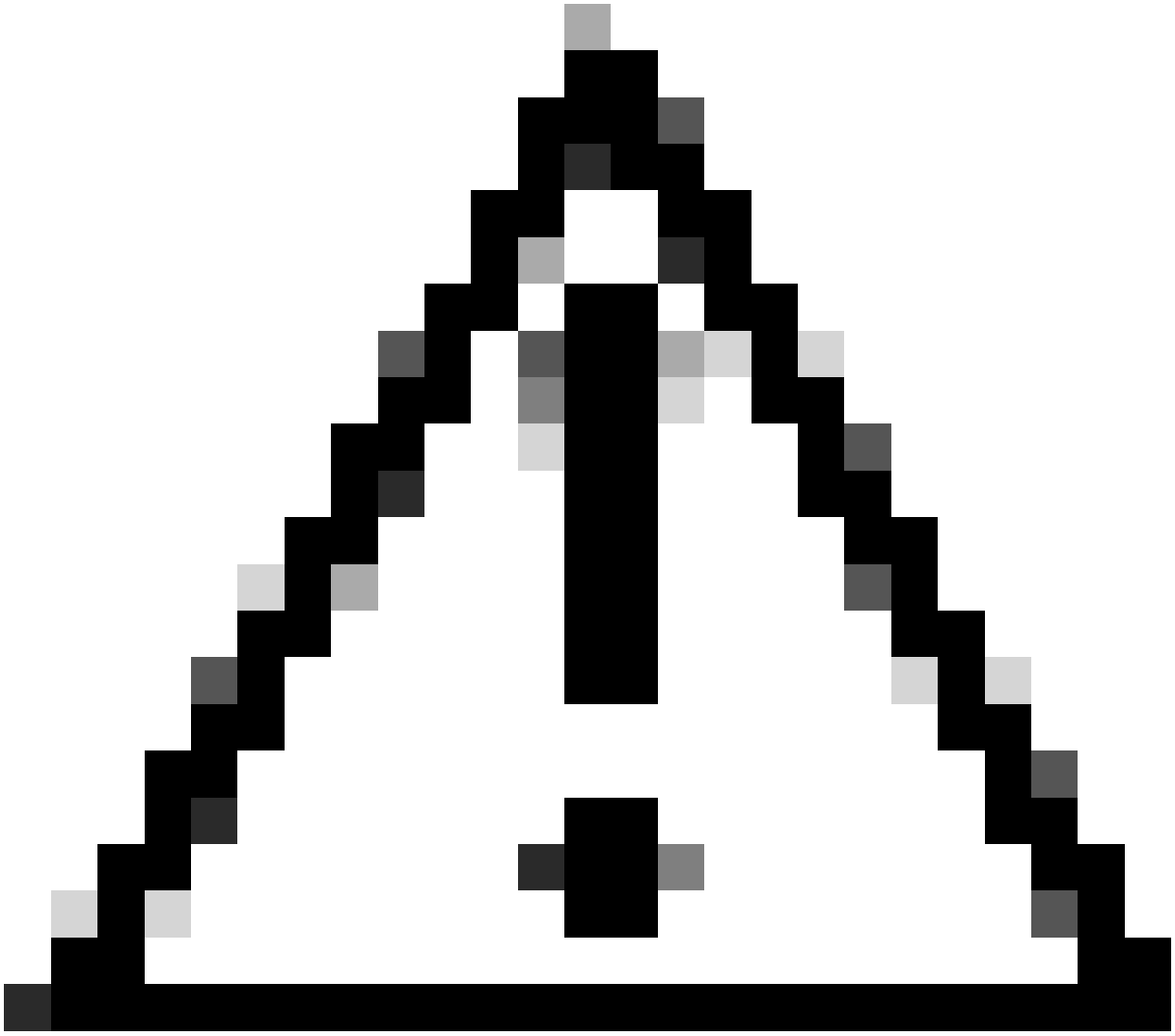
## Importar rota para o usuário a VRF do usuário a VRF

Depois que o RT é identificado e a filtragem é configurada, a rota pode ser importada para o VRF de destino (tenant-b)

Configurar

| | Comando ou Ação | Propósito |
|---|---|---|
| Passo 1 | LEAF#configure terminal<br>Enter configuration commands, one per line. Finalize com CNTL/Z. | Entra no modo de configuração. |
| Passo 2 | LEAF(config)# vrf context tenant-b | Entra na configuração do VRF. |
| Etapa 3 | LEAF(config-vrf)# address-family ipv4 unicast | Digite VRF address-family IPV4. |
| Passo 4 | LEAF(config-vrf-af-ipv4)# import map tenantA-to-tenantB | Rota de importação |

| | | |
|---|---|---|
| | | filtrada com mapa de rota |
| Etapa 5 | LEAF(config-vrf-af-ipv4)#route-target import 65000:303030 | Destino da rota de importação |
| Etapa 6 | LEAF(config-vrf-af-ipv4)# route-target import 65000:303030 evpn | Importar vpn de Destino de Rota |



Cuidado: não usar um mapa de importação pode permitir que todas as rotas do VRF de origem vazem para o VRF de destino. O uso do mapa de importação pode permitir controlar as rotas a serem vazadas.

## Etapas de resumo

1. configure 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. import map tenantA-to-tenantB
8. 65000 de importação de destino de rota:303030
9. route-target import 65000:303030 evpn

## Verificar

Verifique se a rota é importada para o BGP no VRF do locatário 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
```

Verifique se a rota é importada para a tabela de roteamento no VRF do locatário 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)
```

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.