配置并验证Nexus 9000上的VXLAN VRF泄漏

目录

简介

背景信息

先决条件

要求

使用的组件

图解

租户VRF的默认VRF

- 检验路由表
- 过滤路由
  - 配置
- 将路由导入到BGP
  - 配置
  - 验证BGP表
- 将路由导入租户VRF
  - 配置
- 总结步骤
- 验证
  - 检验路由是否已导入到L2VPN。
  - 验证路由是否已导入租户VRF

租户 — VRF到默认VRF

- 检验路由表
- 过滤路由
  - 配置
- 从租户a VRF将路由导出到默认VRF
  - 配置
- 总结步骤
- 验证
  - 验证路由是否导入到默认VRF上的BGP IPV4地址系列
  - 检验路由是否已导入到默认VRF路由表中

租户 — VRF到租户 — VRF

- 检验路由表
- 过滤路由
  - 确定路由目标
  - 配置
- 从租户a VRF导入到租户a VRF的路由
  - 配置
- 总结步骤
- 验证
  - 验证路由是否已导入租户b VRF上的BGP
  - 验证路由是否已导入租户b VRF上的路由表

简介

本文档介绍如何在VXLAN环境中配置和验证VRF泄漏。

背景信息

在VXLAN（虚拟可扩展LAN）环境中，从交换矩阵将VXLAN主机连接到外部主机通常需要使用VRF泄漏和边界枝叶设备。

VRF泄漏在实现VXLAN主机与外部主机之间的通信同时保持网络分段和安全性方面至关重要。

Border Leaf设备用作VXLAN交换矩阵和外部网络之间的网关，在推动此通信方面发挥关键作用。

在此场景中，VRF泄漏的重要性可以总结为以下语句：

1. 与外部网络互连:VRF泄漏允许交换矩阵内的VXLAN主机与交换矩阵外的外部主机通信。这样就可以访问外部网络（例如互联网或其他数据中心）上托管的资源、服务和应用。
2. 网络分段和隔离:VRF泄漏在VXLAN交换矩阵内保持网络分段和隔离，同时实现与外部网络的选择性通信。这可确保VXLAN主机根据其VRF分配保持相互隔离，同时仍能根据需要访问外部资源。
3. 策略实施:VRF泄漏使管理员能够对VXLAN主机和外部主机之间的流量实施网络策略和访问控制。这可确保通信使用预定义的安全策略，并防止对敏感资源的未经授权的访问。
4. 可扩展性和灵活性:VRF泄漏通过允许VXLAN主机与外部主机无缝通信，增强了VXLAN部署的可扩展性和灵活性。它支持在VXLAN和外部网络之间动态分配和共享资源，从而适应不断变化的网络需求，而不会中断现有配置。

在VRF（虚拟路由和转发）泄漏中过滤路由对于维护网络安全、优化路由效率和防止意外数据泄露至关重要。VRF泄漏允许虚拟网络之间进行通信，同时保持它们在逻辑上独立。

过滤路由在VRF泄漏中的重要性可以总结为以下语句：

1. 安全:过滤路由可确保仅特定路由在VRF实例之间泄漏，从而降低未经授权访问或数据泄露的风险。通过控制允许哪些路由跨VRF边界，管理员可以实施安全策略并防止敏感信息暴露给未经授权的实体。
2. 隔离:VRF旨在提供网络分段和隔离，允许不同的租户或部门在同一物理基础设施内独立运行。过滤VRF泄漏中的路由有助于通过限制VRF实例之间的路由传播范围来保持这种隔离，从而

防止意外的通信和潜在的安全漏洞。

3. 优化路由:过滤路由允许管理员选择性地仅泄漏VRF之间的必要路由，从而优化路由效率并减少网络中的不必要流量。通过过滤无关路由，管理员可以确保流量使用最有效的路径，同时最大限度地减少拥塞和延迟。

4. 资源利用率:通过过滤路由，管理员可以控制VRF实例之间的流量传输，从而优化资源利用和带宽分配。这有助于防止网络拥塞，并确保关键资源可用于优先应用或服务。

5. 合规性:过滤VRF泄漏中的路由可帮助组织保持合规性要求和行业标准。通过将路由泄露限制为仅授权实体，组织可以证明遵守了数据保护法规并确保敏感信息的完整性。

6. 精细控制:过滤路由为管理员提供了对VRF实例之间通信的精细控制，允许管理员根据自己的独特需求定义特定策略。这种灵活性使组织能够定制其网络配置，以满足不同应用、用户或部门的需求。

先决条件

带边界路由器的现有VXLAN环境

要求

Cisco 建议您了解以下主题：

- NXOS平台
- VXLAN
- VRF
- 调试输出中显示“BGP

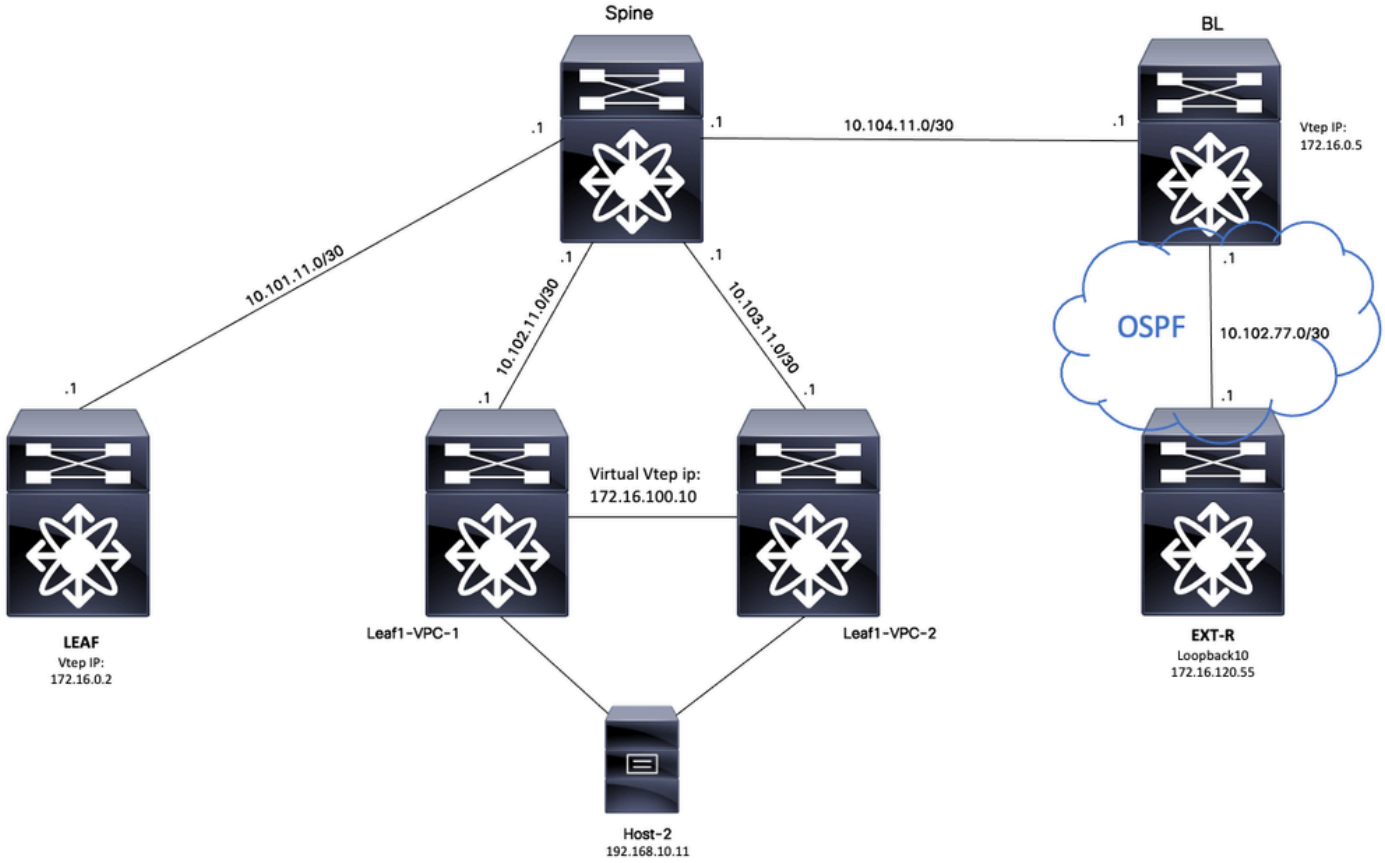
使用的组件

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

名称	Platform	version
主机2	N9K-C92160YC-X	9.3(6)
枝叶 — VPC-1	N9K-C93180YC-EX	9.3(9)
枝叶 — VPC-2	N9K-C93108TC-EX	9.3(9)
枝叶	N9K-C9332D-GX2B	10.2(6)

BL	N9K-C9348D-GX2A	10.2(5)
EXT-R	N9K-C9348D-GX2A	10.2(3)
主干	N9K-C93108TC-FX3P	10.1(1)

图解



将BGP视为应用，BGP是用于执行VRF之间泄漏的应用

租户VRF的默认VRF

在本示例中，边界VTEP(BL)通过默认VRF中的OSFP从外部设备接收172.16.120.55，该VRF将泄漏到租户VRF。

检验路由表

```
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
```

过滤路由

在NXOS中，路由映射需要用作过滤和重新分发路由的参数，例如，将过滤前缀172.16.120.55/32。

配置

	命令或操作	目的
第 1 步	BL#配置终端 输入配置命令，每行一条。以 CNTL/Z 结束。	进入配置模式。
第 2 步	BL(config)# ip prefix-list VXLAN-VRF-default-to-Tenant permit 172.16.120.55/32	创建前缀列表匹配主机。
第 3 步	BL(config)# route-map VXLAN-VRF-default-to-Tenant	创建路由映射。
第 4 步	BL(config-route-map)# match ip address prefix-list VXLAN-VRF-default-to-Tenant	匹配第2步中创建的前缀列表。

将路由导入到BGP

一旦验证默认VRF上存在路由，必须将路由导入BGP进程。

配置

	命令或操作	目的
第 1 步	BL#配置终端	进入配置模式。

	输入配置命令，每行一条。以 CNTL/Z 结束。	
第 2 步	BL(config)# router bgp 65000	进入BGP配置。
第 3 步	BL(config-router)# address-family ipv4 unicast	输入BGP address-famili IPV4。
第 4 步	BL(config-router-af)# redistribute ospf 1 route-map VXLAN-VRF-default-to-Tenant	使用步骤3中创建的路由映射将路由从OSPF重分发到BGP。

验证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
```

将路由导入租户VRF

路由导入到BGP后，现在可以将路由导入到目标VRF（租户 — a）。

配置

	命令或操作	目的
第 1 步	BL(config)# vrf context tenant-a	进入VRF配置。
第 2 步	BL(config-vrf)# address-family ipv4 unicast	输入IPV4地址系列。

第 3 步	BL(config-vrf-af-ipv4)# import vrf default map VXLAN-VRF-default-to-Tenant advertise-vpn	将路由从VRF默认导入租户VRF通告VPN

⚠ 警告：默认情况下，可以从默认VRF导入到非默认VRF的最大IP前缀数量为1000个路由。可以在VRF地址系列IPV4下使用命令更改此值：import vrf <number of prefixes> default map <route-map name> advertise-vpn。

总结步骤

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. 导入vrf默认映射VXLAN-VRF-default-to-Tenant advertise-vpn

验证

检验路由是否已导入到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
```

验证路由是否已导入租户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
```

租户 — VRF到默认VRF

在本示例中，边界VTEP(BL)正在租户a VRF上通过VXLAN接收路由192.168.10.11，该路由将被泄漏到默认VRF。

检验路由表

```
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:
```

过滤路由

在NXOS中，路由映射需要用作过滤和重新分发路由的参数，例如，将过滤前缀172.16.120.55/32。

配置

	命令或操作	目的
第 1 步	BL#配置终端 输入配置命令，每行一条。以 CNTL/Z 结束。	进入配置模式。
第 2 步	BL(config)# ip prefix-list VXLAN-VRF-Tenant-to-default permit 192.168.10.11/32	创建前缀列表匹配主机。
第 3 步	BL(config)# route-map VXLAN-VRF-Tenant-to-default	创建路由映射。
第 4 步	BL(config-route-map)# match ip address prefix-list VXLAN-VRF-Tenant-to-default	匹配第2步中创建的前缀列表。

从租户a VRF将路由导出到默认VRF

由于路由已经在BGP L2VPN进程中，因此只需要将其导出到VRF默认值。

配置

	命令或操作	目的
第 1 步	BL#配置终端 输入配置命令，每行一条。以 CNTL/Z 结束。	进入配置模式。
第 2 步	BL(config)# vrf context tenant-a	进入VRF配置。
第 3 步	BL(config-vrf)# address-family ipv4 unicast	输入VRF地址系列IPV4。

第 4 步	BL(config-vrf-af-ipv4)# export vrf default map VXLAN-VRF-Tenant-to-default allow-vpn	将路由从租户VRF导出到允许VPN的默认VRF

⚠ 警告：默认情况下，可以从非默认VRF导出到默认VRF的最大IP前缀数量为1000个路由。可以在VRF地址系列IPV4下使用命令更改此值：export vrf default <number of prefixes> map <route-map name> allow-vpn。

总结步骤

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. 导出vrf默认映射VXLAN-VRF-Tenant-to-default allow-vpn

验证

验证路由是否导入到默认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
```

检验路由是否已导入到默认VRF路由表中

```
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
```

租户 — VRF到租户 — VRF

在本示例中，nexus LEAF正在接收将泄漏到VRF tenant-b的路由172.16.120.55/32 tenant-a

检验路由表

```
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
```

过滤路由

为了过滤路由需要两个步骤，VRF之间的过滤通过路由目标(RT)完成，RT由<BGP进程ID>:L3VNI ID>和过滤特定子网组成。如果第二步未使用，所有来自源VRF的路由都将泄漏到目标VRF。

注意：路由目标(RT)格式表示为ASN:L3VNI，其中ASN表示发起路由的租户的自治系统编号，L3VNI是第3层VXLAN网络标识符。但是，出于兼容性原因，在BGP中使用4字节ASN时，ASN部分被设置为特殊目的值23456，称为AS_TRANS。此替换可确保与不支持

4字节ASN的设备之间的互操作性。

确定路由目标

<#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
```

在本示例中，路由目标等于：65000:303030和路由172.16.120.55/32将被过滤。

配置

	命令或操作	目的
第 1 步	LEAF#配置终端 输入配置命令，每行一条。以 CNTL/Z 结束。	进入配置模式。
第 2 步	LEAF(config)# ip prefix-list filter-tenant-a-to-tenant-b permit 172.16.120.55/32	创建前缀列

		表匹配主机。
第 3 步	LEAF(config)# route-map tenantA-to-tenantB	创建路由映射。
第 4 步	LEAF(config-route-map)# match ip address prefix-listfilter-tenant-a-to-tenant-b	匹配第2步中创建的前缀列表。

从租户a VRF导入到租户a VRF的路由

确定RT并配置过滤后，路由可以导入到目标VRF（租户 — b）

配置

	命令或操作	目的
第 1 步	LEAF#配置终端 输入配置命令，每行一条。以 CNTL/Z 结束。	进入配置模式。
第 2 步	LEAF(config)# vrf context tenant-b	进入VRF配置。
第 3 步	LEAF(config-vrf)# address-family ipv4 unicast	输入VRF地址系列IPV4。
第 4 步	LEAF(config-vrf-af-ipv4)# import map tenantA-to-tenantB	导入使用路由映射过滤的路由
步骤 5	LEAF(config-vrf-af-ipv4)# route-target import 65000:303030	导入路由目标
第 6 步	LEAF(config-vrf-af-ipv4)# route-target import 65000:303030 evpn	导入路由目标evpn

⚠ 警告：不使用导入映射可以允许来自源VRF的所有路由将其泄漏到目标VRF。使用导入映射可以控制要泄露的路由。

总结步骤

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. 导入映射tenantA-to-tenantB
8. route-target import 65000:303030
9. route-target import 65000:303030 evpn

验证

验证路由是否已导入租户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
```

验证路由是否已导入租户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]
'%



     ' in via output denotes VRF




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)
```

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。