

NSX-T Data Center 管理指南

修改日期：2022 年 5 月 06 日
VMware NSX-T Data Center 2.5

您可以从 VMware 网站下载最新的技术文档:

<https://docs.vmware.com/cn/>。

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

**威睿信息技术（中国）有
限公司**
北京办公室
北京市
朝阳区新源南路 8 号
启皓北京东塔 8 层 801
www.vmware.com/cn

上海办公室
上海市
淮海中路 333 号
瑞安大厦 804-809 室
www.vmware.com/cn

广州办公室
广州市
天河路 385 号
太古汇一座 3502 室
www.vmware.com/cn

版权所有 © 2022 VMware, Inc. 保留所有权利。 [版权和商标信息](#)

目录

关于管理 VMware NSX-T Data Center 13

1 NSX Manager 概览 14

2 Tier-0 网关 17

- 添加 Tier-0 网关 17
- 创建 IP 前缀列表 21
- 创建社区属性列表 22
- 配置静态路由 22
- 创建路由映射 23
- 添加路由映射时使用正则表达式匹配社区属性列表 25
- 配置 BGP 25
- 配置 BFD 28
- 配置 IPv6 第 3 层转发 28
- 创建用于 IPv6 地址分配的 SLAAC 和 DAD 配置文件 29

3 Tier-1 网关 31

- 添加 Tier-1 网关 31

4 分段 34

- 分段配置文件 34
 - 了解 QoS 分段配置文件 35
 - 了解 IP 发现分段配置文件 37
 - 了解 SpoofGuard 分段配置文件 39
 - 了解分段安全分段配置文件 40
 - 了解 MAC 发现分段配置文件 41
- 添加分段 42

5 虚拟专用网络 (VPN) 44

- 了解 IPsec VPN 45
 - 使用基于策略的 IPsec VPN 45
 - 使用基于路由的 IPsec VPN 46
- 了解第 2 层 VPN 47
- 添加 VPN 服务 48
 - 添加 IPsec VPN 服务 50
 - 添加 L2 VPN 服务 51
- 添加 IPsec VPN 会话 53

添加基于策略的 IPSec 会话	53
添加基于路由的 IPSec 会话	56
关于支持的合规性套件	59
了解 TCP MSS 限制	60
添加 L2 VPN 会话	60
添加 L2 VPN 服务器会话	60
添加 L2 VPN 客户端会话	62
下载远程端 L2 VPN 配置文件	63
添加本地端点	64
添加配置文件	65
添加 IKE 配置文件	65
添加 IPSec 配置文件	68
添加 DPD 配置文件	70
将自治 Edge 添加为 L2 VPN 客户端	70
检查 IPSec VPN 会话的已实现状态	73
监控 VPN 会话和排除其故障	76

6 网络地址转换 77

在网关上配置 NAT	77
------------	----

7 负载均衡 79

负载均衡器重要概念	80
缩放负载均衡器资源	80
支持的负载平衡器功能	81
负载均衡器拓扑	82
设置负载平衡器组件	84
添加负载均衡器	84
添加主动监控器	86
添加被动监控器	89
添加服务器池	90
设置虚拟服务器组件	94
为服务器池和虚拟服务器创建的组	113

8 转发策略 114

添加或编辑转发策略	115
-----------	-----

9 IP 地址管理 (IPAM) 116

添加 DNS 区域	116
添加 DNS 转发器服务	117
添加 DHCP 服务器	118
为 Tier-0 或 Tier-1 网关配置 DHCP 中继服务器	119

添加 IP 地址池 120

添加 IP 地址块 120

10 安全 122

安全配置概述 122

安全术语 123

身份防火墙 123

身份防火墙工作流 124

第 7 层上下文配置文件 126

第 7 层防火墙规则工作流 127

属性 128

分布式防火墙 131

防火墙草稿 131

添加分布式防火墙 133

分布式防火墙数据包日志 136

选择默认连接策略 138

管理防火墙排除列表 139

筛选特定域 (FQDN/URL) 139

将安全策略扩展到物理工作负载 140

共享地址集 147

东西向网络安全 - 第三方服务链 147

网络保护（东西向）的重要概念 147

NSX-T Data Center 对东西向流量的要求 148

东西向网络安全的高级别任务 148

为东西向流量自检部署服务 149

添加服务配置文件 150

添加服务链 150

为东西向流量添加重定向规则 151

配置网关防火墙 153

添加网关防火墙策略和规则 153

南北向网络安全 - 插入第三方服务 155

南北向网络安全的高级别任务 156

为南北向流量自检部署服务 156

配置流量重定向 158

为南北向流量添加重定向规则 159

监控流量重定向 160

端点保护 160

了解端点保护 160

配置端点保护 163

管理端点保护 178

安全配置文件 187

- 创建会话定时器 187
- 泛洪保护 189
- 配置 DNS 安全配置文件 191
- 管理组到配置文件的优先级 192

11 清单 193

- 添加服务 193
- 添加组 194
- 添加上下文配置文件 195

12 监控 197

- 添加防火墙 IPFIX 配置文件 197
- 添加交换机 IPFIX 配置文件 198
- 添加 IPFIX 收集器 199
- 添加端口镜像配置文件 199
- 简单网络管理协议 (SNMP) 200
- 使用 vRealize Log Insight 监控系统 201
- 使用 vRealize Operations Manager 监控系统 202
- 使用 vRealize Network Insight Cloud 监控系统 205
- 高级监控工具 213
 - 查看端口连接信息 213
 - 跟踪流 214
 - 监控端口镜像会话 216
 - 为端口镜像会话配置筛选器 219
 - 配置 IPFIX 220
 - 监控逻辑交换机端口活动 393

13 逻辑交换机 395

- 了解 BUM 帧复制模式 396
- 创建逻辑交换机 397
- 将虚拟机连接到逻辑交换机 398
 - 将 vCenter Server 上托管的虚拟机连接到 NSX-T Data Center 逻辑交换机 398
 - 将单独 ESXi 上托管的虚拟机连接到 NSX-T Data Center 逻辑交换机 400
 - 将 KVM 上托管的虚拟机连接到 NSX-T Data Center 逻辑交换机 404
- 创建逻辑交换机端口 405
- 测试第 2 层连接 406
- 为 NSX Edge 上行链路创建 VLAN 逻辑交换机 408
- 逻辑交换机和逻辑端口的交换配置文件 410
 - 了解 QoS 交换配置文件 411
 - 了解端口镜像交换配置文件 413
 - 了解 IP 发现交换配置文件 415

- 了解 SpoofGuard 417
- 了解交换机安全交换配置文件 419
- 了解 MAC 管理交换配置文件 420
- 将自定义配置文件与逻辑交换机相关联 421
- 将自定义配置文件与逻辑端口相关联 422
- 增强型网络堆栈 423
 - 自动分配 ENS 逻辑内核 423
 - 配置客户机 VLAN 间路由 424
- 第 2 层桥接 426
 - 创建 Edge 网桥配置文件 426
 - 配置基于 Edge 的桥接 427
 - 创建支持网桥的第 2 层逻辑交换机 430

14 逻辑路由器 432

- Tier-1 逻辑路由器 432
 - 创建 Tier-1 逻辑路由器 434
 - 在 Tier-1 逻辑路由器上添加下行链路端口 435
 - 在 Tier-0 或 Tier-1 逻辑路由器上添加 VLAN 端口 436
 - 在 Tier-1 逻辑路由器上配置路由通告 436
 - 配置 Tier-1 逻辑路由器静态路由 438
 - 创建独立 Tier-1 逻辑路由器 440
- Tier-0 逻辑路由器 441
 - 创建 Tier-0 逻辑路由器 443
 - 连接 Tier-0 和 Tier-1 444
 - 将 Tier-0 逻辑路由器连接到 NSX Edge 上行链路的 VLAN 逻辑交换机 446
 - 添加环回路由器端口 449
 - 在 Tier-0 或 Tier-1 逻辑路由器上添加 VLAN 端口 450
 - 配置静态路由 451
 - BGP 配置选项 454
 - 在 Tier-0 逻辑路由器上配置 BFD 459
 - 在 Tier-0 逻辑路由器上启用路由重新分发 460
 - 了解 ECMP 路由 463
 - 创建 IP 前缀列表 467
 - 创建社区属性列表 467
 - 创建路由映射 468
 - 配置转发启动定时器 469

15 高级 NAT 470

- 网络地址转换 470
 - Tier-1 NAT 472
 - Tier-0 NAT 478

反射 NAT 479

16 高级分组对象 482

创建 IP 集 482

创建 IP 池 483

创建 MAC 集 483

创建 NS 组 484

配置服务和服务组 485

创建 NS 服务 486

管理虚拟机的标记 486

17 高级 DHCP 488

DHCP 488

创建 DHCP 服务器配置文件 488

创建 DHCP 服务器 489

将 DHCP 服务器连接到逻辑交换机 490

将 DHCP 服务器与逻辑交换机断开连接 490

创建 DHCP 中继配置文件 490

创建 DHCP 中继服务 491

将 DHCP 中继服务添加到逻辑路由器端口 491

删除 DHCP 租约 491

元数据代理 492

添加元数据代理服务器 492

将元数据代理服务器连接到逻辑交换机 493

将元数据代理服务器与逻辑交换机断开连接 493

18 高级 IP 地址管理 494

管理 IP 块 494

管理 IP 块的子网 495

19 高级负载均衡 496

负载均衡器重要概念 497

配置负载均衡器组件 497

创建负载均衡器 498

配置主动运行状况监控器 499

配置被动运行状况监控器 502

添加服务器池用于负载平衡 503

配置虚拟服务器组件 506

20 高级防火墙 525

在逻辑路由器中添加或删除防火墙规则 525

为逻辑交换机网桥端口配置防火墙	526
防火墙区域和防火墙规则	526
启用和禁用分布式防火墙	527
添加防火墙规则区域	527
删除防火墙规则区域	528
启用和禁用区域规则	528
启用和禁用区域日志	529
配置防火墙排除列表	529
关于防火墙规则	529
添加防火墙规则	531
删除防火墙规则	532
编辑默认分布式防火墙规则	533
更改防火墙规则的顺序	533
筛选防火墙规则	534

21 操作和管理 535

查看监控仪表板	536
查看各类别对象的使用情况和容量	538
检查配置更改的已实现状态	539
搜索对象	543
按对象属性筛选	544
添加计算管理器	545
添加 Active Directory	546
添加 LDAP 服务器	547
同步 Active Directory	548
管理用户帐户和基于角色的访问控制	548
管理用户密码	549
重置设备密码	550
身份验证策略设置	551
从 vIDM 主机中获取证书指纹	552
配置 VMware Identity Manager 集成	553
验证 VMware Identity Manager 功能	555
NSX Manager、vIDM 和相关组件之间的时间同步	556
基于角色的访问控制	557
添加角色分配或主体身份	565
备份和还原 NSX Manager	566
配置备份	567
移除旧备份	568
列出可用备份	569
还原备份	570
在升级过程中备份和还原	572

从 vCenter Server 中移除 NSX-T Data Center 扩展	572
管理 NSX Manager 集群	573
查看 NSX Manager 集群的配置和状态	573
关闭 NSX Manager 集群，然后打开其电源。	576
重新引导 NSX Manager	576
更改 NSX Manager 的 IP 地址	576
调整 NSX Manager 节点的大小	578
在 vCenter Server 中添加和移除 ESXi 主机传输节点	578
替换 NSX Edge 集群中的 NSX Edge 传输节点	579
使用 NSX Manager UI 替换 NSX Edge 传输节点	579
使用 API 替换 NSX Edge 传输节点	580
在 vCenter Server 丢失且无法恢复时恢复 NSX-T	581
NSX-T Data Center 的多站点部署	583
配置设备	590
添加许可证密钥并生成许可证使用情况报告	590
设置证书	592
导入证书	592
创建证书签名请求文件	592
导入 CA 证书	594
创建自签名证书	594
替换 NSX Manager 节点或 NSX Manager 集群虚拟 IP 的证书	595
导入证书吊销列表	596
配置 NSX Manager 以检索证书吊销列表	597
为 CSR 导入证书	597
存储公用证书和私钥	598
基于合规性的配置	598
查看合规性状态报告	598
合规性状态报告代码	599
为负载均衡器配置全局 FIPS 合规性模式	601
收集支持包	603
日志消息和错误代码	604
配置远程日志记录	606
日志消息 ID	613
对 Syslog 问题进行故障排除	614
在设备虚拟机上配置串行日志记录	615
客户体验提升计划	615
编辑客户体验提升计划配置	615
将标记添加到对象	616
查找远程服务器的 SSH 指纹	617
查看有关在虚拟机上运行的应用程序的数据	618
配置外部负载均衡器	618

22 使用 NSX Cloud 620

- Cloud Service Manager 快速概览 620
 - 云 620
 - 系统 626
- 使用 NSX Cloud 隔离策略的威胁检测 628
 - NSX 实施模式下的隔离策略 629
 - 云原生实施模式下的隔离策略 634
 - 将虚拟机添加到白名单 634
- NSX 实施模式 635
 - 工作负载虚拟机当前支持的操作系统 635
 - 在 NSX 实施模式下载入虚拟机 636
 - 在 NSX 实施模式下管理虚拟机 644
- 云原生实施模式 645
 - 在云原生实施模式下管理虚拟机 645
- NSX Cloud 支持的 NSX-T Data Center 功能 648
 - 使用 NSX-T Data Center 和公有云标记对虚拟机分组 649
 - 使用云原生服务 652
 - 在公有云中使用服务插入 653
 - 在 NSX 管理的虚拟机上启用 NAT 659
 - 启用 Syslog 转发 660
 - 在 NSX 实施模式下设置 VPN 660
- 常见问题解答 (FAQ) 665

23 使用 NSX Intelligence 668

- NSX Intelligence 入门指南 668
 - NSX Intelligence 主页概览 668
 - 熟悉 NSX Intelligence 图形元素 670
- 了解 NSX Intelligence 视图和流量 672
 - 使用“组”视图 672
 - 使用“虚拟机”视图 676
 - 使用流量流 678
- 使用 NSX Intelligence 建议 680
 - 了解 NSX Intelligence 建议 680
 - 生成新的 NSX Intelligence 建议 681
 - 查看并发布生成的建议 682
- 备份和还原 NSX Intelligence 684
 - 配置 NSX Intelligence 备份 684
 - 备份 NSX Intelligence 685
 - 还原 NSX Intelligence 备份 686
- 解决 NSX Intelligence 问题 687

[检查 NSX Intelligence 设备的状态](#) 687

[收集 NSX Intelligence 支持包](#) 692

关于管理 VMware NSX-T Data Center

NSX-T Data Center 管理指南 提供有关配置和管理 VMware NSX-T™ Data Center 网络的信息，包括如何创建逻辑交换机和端口、如何为分层逻辑路由器设置网络，以及如何配置 NAT、防火墙、SpoofGuard、分组和 DHCP。此外，还介绍了如何配置 NSX Cloud。

目标读者

本文档中的信息适用于任何要配置 NSX-T Data Center 的人员。本文档中的信息是为熟悉虚拟机技术、网络和安全操作且经验丰富的 Windows 或 Linux 系统管理员编写的。

VMware 技术出版物术语表

VMware 技术出版物提供了一个术语表，其中包含一些您可能不熟悉的术语。有关 VMware 技术文档中所使用的术语的定义，请访问 <https://www.vmware.com/topics/glossary>。

NSX Manager 概览

1

NSX Manager 提供了一个基于 Web 的用户界面，您可以在其中管理 NSX-T 环境。它还托管用于处理 API 调用的 API 服务器。

NSX Manager Web 界面提供了两种配置资源的方法。

- “策略”界面：网络、安全、清单和安全规划和故障排除选项卡。
- “高级”界面：高级网络和安全选项卡。

何时使用”策略“或”高级“界面

在使用哪个用户界面上面，请保持一致。使用一个用户界面而不是另一个用户界面的原因有几个。

- 如果要部署具有 NSX-T Data Center 2.4 或更高版本的新环境，在大多数情况下，最好是使用基于策略的新用户界面来创建和管理环境。
 - 某些功能在基于策略的用户界面中不可用。如果需要使用这些功能，请使用“高级”用户界面来完成所有配置。
- 如果要升级到 NSX-T Data Center 2.4 或更高版本，请继续使用高级网络和安全用户界面进行配置更改。

表 1-1. 何时使用”策略“或”高级“界面


“策略”界面	“高级”界面
大多数新的部署应使用基于策略的界面。	使用“高级”界面创建的部署，例如，在出现基于策略的界面之前从版本进行升级。
NSX Cloud 部署	与其他插件集成的部署。例如，NSX Container Plug-in、Openstack 和其他云计算管理平台。

表 1-1. 何时使用”策略“或”高级“界面（续）

“策略”界面	“高级”界面
仅在“策略”界面中提供的网络连接功能： <ul style="list-style-type: none"> ■ DNS 服务和 DNS 区域 ■ VPN ■ NSX Cloud 转发策略 	仅在“高级”界面中提供的网络连接功能： <ul style="list-style-type: none"> ■ 转发启动定时器 ■ 以 BFD 和接口作为下一跃点的静态路由 ■ 元数据代理 ■ 连接到隔离分段和静态绑定的 DHCP 服务器
仅在“策略”界面中提供的安全功能： <ul style="list-style-type: none"> ■ 端点保护 ■ 网络侦测（东西向服务插入） ■ 上下文配置文件 <ul style="list-style-type: none"> ■ L7 应用程序 ■ FQDN ■ 新的分布式防火墙和网关防火墙布局 <ul style="list-style-type: none"> ■ 类别 ■ 自动服务规则 ■ 草稿 	仅在“高级”界面中提供的安全功能： <ul style="list-style-type: none"> ■ CPU 和内存阈值 ■ 网桥防火墙 ■ 基于源和目标中的 IP 的分布式防火墙规则

使用“策略”界面

如果决定使用“策略”界面，请使用该界面创建所有对象。请勿使用“高级”界面创建对象。

您可以使用“高级”界面来修改在“策略”界面中创建的对象。用于策略创建的对象设置可能包含**高级配置**的链接。此链接将转到“高级”界面，您可以在该界面中精确调整配置。您还可以直接在“高级”界面中查看策略创建的对象。由策略管理但在“高级”界面中可见的设置旁边有此图标：。您无法通过“高级”用户界面对其进行修改。

在何处可以找到“策略”界面和“高级”界面

基于策略的界面和“高级”界面显示在 NSX Manager 用户界面的不同部分中，并使用不同的 API URI。

表 1-2. “策略”界面和“高级”界面

“策略”界面	“高级”界面
<ul style="list-style-type: none"> ■ 网络选项卡 ■ 安全选项卡 ■ 清单选项卡 ■ 安全规划和故障排除选项卡 	高级网络和安全选项卡
以 /policy/api 开头的 API URI	以 /api 开头的 API URI

注 系统选项卡可用于所有环境。如果您修改了 Edge 节点、Edge 集群或传输区域，则可能需要长达 5 分钟的时间才能在基于策略的用户界面上显示这些更改。您可以使用 `POST /policy/api/v1/infra/sites/default/enforcement-points/default?action=reload` 立即同步。

有关使用策略 API 的详细信息，请参见《[NSX-T 策略 API 入门指南](#)》。

在“策略”和“高级”界面中所创建的对象名称

您创建的对象具有不同的名称，具体取决于创建这些对象时所使用的界面。

表 1-3. 对象名称

使用“策略”界面创建的对象	使用“高级”界面创建的对象
分段	逻辑交换机
Tier-1 网关	Tier-1 逻辑路由器
Tier-0 网关	Tier-0 逻辑路由器
组	NS 组、IP 集、MAC 集
安全策略	防火墙区域
规则	防火墙规则
网关防火墙	Edge 防火墙

Tier-0 网关

2

Tier-0 网关执行 Tier-0 逻辑路由器的功能。它负责处理逻辑网络和物理网络之间的流量。

NSX Cloud 说明 如果使用 NSX Cloud，请参见 [NSX Cloud 支持的 NSX-T Data Center 功能](#) 以查看自动生成的逻辑实体、支持的功能以及 NSX Cloud 所需的配置的列表。

Edge 节点只能支持一个 Tier-0 网关或逻辑路由器。在创建 Tier-0 网关或逻辑路由器时，请确保您创建的 Tier-0 网关或逻辑路由器没有超过 NSX Edge 群集中的 Edge 节点数。

注 在[高级网络和安全](#)选项卡中，使用术语 Tier-0 逻辑路由器指代 Tier-0 网关。

本章讨论了以下主题：

- [添加 Tier-0 网关](#)
- [创建 IP 前缀列表](#)
- [创建社区属性列表](#)
- [配置静态路由](#)
- [创建路由映射](#)
- [添加路由映射时使用正则表达式匹配社区属性列表](#)
- [配置 BGP](#)
- [配置 BFD](#)
- [配置 IPv6 第 3 层转发](#)
- [创建用于 IPv6 地址分配的 SLAAC 和 DAD 配置文件](#)

添加 Tier-0 网关

Tier-0 网关具有到 Tier-1 网关的下行链路连接，以及到物理网络的上行链路连接。

您可以将 Tier-0 网关的 HA（高可用性）模式配置为活动-活动或活动-备用。仅活动-备用模式支持以下服务：

- NAT
- 负载均衡

- 有状态防火墙
- VPN

对于单层和多层拓扑中的所有接口（上行链路、服务端口和下行链路），Tier-0 和 Tier-1 网关支持以下寻址配置：

- 仅 IPv4
- 仅 IPv6
- 双栈 - IPv4 和 IPv6

要使用 IPv6 或双栈寻址，请在**网络 > 网络设置 > 全局网络配置**中启用 **IPv4 和 IPv6** 以作为 L3 转发模式。

如果为 Tier-0 网关配置路由重新分发，则可以从以下两组源中进行选择：Tier-0 子网和已通告的 Tier-1 子网。Tier-0 子网组中的源包括：

源类型	说明
已连接接口和分段	其中包括已连接到 Tier-0 网关的外部接口子网、服务接口子网和分段子网。
静态路由	在 Tier-0 网关上配置的静态路由。
NAT IP	由 Tier-0 网关所拥有并从 Tier-0 网关上配置的 NAT 规则中发现的 NAT IP 地址。
IPSec 本地 IP	用于建立 VPN 会话的本地 IPSEC 端点 IP 地址。
DNS 转发器 IP	来自客户端的 DNS 查询的侦听器 IP，该 IP 也用作将 DNS 查询转发到上游 DNS 服务器的源 IP。

已通告的 Tier-1 子网组中的源包括：

源类型	说明
已连接接口和分段	其中包括已连接到 Tier-1 网关的分段子网和在 Tier-1 网关上配置的服务接口子网。
静态路由	在 Tier-1 网关上配置的静态路由。
NAT IP	由 Tier-1 网关所拥有并从 Tier-1 网关上配置的 NAT 规则中发现的 NAT IP 地址。
LB VIP	负载均衡虚拟服务器的 IP 地址。
LB SNAT IP	由负载均衡器用于源 NAT 的 IP 地址或 IP 地址范围。
DNS 转发器 IP	来自客户端的 DNS 查询的侦听器 IP，该 IP 也用作将 DNS 查询转发到上游 DNS 服务器的源 IP。
IPSec 本地端点	IPSec 本地端点的 IP 地址。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**网络 > Tier-0 网关**。
- 3 单击**添加 Tier-0 网关**。
- 4 输入网关的名称。

5 选择 HA（高可用性）模式。

默认模式为活动-活动。在活动-活动模式下，将在所有成员之间进行流量负载均衡。在活动-备用模式下，将由选举的活动成员处理所有流量。如果活动成员发生故障，将选举新的成员以作为活动成员。

重要事项 创建网关后，无法更改 HA 模式。

6 如果 HA 模式为活动-备用，请选择故障切换模式。

选项	说明
主动	如果首选节点发生故障并恢复，它将取代对等节点并变为活动节点。对等节点将其状态更改为备用。
非主动	如果首选节点发生故障并恢复，它将检查对等节点是否为活动节点。如果是，首选节点不会取代对等节点并作为备用节点。

7 （可选）选择一个 NSX Edge 集群。

8 （可选）添加一个或多个标记。

9 （可选）单击其他设置。

a 在内部转换子网字段中，输入一个子网。

这是用于该网关内组件之间的通信的子网。默认值为 169.254.0.0/28。

b 在 TO-T1 转换子网字段中，输入一个或多个子网。

这些子网用于该网关及其链接到的所有 Tier-1 网关之间的通信。在创建该网关并将其链接到 Tier-1 网关后，将会在 Tier-O 网关端和 Tier-1 网关端看到分配给链路的实际 IP 地址。该地址显示在 Tier-O 网关页面和 Tier-1 网关页面上的其他设置 > 路由器链路中。默认值为 100.64.0.0/16。

c 为 IPv6 地址配置选择一个 ND 配置文件和 DAD 配置文件。

这些配置文件用于配置 IPv6 地址的无状态地址自动配置 (SLAAC) 和重复地址检测 (DAD)。将创建默认配置文件。

10 单击保存。

11 要配置路由重新分发，请单击路由重新分发和设置。

选择一个或多个以下源：

■ Tier-O 子网：静态路由、NAT IP、IPSec 本地 IP、DNS 转发器 IP、已连接接口和分段。

在已连接接口和分段下方，您可以选择以下一项或多项：服务接口子网、外部接口子网、环回接口子网、已连接分段。

■ 已通告的 Tier-1 子网：DNS 转发器 IP、静态路由、LB VIP、NAT IP、LB SNAT IP、IPSec 本地端点、已连接接口和分段。

在已连接接口和分段下方，您可以选择服务接口子网和/或已连接分段。

12 要配置接口，请单击接口**和**设置**。**

- a 单击**添加接口**。
- b 输入名称。
- c 选择一种类型。

如果 HA 模式为活动-备用，则选项包括**外部**、**服务**和**环回**。如果 HA 模式为活动-活动，则选项包括**外部**和**环回**。

- d 使用 CIDR 格式输入一个 IP 地址。
- e 选择分段。
- f 如果接口类型不是**服务**，请选择 NSX Edge 节点。
- g （可选）如果接口类型不是**环回**，请输入 MTU 值。
- h （可选）添加标记，然后选择一个 ND 配置文件。

13 （可选）如果 HA 模式为活动-备用，请单击 **HA VIP 配置旁边的**设置**，以配置 HA VIP。**

在配置了 HA VIP 时，即使一个上行链路关闭，Tier-0 网关也会正常运行。物理路由器仅与 HA VIP 进行交互。HA VIP 适用于静态路由，而不是 BGP。

- a 单击**添加 HA VIP 配置**。
- b 输入一个 IP 地址和子网掩码。

HA VIP 子网必须与其绑定到的接口的子网相同。

- c 从两个不同的 Edge 节点中选择两个接口。

14 单击路由**以添加 IP 前缀列表、社区属性列表、静态路由和路由映射。****15 单击 **BGP** 以配置 BGP。****16 单击**高级配置**转到**高级网络和安全 > 路由器**页面，以进行其他配置。**

- a 要配置第 3 层转发模式，请单击**全局配置**选项卡。
- b 单击**编辑**。
- c 选择 **IPv4** 或 **IPv4 和 IPv6**。

默认仅选择 IPv4。不支持仅选择 IPv6 要启用 IPv6，请选择 **IPv4 和 IPv6**。

- d 单击**保存**。

创建 IP 前缀列表

IP 前缀列表包含一个或多个分配了访问权限以进行路由通告的 IP 地址。该列表中的 IP 地址是按顺序进行处理的。IP 前缀列表是通过输入或输出方向的 BGP 邻居筛选器或路由映射引用的。

例如，您可以将 IP 地址 192.168.100.3/27 添加到 IP 前缀列表中，并拒绝将路由重新分发到北向路由器。也可以在 IP 地址后面附加小于或等于 (**le**) 或大于或等于 (**ge**) 修饰符以允许或限制路由重新分发。例如，192.168.100.3/27 ge 24 le 30 修饰符与长度大于或等于 24 位且小于或等于 30 位的子网掩码相匹配。

注 路由的默认操作为**拒绝**。在创建一个前缀列表以拒绝或允许特定路由时，如果要允许所有其他路由，请务必创建一个无特定网络地址（从下拉列表中选择**任意**）且操作为**允许**的 IP 前缀。

前提条件

确认配置了一个 Tier-0 网关。请参见[创建 Tier-0 逻辑路由器](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**网络 > Tier-0 网关**。
- 3 要编辑 Tier-0 网关，请单击菜单图标（三个点），然后选择**编辑**。
- 4 单击**路由**。
- 5 单击 **IP 前缀列表** 旁边的**设置**。
- 6 单击**添加 IP 前缀列表**。
- 7 输入 IP 前缀列表的名称。
- 8 单击**设置**以添加 IP 前缀。
- 9 单击**添加前缀**。
 - a 使用 CIDR 格式输入一个 IP 地址。
例如，192.168.100.3/27。
 - b （可选）在 **le** 或 **ge** 修饰符中设置一定范围的 IP 地址位数。
例如，将 **le** 设置为 30 并将 **ge** 设置为 24。
 - c 从下拉菜单中选择**拒绝**或**允许**。
 - d 单击**添加**。
- 10 重复上述步骤以指定其他前缀。
- 11 单击**保存**。

创建社区属性列表

您可以创建 BGP 社区属性列表，以便基于社区属性列表配置路由映射。

社区属性列表是用户定义的社区属性值的列表。这些列表可用于匹配或处理 BGP 更新消息中的社区属性。

支持 BGP 社区属性 (RFC 1997) 及 BGP 大型社区属性 (RFC 8092)。BGP 社区属性是一个已拆分为两个 16 位值的 32 位值。BGP 大型社区属性由 3 部分组成，每一部分均包含 4 个八位字节。

在路由映射中，可以匹配或设置 BGP 社区属性或 BGP 大型社区属性。使用此功能，网络操作员可以基于 BGP 社区属性实施网络策略。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**网络 > Tier-0 网关**。
- 3 要编辑 Tier-0 网关，请单击菜单图标（三个点），然后选择**编辑**。
- 4 单击**路由**。
- 5 单击**社区属性列表**旁边的**设置**。
- 6 单击**添加社区属性列表**。
- 7 输入社区属性列表的名称。
- 8 指定社区属性列表。对于常规社区属性，请使用 **aa:nn** 格式，例如 **300:500**。对于大型社区属性，请使用 **aa:bb:cc** 格式，例如 **11:22:33**。请注意，该列表中不能同时具有常规社区属性和大型社区属性。它必须仅包含常规社区属性或仅包含大型社区属性。

此外，可以选择以下一个或多个常规社区属性：请注意，如果列表中包含大型社区属性，则无法添加这些常规社区属性。

- NO_EXPORT_SUBCONFED - 不通告到 EBGp 对等项。
- NO_ADVERTISE - 不通告到任何对等项。
- NO_EXPORT - 不通告到外部 BGP 联合。

- 9 单击**保存**。

配置静态路由

可以在 Tier-0 网关上配置到外部网络的静态路由。在配置静态路由后，不需要将该路由从 Tier-0 通告到 Tier-1，因为 Tier-1 网关自动具有到它连接的 Tier-0 网关的静态默认路由。

支持递归静态路由。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**网络 > Tier-0 网关**。

- 3 要编辑 Tier-0 网关，请单击菜单图标（三个点），然后选择**编辑**。
- 4 单击**路由**。
- 5 单击**静态路由**旁边的**设置**。
- 6 单击**添加静态路由**。
- 7 以 CIDR 格式输入名称和网络地址。支持基于 IPv6 的静态路由。IPv6 前缀只能有 IPv6 下一跃点。
- 8 单击**设置下一跃点**以添加下一跃点的信息。
- 9 单击**添加下一跃点**。
- 10 输入 IP 地址。
- 11 指定管理距离。
- 12 从下拉列表中选择接口。
- 13 单击**添加**按钮。

后续步骤

检查是否正确配置了静态路由。请参见[验证静态路由](#)。

创建路由映射

路由映射由一系列 IP 前缀列表、BGP 路径属性和关联的操作组成。路由器扫描该序列以查找匹配的 IP 地址。如果找到一个匹配的地址，路由器将执行操作，而不再扫描其他地址。

可以在 BGP 邻居级别和路由重新分发中引用路由映射。

前提条件

- 确认已配置了 IP 前缀列表或社区属性列表。请参阅[创建 IP 前缀列表](#)或[创建社区属性列表](#)。
- 有关如何使用正则表达式为社区属性列表定义路由映射匹配条件的详细信息，请参见[添加路由映射时使用正则表达式匹配社区属性列表](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**网络 > Tier-0 网关**。
- 3 要编辑 Tier-0 网关，请单击菜单图标（三个点），然后选择**编辑**。
- 4 单击**路由**。
- 5 单击**路由映射**旁边的**设置**。
- 6 单击**添加路由映射**。
- 7 输入名称，然后单击**设置**以添加匹配条件。
- 8 单击**添加匹配条件**以添加一个或多个匹配条件。

9 对于每个条件，请选择 **IP 前缀**或**社区属性列表**，然后单击**设置**以指定一个或多个匹配表达式。

a 如果选择了**社区属性列表**，请指定匹配表达式，用于定义如何匹配社区属性列表成员。对于每个社区属性列表，以下匹配选项可用：

- **匹配任意** - 如果社区属性列表中有任意社区属性匹配，在路由映射中执行设置操作。
- **匹配所有** - 如果社区属性列表中的所有社区属性不论顺序如何均匹配，在路由映射中执行设置操作。
- **精确匹配** - 如果社区属性列表中的所有社区属性按完全相同的顺序匹配，在路由映射中执行设置操作。
- **匹配社区属性正则表达式** - 如果与 **NRLI** 关联的所有常规社区属性均与正则表达式匹配，请在路由映射中执行设置的操作。
- **匹配大型社区属性正则表达式** - 如果与 **NRLI** 关联的所有大型社区属性均与正则表达式匹配，请在路由映射中执行设置的操作。

您应使用匹配条件“**MATCH_COMMUNITY_REGEX**”来根据标准社区属性匹配路由，使用匹配条件“**MATCH_LARGE_COMMUNITY_REGEX**”来根据大型社区属性匹配路由。如果要允许包含标准社区属性或大型社区属性值的路由，则必须创建两个匹配条件。如果匹配表达式是在同一匹配条件下提供的，则将仅允许同时包含标准社区属性和大型社区属性的路由。

对于任何匹配条件，如果匹配表达式应用于 **AND** 运算中，则意味着必须满足所有匹配表达式才会出现匹配。如果存在多个匹配条件，并且这些条件应用于 **OR** 运算中，则意味着如果满足任何一个匹配条件，便会出现一个匹配。

10 设置 BGP 属性。

BGP 属性	说明
AS 路径前置	在路径前面放置一个或多个 AS （自主系统）编号以使路径更长，因此，通常不是首选的路径。
MED	多出口区分符向外部对等项指示 AS 的首选路径。
权重	设置权重以影响路径选择。范围是 0-65535。
社区属性	指定社区属性列表。对于常规社区属性，请使用 aa:nn 格式，例如 300:500 。对于大型社区属性，请使用 aa:bb:cc 格式，例如 11:22:33 。或者，使用下拉菜单选择以下选项之一： <ul style="list-style-type: none"> ■ NO_EXPORT_SUBCONFED - 不通告到 EBGp 对等项。 ■ NO_ADVERTISE - 不通告到任何对等项。 ■ NO_EXPORT - 不通告到外部 BGP 联合。
本地首选项	使用此值可选择出站外部 BGP 路径。首选具有最高值的路径。

11 在“操作”列中，选择**允许**或**拒绝**。

您可以允许或拒绝通告那些与 **IP 前缀列表**或**社区属性列表**匹配的 **IP 地址**。

12 单击**保存**。

添加路由映射时使用正则表达式匹配社区属性列表

您可以使用正则表达式定义社区属性列表的路由映射匹配条件。BGP 正则表达式基于 POSIX 1003.2 正则表达式。

以下表达式是 POSIX 正则表达式的子集。

表达式	说明
。	匹配任何单个字符。
*	匹配 0 个或多个模式出现的实例。
+	匹配 1 个或多个模式出现的实例。
?	匹配 0 个或 1 个模式出现的实例。
^	匹配行首。
\$	匹配行尾。
-	此字符在 BGP 正则表达式中具有特殊含义。它与空格、逗号、AS 集合分隔符 { 和 } 和 AS 联合分隔符 (和) 匹配。它还与行首和行尾匹配。因此，可以使用该字符匹配 AS 值边界。此字符在技术上评估为 (^ [,{}() \$)。

以下是在路由映射中使用正则表达式的一些示例：

表达式	说明
^101	匹配具有以 101 开头的社区属性的路由。
^[0-9]+	匹配社区属性以 0-9 开头且具有一个或多个此类数字实例的路由。
。	匹配具有任何社区属性或没有社区属性的路由。
。	匹配具有任何社区属性值的路由。
^\$	匹配没有或具有 NULL 社区属性值的路由。

配置 BGP

为了使虚拟机与外界之间能够相互访问，您可以在 Tier-0 网关与物理基础架构中的路由器之间配置外部或内部 BGP (eBGP 或 iBGP) 连接。

在配置 BGP 时，您必须为 Tier-0 网关配置本地自治系统 (AS) 编号。您还必须配置远程 AS 编号。EBGP 邻居必须直接连接并与 Tier-0 上行链路位于同一子网中。如果它们不在同一子网中，那么应使用 BGP 多点跳跃。

BGPv6 受单跃点和多跃点支持。BGPv6 邻居仅支持 IPv6 地址。IPv6 前缀支持重新分发、前缀列表和路由映射。

在活动-活动模式下 Tier-0 网关支持 SR（服务路由器）间 iBGP。如果网关 #1 无法与北向物理路由器通信，则在活动-活动集群中流量将重新路由到网关 #2。如果网关 #2 能够与物理路由器通信，则网关 #1 和物理路由器之间的流量不受影响。

NSX Edge 上的 ECMP 实现基于协议号、源和目标地址以及源和目标端口的五元组。

iBGP 功能具有以下功能和限制：

- 支持重新分发、前缀列表和路由映射。
- 不支持路由反射器。
- 不支持 BGP 联盟。

步骤

1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。

2 选择**网络 > Tier-0 网关**。

3 要编辑 Tier-0 网关，请单击菜单图标（三个点），然后选择**编辑**。

4 单击 **BGP**。

a 输入本地 AS 编号。

在活动-活动模式下，已填写默认 ASN 值，即 65000。在活动-备用模式下，没有默认 ASN 值。

b 单击 **BGP** 开关以启用或禁用 BGP。

在活动-活动模式下，将默认启用 **BGP**。在活动-备用模式下，将默认禁用 **BGP**。

c 如果此网关处于活动-活动模式，则单击 **服务路由器间 iBGP** 开关以启用或禁用 SR 间 iBGP。默认情况下处于启用状态。

如果网关处于活动-备用模式，则此功能不可用。

d 单击 **ECMP** 切换按钮以启用或禁用 ECMP。

e 单击**多路径负载分担**切换按钮，以在仅 AS 路径属性值不同但具有相同的 AS 路径长度的多个路径中启用或禁用负载共享。

注 必须已启用 **ECMP**，才能使**多路径负载分担**起作用。

f 在**平滑重启**字段中，选择**禁用**、**仅帮助程序**或**平滑重启和帮助程序**。

您可以选择更改**平滑重启定时器**和**平滑重启失效定时器**。

默认情况下，平滑重启模式设置为**仅帮助程序**。要消除和/或减少与从能够平滑重启的邻居发现的路由关联的流量中断，帮助程序模式是非常有用的。该邻居必须能够在重新启动时保留其转发表。

建议不要在 Tier-0 网关上启用平滑重启功能，因为来自所有网关的 BGP 对等连接始终处于活动状态。在故障切换时，平滑重启功能将增加远程邻居选择备用 Tier-0 网关所花的时间。这会延迟基于 BFD 的聚合。

注意：除非被邻居特定的配置覆盖，否则，Tier-0 配置适用于所有 BGP 邻居。

5 通过添加 IP 地址前缀，配置**路由聚合**。

a 单击**添加前缀**。

b 使用 CIDR 格式输入一个 IP 地址前缀。

c 对于选项**仅汇总**，选择**是**或**否**。

6 单击保存。

必须先保存全局 BGP 配置，然后才能配置 BGP 邻居。

7 配置 BGP 邻居。

a 输入邻居的 IP 地址。

b 启用或禁用 BFD。

c 输入远程 AS 编号的值。

对于 iBGP，请输入与步骤 4a 相同的 AS 编号。对于 eBGP，请输入物理路由器的 AS 编号。

d 配置出站筛选器。

e 配置入站筛选器。

f 启用或禁用 Allowas-in 功能。

默认情况下禁用此功能。启用此功能时，BGP 邻居可以接收具有相同 AS 的路由，例如，使用同一服务提供商将两个位置互连时。此功能适用于所有地址系列，但不能应用于特定的地址系列。

g 在源地址字段中，您可以选择一个源地址，以便使用此特定源地址与邻居建立对等连接会话。如果您未选择任何源地址，则网关将自动选择一个源地址。

h 在 IP 地址系列字段中，选择 IPv4、IPv6 或已禁用。

i 输入最大跃点限制的值。

j 在平滑重启字段中，您可以选择禁用、仅帮助程序或平滑重启和帮助程序。

选项	说明
未选择任何选项	该邻居的平滑重启将采用 Tier-0 网关 BGP 配置。
禁用	<ul style="list-style-type: none"> ■ 如果为 Tier-0 网关 BGP 配置了禁用，将为该邻居禁用平滑重启。 ■ 如果为 Tier-0 网关 BGP 配置了仅帮助程序，将为该邻居禁用平滑重启。 ■ 如果为 Tier-0 网关 BGP 配置了平滑重启和帮助程序，将为该邻居禁用平滑重启。
仅帮助程序	<ul style="list-style-type: none"> ■ 如果为 Tier-0 网关 BGP 配置了禁用，该邻居的平滑重启将配置为“仅帮助程序”。 ■ 如果为 Tier-0 网关 BGP 配置了仅帮助程序，该邻居的平滑重启将配置为“仅帮助程序”。 ■ 如果为 Tier-0 网关 BGP 配置了平滑重启和帮助程序，该邻居的平滑重启将配置为“仅帮助程序”。
平滑重启和帮助程序	<ul style="list-style-type: none"> ■ 如果为 Tier-0 网关 BGP 配置了禁用，该邻居的平滑重启将配置为“平滑重启和帮助程序”。 ■ 如果为 Tier-0 网关 BGP 配置了仅帮助程序，该邻居的平滑重启将配置为“平滑重启和帮助程序”。 ■ 如果为 Tier-0 网关 BGP 配置了平滑重启和帮助程序，该邻居的平滑重启将配置为“平滑重启和帮助程序”。

k 单击定时器和密码。

l 输入 BFD 间隔的值。

单位为毫秒。对于在虚拟机中运行的 Edge 节点，最小值为 1000。对于裸机 Edge 节点，最小值为 300。

m 输入 BFD 倍数的值。

- n 输入抑制时间的值。
- o 输入保持活动状态时间的值。
- p 输入密码。

如果在 BGP 对等项之间配置 MD5 身份验证，则这是必需的。

8 单击保存。

配置 BFD

BFD（双向转发检测）是一种可以检测转发路径故障的协议。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**网络 > Tier-0 网关**。
- 3 要编辑 Tier-0 网关，请单击菜单图标（三个点），然后选择**编辑**。
- 4 单击**高级配置**。

此时将转到**高级网络和安全 > 路由器**页面。网关将显示为一个逻辑路由器。请按照在 [Tier-0 逻辑路由器上配置 BFD](#) 中的说明操作。

配置 IPv6 第 3 层转发

默认情况下，将启用 IPv4 第 3 层转发。您也可以配置 IPv6 第 3 层转发。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**网络 > Tier-0 网关**。
- 3 单击菜单图标（三个点）并选择**编辑**以编辑 Tier-0 网关。
- 4 单击**高级配置**。

此时将转到**高级网络和安全 > 路由器**页面。网关将显示为一个逻辑路由器。

- 5 单击**全局配置**选项卡。
- 6 在 **L3 转发模式**字段中，选择 **IPv4 和 IPv6**。

不支持仅选择 IPv6

- 7 转到**网络**选项卡，以再次编辑网关。
- 8 转到**其他设置**。

- a **内部转换子网**没有可配置的 IPv6 地址。系统自动使用 IPv6 链路本地地址。
- b 在 **TO-T1 转换子网**中输入一个 IPv6 子网。

9 转到**接口**，然后为 IPv6 添加一个接口。

创建用于 IPv6 地址分配的 SLAAC 和 DAD 配置文件

在逻辑路由器接口上使用 IPv6 时，您可以为 IP 地址分配设置无状态地址自动配置 (SLAAC)。SLAAC 允许根据通过路由器通告在本地网络路由器中通告的网络前缀对主机进行寻址。重复地址检测 (DAD) 可确保 IP 地址的唯一性。

前提条件

导航到**高级网络和安全 > 路由器 > 全局配置**，然后选择 **IPv4** 和 **IPv6** 作为 **L3 转发模式**

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**网络 > Tier-0 网关**。
- 3 要编辑 Tier-0 网关，请单击菜单图标（三个点），然后选择**编辑**。
- 4 单击**其他设置**。
- 5 要创建 **ND 配置文件**（SLAAC 配置文件），请单击菜单图标（三个点），然后选择**新建**。
 - a 输入配置文件的名称。
 - b 选择模式：
 - **已禁用** - 已禁用路由器通告消息。
 - **RA 通告 DNS 的 SLAAC 模式** - 使用路由器通告消息生成地址和 DNS 信息。
 - **DHCP 分配 DNS 的 SLAAC 模式** - 使用路由器通告消息生成地址，通过 DHCP 服务器生成 DNS 信息。
 - **DHCP 分配地址和 DNS 的 DHCP 模式** - 通过 DHCP 服务器生成地址和 DNS 信息。
 - **DHCP 分配地址和 DNS 的 SLAAC 模式** - 通过 DHCP 服务器生成地址和 DNS 信息。仅 NSX Edge 支持此选项，KVM 主机或 ESXi 主机都不支持此选项。
 - c 输入路由器通告消息的可访问时间和重新传输时间间隔。
 - d 输入域名并指定其生存期。仅在 **RA 通告 DNS 的 SLAAC 模式**这一模式下，输入这些值。

- e 输入 DNS 服务器并指定其生存期。仅在 **RA 通告 DNS 的 SLAAC 模式**这一模式下，输入这些值。
 - f 输入路由器通告的值：
 - **RA 间隔** - 传输连续路由器通告消息之间的时间间隔。
 - **跃点限制** - 通告的路由的生存期。
 - **路由器生存期** - 路由器的生存期。
 - **前缀生存期** - 前缀的生存期，以秒为单位。
 - **前缀首选时间** - 某个有效地址作为首选地址的时间。
- 6 要创建 **DAD 配置文件**，请单击菜单图标（三个点），然后选择**新建**。
- a 输入配置文件的名称。
 - b 选择模式：
 - **宽松** - 检测到重复地址后，收到了指示地址重复的通知，但未执行任何操作。
 - **严格** - 收到了指示地址重复的通知，且不再使用重复地址。
 - c 输入**等待时间 (秒)**，以指定各个 **NS** 数据包之间的时间间隔。
 - d 输入 **NS 重试次数**，以指定按**等待时间 (秒)**中定义的时间间隔检测重复地址时所需使用的 **NS** 数据包的数量

Tier-1 网关

3

Tier-1 网关执行 Tier-1 逻辑路由器的功能。它具有通往分段的下行链路连接和通往 Tier-0 网关的上行链路连接。

注 在**高级网络 and 安全性**选项卡上，使用 Tier-1 逻辑路由器一词来指示 Tier-1 网关。

您可以在 Tier-1 网关上配置路由通告和静态路由。支持递归静态路由。

本章讨论了以下主题：

- 添加 Tier-1 网关

添加 Tier-1 网关

Tier-1 网关通常在北向方向连接到 Tier-0 网关，在南向方向连接到分段。

对于单层和多层拓扑中的所有接口（上行链路、服务端口和下行链路），Tier-0 和 Tier-1 网关支持以下寻址配置：

- 仅 IPv4
- 仅 IPv6
- 双栈 - IPv4 和 IPv6

要使用 IPv6 或双栈寻址，请在**网络 > 网络设置 > 全局网络配置**中启用 **IPv4** 和 **IPv6** 以作为 L3 转发模式。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 选择**网络 > Tier-1 网关**。
- 3 单击**添加 Tier-1 网关**。
- 4 输入网关的名称。
- 5 （可选）选择一个 Tier-0 网关以连接到该 Tier-1 网关，以便创建一个多层拓扑。

6 选择一种故障切换模式。

选项	说明
主动	如果首选 NSX Edge 节点发生故障并恢复，它将取代对等节点并变为活动节点。对等节点将其状态更改为备用。
非主动	如果首选 NSX Edge 节点发生故障并恢复，它将检查对等节点是否为活动节点。如果是，首选节点不会取代对等节点并作为备用节点。这是默认选项。

7 （可选）如果您希望该 Tier-1 网关托管有状态服务（NAT、负载均衡器、防火墙），请选择一个 NSX Edge 集群。

如果选择了 NSX Edge 集群，则会始终创建一个服务路由器（即使未配置有状态服务），从而影响南北向流量模式。

8 （可选）选择 NSX Edge 节点。

9 （可选）单击**启用备用重新放置**切换开关以启用或禁用备用重新放置。

备用重新放置意味着，如果运行活动或备用逻辑路由器的 Edge 节点发生故障，则会在另一个 Edge 节点上创建新的备用逻辑路由器以保持高可用性。如果发生故障的 Edge 节点正在运行活动逻辑路由器，原始备用逻辑路由器将变为活动逻辑路由器，并创建新的备用逻辑路由器。如果发生故障的 Edge 节点正在运行备用逻辑路由器，新的备用逻辑路由器将替换该路由器。

10 单击**保存**。

11 （可选）单击**路由通告**。

选择一个或多个以下选项：

- 所有静态路由
- 所有 NAT IP
- 所有 DNS 转发器路由
- 所有 LB VIP 路由
- 所有已连接分段和服务端口
- 所有 LB SNAT IP 路由
- 所有 IPsec 本地端点

在**设置路由通告规则**字段中，单击**设置**以添加路由通告规则。

12 （可选）单击**服务接口**和**设置**以配置与分段的连接。需要在某些拓扑中执行该步骤，例如 VLAN 支持的分段或单臂负载均衡。

- a 单击**添加接口**。
- b 以 CIDR 格式输入名称和 IP 地址。
- c 选择分段。
- d 在 **MTU** 字段中，输入一个介于 64 和 9000 之间的值。

e 在 **ND 配置文件** 字段中，选择一个配置文件。

f 单击 **保存**。

13 （可选）单击 **静态路由** 和 **设置** 以配置静态路由。

a 单击 **添加静态路由**。

b 使用 CIDR 或 IPv6 CIDR 格式输入一个名称和网络地址。

c 单击 **设置下一跃点** 以添加下一跃点信息。

d 单击 **保存**。

分段执行逻辑交换机的功能。

注 在**高级网络 and 安全性**选项卡上，使用逻辑交换机一词来指示分段。

本章讨论了以下主题：

- 分段配置文件
- 添加分段

分段配置文件

分段配置文件包括分段和分段端口的第 2 层网络连接配置详细信息。NSX Manager 支持多种类型的分段配置文件。

可以使用以下类型的分段配置文件。

- QoS（服务质量）
- IP 发现
- SpoofGuard
- 分段安全
- MAC 管理

注 不能编辑或删除默认分段配置文件。如果您需要默认分段配置文件中设置的替代设置，则可以创建一个自定义分段配置文件。默认情况下，除分段安全配置文件之外的其他所有自定义分段配置文件都将继承相应默认分段配置文件的设置。例如，默认情况下，自定义 IP 发现分段配置文件将具有与默认 IP 发现分段配置文件相同的设置。

每个默认或自定义的分段配置文件都具有唯一标识符。可以使用此标识符将分段配置文件与分段或分段端口相关联。

分段或分段端口只能与每种类型的一个分段配置文件相关联。例如，不能将两个 QoS 分段配置文件与一个分段或分段端口相关联。

如果创建分段时未关联分段配置文件，则 NSX Manager 将关联对应的系统定义的默认分段配置文件。子分段端口从父分段中继承系统定义的默认分段配置文件。

创建或更新分段或分段端口时，可以选择关联默认或自定义的分段配置文件。如果将分段配置文件与分段关联或解除关联，将根据以下条件应用于子分段端口的分段配置文件。

- 如果父分段具有关联的配置文件，子分段端口将从父分段中继承分段配置文件。
- 如果父分段没有关联的分段配置文件，则为该分段分配默认分段配置文件，并且该分段端口继承该默认分段配置文件。
- 如果显式地将自定义配置文件与一个分段端口相关联，则此自定义的配置文件覆盖现有的分段配置文件。

注 如果已将自定义的分段配置文件与一个分段相关联，但希望保留某个子分段端口的默认分段配置文件，您必须创建一个默认分段配置文件副本并将其与特定分段端口相关联。

如果将自定义分段配置文件与一个分段或分段端口相关联，则无法删除该配置文件。您可以转到“摘要”视图的“分配给”部分并单击列出的分段和分段端口，以确定任何分段和分段端口是否与自定义分段配置文件相关联。

了解 QoS 分段配置文件

QoS 为需要高带宽的首选流量提供高质量和专用网络性能。QoS 机制确定分配足够带宽的优先顺序，控制延迟和抖动以及甚至在发生网络拥塞时减少首选数据包的数据丢失，从而实现该目的。该级别的网络服务是有效地使用现有的网络资源提供的。

对于该版本，支持调整和流量标记，即 CoS 和 DSCP。在由于拥塞而在分段中缓冲流量时，第 2 层服务等级 (Class of Service, CoS) 允许您指定数据包的优先级。第 3 层差分服务代码点 (Differentiated Services Code Point, DSCP) 根据 DSCP 值检测数据包。CoS 始终应用于数据包，而不考虑受信任模式。

NSX-T Data Center 信任虚拟机应用的 DSCP 设置，或者在分段级别修改和设置 DSCP 值。在每种情况下，DSCP 值都将传播到封装帧的外部 IP 标头。这样，外部物理网络就可以根据外部标头上的 DSCP 设置优先处理流量。在 DSCP 处于受信任模式时，将从内部标头中复制 DSCP 值。在处于不受信任模式时，不会保留内部标头的 DSCP 值。

注 DSCP 设置仅适用于隧道流量。这些设置不适用于同一 Hypervisor 中的流量。

您可以使用 QoS 交换配置文件配置平均输入和输出带宽值以设置传输限制速率。峰值带宽速率用于支持允许分段的突发流量，以防止在北向网络链路上发生拥塞。这些设置并不能保证带宽，但有助于限制使用网络带宽。您将观察到的实际带宽取决于端口的链路速度或交换配置文件中的值（以较低者为准）。

QoS 交换配置文件设置将应用于分段，并且子分段端口将继承这些设置。

创建 QoS 分段配置文件

您可以定义 DSCP 值并配置输入和输出设置以创建自定义 QoS 交换配置文件。

前提条件

- 熟悉 QoS 交换配置文件概念。请参见[了解 QoS 交换配置文件](#)。
- 确定要优先处理的网络流量。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 选择 **网络 > 分段 > 分段配置文件**。
- 3 单击 **添加分段配置文件** 并选择 **QoS**。
- 4 填写 QoS 交换配置文件详细信息。

选项	说明
名称	配置文件的名称。
模式	<p>从“模式”下拉菜单中选择 受信任 或 不受信任 选项。</p> <p>在选择“受信任”模式时，内部标头 DSCP 值将应用于 IP/IPv6 流量的外部 IP 标头。对于非 IP/IPv6 流量，外部 IP 标头使用默认值。在基于覆盖网络的逻辑端口上支持“受信任”模式。默认值为 0。</p> <p>在基于覆盖网络和基于 VLAN 的逻辑端口上支持“不受信任”模式。对于基于覆盖网络的逻辑端口，出站 IP 标头的 DSCP 值设置为配置的值，而不考虑逻辑端口的内部数据包类型。对于基于 VLAN 的逻辑端口，IP/IPv6 数据包的 DSCP 值设置为配置的值。“不受信任”模式的 DSCP 值范围是 0 到 63 之间。</p> <p>注 DSCP 设置仅适用于隧道流量。这些设置不适用于同一 Hypervisor 中的流量。</p>
优先级	<p>设置 CoS 优先级值。</p> <p>优先级值范围是 0 到 63，其中 0 具有最高优先级。</p>
服务类别	<p>设置 CoS 值。</p> <p>在基于 VLAN 的逻辑端口上支持 CoS。CoS 将网络中具有类似类型的流量划分到一起，并将每种类型的流量视为具有自己的服务优先级的等级。将减慢较低优先级的流量，或者在某些情况下，丢弃这些流量，以便为较高优先级的流量提供更好的吞吐量。也可以为具有零个数据包的 VLAN ID 配置 CoS。</p> <p>CoS 值范围是 0 到 7，其中 0 是最佳效果服务。</p>
输入	<p>为从虚拟机到逻辑网络的出站网络流量设置自定义值。</p> <p>您可以使用平均带宽以减少网络拥塞。峰值带宽速率用于支持突发流量，并且突发大小基于峰值带宽的持续时间。您可以在突发大小设置中设置突发持续时间。您不能保证带宽。不过，您可以使用“平均值”、“峰值”和“突发大小”设置以限制网络带宽。</p> <p>例如，如果平均带宽为 30 Mbps，峰值带宽为 60 Mbps，允许的持续时间为 0.1 秒，则突发大小为 $60 * 1000000 * 0.10/8 = 750000$ 字节。</p> <p>默认值 0 在输入流量上禁用速率限制。</p>
输入广播	<p>为从虚拟机到逻辑网络的基于广播的出站网络流量设置自定义值。</p> <p>例如，如果将逻辑交换机的平均带宽设置为 3000 Kbps，峰值带宽为 6000 Kbps，允许的持续时间为 0.1 秒，则突发大小为 $6000 * 1000 * 0.10/8 = 75000$ 字节。</p> <p>默认值 0 在输入广播流量上禁用速率限制。</p>
输出	<p>为从逻辑网络到虚拟机的入站网络流量设置自定义值。</p> <p>默认值 0 在输出流量上禁用速率限制。</p>

如果未配置输入、输入广播和输出选项，则使用默认值。

- 5 单击 **保存**。

了解 IP 发现分段配置文件

IP 发现使用 DHCP 和 DHCPv6 侦听、地址解析协议 (Address Resolution Protocol, ARP) 侦听、邻居发现 (Neighbor Discovery, ND) 侦听和 VMware Tools 来发现 MAC 和 IP 地址。

注 IPv6 的 IP 发现方法在默认 IP 发现分段配置文件中处于禁用状态。要为分段启用 IPv6 的 IP 发现，必须创建一个启用了 IPv6 选项的 IP 发现配置文件，并将该配置文件连接到分段。此外，请确保分布式防火墙允许所有工作负载之间的 IPv6 邻居发现数据包（默认情况下允许）。

已发现的 MAC 和 IP 地址用于实现 ARP/ND 抑制，以最大限度地减少连接到同一分段的虚拟机之间的流量。这些地址也供 SpoofGuard 和分布式防火墙 (DFW) 组件使用。DFW 使用地址绑定来确定防火墙规则中的对象的 IP 地址。

DHCP/DHCPv6 侦听检查在 DHCP/DHCPv6 客户端和服务器之间交换的 DHCP/DHCPv6 数据包以发现 IP 和 MAC 地址。

ARP 侦听检查虚拟机的出站 ARP 和 GARP（免费 ARP）数据包以发现 IP 和 MAC 地址。

VMware Tools 是一个在 ESXi 托管的虚拟机上运行的软件，可以提供该虚拟机的配置信息，包括 MAC 和 IP 或 IPv6 地址。该 IP 发现方法仅适用于在 ESXi 主机上运行的虚拟机。

ND 侦听相当于 IPv6 的 ARP 侦听。它会检查邻居请求 (NS) 和邻居通告 (NA) 消息，以发现 IP 和 MAC 地址。

重复地址检测会检查新发现的 IP 地址是否已存在于不同端口的已实现绑定列表中。对同一分段上的端口执行此检查。如果检测到重复地址，则新发现的地址会添加到已发现列表中，而不会将其添加到已实现绑定列表中。所有重复 IP 都有关联的发现时间戳。如果通过将已实现绑定列表上的 IP 添加到忽略绑定列表或者禁用侦听移除该 IP，那么会将具有最早时间戳的重复 IP 移动到已实现绑定列表。通过 API 调用可获得重复地址信息。

默认情况下，发现方法 ARP 侦听和 ND 侦听在“首次使用时信任 (Trust on First Use, TOFU)”模式下运行。在 TOFU 模式中，当发现一个地址并将其添加到已实现绑定列表中时，该绑定将永久保留在已实现列表中。TOFU 会应用到使用 ARP/ND 侦听发现的前“n”个唯一 <IP, MAC, VLAN> 绑定，其中“n”是您可以配置的绑定限制。对于 ARP/ND 侦听，您可以禁用 TOFU。然后，这些方法将在“每次使用时信任” (Trust On Every Use, TOEU) 模式下运行。在 TOEU 模式下，如果发现一个地址，则会将该地址添加到已实现绑定列表中，当该地址被删除或过期时，将从已实现的绑定列表中将其移除。DHCP 侦听和 VM Tools 始终在 TOEU 模式下运行。

注 TOFU 与 SpoofGuard 不同，它不会以与 SpoofGuard 相同的方式来阻止流量。有关详细信息，请参见 [了解 SpoofGuard 分段配置文件](#)。

对于 Linux 虚拟机，ARP 不稳定问题可能会导致 ARP 侦听获取不正确的信息。可以使用 ARP 筛选器防止该问题。有关详细信息，请参见 <http://linux-ip.net/html/ether-arp.html#ether-arp-flux>。

对于每个端口，NSX Manager 都会维护一个忽略绑定列表，其中包含无法绑定到该端口的 IP 地址。通过导航到 **高级网络和安全 > 交换 > 端口** 并选择一个端口，您可以将发现的绑定添加到忽略绑定列表。您也可以通过将现有已发现或已实现绑定复制到 **忽略绑定** 来删除这些绑定。

创建 IP 发现分段配置文件

NSX-T Data Center 有多个默认的 IP 发现交换配置文件。也可以创建更多的配置文件。

前提条件

熟悉 IP 发现交换配置文件概念。请参见[了解 IP 发现交换配置文件](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 选择 **网络 > 分段 > 分段配置文件**。
- 3 单击 **添加分段配置文件** 并选择 **IP 发现**。
- 4 指定 IP 发现交换配置文件详细信息。

选项	说明
名称	输入名称。
ARP 侦听	适用于 IPv4 环境。虚拟机具有静态 IP 地址时适用。
ARP 绑定限制	可以绑定到一个端口的最大 IPv4 IP 地址数量。允许的最小值为 1（默认值），最大值为 256。
ARP ND 绑定限制超时	如果禁用 TOFU，ARP/ND 绑定表中 IP 地址的超时值（以分钟为单位）。如果某地址超时，新发现的地址将取代该地址。
DHCP 侦听	适用于 IPv4 环境。虚拟机具有 IPv4 地址时适用。
DHCP V6 侦听	适用于 IPv6 环境。虚拟机具有 IPv6 地址时适用。
VM Tools	仅适用于 ESXi 托管的虚拟机。
VM Tools (IPv6)	仅适用于 ESXi 托管的虚拟机。
邻居发现侦听	适用于 IPv6 环境。虚拟机具有静态 IP 地址时适用。
邻居发现绑定限制	可以绑定到一个端口的最大 IPv6 地址数量。
首次使用时信任	适用于 ARP 和 ND 侦听。
重复的 IP 检测	适用于所有侦听方法以及 IPv4 和 IPv6 环境。

- 5 单击 **保存**。

了解 SpoofGuard 分段配置文件

SpoofGuard 有助于防止一种称为“网络欺骗”或“网络钓鱼”的恶意攻击。SpoofGuard 策略阻止确定为欺骗的流量。

SpoofGuard 工具旨在防止您的环境中的虚拟机发送某种流量，该流量带有未经授权终止流量的 IP 地址。如果虚拟机的 IP 地址与 SpoofGuard 上的相应逻辑端口和分段地址绑定中的 IP 地址不匹配，将完全禁止虚拟机的 vNIC 访问网络。可以在端口或分段级别配置 SpoofGuard。在您的环境中使用 SpoofGuard 可能有以下几个原因：

- 防止恶意虚拟机使用现有虚拟机的 IP 地址。
- 确保无法在没有干预的情况下更改虚拟机的 IP 地址 - 在某些环境中，在没有正确的更改控制检查的情况下，最好禁止虚拟机更改其 IP 地址。SpoofGuard 确保虚拟机所有者无法直接更改 IP 地址并继续工作而不会受到妨碍，从而简化了该过程。
- 保证不会无意（或有意）绕过分布式防火墙 (Distributed Firewall, DFW) 规则 - 对于将 IP 集作为源或目标创建的 DFW 规则，始终存在虚拟机可能在数据包标头中伪造其 IP 地址的可能性，从而绕过相关的规则。

NSX-T Data Center SpoofGuard 配置包括以下内容：

- MAC SpoofGuard - 验证数据包的 MAC 地址。
- IP SpoofGuard - 验证数据包的 IP 地址。
- 动态地址解析协议 (Dynamic Address Resolution Protocol, ARP) 检查（即，ARP）以及无故地址解析协议 (Gratuitous Address Resolution Protocol, GARP) SpoofGuard 和邻居发现 (Neighbor Discovery, ND) SpoofGuard 验证针对的都是 ARP/GARP/ND 负载中的 MAC 源、IP 源和 IP-MAC 源映射。

在端口级别，允许的 MAC/VLAN/IP 白名单是通过端口的地址绑定属性提供的。在虚拟机发送流量时，如果流量的 IP/MAC/VLAN 与端口的 IP/MAC/VLAN 属性不匹配，则会丢弃该流量。端口级别 SpoofGuard 处理流量验证，即，流量与 VIF 配置是否一致。

在分段级别，允许的 MAC/VLAN/IP 白名单是通过分段的地址绑定属性提供的。这通常是分段的允许的 IP 范围/子网，分段级别 SpoofGuard 处理流量授权。

端口级别和分段级别 SpoofGuard 必须允许流量，然后才允许流量进入分段。可以使用 SpoofGuard 分段配置文件控制启用或禁用端口和分段级别 SpoofGuard。

创建 SpoofGuard 分段配置文件

在配置 SpoofGuard 时，如果某个虚拟机的 IP 地址发生变化，可能会阻止来自该虚拟机的流量，直到将配置的相应端口/分段地址绑定更新为新 IP 地址。

为包含客户机的端口组启用 SpoofGuard。如果为每个网络适配器启用 SpoofGuard，它将检查数据包以查找指定的 MAC 及其相应的 IP 地址。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。

- 2 选择**网络 > 分段 > 分段配置文件**。
- 3 单击**添加分段配置文件**并选择 **SpoofGuard**。
- 4 输入名称。
- 5 要启用端口级别的 SpoofGuard，请将**端口绑定**设置为已启用。
- 6 单击**保存**。

了解分段安全分段配置文件

分段安全通过以下方法提供无状态第 2 层和第 3 层安全性：检查分段的输入流量，并将 IP 地址、MAC 地址和协议与一组允许的地址和协议进行匹配以丢弃从虚拟机发送的未经授权的数据包。您可以使用分段安全筛选掉来自网络中的虚拟机的恶意攻击以保护分段完整性。

请注意，默认分段安全配置文件启用了 DHCP 设置 Server Block 和 Server Block - IPv6。这意味着，使用默认分段安全配置文件的分段将阻止从 DHCP 服务器到 DHCP 客户端的流量。如果希望分段允许 DHCP 服务器流量，您必须为该分段创建自定义分段安全配置文件。

创建分段安全分段配置文件

您可以使用允许的 BPDU 列表中的 MAC 目标地址创建自定义分段安全分段配置文件并配置速率限制。

前提条件

熟悉分段安全分段配置文件概念。请参见[了解交换机安全交换配置文件](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**网络 > 分段 > 分段配置文件**。
- 3 单击**添加分段配置文件**，然后选择**分段安全**。
- 4 填写分段安全配置文件详细信息。

选项	说明
名称	配置文件的名称。
BPDU 筛选器	切换 BPDU 筛选器 按钮以启用 BPDU 筛选。默认情况下，将禁用该按钮。 如果启用了 BPDU 筛选器，将阻止到 BPDU 目标 MAC 地址的所有流量。如果启用，BPDU 筛选器还会在逻辑交换机端口上禁用 STP，因为这些端口应该不会加入 STP。
BPDU 筛选器允许列表	单击 BPDU 目标 MAC 地址列表中的目标 MAC 地址以允许将流量传输到允许的目标。您必须启用 BPDU 筛选器 才能从该列表中进行选择。
DHCP 筛选器	切换 服务器阻止 按钮和 客户端阻止 按钮以启用 DHCP 筛选。默认情况下，将禁用这两个按钮。 “DHCP 服务器阻止”阻止从 DHCP 服务器到 DHCP 客户端的流量。请注意，它不会阻止从 DHCP 服务器到 DHCP 中继代理的流量。 “DHCP 客户端阻止”阻止 DHCP 请求以禁止虚拟机获取 DHCP IP 地址。

选项	说明
DHCPv6 筛选器	<p>切换服务器阻止 - IPv6按钮和客户端阻止 - IPv6按钮以启用 DHCP 筛选。默认情况下，将禁用这两个按钮。</p> <p>“DHCPv6 服务器阻止”可阻止从 DHCPv6 服务器到 DHCPv6 客户端的流量。请注意，它不会阻止从 DHCP 服务器到 DHCP 中继代理的流量。筛选出 UDP 源端口号为 547 的数据包。</p> <p>“DHCPv6 客户端阻止”会阻止 DHCP 请求以禁止虚拟机获取 DHCP IP 地址。筛选出 UDP 源端口号为 546 的数据包。</p>
阻止非 IP 流量	<p>切换阻止非 IP 流量按钮以仅允许 IPv4、IPv6、ARP、GARP 和 BPDU 流量。</p> <p>将阻止其余非 IP 流量。允许的 IPv4、IPv6、ARP、GARP 和 BPDU 流量基于在地址绑定和 SpoofGuard 配置中设置的其他策略。</p> <p>默认情况下，将禁用该选项以允许将非 IP 流量作为常规流量进行处理。</p>
RA 防护	<p>切换RA 防护按钮以筛选出输入 IPv6 路由器通告。筛选出 ICMPv6 类型的 134 个数据包。默认情况下，将启用该选项。</p>
速率限制	<p>设置广播和多播流量的速率限制。默认情况下，将启用该选项。</p> <p>可以使用速率限制保护逻辑交换机或虚拟机，以免受到广播风暴等事件的影响。</p> <p>为了避免任何连接问题，最小速率限制值必须大于或等于 10 pps。</p>

5 单击保存。

了解 MAC 发现分段配置文件

MAC 管理分段配置文件支持两种功能：MAC 发现和 MAC 地址更改。

MAC 地址更改功能允许虚拟机更改其 MAC 地址。连接到端口的虚拟机可以运行管理命令以更改其 vNIC 的 MAC 地址，并仍然在该 vNIC 上发送和接收流量。仅在 ESXi 上支持该功能，而在 KVM 上不支持。默认情况下，将禁用该属性。

MAC 发现提供到在一个 vNIC 后面配置多个 MAC 地址的部署的网络连接，例如，在嵌套管理程序部署中，ESXi 虚拟机在 ESXi 主机上运行，并且多个虚拟机在 ESXi 虚拟机中运行。如果未使用 MAC 发现，在 ESXi 虚拟机的 vNIC 连接到分段端口时，其 MAC 地址是静态的。在 ESXi 虚拟机中运行的虚拟机没有网络连接，因为其数据包具有不同的源 MAC 地址。通过使用 MAC 发现，vSwitch 检查来自 vNIC 的每个数据包的源 MAC 地址，发现 MAC 地址并允许数据包通过。如果在特定时间段内未使用发现的 MAC 地址，则会将其移除。无法配置此时间段。**MAC 学习老化时间**字段会显示预定义的值，即 600。

MAC 学习还支持未知单播泛洪。通常，在端口收到的数据包具有未知目标 MAC 地址时，将丢弃该数据包。在启用未知单播泛洪的情况下，端口将未知单播流量泛洪到交换机上启用了 MAC 学习和未知单播泛洪的每个端口。默认情况下，将启用该属性，但只有在启用 MAC 发现时才启用。

可以配置可学习 MAC 地址的数量。最大值为 4096，这是默认值。您还可以设置达到限制设置时实施的策略。选项包括：

- **丢弃** - 来自未知源 MAC 地址的数据包被丢弃。此 MAC 地址的入站数据包将被视为未知单播。仅当端口启用了未知单播泛洪时，端口才会接收数据包。
- **允许** - 尽管不会学习该地址，但会转发来自未知源 MAC 地址的数据包。此 MAC 地址的入站数据包将被视为未知单播。仅当端口启用了未知单播泛洪时，端口才会接收数据包。

如果启用 MAC 发现或 MAC 地址更改以提高安全性，还要配置 SpoofGuard。

创建 MAC 发现分段配置文件

您可以创建 MAC 发现分段配置文件以管理 MAC 地址。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择 **网络 > 分段 > 分段配置文件**。
- 3 单击 **添加分段配置文件**，然后选择 **MAC 发现**。
- 4 填写 MAC 发现配置文件详细信息。

选项	说明
名称	配置文件的名称。
MAC 更改	启用或禁用 MAC 地址更改功能。默认禁用该功能。
MAC 学习	启用或禁用 MAC 学习功能。默认禁用该功能。
MAC 限制策略	选择 允许 或 丢弃 。默认操作为 允许 。此选项在启用 MAC 学习时可用
未知的单播泛洪	启用或禁用未知的单播泛洪功能。默认启用该功能。此选项在启用 MAC 学习时可用
MAC 限制	设置 MAC 地址的最大数量。默认值为 4096。此选项在启用 MAC 学习时可用
MAC 学习老化时间	仅供参考。无法配置该选项。预定义值为 600。

- 5 单击 **保存**。

添加分段

分段连接到网关和虚拟机。分段执行逻辑交换机的功能。

有关如何查找虚拟机的 VIF ID 的信息，请参见 [将虚拟机连接到逻辑交换机](#)。

注 配置为增强型数据路径模式的 N-VDS 交换机支持 IP 发现、SpoofGuard 和 IPFIX 配置文件。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择 **网络 > 分段**。
- 3 单击 **添加分段**。
- 4 输入分段的名称。
- 5 选择一个已连接的网关。

可以选择现有的 Tier-0 或 Tier-1 网关，也可以选择 **无**。默认值为 **无**，这意味着分段只是一个逻辑交换机。配置子网后，它可以链接到 Tier-0 或 Tier-1 网关。

- 6 如果已连接的网关为 Tier-1 网关，请选择类型：**灵活** 或 **固定**。

灵活的分段可取消与网关的链接。固定的分段可以删除，但不能取消与网关的链接。

- 7 要指定子网，请单击**设置子网**。
- 8 选择一个传输区域，可以是覆盖网络或 VLAN。
- 9 如果传输区域的类型为 VLAN，请指定 VLAN ID 列表。
- 10 如果要使用第 2 层 VPN 扩展分段，请单击 **L2 VPN** 文本框，然后选择 L2 VPN 服务器或客户端会话。

您可以选择多个会话。

- 11 在 **VPN 隧道 ID** 中，输入用于标识分段的唯一值。
- 12 单击**保存**。
- 13 要添加分段端口，请在系统提示您是否要继续配置分段时，单击**是**。

- a 依次单击**端口**和**设置**。
- b 单击**添加分段端口**。
- c 输入端口名称。
- d 对于 **ID**，输入连接到此端口的虚拟机或服务器的 VIF UUID。
- e 选择类型：**父项**、**子项**或**独立**。

将此文本框留空，但容器或 VMware HCX 等用例除外。如果此端口用于虚拟机中的容器，请选择**子项**。如果此端口用于容器主机虚拟机，请选择**父项**。如果此端口用于裸机容器或服务器，请选择**独立**。

- f 输入上下文 ID。

如果**类型**为**子项**，请输入父 VIF ID；如果**类型**为**独立**，请输入传输节点 ID。

- g 输入流量标记。

在容器和其他用例中输入 VLAN ID。

- h 选择地址分配方法：**IP 池**、**MAC 池**、**二者或无**。

- i 指定标记。

- j 通过指定要将地址绑定应用到的逻辑端口的 IP（IPv4 地址、IPv6 地址或 IPv6 子网）和 MAC 地址来应用地址绑定。例如，对于 IPv6，2001::/64 是 IPv6 子网，2001::1 是主机 IP，而 2001::1/64 则是无效输入。还可以指定 VLAN ID。

手动地址绑定（如已指定）将覆盖自动发现的地址绑定。

- k 为此端口选择分段配置文件。

- 14 要选择分段配置文件，请单击**分段配置文件**。

- 15 单击**保存**。

虚拟专用网络 (VPN)

5

NSX-T Data Center 在 NSX Edge 节点上支持 IPsec 虚拟专用网络 (IPsec VPN) 和第 2 层 VPN (L2 VPN)。IPsec VPN 在 NSX Edge 节点和远程站点之间提供站点到站点连接。借助 L2 VPN，可以使虚拟机在使用相同 IP 地址的同时跨地域界限保持其网络连接，从而扩展数据中心。

注 IPsec VPN 和 L2 VPN 在 NSX-T Data Center Limited Export 版本中不受支持。

您必须具有一个正常工作的 NSX Edge 节点（配置了至少一个 Tier-0 或 Tier-1 网关），然后才能配置 VPN 服务。有关详细信息，请参见《NSX-T Data Center 安装指南》中的“NSX Edge 安装”。

从 NSX-T Data Center 2.4 开始，还可以使用 NSX Manager 用户界面配置新的 VPN 服务。在早期版本的 NSX-T Data Center 中，您只能使用 REST API 调用配置 VPN 服务。

重要事项 使用 NSX-T Data Center 2.4 或更高版本配置 VPN 服务时，必须使用通过 NSX-T Data Center 2.4 或更高版本随附的 NSX Manager UI 或策略 API 创建的新对象（如 Tier-0 网关）。要使用通过 NSX-T Data Center 2.4 之前的版本配置的现有 Tier-0 或 Tier-1 逻辑路由器，您必须继续使用 API 调用配置 VPN 服务。

带有预定义值和设置的系统默认配置文件可在 VPN 服务配置期间供您使用。此外，也可以使用不同的设置定义新的配置文件，并在 VPN 服务配置期间选择这些配置文件。

本章讨论了以下主题：

- 了解 IPsec VPN
- 了解第 2 层 VPN
- 添加 VPN 服务
- 添加 IPsec VPN 会话
- 添加 L2 VPN 会话
- 添加本地端点
- 添加配置文件
- 将自治 Edge 添加为 L2 VPN 客户端
- 检查 IPsec VPN 会话的已实现状态
- 监控 VPN 会话和排除其故障

了解 IPsec VPN

Internet 协议安全性 (IPsec) VPN 可以保护经 IPsec 网关（称为端点）在通过公共网络连接的两个网络之间流动的流量。NSX Edge 仅支持隧道模式，该模式将 IP 隧道与封装安全负载 (Encapsulating Security Payload, ESP) 结合使用。ESP 使用 IP 协议号 50 直接在 IP 顶层运行。

IPsec VPN 使用 IKE 协议来协商安全参数。默认 UDP 端口设置为 500。如果在网关中检测到 NAT，则该端口设置为 UDP 4500。

NSX Edge 支持基于策略或基于路由的 IPsec VPN。

支持在 Tier-0 网关上应用 IPsec VPN 服务，且网关必须处于 Active-Standby 高可用性模式。请参见[添加 Tier-0 网关](#)，了解相关信息。从 NSX-T Data Center 2.5 开始，在 Tier-1 网关上也支持 IPsec VPN。可以使用在配置 IPsec VPN 服务时连接到 Tier-0 或 Tier-1 网关的分段。

NSX-T Data Center 中的 IPsec VPN 服务使用网关级别的故障切换功能，以支持高可用性服务。故障切换时将重新建立隧道并同步 VPN 配置数据。重新建立隧道时不同步 IPsec VPN 状态。

在 NSX Edge 节点和远程 VPN 站点之间支持预共享密钥模式身份验证和 IP 单播流量。此外，从 NSX-T Data Center 2.4 开始，还支持证书身份验证。仅支持通过以下签名哈希算法之一签名的证书类型。

- SHA256withRSA
- SHA384withRSA
- SHA512withRSA

使用基于策略的 IPsec VPN

基于策略的 IPsec VPN 要求将 VPN 策略应用到数据包，以确定哪些流量将受到 IPsec 的保护，然后通过 VPN 隧道。

这种类型的 VPN 视为静态的，因为当本地网络拓扑和配置更改时，还必须更新 VPN 策略设置以适应更改。

在将基于策略的 IPsec VPN 与 NSX-T Data Center 一起使用时，您可以使用 IPsec 隧道将 NSX Edge 节点后面的一个或多个本地子网连接到远程 VPN 站点上的对等子网。

您可以在 NAT 设备后面部署 NSX Edge 节点。在该部署中，NAT 设备将 NSX Edge 节点的 VPN 地址转换为面向 Internet 的公开访问地址。远程 VPN 站点使用该公共地址访问 NSX Edge 节点。

您也可以将远程 VPN 站点置于 NAT 设备的后面。您必须提供远程 VPN 站点的公用 IP 地址及其 ID（FQDN 或 IP 地址）才能设置 IPsec 隧道。在通道两端，VPN 地址需要静态一对一 NAT。

注 配置了基于策略的 IPsec VPN 的 Tier-1 网关上不支持 DNAT。

NSX Edge 节点大小决定了支持的最大隧道数，如下表中所示。

表 5-1. 支持的 IPsec 隧道数量

Edge 节点大小	每个 VPN 会话的 IPsec 隧道数量（基于策略）	每个 VPN 服务的会话数量	每个 VPN 服务的 IPsec 隧道数量（每个会话 16 个隧道）
小型	不适用（仅 POC/Lab）	不适用（仅 POC/Lab）	不适用（仅 POC/Lab）
中等	128	128	2048
大型	128（软限制）	256	4096
裸机	128（软限制）	512	6000

限制 基于策略的 IPsec VPN 的内在架构会限制您设置 VPN 隧道冗余。

有关配置基于策略的 IPsec VPN 的信息，请参见[添加 IPsec VPN 服务](#)。

使用基于路由的 IPsec VPN

基于路由的 IPsec VPN 根据静态路由或通过特殊接口（称为虚拟隧道接口 (VTI)）使用 BGP 等协议动态发现的路由提供流量隧道。IPsec 会保护流经 VTI 的所有流量。

注

- 通过 IPsec VPN 隧道进行路由时不支持 OSPF 动态路由。
- 在基于 Tier-1 网关的 VPN 上不支持 VTI 动态路由。

基于路由的 IPsec VPN 类似于通过 IPsec 的常规路由封装 (Generic Routing Encapsulation, GRE)，区别在于应用 IPsec 处理之前不会向数据包添加额外的封装。

在该 VPN 隧道方法中，将在 NSX Edge 节点上创建 VTI。每个 VTI 都与一个 IPsec 隧道相关联。加密流量通过 VTI 接口从一个站点路由到另一个站点。IPsec 处理仅在 VTI 进行。

VPN 隧道冗余

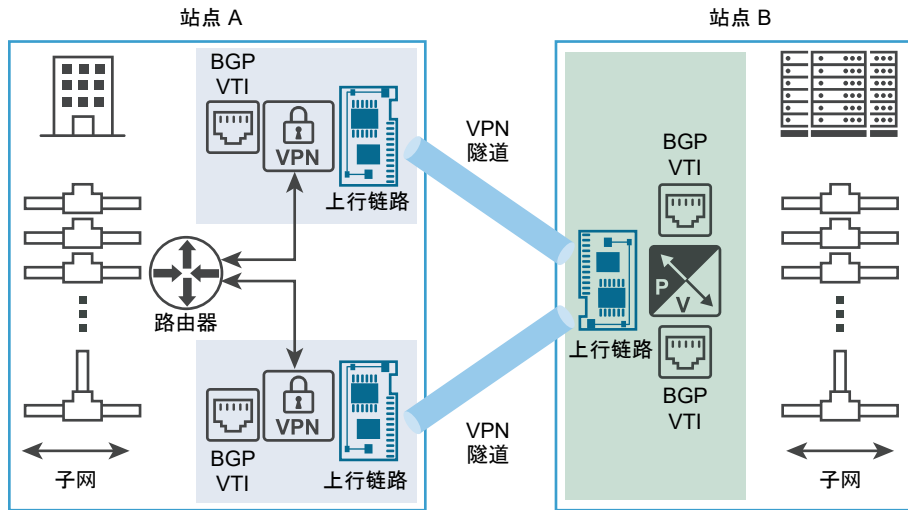
您可以使用在 Tier-0 网关上配置的基于路由的 IPsec VPN 会话配置 VPN 隧道冗余。通过使用隧道冗余，可以在两个站点之间设置多个隧道，将一个隧道作为主隧道并在主隧道变得不可用时故障切换到其他隧道。在站点具有多个连接选项（例如，连接到不同的 ISP 以提供链路冗余）时，该功能是非常有用的。

重要事项

- 在 NSX-T Data Center 中，仅支持通过 BGP 提供 IPsec VPN 隧道冗余。
- 在基于路由的 IPsec VPN 隧道中，请勿使用静态路由来实现 VPN 隧道冗余。

下图显示了两个站点之间的 IPsec VPN 隧道冗余的逻辑表示。在此图中，站点 A 和站点 B 表示两个数据中心。对于此示例，假设 NSX-T Data Center 不在站点 A 中管理 Edge VPN 网关，NSX-T Data Center 在站点 B 中管理 Edge 网关虚拟设备。

图 5-1. 基于路由的 IPSec VPN 中的隧道冗余



如图所示，您可以使用 VTI 配置两个独立的 IPSec VPN 隧道。使用 BGP 协议配置动态路由，以实现隧道冗余。如果这两个 IPSec VPN 隧道都可用，将一直提供服务。通过 NSX Edge 节点从站点 A 传输到站点 B 的所有流量是通过 VTI 路由的。数据流量将进行 IPSec 处理，然后从关联的 NSX Edge 节点上行链路接口中传出。从 NSX Edge 节点上行链路接口上的站点 B VPN 网关收到的所有入站 IPSec 流量将在解密后转发到 VTI，然后进行正常路由。

必须配置 BGP HoldDown 定时器和 KeepAlive 定时器值，以检测在所需的故障切换时间内与对等站点的连接是否中断。请参见[配置 BGP](#)。

了解第 2 层 VPN

通过使用第 2 层 VPN (L2 VPN)，您可以将第 2 层网络（VNI 或 VLAN）扩展到同一广播域上的多个站点。该连接是使用 L2 VPN 服务器和 L2 VPN 客户端之间的基于路由的 IPSec 隧道保护的。

注 此 L2 VPN 功能仅适用于 NSX-T Data Center，没有任何第三方互操作性。

扩展的网络是具有单个广播域的单个子网，因此，在站点之间移动虚拟机时，它们仍位于同一子网上，并且 IP 地址保持不变。因此，企业可以在网络站点之间无缝地迁移虚拟机。虚拟机可以在基于 VNI 的网络或基于 VLAN 的网络上运行。对于云服务提供商而言，L2 VPN 向加入租户提供了一种机制，这种机制无需修改其工作负载和应用程序使用的现有 IP 地址。

除了支持数据中心迁移外，通过 L2 VPN 扩展的内部部署网络对灾难恢复计划很有用，可动态占用外部部署计算资源以满足增加的需求。

每个 L2 VPN 会话都具有一个通用路由封装 (GRE) 隧道。不支持隧道冗余。一个 L2 VPN 会话最多可以扩展到 4094 个 L2 分段。

在 NSX-T Data Center 中，仅在 Tier-0 网关上支持 L2 VPN 服务。分段可以连接到 Tier-0 或 Tier-1 网关，并使用 L2 VPN 服务。

从 NSX-T Data Center 2.5 版开始，可以使用 L2 VPN 服务在 NSX-T Data Center 环境中管理的 NSX Edge 上扩展基于 VLAN 的分段。这种支持允许将 L2 网络从 VLAN 扩展到 VNI、从 VLAN 扩展到 VLAN，以及从 VNI 扩展到 VNI。

此外，还支持使用 ESX NSX 管理的虚拟分布式交换机 (N-VDS) 的 VLAN 中继。如果计算和 I/O 资源允许，VLAN 中继允许一个 NSX Edge 集群在单个接口上扩展多个 VLAN 网络。

以下方案中提供 L2 VPN 服务支持。

- 在 NSX Data Center for vSphere 环境中管理的 NSX Edge 上托管的 NSX-T Data Center L2 VPN 服务器和 L2 VPN 客户端之间。受管 L2 VPN 客户端支持 VLAN 和 VNI。
- 在独立或非受管 NSX Edge 上托管的 NSX-T Data Center L2 VPN 服务器和 L2 VPN 客户端之间。非受管 L2 VPN 客户端仅支持 VLAN。
- 在自治 NSX Edge 上托管的 NSX-T Data Center L2 VPN 服务器和 L2 VPN 客户端之间。自治 L2 VPN 客户端仅支持 VLAN。
- 从 NSX-T Data Center 2.4 版本开始，L2 VPN 服务支持在 NSX-T Data Center L2 VPN 服务器和 NSX-T Data Center L2 VPN 客户端之间可用。在此场景中，您可以在两个内部部署软件定义的数据中心 (Software-Defined Data Center, SDDC) 之间扩展逻辑 L2 分段

添加 VPN 服务

您可以使用 NSX Manager 用户界面 (UI) 添加 IPsec VPN（基于策略或基于路由）或 L2 VPN。

以下几节提供了有关在设置所需的 VPN 服务时需要使用的工作流的信息。这些章节后面的主题提供有关如何使用 NSX Manager 用户界面添加 IPsec VPN 或 L2 VPN 的详细信息。

基于策略的 IPsec VPN 配置工作流

配置基于策略的 IPsec VPN 服务工作流需要执行以下汇总步骤。

- 1 使用现有 Tier-0 或 Tier-1 网关创建并启用一个 IPsec VPN 服务。请参见[添加 IPsec VPN 服务](#)。
- 2 如果您不希望使用系统默认值，请创建 DPD（不活动对等检测）配置文件。请参见[添加 DPD 配置文件](#)。
- 3 要使用非系统默认 IKE 配置文件，请定义 IKE（Internet 密钥交换）配置文件。请参见[添加 IKE 配置文件](#)。
- 4 使用[添加 IPsec 配置文件](#)配置 IPsec 配置文件。
- 5 使用[添加本地端点](#)创建一个在 NSX Edge 上托管的 VPN 服务器。
- 6 配置基于策略的 IPsec VPN 会话，应用配置文件，并向其附加本地端点。请参见[添加基于策略的 IPsec 会话](#)。指定要用于隧道的本地和对等子网。从本地子网传输到对等子网的流量使用会话中定义的隧道进行保护。

基于路由的 IPSec VPN 配置 workflow

基于路由的 IPSec VPN 配置 workflow 需要执行以下汇总步骤。

- 1 使用现有 Tier-0 或 Tier-1 网关配置并启用一个 IPSec VPN 服务。请参见[添加 IPSec VPN 服务](#)。
- 2 如果您不希望使用默认 IKE 配置文件，请定义 IKE 配置文件。请参见[添加 IKE 配置文件](#)。
- 3 如果您决定不使用系统默认的 IPSec 配置文件，请使用[添加 IPSec 配置文件](#)创建一个。
- 4 如果不希望使用默认 DPD 配置文件，请创建一个 DPD 配置文件。请参见[添加 DPD 配置文件](#)。
- 5 使用[添加本地端点](#)添加本地端点。
- 6 配置一个基于路由的 IPSec VPN 会话，应用配置文件，并将本地端点附加到该会话。在配置中提供一个 VTI IP，并使用相同的 IP 配置路由。路由可能是静态或动态的（使用 BGP）。请参见[添加基于路由的 IPSec 会话](#)。

L2 VPN 配置 workflow

配置 L2 VPN 需要在服务器模式下配置 L2 VPN 服务，然后在客户端模式下配置另一个 L2 VPN 服务。您还必须为 L2 VPN 服务器配置会话，并使用 L2 VPN 服务器生成的对等代码为 L2 VPN 客户端配置会话。下面是配置 L2 VPN 服务的汇总 workflow。

- 1 在服务器模式下创建 L2 VPN 服务。
 - a 使用 Tier-0 网关配置基于路由的 IPSec VPN 隧道，然后使用该基于路由的 IPSec 隧道配置 L2 VPN 服务器服务。请参见[添加 L2 VPN 服务器服务](#)。
 - b 配置 L2 VPN 服务器会话，将新创建的基于路由的 IPSec VPN 服务和 L2 VPN 服务器服务绑定在一起，并自动分配 GRE IP 地址。请参见[添加 L2 VPN 服务器会话](#)。
 - c 将分段添加到 L2 VPN 服务器会话。此步骤在[添加 L2 VPN 服务器会话](#)中也进行了介绍。
 - d 使用[下载远程端 L2 VPN 配置文件](#)获取 L2 VPN 服务器服务会话的对等代码，必须在远程站点上应用该代码并用于自动配置 L2 VPN 客户端会话。
- 2 在客户端模式下创建 L2 VPN 服务。
 - a 使用不同的 Tier-0 网关配置另一个基于路由的 IPSec VPN 服务，然后使用刚刚配置的 Tier-0 网关配置 L2 VPN 客户端服务。请参见[添加 L2 VPN 客户端服务](#)，了解相关信息。
 - b 通过导入 L2 VPN 服务器服务生成的对等代码定义 L2 VPN 客户端会话。请参见[添加 L2 VPN 客户端会话](#)。
 - c 将分段添加到上一步定义的 L2 VPN 客户端会话。此步骤在[添加 L2 VPN 客户端会话](#)中进行了介绍。

添加 IPsec VPN 服务

NSX-T Data Center 在 Tier-0 或 Tier-1 网关和远程站点之间支持站点到站点 IPsec VPN 服务。您可以创建基于策略或基于路由的 IPsec VPN 服务。在可以配置基于策略或基于路由的 IPsec VPN 会话之前，您必须首先创建 IPsec VPN 服务。

注 IPsec VPN 在 NSX-T Data Center Limited Export 版本中不受支持。

在本地端点 IP 地址在配置了 IPsec VPN 会话的同一逻辑路由器中执行 NAT 时，不支持 IPsec VPN。

前提条件

- 熟悉 IPsec VPN。请参见[了解 IPsec VPN](#)。
- 您必须配置了至少一个 Tier-0 或 Tier-1 网关，并且可以使用这些网关。有关详细信息，请参见[添加 Tier-0 网关](#)或[添加 Tier-1 网关](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 导航到 **网络 > VPN > VPN 服务**。
- 3 选择**添加服务 > IPsec**。
- 4 输入 IPsec 服务的名称。
此名称是必填字段。
- 5 从**网关**下拉菜单中，选择要与该 IPsec VPN 服务关联的 Tier-0 或 Tier-1 网关。
- 6 启用或禁用**管理状态**。
默认情况下，该值设置为 `Enabled`，这意味着在配置新的 IPsec VPN 服务后在 Tier-0 或 Tier-1 网关上启用了 IPsec VPN 服务。
- 7 设置 **IKE 日志级别**的值。
默认值设置为 `Info` 级别。
- 8 如果您希望在标记组中包括此服务，请输入**标记**的值。
- 9 如果要允许在指定的本地和远程 IP 地址之间交换数据数据包而不进行任何 IPsec 保护，请单击**全局绕过规则**，即使在 IPsec 会话规则中指定了 IP 地址也是如此。在**本地网络**和**远程网络**文本框中，输入要在之间应用绕过规则的本地和远程子网列表。
默认设置是在本地和远程站点之间交换数据时使用 IPsec 保护。这些规则适用于在该 IPsec VPN 服务中创建的所有 IPsec VPN 会话。
- 10 单击**保存**。
成功创建新 IPsec VPN 服务后，系统会询问您是否要继续进行其余的 IPsec VPN 配置。如果单击**是**，您将返回到“添加 IPsec VPN 服务”面板。**会话**链接现已启用，您可以单击该链接以添加 IPsec VPN 会话。

后续步骤

使用[添加 IPsec VPN 会话](#)中的信息引导您添加 IPsec VPN 会话。您还将提供完成 IPsec VPN 配置所需的配置文件和本地端点的信息。

添加 L2 VPN 服务

您可以在 Tier-0 网关上配置 L2 VPN 服务。要启用 L2 VPN 服务，必须先在 Tier-0 网关上创建 IPsec VPN 服务（如果尚不存在）。然后，在 L2 VPN 服务器（目标网关）和 L2 VPN 客户端（源网关）之间配置 L2 VPN 隧道。

要配置 L2 VPN 服务，请使用本节后面主题中的信息。

前提条件

- 熟悉 IPsec VPN 和 L2 VPN。请参见[了解 IPsec VPN](#)和[了解第 2 层 VPN](#)。
- 您必须至少已配置一个 Tier-0 网关且可供使用。请参见[添加 Tier-0 网关](#)。

步骤

1 添加 L2 VPN 服务器服务

要配置 L2 VPN 服务器服务，必须在 L2 VPN 客户端将连接到的目标 NSX Edge 上以服务器模式配置 L2 VPN 服务。

2 添加 L2 VPN 客户端服务

配置 L2 VPN 服务器服务后，在客户端模式下，在另一个 NSX Edge 实例上配置 L2 VPN 服务。

添加 L2 VPN 服务器服务

要配置 L2 VPN 服务器服务，必须在 L2 VPN 客户端将连接到的目标 NSX Edge 上以服务器模式配置 L2 VPN 服务。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 （可选）如果要配置为 L2 VPN 服务器的 Tier-0 网关上尚不存在 IPsec VPN 服务，请使用以下步骤来创建该服务。
 - a 导航到**网络 > VPN > VPN 服务**选项卡，然后选择**添加服务 > IPsec**。
 - b 输入 IPsec VPN 服务的名称。
 - c 从 **Tier-0 网关**下拉菜单中，选择要与 L2 VPN 服务器一起使用的 Tier-0 网关。
 - d 如果要使用不同于系统默认值的值，请根据需要在“添加 IPsec 服务”窗格中设置其余属性。
 - e 单击**保存**，然后在系统提示是否要继续配置 IPsec VPN 服务时，选择**否**。
- 3 导航到**网络 > VPN > VPN 服务**选项卡，然后选择**添加服务 > L2 VPN 服务器**以创建 L2 VPN 服务器。
- 4 输入 L2 VPN 服务器的名称。

- 5 从 **Tier-0 网关** 下拉菜单中，选择用于片刻之前创建的 IPsec 服务的同一 Tier-0 网关。
- 6 输入此 L2 VPN 服务器的可选说明。
- 7 如果您希望在标记组中包括此服务，请输入**标记**的值。
- 8 启用或禁用**中心和分支**属性。

默认情况下，该值设置为 Disabled，这意味着仅将从 L2 VPN 客户端收到的流量复制到 L2 VPN 服务器连接的分段。如果此属性设置为 Enabled，那么来自任何 L2 VPN 客户端的流量都会被复制到所有其他 L2 VPN 客户端。

- 9 单击**保存**。

成功创建新 L2 VPN 服务器后，系统会询问您是否要继续进行其余的 L2 VPN 服务配置。如果单击**是**，您将返回到“添加 L2 VPN 服务器”窗格，并且**会话**链接已启用。可以使用此链接创建 L2 VPN 服务器会话，或者使用**网络 > VPN > L2 VPN 会话**选项卡。

后续步骤

为使用添加 **L2 VPN 服务器会话** 中的信息作为指导配置的 L2 VPN 服务器配置 L2 VPN 服务器会话。

添加 L2 VPN 客户端服务

配置 L2 VPN 服务器服务后，在客户端模式下，在另一个 NSX Edge 实例上配置 L2 VPN 服务。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 （可选）如果此类服务尚不存在，请使用以下步骤为 L2 VPN 客户端服务创建一个 IPsec VPN 服务。
 - a 导航到**网络 > VPN > VPN 服务**选项卡，然后选择**添加服务 > IPsec**。
 - b 输入 IPsec VPN 服务的名称。
 - c 从 **Tier-0 网关** 下拉菜单中，选择一个与 L2 VPN 客户端一起使用的 Tier-0 网关。
 - d 如果要使用不同于系统默认值的值，请根据需要在“添加 IPsec 服务”窗格中设置其余属性。
 - e 单击**保存**，然后在系统提示是否要继续配置 IPsec VPN 服务时，选择**否**。
- 3 导航到**网络 > VPN > VPN 服务**选项卡，然后选择**添加服务 > L2 VPN 客户端**。
- 4 输入 L2 VPN 客户端服务的名称。
- 5 从 **Tier-0 网关** 下拉菜单中，选择与刚才创建的基于路由的 IPsec 隧道一起使用的相同 Tier-0 网关。
- 6 （可选）设置**描述**和**标记**值。
- 7 单击**保存**。

成功创建新的 L2 VPN 客户端服务后，系统会询问您是否要继续配置其余的 L2 VPN 客户端。如果单击**是**，您将返回到“添加 L2 VPN 客户端”窗格并启用**会话**链接。可使用此链接创建 L2 VPN 客户端会话，也可使用**网络 > VPN > L2 VPN 会话**选项卡。

后续步骤

为配置的 L2 VPN 客户端服务配置 L2 VPN 客户端会话。使用添加 [L2 VPN 客户端会话](#) 中的信息作为指导。

添加 IPsec VPN 会话

在配置 IPsec VPN 服务后，您必须添加基于策略的 IPsec VPN 会话或基于路由的 IPsec VPN 会话，具体取决于要配置的 IPsec VPN 类型。您还应提供本地端点和配置文件的信息，以用于完成 IPsec VPN 服务配置。

添加基于策略的 IPsec 会话

在添加基于策略的 IPsec VPN 时，可以使用 IPsec 隧道将 NSX Edge 节点后面的多个本地子网连接到远程 VPN 站点上的对等子网。

以下步骤使用 NSX Manager UI 上的 **IPsec 会话** 选项卡创建基于策略的 IPsec 会话。还可以添加隧道、IKE 和 DPD 配置文件的信息，然后选择现有的本地端点用于基于策略的 IPsec VPN。

注 也可以在成功配置 IPsec VPN 服务后立即添加 IPsec VPN 会话。在系统提示您继续进行 IPsec VPN 服务配置时单击**是**，然后在“添加 Ipsec 服务”面板上选择**会话 > 添加会话**。在以下过程的前几步中，假定系统提示您继续进行 IPsec VPN 服务配置时您选择了**否**。如果您已选择**是**，请继续执行以下步骤中的步骤 3，以引导您完成其余基于策略的 IPsec VPN 会话配置。

前提条件

- 必须先配置 IPsec VPN 服务才能继续操作。请参见[添加 IPsec VPN 服务](#)。
- 获取本地端点的信息以及对等站点、本地网络子网和远程网络子网的 IP 地址，以用于要添加的基于策略的 IPsec VPN 会话。要创建本地端点，请参见[添加本地端点](#)。
- 如果要使用预共享密钥 (PSK) 进行身份验证，请获取 PSK 值。
- 如果要使用证书进行身份验证，请确保已导入必要的服务器证书和对应的 CA 签名证书。请参见[设置证书](#)。
- 如果不希望为 NSX-T Data Center 提供的 IPsec 隧道、IKE 或不活动对等检测 (DPD) 配置文件使用默认设置，请改为配置您要使用的配置文件。请参见[添加配置文件](#)，了解相关信息。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 导航到 **网络 > VPN > IPsec 会话** 选项卡。
- 3 选择**添加 IPsec 会话 > 基于策略**。
- 4 输入基于策略的 IPsec VPN 会话的名称。

- 5 从 **VPN 服务** 下拉菜单中，选择要向其添加此新的 IPsec 会话的 IPsec VPN 服务。

注 如果要从**添加 IPsec 会话**对话框中添加此 IPsec 会话，则**添加 IPsec 会话**按钮上方会指示 VPN 服务名称。

- 6 从下拉菜单中选择现有本地端点。

需要输入该本地端点值，它标识本地 NSX Edge 节点。如果要创建不同的本地端点，请单击三点菜单 (⋮)，然后选择**添加本地端点**。

- 7 在**远程 IP** 文本框中，输入远程站点的所需 IP 地址。

需要输入此值。

- 8 输入此基于策略的 IPsec VPN 会话的可选说明。

最大长度为 1024 个字符。

- 9 要启用或禁用 IPsec VPN 会话，请单击**管理状态**。

默认情况下，该值设置为 Enabled，这意味着将配置到 NSX Edge 节点的 IPsec VPN 会话。

- 10 (可选) 从**合规性套件**下拉菜单中，选择一个安全合规性套件。

注 从 NSX-T Data Center 2.5 开始，将提供合规性套件支持。有关详细信息，请参见[关于支持的合规性套件](#)。

选择的默认值为 None。如果选择一个合规性套件，则**身份验证模式**设置为 Certificate，并且**高级属性**部分中的 **IKE 配置文件**和 **IPsec 配置文件**值设置为系统为选定安全合规性套件定义的配置文件。您无法编辑这些系统定义的配置文件。

- 11 如果**合规性套件**设置为 None，请从**身份验证模式**下拉菜单中选择一种模式。

使用的默认身份验证模式为 PSK，这意味着将 NSX Edge 和远程站点之间共享的私钥用于 IPsec VPN 会话。如果选择 Certificate，则使用用于配置本地端点的站点证书进行身份验证。

- 12 在“本地网络”和“远程网络”文本框中，至少输入一个 IP 子网地址以用于该基于策略的 IPsec VPN 会话。

这些子网必须采用 CIDR 格式。

- 13 如果**身份验证模式**设置为 PSK，请在**预共享密钥**文本框中输入密钥值。

此私钥可以是最大长度为 128 个字符的字符串。

小心 在共享和存储 PSK 值时要格外小心，因为它包含一些非常敏感的信息。

14 要标识对等站点，请在**远程 ID** 中输入值。

对于使用 PSK 身份验证的对等站点，该 ID 值必须是对等站点的公用 IP 地址或 FQDN。对于使用证书身份验证的对等站点，该 ID 值必须是在对等站点的证书中使用的公用名称 (Common Name, CN) 或标识名 (Distinguished Name, DN)。

注 如果对等站点的证书在 DN 字符串中包含电子邮件地址，例如，

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123/emailAddress=user1@mycompany.com
```

则使用以下格式输入**远程 ID** 值以作为一个示例。

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123, MAILTO=user1@mycompany.com"
```

如果本地站点的证书在 DN 字符串中包含电子邮件地址，并且对等站点使用 strongSwan IPsec 实施，请在该对等站点中输入本地站点的 ID 值。以下是一个示例。

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123, E=user1@mycompany.com"
```

15 要更改配置文件、启动模式、TCP MSS 限制模式以及基于策略的 IPsec VPN 会话使用的标记，请单击**高级属性**。

默认情况下，使用系统生成的配置文件。如果不希望使用默认配置文件，则选择其他可用的配置文件。如果要使用尚未配置的配置文件，请单击三点菜单 (...) 以创建其他配置文件。请参见[添加配置文件](#)。

- 如果启用了 **IKE 配置文件** 下拉菜单，请选择 IKE 配置文件。
- 如果未禁用 **IPsec 配置文件** 下拉菜单，请选择 IPsec 隧道配置文件。
- 如果启用了 **DPD 配置文件** 下拉菜单，请选择首选的 DPD 配置文件。
- 从**连接启动模式**下拉菜单中，选择首选模式。

连接启动模式定义在隧道创建过程中由本地端点使用的策略。默认值为 **Initiator**。下表说明可用的不同连接启动模式。

表 5-2. 连接启动模式

连接启动模式	说明
Initiator	默认值。在此模式下，本地端点启动 IPsec VPN 隧道创建，并对来自对等网关的入站隧道设置请求进行响应。
On Demand	在此模式下，在收到与策略规则匹配的第二个数据包后，本地端点启动 IPsec VPN 隧道创建。它还对入站启动请求进行响应。
Respond Only	IPsec VPN 从不启动连接。对等站点始终启动连接请求，本地端点会对该连接请求进行响应。

- e 如果要在 IPsec 连接期间减少 TCP 会话的最大分段大小 (MSS) 负载, 请启用 **TCP MSS 限制**, 选择 **TCP MSS 方向值**, 并且可以选择设置 **TCP MSS 值**。

有关详细信息, 请参见[了解 TCP MSS 限制](#)。

- f 如果要将此会话包含在特定组中, 请在**标记**中输入标记名称。

16 单击保存。

结果

成功配置基于策略的新 IPsec VPN 会话后, 它将添加到可用 IPsec VPN 会话列表中。它处于只读模式。

后续步骤

- 确认 IPsec VPN 隧道状态为“已启动”。请参见[监控 VPN 会话和排除其故障](#), 了解相关信息。
- 如有必要, 请通过单击会话行左侧的三点菜单 (...) 来管理 IPsec VPN 会话信息。选择允许执行的操作之一。

添加基于路由的 IPsec 会话

添加基于路由的 IPsec VPN 时, 会在流量上提供隧道, 而流量基于使用首选协议 (如 BGP) 通过虚拟隧道接口 (VTI) 动态发现的路由。IPsec 会保护流经 VTI 的所有流量。

本主题中所述的步骤使用 **IPsec 会话**选项卡创建基于路由的 IPsec 会话。也可以添加有关隧道、IKE 和 DPD 配置文件的信息, 然后选择现有的本地端点以用于基于路由的 IPsec VPN。

注 也可以在成功配置 IPsec VPN 服务后立即添加 IPsec VPN 会话。在系统提示您继续进行 IPsec VPN 服务配置时单击**是**, 然后在“添加 Ipsec 服务”面板上选择**会话 > 添加会话**。在以下过程的前几步中, 假定系统提示您继续进行 IPsec VPN 服务配置时您选择了**否**。如果选择**是**, 则继续执行以下步骤中的步骤 3, 以指导您进行基于路由的 IPsec VPN 会话配置的其余部分。

前提条件

- 必须先配置 IPsec VPN 服务才能继续操作。请参见[添加 IPsec VPN 服务](#)。
- 获取本地端点、对等站点的 IP 地址和隧道服务 IP 子网地址的信息以用于要添加的基于路由的 IPsec 会话。要创建本地端点, 请参见[添加本地端点](#)。
- 如果要使用预共享密钥 (PSK) 进行身份验证, 请获取 PSK 值。
- 如果要使用证书进行身份验证, 请确保已导入必要的服务器证书和对应的 CA 签名证书。请参见[设置证书](#)。
- 如果不希望使用 NSX-T Data Center 提供的 IPsec 隧道、IKE 或失效对等检测 (DPD) 配置文件的默认值, 则改为配置要使用的配置文件。请参见[添加配置文件](#), 了解相关信息。

步骤

- 1 从浏览器中, 使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 导航到 **网络 > VPN > IPsec 会话**。

- 3 选择**添加 IPsec 会话 > 基于路由**。
- 4 为基于路由的 IPsec 会话输入名称。
- 5 从 **VPN 服务** 下拉菜单中，选择要向其添加此新的 IPsec 会话的 IPsec VPN 服务。

注 如果要从**添加 IPsec 会话**对话框中添加此 IPsec 会话，则**添加 IPsec 会话**按钮上方会指示 VPN 服务名称。

- 6 从下拉菜单中选择现有本地端点。
需要输入该本地端点值，它标识本地 NSX Edge 节点。如果要创建不同的本地端点，请单击三点菜单 (⋮)，然后选择**添加本地端点**。
- 7 在**远程 IP** 文本框中，输入远程站点的 IP 地址。
需要输入此值。
- 8 输入此基于路由的 IPsec VPN 会话的可选说明。
最大长度为 1024 个字符。
- 9 要启用或禁用 IPsec 会话，请单击**管理状态**。
默认情况下，该值设置为 Enabled，这意味着将配置到 NSX Edge 节点的 IPsec 会话。
- 10 (可选) 从**合规性套件**下拉菜单中，选择一个安全合规性套件。

注 从 NSX-T Data Center 2.5 开始，将提供合规性套件支持。有关详细信息，请参见[关于支持的合规性套件](#)。

默认值设置为 None。如果选择一个合规性套件，则**身份验证模式**设置为 Certificate，并且**高级属性**部分中的 **IKE 配置文件**和 **IPsec 配置文件**值设置为系统为选定合规性套件定义的配置文件。您无法编辑这些系统定义的配置文件。

- 11 使用 CIDR 表示法在**隧道接口**中输入 IP 子网地址。
需要输入此地址。
- 12 如果**合规性套件**设置为 None，请从**身份验证模式**下拉菜单中选择一种模式。
使用的默认身份验证模式为 PSK，这意味着将 NSX Edge 和远程站点之间共享的私钥用于 IPsec VPN 会话。如果选择 Certificate，则使用用于配置本地端点的站点证书进行身份验证。
- 13 如果选择 PSK 身份验证模式，则在**预共享密钥**文本框中输入密钥值。
此私钥可以是最大长度为 128 个字符的字符串。

小心 在共享和存储 PSK 值时要格外小心，因为它包含一些非常敏感的信息。

14 在远程 ID 中输入值。

对于使用 PSK 身份验证的对等站点，该 ID 值必须是对等站点的公用 IP 地址或 FQDN。对于使用证书身份验证的对等站点，该 ID 值必须是在对等站点的证书中使用的公用名称 (Common Name, CN) 或标识名 (Distinguished Name, DN)。

注 如果对等站点的证书在 DN 字符串中包含电子邮件地址，例如，

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123/emailAddress=user1@mycompany.com
```

则使用以下格式输入**远程 ID**值以作为一个示例。

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123, MAILTO=user1@mycompany.com"
```

如果本地站点的证书在 DN 字符串中包含电子邮件地址，并且对等站点使用 strongSwan IPsec 实施，请在该对等站点中输入本地站点的 ID 值。以下是一个示例。

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123, E=user1@mycompany.com"
```

15 如果要将此 IPsec 会话作为特定组标记的一部分包括，请在**标记**中输入标记名称。

16 要更改配置文件、启动模式、TCP MSS 限制模式以及基于路由的 IPsec VPN 会话使用的标记，请单击**高级属性**。

默认情况下，将使用系统生成的配置文件。如果不希望使用默认配置文件，则选择其他可用的配置文件。如果要使用尚未配置的配置文件，请单击三点菜单 (...) 以创建其他配置文件。请参见[添加配置文件](#)。

- a 如果启用了 **IKE 配置文件** 下拉菜单，请选择 IKE 配置文件。
- b 如果未禁用 **IPsec 配置文件** 下拉菜单，请选择 IPsec 隧道配置文件。
- c 如果启用了 **DPD 配置文件** 下拉菜单，请选择首选的 DPD 配置文件。
- d 从**连接启动模式**下拉菜单中，选择首选模式。

连接启动模式定义在隧道创建过程中由本地端点使用的策略。默认值为 **Initiator**。下表说明可用的不同连接启动模式。

表 5-3. 连接启动模式

连接启动模式	说明
Initiator	默认值。在此模式下，本地端点启动 IPsec VPN 隧道创建，并对来自对等网关的入站隧道设置请求进行响应。
On Demand	不要与基于路由的 VPN 一起使用。该模式仅适用于基于策略的 VPN。
Respond Only	IPsec VPN 从不启动连接。对等站点始终启动连接请求，本地端点会对该连接请求进行响应。

- 17 如果要在 IPSec 连接期间减少 TCP 会话的最大分段大小 (MSS) 负载，请启用 **TCP MSS 限制**，选择 **TCP MSS 方向值**，并且可以选择设置 **TCP MSS 值**。

有关详细信息，请参见[了解 TCP MSS 限制](#)。

- 18 如果要将此 IPSec 会话作为特定组标记的一部分包括，请在**标记**中输入标记名称。

- 19 单击**保存**。

结果

成功配置新的基于路由的 IPSec VPN 会话后，会将它添加到可用 IPsec VPN 会话的列表。它处于只读模式。

后续步骤

- 确认 IPSec VPN 隧道状态为“已启动”。请参见[监控 VPN 会话和排除其故障](#)，了解相关信息。
- 使用静态路由或 BGP 配置路由。请参见[配置静态路由](#)或[配置 BGP](#)。
- 如有必要，请单击会话行左侧的三个点菜单 (...) 以管理 IPSec VPN 会话信息。选择您可以执行的操作之一。

关于支持的合规性套件

从 NSX-T Data Center 2.5 开始，您可以指定一个安全合规性套件，以用来配置用于 IPSec VPN 会话的安全配置文件。

安全合规性套件具有预定义的值以用于不同的安全参数，并且无法修改这些值。在选择合规性套件时，预定义的值将自动用于所配置的 IPSec VPN 会话的安全配置文件。

下表列出了 NSX-T Data Center 中的 IKE 配置文件支持的合规性套件以及为每个套件预定义的值。

合规性套件名称	IKE 版本	加密算法	摘要算法	Diffie-Hellman 组
CNSA	IKEv2	AES 256	SHA2 384	组 15、组 20
FIPS	IKE-Flex	AES 128	SHA2 256	组 20
基础	IKEv1	AES 128	SHA2 256	组 14
PRIME	IKEv2	AES GCM 128	未设置	组 19
Suite-B-GCM-128	IKEv2	AES 128	SHA2 256	组 19
Suite-B-GCM-256	IKEv2	AES 256	SHA2 384	组 20

下表列出了 NSX-T Data Center 中的 IPSec 配置文件支持的合规性套件以及为每个套件预定义的值。

合规性套件名称	加密算法	摘要算法	PFS 组	Diffie-Hellman 组
CNSA	AES 256	SHA2 384	已启用	组 15、组 20
FIPS	AES GCM 128	未设置	已启用	组 20
基础	AES 128	SHA2 256	已启用	组 14

合规性套件名称	加密算法	摘要算法	PFS 组	Diffie-Hellman 组
PRIME	AES GCM 128	未设置	已启用	组 19
Suite-B-GCM-128	AES GCM 128	未设置	已启用	组 19
Suite-B-GCM-256	AES GCM 256	未设置	已启用	组 20

了解 TCP MSS 限制

通过使用 TCP MSS 限制，您可以减少在通过 IPsec 隧道建立连接期间 TCP 会话使用的最大分段大小 (MSS) 值。从 NSX-T Data Center 2.5 开始支持该功能。

TCP MSS 是主机希望在单个 TCP 分段中接受的最大数据量（以字节为单位）。TCP 连接的每一端在三向握手期间将所需的 MSS 值发送到对等端，其中 MSS 是 TCP SYN 数据包中使用的 TCP 标头选项之一。TCP MSS 是根据发送方主机的输出接口的最大传输单元 (MTU) 计算的。

在 TCP 流量通过 IPsec VPN 或任何类型的 VPN 隧道时，将在原始数据包中添加额外的标头以保证安全。对于 IPsec 隧道模式，使用的额外标头是 IP、ESP 和可选的 UDP（如果在网络中存在端口转换）。由于这些额外的标头，封装的数据包大小超出 VPN 接口的 MTU。根据 DF 策略，数据包可能会碎片化或被丢弃。

为了避免数据包碎片化或丢弃，您可以启用 TCP MSS 限制功能以调整 IPsec 会话的 MSS 值。导航到**网络 > VPN > IPsec 会话**。在添加 IPsec 会话或编辑现有会话时，展开**高级属性**部分，然后启用 **TCP MSS 限制**。

您可以设置 **TCP MSS 方向**和 **TCP MSS 值**，以配置适用于 IPsec 会话的预计算 MSS 值。配置的 MSS 值用于 MSS 限制。您可以选择设置 **TCP MSS 方向**，并将 **TCP MSS 值**保留空白以使用动态 MSS 计算。MSS 值是根据 VPN 接口 MTU、VPN 开销以及已确定的路径 MTU (PMTU) 自动计算的。在每次 TCP 握手期间，将重新计算有效的 MSS 以动态处理 MTU 或 PMTU 变化。

添加 L2 VPN 会话

配置 L2 VPN 服务器和 L2 VPN 客户端后，必须为两者添加 L2 VPN 会话才能完成 L2 VPN 服务配置。

添加 L2 VPN 服务器会话

创建 L2 VPN 服务器服务后，必须添加 L2 VPN 会话，并将其附加到现有的分段。

以下步骤使用 NSX Manager UI 上的 **L2 VPN 会话**选项卡创建 L2 VPN 服务器会话。也可以选择现有的本地端点和分段以附加到 L2 VPN 服务器会话。

注 也可以在成功配置 L2 VPN 服务器服务后立即添加 L2 VPN 服务器会话。系统提示继续进行 L2 VPN 服务器配置时单击**是**，然后在“添加 L2 VPN 服务器”面板上选择**会话 > 添加会话**。在以下过程的前几步中，假定系统提示您继续进行 L2 VPN 服务器配置时选择了**否**。如果选择**是**，则继续执行以下步骤中的步骤 3，以指导您进行 L2 VPN 服务器会话配置的其余部分。

前提条件

- 必须先配置 L2 VPN 服务器服务才能继续操作。请参见[添加 L2 VPN 服务器服务](#)。
- 获取本地端点和远程 IP 的信息以用于要添加的 L2 VPN 服务器会话。要创建本地端点，请参见[添加本地端点](#)。
- 获取预共享密钥 (PSK) 和隧道接口子网的值以用于 L2 VPN 服务器会话。
- 获取要附加到所创建的 L2 VPN 服务器会话的现有分段的名称。请参见[添加分段](#)，了解相关信息。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 导航到 **网络 > VPN > L2 VPN 会话** 选项卡。
- 3 选择**添加 L2 VPN 会话 > L2 VPN 服务器**。
- 4 输入 L2 VPN 服务器会话的名称。
- 5 从 **L2 VPN 服务** 下拉菜单中，选择要为其创建 L2 VPN 会话的 L2 VPN 服务器服务。

注 如果从“设置 L2VPN 服务器会话”对话框添加此 L2 VPN 服务器会话，则**添加 L2 会话**按钮上方会指示 L2 VPN 服务器服务。

- 6 从下拉菜单中选择现有本地端点。

如果要创建不同的本地端点，请单击三点菜单 (⋮)，然后选择**添加本地端点**。

- 7 输入远程站点的 IP 地址。
- 8 要启用或禁用 L2 VPN 服务器会话，请单击**管理状态**。

默认情况下，该值设置为**已启用**，这意味着将配置到 NSX Edge 节点的 L2 VPN 服务器会话。

- 9 在**预共享密钥**中输入私钥值。

小心 在共享和存储 PSK 值时要格外小心，因为它包含一些非常敏感的信息。

- 10 使用 CIDR 表示法在**隧道接口**中输入 IP 子网地址。

例如，4.5.6.6/24。需要输入此子网地址。

- 11 在**远程 ID**中输入值。

对于使用证书身份验证的对等站点，此 ID 必须是对等站点证书中的公用名称。对于 PSK 对等站点，此 ID 可以是任何字符串。最好使用 VPN 的公用 IP 地址或者 VPN 服务的 FQDN 作为 Remote ID。

- 12 如果要将此会话包含在特定组中，请在**标记**中输入标记名称。

- 13 单击**保存**，然后在系统提示您要继续进行 VPN 服务配置时单击**是**。

将返回到“添加 L2VPN 会话”面板，**分段**链接现在已启用。

14 将现有分段附加到 L2 VPN 服务器会话。

- a 单击**分段 > 设置分段**。
- b 在**设置分段**对话框中，单击**设置分段**将现有分段附加到 L2 VPN 服务器会话。
- c 从**分段**下拉菜单中，选择要附加到会话的基于 VNI 或 VLAN 的分段。
- d 在 **VPN 隧道 ID** 中输入唯一的值，以用于标识选定的分段。
- e 依次单击**保存**和**关闭**。

在“设置 L2VPN 会话”窗格或对话框中，系统已增加 L2 VPN 服务器会话的**分段**计数。

15 要完成 L2 VPN 服务器会话配置，请单击**关闭编辑**。

结果

在 **VPN 服务**选项卡中，系统已增加所配置的 L2 VPN 服务器服务的**会话**计数。

后续步骤

要完成 L2 VPN 服务配置，还必须在客户端模式和 L2 VPN 客户端会话中创建 L2 VPN 服务。请参见[添加 L2 VPN 客户端服务](#)和[添加 L2 VPN 客户端会话](#)。

添加 L2 VPN 客户端会话

创建 L2 VPN 客户端服务后，您必须添加一个 L2 VPN 客户端会话，然后将其附加到现有分段。

以下步骤使用 NSX Manager UI 上的 **L2 VPN 会话**选项卡创建 L2 VPN 客户端会话。还可以选择现有的本地端点和分段附加到 L2 VPN 客户端会话。

注 成功配置 L2 VPN 客户端服务后，还可以立即添加 L2 VPN 客户端会话。系统提示继续执行 L2 VPN 客户端配置时，单击**是**，然后在“添加 L2 VPN 客户端”面板上选择**会话 > 添加会话**。以下过程的前几步假设您针对提示选择**否**的情况下继续进行 L2 VPN 客户端配置。如果您已选择**是**，请继续执行以下步骤中的步骤 3，以引导您完成其余的 L2 VPN 客户端会话配置。

前提条件

- 在继续操作之前，您必须先配置 L2 VPN 客户端服务。请参见[添加 L2 VPN 客户端服务](#)。
- 获取本地 IP 和远程 IP 的 IP 地址信息以用于您正添加的 L2 VPN 客户端会话。
- 获取在 L2 VPN 服务器配置期间生成的对等代码。请参见[下载远程端 L2 VPN 配置文件](#)。
- 获取要附加到正创建的 L2 VPN 客户端会话的现有分段的名称。请参见[添加分段](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**网络 > VPN > L2 VPN 会话**。
- 3 选择**添加 L2 VPN 会话 > L2 VPN 客户端**。
- 4 输入 L2 VPN 客户端会话的名称。

- 5 从 **VPN 服务** 下拉菜单中，选择 L2 VPN 会话要关联的 L2 VPN 客户端服务。

注 如果要从“设置 L2VPN 客户端会话”对话框中添加此 L2 VPN 客户端会话，那么会在**添加 L2 会话**按钮上方指示 L2 VPN 客户端服务。

- 6 在**本地 IP 地址**文本框中，输入 L2 VPN 客户端会话的 IP 地址。
- 7 输入用于 L2 VPN 客户端会话的 IPSec 隧道的远程 IP 地址。
- 8 在**对等配置**文本框中，输入配置 L2 VPN 服务器服务时生成的对等代码。
- 9 启用或禁用**管理状态**。
默认情况下，该值设置为**已启用**，这意味着将配置到 NSX Edge 节点的 L2 VPN 服务器会话。
- 10 单击**保存**，然后在系统提示您要继续进行 VPN 服务配置时单击**是**。
- 11 将现有分段附加到 L2 VPN 客户端会话。
 - a 选择**分段 > 添加分段**。
 - b 在**设置分段**对话框中，单击**添加分段**。
 - c 从**分段**下拉菜单中，选择要附加到 L2 VPN 客户端会话的基于 VNI 或 VLAN 的分段。
 - d 在 **VPN 隧道 ID** 中输入唯一的值，以用于标识选定的分段。
 - e 单击**关闭**。
- 12 要完成 L2 VPN 客户端会话配置，请单击**关闭编辑**。

结果

在 **VPN 服务** 选项卡中，将针对您配置的 L2 VPN 客户端服务更新会话计数。

下载远程端 L2 VPN 配置文件

要配置 L2 VPN 客户端会话，您必须获取在配置 L2 VPN 服务器会话时生成的对等代码。

前提条件

- 必须在继续之前已成功配置 L2 VPN 服务器服务和会话。请参见**添加 L2 VPN 服务器服务**。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 导航到 **网络 > VPN > L2 VPN 会话** 选项卡。
- 3 在 L2 VPN 会话表中，展开计划用于 L2 VPN 客户端会话配置的 L2 VPN 服务器会话对应的行。
- 4 单击**下载配置**，然后在“警告”对话框中单击**是**。

将下载名称为 `L2VPNSession_<name-of-L2-VPN-server-session>_config.txt` 的文本文件。该文件包含远程端 L2 VPN 配置的对等代码。

小心 在存储和共享对等代码时要格外小心，因为它包含 PSK 值，这被视为非常敏感的信息。

例如，L2VPNSession_L2VPNServer_config.txt 包含以下配置。

```
[
  {
    "transport_tunnel_path": "/infra/tier-0s/ServerT0_AS/locale-services/1-
policyconnectivity-693/ipsec-vpn-services/IpsecService1/sessions/Routebase1",
    "peer_code":
    "MCw3ZjBjYzdjLHsic2l0ZU5hbWUiOiJSb3V0ZWJhc2UxIiwic3JjVGFwSXAiOiIxNjkuMjU0LjY0LjIiLCJkc3RUYX
BJcCI6IjE2OS4yNTQuNjQuMSIsImlrZU9wdG1
vbiI6ImlrZXlyIiwic2l0ZU5hbWUiOiJSb3V0ZWJhc2UxIiwic3JjVGFwSXAiOiIxNjkuMjU0LjY0LjIiLCJkc3RUYX
VzdCI6ImFlcylnY20vc2hhLTl1NiIsInBzayI
6IlZN2d2FyZTEyMyIsInRlbm5lbHMlOl7ImxvY2FsSWQiOiI2MC42MC42MC4xIiwicGVlc2klkIjoNTAuNTAuNTAuMS
IsImxvY2FsVnR5SXAiOiIxNjkuMjU0LjY0LjIiLCJkc3RUYX
    }
]
```

5 复制对等代码，可用于配置 L2 VPN 客户端服务和会话。

在使用上述配置文件示例时，您需要复制以下对等代码以用于 L2 VPN 客户端配置。

```
MCw3ZjBjYzdjLHsic2l0ZU5hbWUiOiJSb3V0ZWJhc2UxIiwic3JjVGFwSXAiOiIxNjkuMjU0LjY0LjIiLCJkc3RUYXB
JcCI6IjE2OS4yNTQuNjQuMSIsImlrZU9wdG1
vbiI6ImlrZXlyIiwic2l0ZU5hbWUiOiJSb3V0ZWJhc2UxIiwic3JjVGFwSXAiOiIxNjkuMjU0LjY0LjIiLCJkc3RUYX
VzdCI6ImFlcylnY20vc2hhLTl1NiIsInBzayI
6IlZN2d2FyZTEyMyIsInRlbm5lbHMlOl7ImxvY2FsSWQiOiI2MC42MC42MC4xIiwicGVlc2klkIjoNTAuNTAuNTAuMS
IsImxvY2FsVnR5SXAiOiIxNjkuMjU0LjY0LjIiLCJkc3RUYX
```

后续步骤

配置 L2 VPN 客户端服务和会话。请参见[添加 L2 VPN 客户端服务](#)和[添加 L2 VPN 客户端会话](#)。

添加本地端点

必须配置本地端点以用于要配置的 IPsec VPN。

以下步骤使用 NSX Manager UI 上的**本地端点**选项卡。也可以在添加 IPsec VPN 会话的过程中创建本地端点，方法是单击三点菜单 (⋮)，然后选择**添加本地端点**。如果处于配置 IPsec VPN 会话的中间，则继续执行以下步骤中的步骤 3 以指导您创建新的本地端点。

前提条件

- 如果要将基于证书的身份验证模式用于要使用所配置的本地端点的 IPsec VPN 会话，请获取有关本地端点必须使用的证书的信息。
- 确保您已配置要将此本地端点关联到的 IPsec VPN 服务。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 导航到 **网络 > VPN > 本地端点**，然后单击**添加本地端点**。
- 3 输入本地端点的名称。

4 从 **VPN 服务** 下拉菜单中，选择要与该本地端点关联的 IPsec VPN 服务。

5 输入本地端点的 IP 地址。

对于在 Tier-0 网关上运行的 IPsec VPN 服务，本地端点 IP 地址不能与 Tier-0 网关的上行链路接口 IP 地址相同。您提供的本地端点 IP 地址与 Tier-0 网关的环回接口关联，并且还在上行链路接口上作为可路由 IP 地址发布。对于在 Tier-1 网关上运行的 IPsec VPN 服务，为了能够路由本地端点 IP 地址，必须在 Tier-1 网关配置中启用 IPsec 本地端点的路由通告。有关详细信息，请参见[添加 Tier-1 网关](#)。

6 如果要将基于证书的身份验证模式用于 IPsec VPN 会话，请从**站点证书**下拉菜单中，选择本地端点要使用的证书。

7 （可选）（可选）在**描述**中添加描述。

8 输入用于标识本地 NSX Edge 实例的**本地 ID** 值。

此本地 ID 是远程站点上的对等 ID。本地 ID 必须是远程站点的公用 IP 地址或 FQDN。对于使用本地端点定义的基于证书的 VPN 会话，本地 ID 派生自与本地端点关联的证书。在**本地 ID** 文本框中指定的 ID 将被忽略。来自 VPN 会话证书的本地 ID 取决于证书中包含的扩展。

- 如果在证书中不包含 X509v3 扩展 X509v3 Subject Alternative Name，则将标识名 (Distinguished Name, DN) 作为本地 ID 值。
- 如果在证书中找到 X509v3 扩展 X509v3 Subject Alternative Name，则将其中的一个主体备用名称作为本地 ID 值。

9 从**受信任的 CA 证书**和**证书吊销列表**下拉菜单中，选择本地端点所需的相应证书。

10 如果需要，请指定标记。

11 单击**保存**。

添加配置文件

NSX-T Data Center 提供系统生成的 IPsec 隧道配置文件和 IKE 配置文件，默认情况下在配置 IPsec VPN 或 L2 VPN 服务时分配这些配置文件。为 IPsec VPN 配置创建系统生成的 DPD 配置文件。

IKE 和 IPsec 配置文件提供有关在网络站点之间进行身份验证、加密和建立共享密钥所使用的算法的信息。DPD 配置文件提供有关各探测之间等待秒数的信息。

如果您决定不使用 NSX-T Data Center 提供的默认配置文件，可以使用本节后面主题中的信息配置自己的配置文件。

添加 IKE 配置文件

Internet 密钥交换 (IKE) 配置文件提供有关在建立 IKE 隧道时用于在网络站点之间进行身份验证、加密和建立共享密钥的算法的信息。

NSX-T Data Center 提供系统生成的 IKE 配置文件，默认情况下在配置 IPsec VPN 或 L2 VPN 服务时进行分配。下表列出了提供的默认配置文件。

表 5-4. 用于 IPSec VPN 或 L2 VPN 服务的默认 IKE 配置文件

默认 IKE 配置文件名称	说明
nsx-default-l2vpn-ike-profile	<ul style="list-style-type: none"> ■ 用于 L2 VPN 服务配置。 ■ 使用 IKE V2、AES 128 加密算法、SHA2 256 算法和 Diffie-Hellman 组 14 密钥交换算法进行配置。
nsx-default-l3vpn-ike-profile	<ul style="list-style-type: none"> ■ 用于 IPSec VPN 服务配置。 ■ 使用 IKE V2、AES 128 加密算法、SHA2 256 算法和 Diffie-Hellman 组 14 密钥交换算法进行配置。

您还可以选择从 NSX-T Data Center 2.5 开始支持的合规性套件之一，而不是使用的默认 IKE 配置文件。有关详细信息，请参见[关于支持的合规性套件](#)。

如果您决定不使用提供的默认 IKE 配置文件或合规性套件，您可以使用以下步骤配置自己的 IKE 配置文件。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 单击 **网络 > VPN > 配置文件** 选项卡。
- 3 选择 **IKE 配置文件** 类型，然后单击 **添加 IKE 配置文件**。
- 4 输入 IKE 配置文件的名称。
- 5 从 **IKE 版本** 下拉菜单中，选择要用于在 IPSec 协议组中设置安全关联 (SA) 的 IKE 版本。

表 5-5. IKE 版本

IKE 版本	说明
IKEv1	选择此版本时，IPSec VPN 将启动，并且仅响应 IKEv1 协议。
IKEv2	此版本是默认版本。选择此版本时，IPSec VPN 将启动，并且仅响应 IKEv2 协议。
IKE-Flex	如果选择此版本，当使用 IKEv2 协议建立隧道失败时，源站点不会改为使用 IKEv1 协议启动连接。不过，如果远程站点使用 IKEv1 协议启动连接，则会接受该连接。

- 6 从下拉菜单中选择加密、摘要和 Diffie-Hellman 组算法。您可以选择要应用的多个算法，或者取消选择不希望应用的任何选定算法。

表 5-6. 使用的算法

算法类型	有效值	说明
加密	<ul style="list-style-type: none"> ■ AES 128（默认） ■ AES 256 ■ AES GCM 128 ■ AES GCM 192 ■ AES GCM 256 	<p>在 Internet 密钥交换 (IKE) 协商期间使用的加密算法。</p> <p>与 IKEv2 一起使用时，支持 AES-GCM 算法。与 IKEv1 一起使用时，不支持这些算法。</p>
摘要	<ul style="list-style-type: none"> ■ SHA2 256（默认） ■ SHA1 ■ SHA2 384 ■ SHA2 512 	<p>在 IKE 协商期间使用的安全哈希算法。</p> <p>如果 AES-GCM 是在加密算法文本框中选择的唯一加密算法，则无法在摘要算法文本框中指定任何哈希算法（根据 RFC 5282 中的第 8 节）。此外，将会在 IKE 安全关联 (SA) 协商中隐式选择并使用伪随机函数 (Psuedo Random Function, PRF) 算法 PRF-HMAC-SHA2-256。还必须在对等网关上配置 PRF-HMAC-SHA2-256 算法，以成功完成 IKE SA 协商的第 1 阶段。</p> <p>除了 AES-GCM 算法以外，如果还在加密算法文本框中指定了其他算法，则可以在摘要算法文本框中选择一个或多个哈希算法。此外，IKE SA 协商中使用的 PRF 算法是根据配置的哈希算法隐式确定的。还必须在对等网关上配置至少一个匹配的 PRF 算法，以成功完成 IKE SA 协商的第 1 阶段。例如，如果加密算法文本框包含 AES 128 和 AES GCM 128，并在摘要算法文本框中指定了 SHA1，则在 IKE SA 协商期间使用 PRF-HMAC-SHA1 算法。还必须在对等网关中配置该算法。</p>
Diffie-Hellman 组	<ul style="list-style-type: none"> ■ 组 14（默认） ■ 组 2 ■ 组 5 ■ 组 15 ■ 组 16 ■ 组 19 ■ 组 20 ■ 组 21 	<p>对等站点和 NSX Edge 用于在不安全的通信通道上建立共享密钥的加密方案。</p>

注 在尝试使用两种加密算法或两种摘要算法与 GUARD VPN 客户端（以前为 QuickSec VPN 客户端）建立 IPsec VPN 隧道时，GUARD VPN 客户端在建议的协商列表中添加额外的算法。例如，如果在用于建立 IPsec VPN 隧道的 IKE 配置文件中将 AES 128 和 AES 256 指定为要使用的加密算法，并将 SHA2 256 和 SHA2 512 指定为摘要算法，GUARD VPN 客户端还会在协商列表中建议 AES 192 和 SHA2 384。在这种情况下，NSX-T Data Center 使用您在建立 IPsec VPN 隧道时选择的第一种加密算法。

- 7 如果您希望不同于 86400 秒（24 小时）的默认值，请以秒为单位输入安全关联 (SA) 生命周期值。
- 8 提供说明，然后根据需要添加标记。
- 9 单击**保存**。

结果

此时将向可用 IKE 配置文件表中添加一个新行。要编辑或删除非系统创建的配置文件，请单击三点菜单 (⋮)，然后从可用操作列表中选择。

添加 IPsec 配置文件

Internet 协议安全性 (IPsec) 配置文件提供有关在建立 IPsec 隧道时用于在网络站点之间进行身份验证、加密和建立共享密钥的算法的信息。

NSX-T Data Center 提供系统生成的 IPsec 配置文件，默认情况下在配置 IPsec VPN 或 L2 VPN 服务时进行分配。下表列出了提供的默认 IPsec 配置文件。

表 5-7. 用于 IPsec VPN 或 L2 VPN 服务的默认 IPsec 配置文件

默认 IPsec 配置文件名称	说明
nsx-default-l2vpn-tunnel-profile	<ul style="list-style-type: none"> ■ 用于 L2 VPN。 ■ 使用 AES GCM 128 加密算法和 Diffie-Hellman 组 14 密钥交换算法进行配置。
nsx-default-l3vpn-tunnel-profile	<ul style="list-style-type: none"> ■ 用于 IPsec VPN。 ■ 使用 AES GCM 128 加密算法和 Diffie-Hellman 组 14 密钥交换算法进行配置。

您还可以选择从 NSX-T Data Center 2.5 开始支持的合规性套件之一，而不是默认 IPsec 配置文件。有关详细信息，请参见[关于支持的合规性套件](#)。

如果您决定不使用提供的默认 IPsec 配置文件或合规性套件，您可以使用以下步骤配置自己的 IPsec 配置文件。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 导航到 **网络 > VPN > 配置文件** 选项卡。
- 3 选择 **IPsec 配置文件** 类型，然后单击 **添加 IPsec 配置文件**。
- 4 输入 IPsec 配置文件的名称。
- 5 从下拉菜单中，选择加密、摘要和 Diffie-Hellman 算法。您可以选择要应用的多个算法。
取消选择不希望使用的算法。

表 5-8. 使用的算法

算法类型	有效值	说明
加密	<ul style="list-style-type: none"> ■ AES GCM 128（默认） ■ AES 128 ■ AES 256 ■ AES GCM 192 ■ AES GCM 256 ■ 无加密身份验证 AES GMAC 128 ■ 无加密身份验证 AES GMAC 192 ■ 无加密身份验证 AES GMAC 256 ■ 未加密 	在 Internet 协议安全性 (IPSec) 协商期间使用的加密算法。
摘要	<ul style="list-style-type: none"> ■ SHA1 ■ SHA2 256 ■ SHA2 384 ■ SHA2 512 	在 IPSec 协商期间使用的安全哈希算法。
Diffie-Hellman 组	<ul style="list-style-type: none"> ■ 组 14（默认） ■ 组 2 ■ 组 5 ■ 组 15 ■ 组 16 ■ 组 19 ■ 组 20 ■ 组 21 	对等站点和 NSX Edge 用于在不安全的通信通道上建立共享密钥的加密方案。

- 6 如果您决定不在 VPN 服务上使用 PFS 组协议，请取消选择 **PFS 组**。

默认情况下处于选择状态。

- 7 在 **SA 生命周期** 文本框中，修改必须重新建立 IPSec 隧道之前的默认秒数。

默认情况下，使用 24 小时（86400 秒）的 SA 生命周期。

- 8 为 **DF 位** 选择要用于 IPSec 隧道的值。

此值确定如何处理收到的数据包中包含的“不分段” (DF) 位。可接受的值如下表所述。

表 5-9. DF 位值

DF 位值	说明
COPY	默认值。选择此值后，NSX-T Data Center 将 DF 位的值从接收的数据包复制到转发的数据包。此值意味着，如果收到的数据包设置了 DF 位，那么在加密后，数据包也会设置 DF 位。
CLEAR	选择此值后，NSX-T Data Center 将忽略收到的数据包中的 DF 位值，并且加密数据包中的 DF 位始终为 0。

- 9 提供说明，然后根据需要添加标记。

- 10 单击**保存**。

结果

此时将向可用 IPsec 配置文件表中添加一个新行。要编辑或删除非系统创建的配置文件，请单击三点菜单 (⋮)，然后从可用操作列表中选择。

添加 DPD 配置文件

DPD（不活动对等检测）配置文件提供两次探测之间等待秒数的相关信息，用于检测 IPsec 对等项是否处于活动状态。

NSX-T Data Center 提供一个系统生成的 DPD 配置文件，名为 `nsx-default-l3vpn-dpd-profile`，默认情况下，配置 IPsec VPN 服务时分配此配置文件。

如果决定不使用提供的默认 DPD 配置文件，可以通过以下步骤配置自己的配置文件。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 导航到 **网络 > VPN > 配置文件**。
- 3 选择 **DPD 配置文件** 配置文件类型，然后单击 **添加 DPD 配置文件**。
- 4 输入 DPD 配置文件的名称。
- 5 在 **DPD 探测间隔** 文本框中，输入在发送下一个 DPD 探测之前您希望 NSX-T Data Center 等待的秒数。默认为 60 秒。

如果 NSX Edge 节点从远程对等站点收到响应，则会重新启动 DPD 探测间隔定时器。在发送下一个 DPD 探测后的 0.5 秒内，如果 NSX Edge 节点没有从对等站点收到响应，则会将重新发送定时器设置为 0.5 秒。在达到重新发送定时器后，NSX Edge 节点将重新发送下一个 DPD 探测。如果远程对等站点仍然没有响应，则重新发送定时器呈指数增加到最大限制（6 秒）。在每次重新发送定时器到期时，NSX Edge 节点继续重新发送 DPD 探测。在将对等站点声明为失效并解除失效对等站点链路上的安全关联 (Security Association, SA) 之前，NSX Edge 节点最多重新发送 30 次。重新发送 DPD 探测 30 次所花的总时间大约为 2 分 45 秒。

- 6 提供说明，然后根据需要添加标记。
- 7 单击 **保存**。

结果

将在可用 DPD 配置文件表中新添加一行。要编辑或删除非系统创建的配置文件，请单击三点菜单 (⋮)，然后从可用操作列表中选择。

将自治 Edge 添加为 L2 VPN 客户端

您可以使用 L2 VPN 将第 2 层网络扩展到不受 NSX-T Data Center 管理的站点。可以在站点上将自治 NSX Edge 部署为 L2 VPN 客户端。自治 NSX Edge 便于部署、可通过编程轻松实现，且可以提供高性能 VPN。可使用 OVF 文件在不受 NSX-T Data Center 管理的主机上部署自治 NSX Edge。您也可以通过部署主和辅助自治 L2 VPN Edge 客户端来启用 HA 以实现 VPN 冗余。

前提条件

- 创建端口组，并将其绑定到主机上的 vSwitch。
- 为内部 L2 扩展端口创建端口组。
- 获取本地 IP 和远程 IP 的 IP 地址以用于您正添加的 L2 VPN 客户端会话。
- 获取在 L2 VPN 服务器配置期间生成的对等代码。

步骤

- 1 使用 vSphere Web Client 登录到用于管理非 NSX 环境的 vCenter Server。
- 2 选择**主机和集群**，并展开集群以显示可用主机。
- 3 右键单击要安装自治 NSX Edge 的主机，然后选择**部署 OVF 模板**。
- 4 输入 URL 以从 Internet 下载并安装 OVF 文件，或单击**浏览**找到计算机中自治 NSX Edge 的 OVF 文件所在的文件夹，然后单击**下一步**。
- 5 在**选择名称和文件夹**页面上，输入自治 NSX Edge 的名称，并选择要在其中执行部署操作的文件夹或数据中心。然后，单击**下一步**。
- 6 在**选择计算资源**页面上，选择计算资源的目标。
- 7 在“OVF 模板详细信息”页面上，检查模板详细信息并单击**下一步**。
- 8 在**配置**页面上，选择一个部署配置选项。
- 9 在**选择存储**页面上，选择要存储配置文件和磁盘文件的位置。
- 10 在**选择网络**页面上，配置已部署模板必须使用的网络。选择为上行链路接口创建的端口组，即为 L2 扩展端口创建的端口组，然后输入 HA 接口。单击**下一步**。
- 11 在**自定义模板**页面上，输入以下值，然后单击**下一步**。
 - a 键入并再次键入 CLI 管理员密码。
 - b 键入并再次键入 CLI 启用密码。
 - c 键入并再次键入 CLI 根密码。
 - d 输入管理网络的 IPv4 地址。
 - e 输入 VLAN ID、退出接口、IP 地址和 IP 前缀长度的**外部端口**详细信息，以便退出接口映射到含有上行链路接口端口组的网络。
 如果退出接口已连接到中继端口组，请指定 VLAN ID。例如，**20,eth2,192.168.5.1,24**。您还可以使用 VLAN ID 配置端口组，并将 VLAN 0 用于**外部端口**。
 - f （可选）要配置高可用性，请输入 **HA 端口**详细信息，以便退出接口映射到相应 HA 网络。
 - g （可选）将自治 NSX Edge 部署为 HA 的辅助节点时，选择**将此自治 Edge 部署为辅助节点**。
 使用与主节点相同的 OVF 文件，并输入主节点的 IP 地址、用户名、密码和指纹。

要检索主节点的指纹，请登录到主节点，然后运行以下命令：

```
get certificate api thumbprint
```

确保主节点和辅助节点的 VTEP IP 地址位于同一子网中，且连接到相同的端口组。完成部署并启动辅助 Edge 后，辅助 Edge 会连接到主节点以形成一个 Edge 集群。

12 在**即将完成**页面上，检查自治 Edge 设置，然后单击**完成**。

注 如果部署过程中出现错误，CLI 上会显示当天的相关消息。您还可以使用 API 调用来检查错误：

```
GET https://<nsx-mgr>/api/v1/node/status
```

错误分为软错误 and 硬错误。可根据需要使用 API 调用来解决软错误。您可以使用 API 调用清除每日消息：

```
POST /api/v1/node/status?action=clear_bootup_error
```

13 打开自治 NSX Edge 设备的电源。

14 登录到自治 NSX Edge 客户端。

15 选择 **L2VPN > 添加会话**，然后输入以下值：

- a 输入一个会话名称。
- b 输入本地 IP 地址和远程 IP 地址。
- c 输入从 L2VPN 服务器获取的对等代码。有关获取对等代码的详细信息，请参见[下载远程端 L2 VPN 配置文件](#)。

16 单击**保存**。

17 选择**端口 > 添加端口**以创建 L2 扩展端口。

18 输入名称、VLAN，然后选择一个退出接口。

19 单击**保存**。

20 选择 **L2VPN > 连接端口**，然后输入以下值：

- a 选择您创建的 L2 VPN 会话。
- b 选择您创建的 L2 扩展端口。
- c 输入隧道 ID。

21 单击**连接**。

如果需要扩展多个 L2 网络，则可以创建更多 L2 扩展端口并将其连接到会话。

22 使用浏览器登录到自治 NSX Edge，或使用 API 调用查看 L2VPN 会话的状态。

注 如果 L2VPN 服务器配置发生变化，请确保再次下载对等代码并使用新的对等代码更新会话。

检查 IPsec VPN 会话的已实现状态

发送 IPsec VPN 会话的配置更新请求后，可以检查请求的状态是否已在传输节点上的 NSX-T Data Center 本地控制平面中成功处理。

创建 IPsec VPN 会话时，会创建多个实体：IKE 配置文件、DPD 配置文件、隧道配置文件、本地端点、IPsec VPN 服务和 IPsec VPN 会话。所有这些实体都共享同一个 IPsecVPNSession SPAN，因此可以使用相同的 GET API 调用获取 IPsec VPN 会话的所有实体的实现状态。可以仅使用 API 检查实现状态。

前提条件

- 熟悉 IPsec VPN。请参见[了解 IPsec VPN](#)。
- 确认已配置 IPsec VPN。请参见[添加 IPsec VPN 服务](#)。
- 您必须具有 NSX Manager API 的访问权限。

步骤

- 1 发送 POST、PUT 或 DELETE 请求 API 调用。

例如：

```
PUT https://<nsx-mgr>/api/v1/vpn/ipsec/sessions/8dd1c386-9b2c-4448-85b8-51ff649fae4f
{
  "resource_type": "PolicyBasedIPsecVPNSession",
  "id": "8dd1c386-9b2c-4448-85b8-51ff649fae4f",
  "display_name": "Test RZ_UPDATED",
  "ipsec_vpn_service_id": "7adfa455-a6fc-4934-a919-f5728957364c",
  "peer_endpoint_id": "17263ca6-dce4-4c29-bd8a-e7d12bd1a82d",
  "local_endpoint_id": "91ebfa0a-820f-41ab-bd87-f0fb1f24e7c8",
  "enabled": true,
  "policy_rules": [
    {
      "id": "1026",
      "sources": [
        {
          "subnet": "1.1.1.0/24"
        }
      ],
      "logged": true,
      "destinations": [
        {
          "subnet": "2.1.4..0/24"
        }
      ],
      "action": "PROTECT",
      "enabled": true,
      "_revision": 1
    }
  ]
}
```

- 2 在返回的响应标头中找到 `x-nsx-requestid` 的值并复制。

例如：

```
x-nsx-requestid    e550100d-f722-40cc-9de6-cf84d3da3ccb
```

- 3 使用以下 GET 调用请求 IPsec VPN 会话的实现状态。

```
GET https://<nsx-mgr>/api/v1/vpn/ipsec/sessions/<ipsec-vpn-session-id>/state?request_id=<request-id>
```

以下 API 调用使用上述步骤所用示例中的 `id` 和 `x-nsx-requestid` 值。

```
GET https://<nsx-mgr>/api/v1/vpn/ipsec/sessions/8dd1c386-9b2c-4448-85b8-51ff649fae4f/state?request_id=e550100d-f722-40cc-9de6-cf84d3da3ccb
```

以下是实现状态为 `in_progress` 时收到的响应示例。

```
{
  "details": [
    {
      "sub_system_type": "TransportNode",
      "sub_system_id": "fe651e63-04bd-43a4-a8ec-45381a3b71b9",
      "state": "in_progress",
      "failure_message": "CCP Id:ab5958df-d98a-468e-a72b-d89dcdae5346, Message:State realization is in progress at the node."
    },
    {
      "sub_system_type": "TransportNode",
      "sub_system_id": "ebe174ac-e4f1-4135-ba72-3dd2eb7099e3",
      "state": "in_sync"
    }
  ],
  "state": "in_progress",
  "failure_message": "The state realization is in progress at transport nodes."
}
```

以下是实现状态为 `in_sync` 时收到的响应示例。

```
{
  "details": [
    {
      "sub_system_type": "TransportNode",
      "sub_system_id": "7046e8f4-a680-11e8-9bc3-020020593f59",
      "state": "in_sync"
    }
  ],
  "state": "in_sync"
}
```

以下是实现状态为 unknown 时可能收到的响应示例。

```
{
  "state": "unknown",
  "failure_message": "Unable to get response from any CCP node. Please retry operation
after some time."
}
```

```
{
  "details": [
    {
      "sub_system_type": "TransportNode",
      "sub_system_id": "3e643776-5def-11e8-94ae-020022e7749b",
      "state": "unknown",
      "failure_message": "CCP Id:ab5958df-d98a-468e-a72b-d89dcdae5346, Message: Unable
to get response from the node. Please retry operation after some time."
    },
    {
      "sub_system_type": "TransportNode",
      "sub_system_id": "4784ca0a-5def-11e8-93be-020022f94b73",
      "state": "in_sync"
    }
  ],
  "state": "unknown",
  "failure_message": "The state realization is unknown at transport nodes"
}
```

执行实体 DELETE 操作后，可能会收到 NOT_FOUND 状态，如下例所示。

```
{
  "http_status": "NOT_FOUND",
  "error_code": 600,
  "module_name": "common-services",
  "error_message": "The operation failed because object identifier LogicalRouter/
61746f54-7ab8-4702-93fe-6ddeb804 is missing: Object identifiers are case sensitive.."
}
```

如果禁用与会话关联的 IPsec VPN 服务，则会收到 BAD_REQUEST 响应，如下例所示。

```
{
  "httpStatus": "BAD_REQUEST",
  "error_code": 110199,
  "module_name": "VPN",
  "error_message": "VPN service f9cfe508-05e3-4e1d-b253-fed096bb2b63 associated with the
session 8dd1c386-9b2c-4448-85b8-51ff649fae4f is disabled. Can not get the realization
status."
}
```

监控 VPN 会话和排除其故障

配置 IPsec 或 L2 VPN 会话后，可以使用 NSX Manager 用户界面监控 VPN 隧道状态，并对报告的任何隧道问题进行故障排除。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 导航到**网络 > VPN > IPsec 会话**或**网络 > VPN > L2 VPN 会话**选项卡。
- 3 展开要监控或排除故障的 VPN 会话所在的行。
- 4 要查看 VPN 隧道状态，请单击信息图标。
将显示“状态”对话框，并列出可用的状态。
- 5 要查看 VPN 隧道流量统计信息，请在“状态”列中单击**查看统计信息**。
“统计信息”对话框将显示 VPN 隧道的流量统计信息。
- 6 要查看错误统计信息，请在“统计信息”对话框中单击**查看更多**链接。
- 7 要关闭**统计信息**对话框，请单击**关闭**。

网络地址转换 (NAT) 将一个 IP 地址空间映射到另一个 IP 地址空间。可以在 Tier-0 和 Tier-1 网关上配置 NAT。

本章讨论了以下主题：

- 在网关上配置 NAT

在网关上配置 NAT

可以在 Tier-0 或 Tier-1 网关上配置源 NAT (SNAT)、目标 NAT (DNAT) 或反射 NAT。

如果 Tier-0 网关在活动-活动模式下运行，则无法配置 SNAT 或 DNAT，因为不对称的路径可能会导致出现问题。只能配置反射 NAT（有时称为无状态 NAT）。如果 Tier-0 网关在活动-备用模式下运行，则可以配置 SNAT、DNAT 或反射 NAT。

还可以为 IP 地址或地址范围禁用 SNAT 或 DNAT。如果某个地址具有多个 NAT 规则，将应用具有最高优先级的规则。

注 配置了基于策略的 IPsec VPN 的 Tier-1 网关上不支持 DNAT。

在 Tier-0 网关的一个外部接口上配置的 SNAT 将处理来自 Tier-1 网关以及 Tier-0 网关上另一个外部接口的流量。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**网络 > NAT**。
- 3 选择网关。
- 4 单击**添加 NAT 规则**。
- 5 选择操作。

对于 Tier-1 网关，可用操作包括 **SNAT**、**DNAT**、**反射**、**无 SNAT** 和**无 DNAT**。

对于活动-备用模式下的 Tier-0 网关，可用操作包括 **SNAT**、**DNAT**、**无 SNAT** 和**无 DNAT**。

对于活动-活动模式下的 Tier-0 网关，可用操作为**反射**。

- 6 在**服务列**中，单击**设置**以选择服务。

- 7 （必选）对于**源 IP**，以 CIDR 格式指定一个 IP 地址或 IP 地址范围。

如果将此字段留空，此 NAT 规则将应用于本地子网外部的所有源。

- 8 对于**目标 IP**，以 CIDR 格式指定一个 IP 地址或 IP 地址范围。

- 9 对于**转换的 IP**，以 CIDR 格式指定一个 IP 地址或 IP 地址范围。

- 10 输入**转换的端口**的值。

- 11 从以下选项选择一个防火墙设置：

- **匹配外部地址** - 通过与转换的 IP 地址和转换的端口组合相匹配的防火墙规则处理数据包。
 - 对于 SNAT，外部地址是执行 NAT 后转换的源地址。
 - 对于 DNAT，外部地址是执行 NAT 之前的原始目标地址。
 - 对于“反射”，针对输出流量，防火墙将在执行 NAT 之后应用于转换后的源地址。针对输入流量，防火墙将在执行 NAT 之前应用于原始目标地址。
- **匹配内部地址** - 通过与原始 IP 地址和原始端口的组合相匹配的防火墙规则处理数据包。
 - 对于 SNAT，内部地址是执行 NAT 之前的原始源地址。
 - 对于 DNAT，内部地址是执行 NAT 后转换的目标地址。
 - 对于“反射”，针对输出流量，防火墙将在执行 NAT 之前应用于原始源地址。针对输入流量，防火墙将在执行 NAT 之后应用于转换后的目标地址。
- **绕过** - 数据包绕过防火墙规则。

- 12 （必选）更改日志记录状态。

- 13 （必选）对于**应用对象**，选择应用此规则的对象。

可用对象包括 **Tier-0 网关、接口、标签、服务实例端点和虚拟端点**。

- 14 指定优先级值。

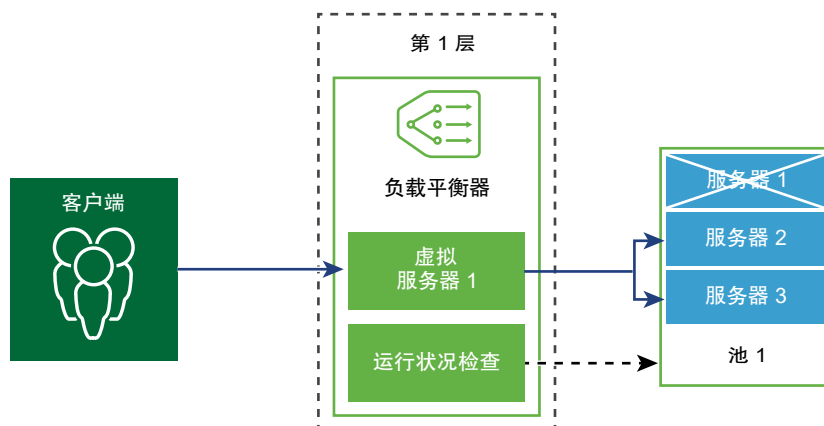
较低的值意味着更高的优先级。默认值为 100。

- 15 单击**保存**。

负载均衡

7

NSX-T Data Center 逻辑负载均衡器为应用程序提供高可用性服务并将网络流量负载分布在多个服务器之间。



负载均衡器将入站服务请求均匀分布在多个服务器中，从方式上确保负载分配对用户透明。负载均衡有助于实现最佳的资源利用率，最大程度地提高吞吐量和减少响应时间，并避免过载。

您可以将虚拟 IP 地址映射到一组池服务器进行负载均衡。负载均衡器可接受虚拟 IP 地址上的 TCP、UDP、HTTP 或 HTTPS 请求，并确定要使用的池服务器。

根据环境要求，您可以增加现有的虚拟服务器和池成员来处理繁重的网络流量负载，从而提高负载均衡器性能。

注 仅在 Tier-1 网关上支持逻辑负载均衡器。一个负载均衡器只能连接到一个 Tier-1 网关。

本章讨论了以下主题：

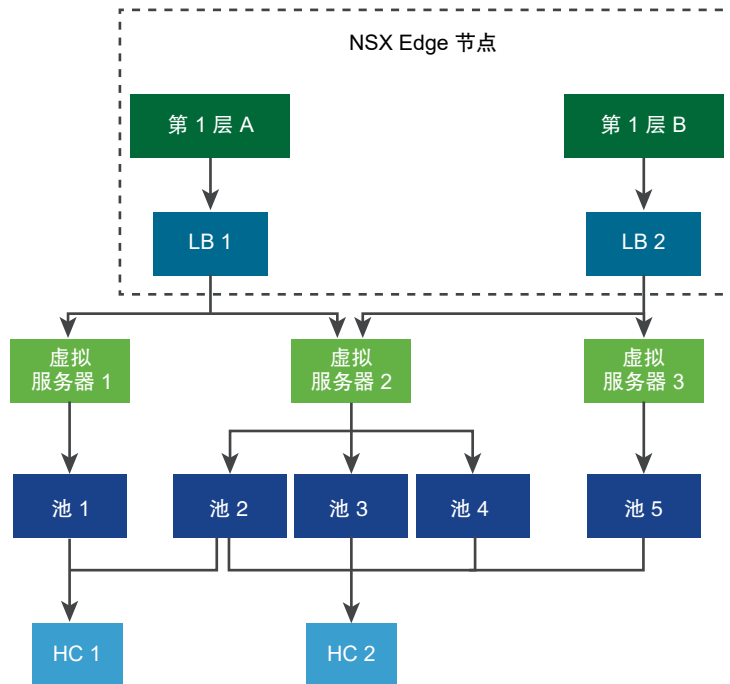
- 负载均衡器重要概念
- 设置负载均衡器组件
- 为服务器池和虚拟服务器创建的组

负载均衡器重要概念

负载均衡器包括虚拟服务器、服务器池和运行状况检查监控器。

负载均衡器连接到 Tier-1 逻辑路由器。负载均衡器托管一个或多个虚拟服务器。虚拟服务器是应用程序服务的一种抽象，由 IP、端口和协议的唯一组合表示。虚拟服务器与单个到多个服务器池相关联。服务器池包含一组服务器。服务器池包括各个服务器池成员。

要测试每个服务器是否在正常运行应用程序，您可以添加运行状况检查监控器来检查服务器的运行状况。



缩放负载均衡器资源

配置负载均衡器时，您可以指定大小（小型、中型或大型）。该大小决定了负载均衡器可以支持的虚拟服务器、服务器池和池成员的数量。

负载均衡器在 Tier-1 网关上运行，该网关必须处于“活动-备用”模式。网关在 NSX Edge 节点上运行。NSX Edge 节点的规格（裸机、小型、中型或大型）决定了 NSX Edge 节点可以支持的负载均衡器数量。请注意，在**高级网络和安全**选项卡上，使用逻辑路由器一词来指示网关。

有关不同负载均衡大小和 NSX Edge 规格可以支持的内容的详细信息，请参见 <https://configmax.vmware.com>。

注意，不建议在生产环境中使用小型 NSX Edge 节点运行小型负载均衡器。

您可以调用 API 以获取 NSX Edge 节点的负载均衡器使用情况信息：如果使用**网络**选项卡来配置负载均衡，请运行以下命令：

```
GET /policy/api/v1/infra/lb-node-usage?node_path=<node-path>
```

如果使用**高级网络和安全**选项卡来配置负载均衡，请运行以下命令：

GET /api/v1/loadbalancer/usage-per-node/<node-id>

使用情况信息包括在节点上配置的负载均衡器对象的数量（如负载均衡器服务、虚拟服务器、服务器池和池成员）。有关详细信息，请参阅《NSX-T Data Center API 指南》。

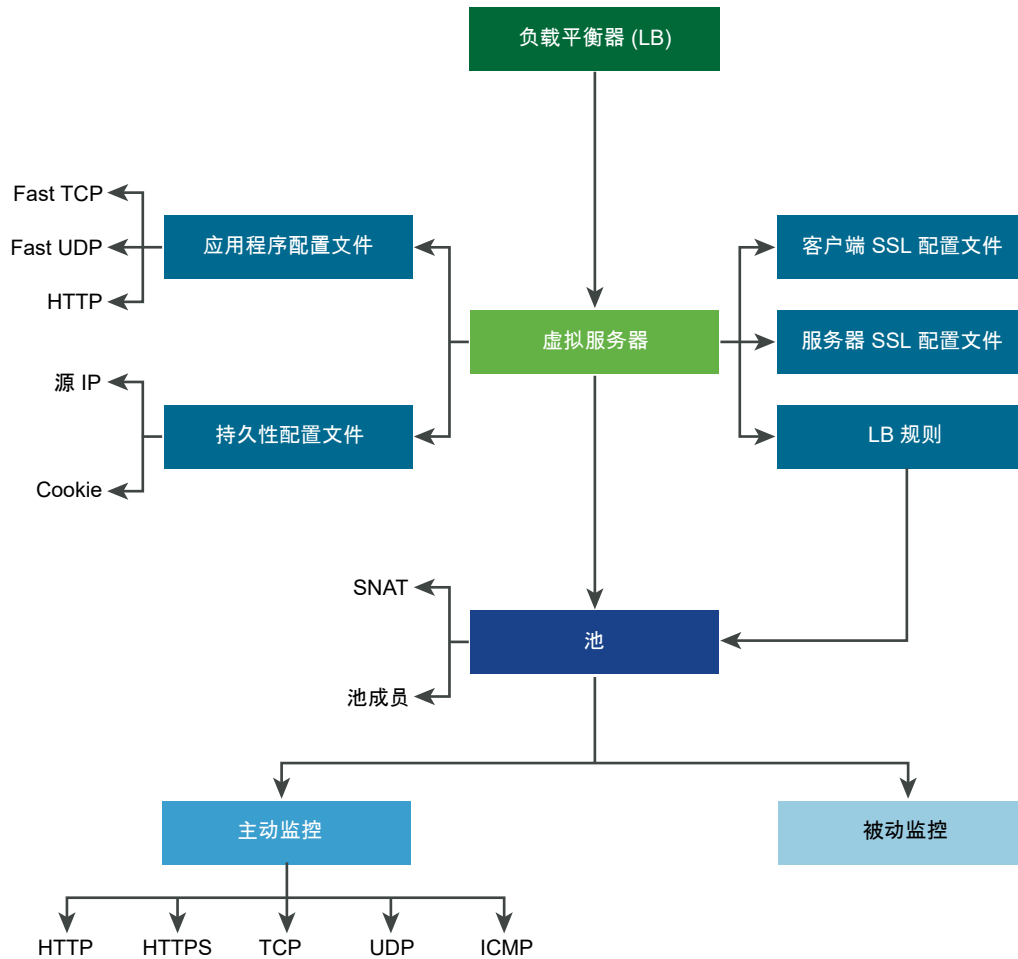
支持的负载均衡器功能

NSX-T Data Center 负载均衡器支持以下功能。

- 第 4 层 - TCP 和 UDP
- 第 7 层 - 支持负载均衡器规则的 HTTP 和 HTTPS
- 服务器池 - 静态和动态（含 NS 组）
- 持久性 - 源 IP 和 Cookie 持久性模式
- 运行状况检查监控器 - 主动监控器（包括 HTTP、HTTPS、TCP、UDP 和 ICMP）和被动监控器
- SNAT - 透明、自动映射和 IP 列表
- HTTP 升级 - 对于使用 HTTP 升级的应用程序（例如 WebSocket），为支持的 HTTP 升级客户端或服务器。默认情况下，NSX-T Data Center 使用 HTTP 应用程序配置文件来支持并接受 HTTPS 升级客户端请求。

为检测非活动客户端或服务器通信，负载均衡器使用 HTTP 应用程序配置文件响应超时功能（设置为 60 秒）。如果服务器未在 60 秒间隔内发送流量，NSX-T Data Center 将终止客户端和服务器端的连接。

注意：SSL 终止模式和代理模式在 NSX-T Data Center Limited Export 版本中不受支持。

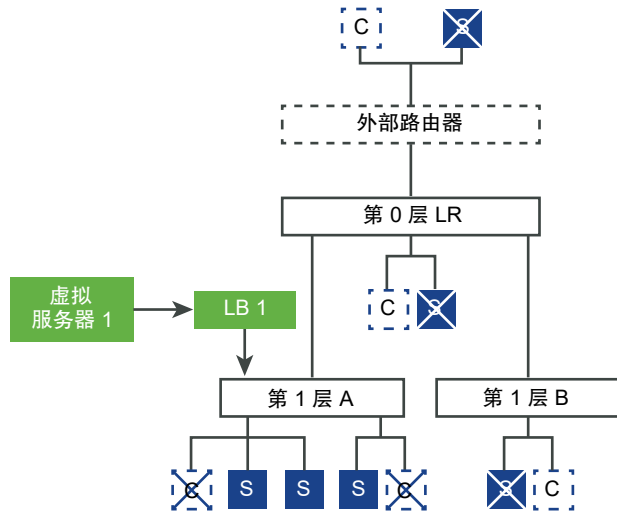


负载均衡器拓扑

负载均衡器通常在内嵌或单臂模式下部署。单臂模式需要虚拟服务器源 NAT (SNAT) 配置，而内嵌模式则不需要。

内嵌拓扑

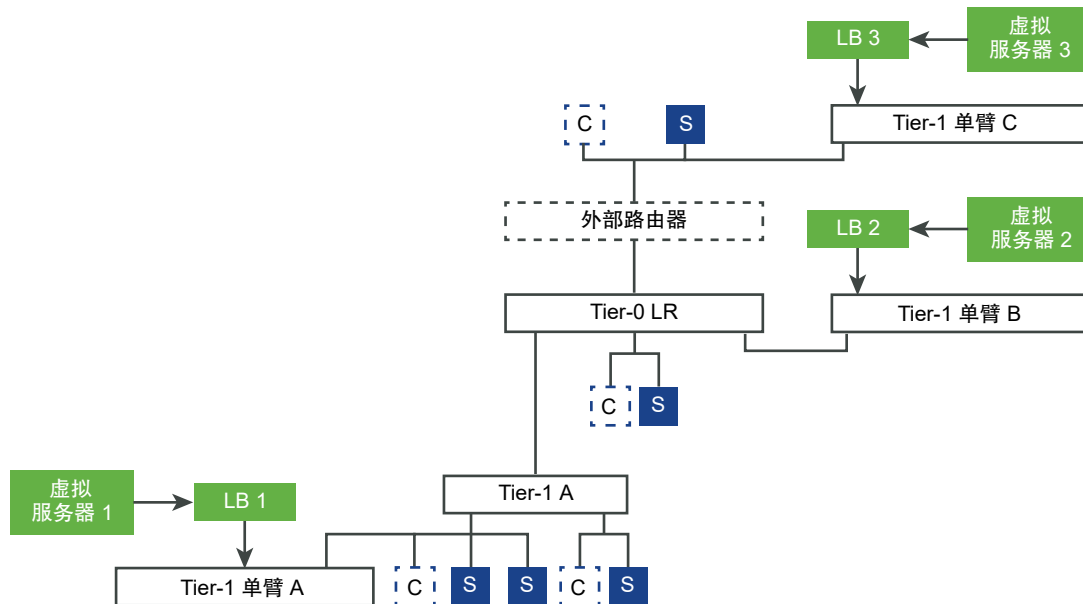
在内嵌模式下，负载均衡器位于客户端和服务端之间的流量路径中。如果负载均衡器上的 **SNAT** 不是所需的配置，则不应将客户端和服务端连接到同一个 Tier-1 逻辑路由器上的覆盖网络分段。如果客户端和服务端连接到同一个 Tier-1 逻辑路由器上的覆盖网络分段，则需要 **SNAT**。



单臂拓扑

在单臂模式下，负载均衡器不位于客户端和服务端之间的流量路径中。在此模式下，客户端和服务端可以是任意位置。负载均衡器执行源 NAT (SNAT) 以强制返回从服务器发送到客户端的流量，使其通过负载均衡器。此拓扑需要启用虚拟服务器 SNAT。

当负载均衡器收到发往虚拟 IP 地址的客户端流量时，负载均衡器会选择一个服务器池成员并将客户端流量转发给该成员。在单臂模式下，负载均衡器将客户端 IP 地址替换为负载均衡器 IP 地址，以便服务器响应始终发送到负载均衡器。负载均衡器会将该响应转发给客户端。



Tier-1 服务链

如果 Tier-1 网关或逻辑路由器托管不同的服务（如 NAT、防火墙和负载均衡器），则将按照以下顺序应用这些服务：

- 输入

DNAT - 防火墙 - 负载均衡器

注意：如果 DNAT 配置了防火墙绕过，则将跳过防火墙，但不会跳过负载均衡器。

■ 输出

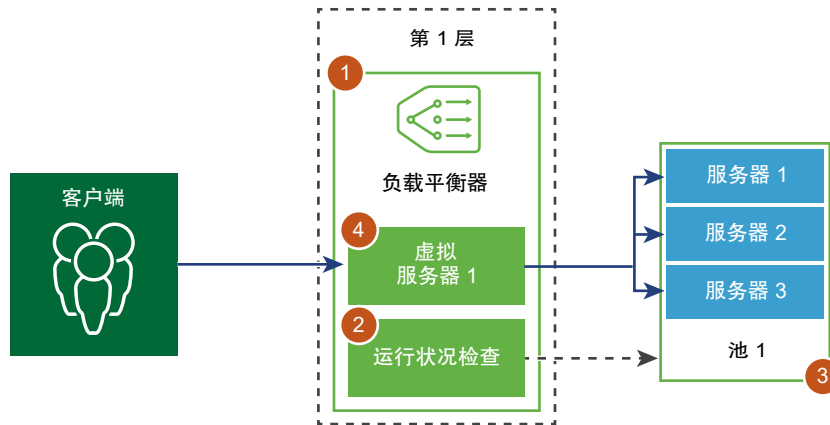
负载均衡器 - 防火墙 - SNAT

设置负载均衡器组件

要使用逻辑负载均衡器，必须首先配置负载均衡器并将其连接到 Tier-1 网关。

注 在**高级和安全**选项卡中，术语 Tier-1 逻辑路由器用于指 Tier-1 网关。

接下来，设置服务器的运行状况检查监控。然后，必须为负载均衡器配置服务器池。最后，必须为负载均衡器创建第 4 层或第 7 层虚拟服务器，并将新创建的虚拟服务器连接到负载均衡器。



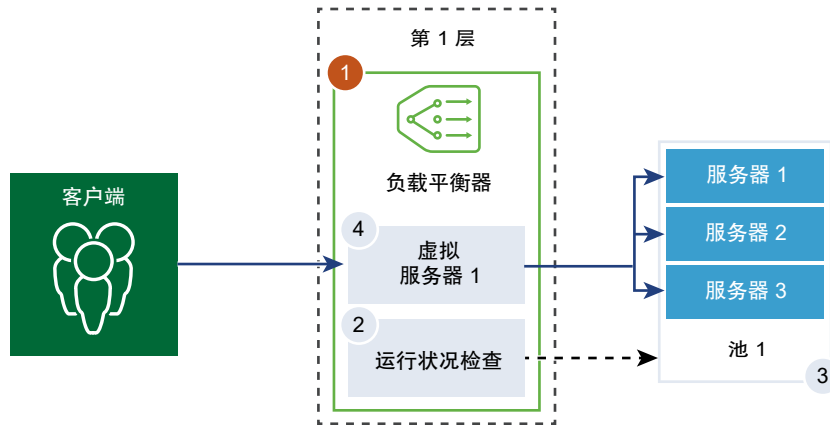
添加负载均衡器

创建负载均衡器并将其连接到 Tier-1 网关。

注 在**高级和安全**选项卡中，术语 Tier-1 逻辑路由器用于指 Tier-1 网关。

您可以配置希望负载均衡器添加到错误日志的错误消息级别。

注 如果输出到日志的消息数量既影响性能又会产生巨大流量，则在此类负载均衡器上，避免将日志级别设置为调试。



前提条件

确认配置了一个 Tier-1 网关。请参见第 3 章 [Tier-1 网关](#)。

步骤

1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。

2 选择 **网络 > 负载均衡 > 添加负载均衡器**。

3 输入负载均衡器的名称和描述。

4 根据可用资源选择负载均衡器的虚拟服务器大小和池成员数量。

5 从下拉菜单中选择要连接到此负载均衡器的已配置 Tier-1 网关。

Tier-1 网关必须处于主动-备用模式。

6 在下拉菜单中定义错误日志的严重性级别。

负载均衡器将遇到的不同严重性级别的问题的相关问题收集到错误日志。

7 （可选）输入标记可使搜索变得更容易。

可以指定一个标记以设置标记的范围。

8 单击 **保存**。

创建负载均衡器并将负载均衡器连接到 Tier-1 网关大约需要三分钟，且配置状态显示为绿色和“开启”。

如果状态为“关闭”，请单击信息图标并解决错误，然后再继续。

9 （可选）删除负载均衡器。

a 将负载均衡器与虚拟服务器和 Tier-1 网关断开连接。

b 选择负载均衡器。

c 单击垂直省略号按钮。

d 选择 **删除**。

添加主动监控器

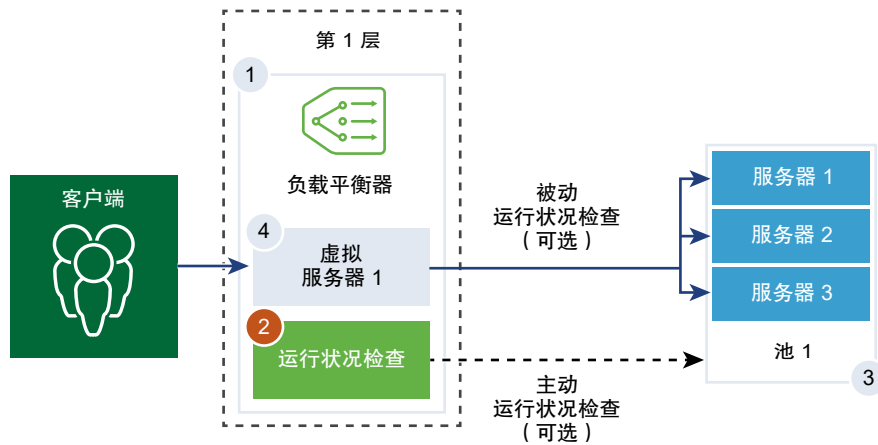
主动运行状况监控器用于检测服务器是否可用。主动运行状况监控器使用几种类型的测试，例如，向服务器发送基本的 ping 操作，或发送高级 HTTP 请求以监控应用程序运行状况。

注 在**高级和安全**选项卡中，术语 Tier-1 逻辑路由器用于指 Tier-1 网关。

无法在特定时段内做出响应或响应错误的服务器将从未来的连接处理中排除，直到后续的定期运行状况检查认为这些服务器处于正常状态为止。

当服务器池成员连接到某个虚拟服务器且该虚拟服务器连接到 Tier-1 网关后，会对池成员执行主动运行状况检查。Tier-1 上行链路 IP 地址用于运行状况检查。

注 可以为每个服务器池配置一个主动运行状况监控器。



步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**网络 > 负载均衡 > 监控器 > 主动 > 添加主动监控器**。
- 3 从下拉菜单中为服务器选择协议。

也可以将预定义协议（HTTP、HTTPS、ICMP、TCP 和 UDP）用于 NSX Manager。

- 4 选择 **HTTP** 协议。
- 5 配置用于监控服务池的值。

您也可以接受主动运行状况监控器的默认值。

选项	说明
名称和说明	输入主动运行状况监控器的名称和描述。
监控端口	设置监控端口的值。
监控间隔	设置监控器向服务器发送另一个连接请求的时间（秒）。
超时期限	设置在将服务器视为 DOWN 之前测试的次数。

选项	说明
失败检查计数	设置一个值，当连续失败的次数达到此值时，服务器被视为暂时不可用。
成功检查计数	设置一个数字，在此超时期限过后，服务器会再次尝试建立新连接，以查看其是否可用。
标记	输入标记可使搜索变得更容易。 可以指定一个标记以设置标记的范围。

例如，如果监控间隔设置为 5 秒且超时设置为 15 秒，则负载均衡器会每 5 秒向服务器发送一次请求。在每次探测中，如果在 15 秒内收到来自服务器的预期响应，则运行状况检查结果为 OK。如果没有收到响应，则结果为 CRITICAL。如果最近三次的运行状况检查结果均为 UP，则服务器将被视为 UP。

6 单击配置。

7 输入 HTTP 请求和响应的配置详细信息。

选项	说明
HTTP 方法	从下拉菜单中选择检测服务器状态的方法：GET、OPTIONS、POST、HEAD 和 PUT。
HTTP 请求 URL	输入方法的请求 URI。
HTTP 请求版本	从下拉菜单中选择支持的请求版本。 也可以接受默认版本 HTTP_VERSION_1。
HTTP 响应标头	单击 添加 ，然后输入 HTTP 响应标头名称和对应的值。 默认标头值为 4000。最大标头值为 64,000。
HTTP 请求正文	输入请求正文。 对 POST 和 PUT 方法有效。
HTTP 响应代码	输入监控器要求与 HTTP 响应正文状态行匹配的字符串。 响应代码是以逗号分隔的列表。 例如，200,301,302,401。
HTTP 响应正文	如果 HTTP 响应正文字符串与 HTTP 运行状况检查响应正文匹配，则将服务器视为正常。

8 选择 HTTPS 协议。

9 完成步骤 5。

10 单击配置。

11 输入 HTTP 请求和响应以及 SSL 配置详细信息。

选项	说明
名称和说明	输入主动运行状况监控器的名称和描述。
HTTP 方法	从下拉菜单中选择检测服务器状态的方法：GET、OPTIONS、POST、HEAD 和 PUT。
HTTP 请求 URL	输入方法的请求 URI。
HTTP 请求版本	从下拉菜单中选择支持的请求版本。 也可以接受默认版本 HTTP_VERSION_1。

选项	说明
HTTP 响应标头	单击 添加 ，然后输入 HTTP 响应标头名称和对应的值。 默认标头值为 4000。最大标头值为 64,000。
HTTP 请求正文	输入请求正文。 对 POST 和 PUT 方法有效。
HTTP 响应代码	输入监控器要求与 HTTP 响应正文状态行匹配的字符串。 响应代码是以逗号分隔的列表。 例如，200,301,302,401。
HTTP 响应正文	如果 HTTP 响应正文字符串与 HTTP 运行状况检查响应正文匹配，则将服务器视为正常。
服务器 SSL	切换该按钮以启用 SSL 服务器。
客户端证书	(可选) 从下拉菜单中选择一个证书，以在服务器未托管同一 IP 地址上的多个主机名或客户端不支持 SNI 扩展时使用。
服务器 SSL 配置文件	(可选) 从下拉菜单中分配一个定义可重用的和独立于应用程序的客户端 SSL 属性的默认 SSL 配置文件。 单击垂直省略号，并创建自定义 SSL 配置文件。
受信任的 CA 证书	(可选) 可以要求客户端具有 CA 证书以进行身份验证。
强制服务器身份验证	(可选) 切换该按钮以启用服务器身份验证。
证书链深度	(可选) 为客户端证书链设置身份验证深度。
证书吊销列表	(可选) 在客户端 SSL 配置文件中设置证书吊销列表 (CRL) 以拒绝损坏的客户端证书。

12 选择 **ICMP** 协议。

13 完成步骤 5，并分配 ICMP 运行状况检查数据包的数据大小（字节）。

14 选择 **TCP** 协议。

15 完成步骤 5，可以将 TCP 数据参数留空。

如果发送的数据和预期数据均未列出，则建立三次握手 TCP 连接来验证服务器运行状况。不会发送数据。

列出的预期数据必须是字符串。不支持正则表达式。

16 选择 **UDP** 协议。

17 完成步骤 5 并配置 UDP 数据。

必需选项	说明
发送的 UDP 数据	输入要在建立连接后发送到服务器的字符串。
预期 UDP 数据	输入要从服务器接收的字符串。 只有在收到的字符串与该定义匹配时，才会将服务器视为 UP。

后续步骤

将主动运行状况监控器与服务器池相关联。请参见[添加服务器池](#)。

添加被动监控器

负载均衡器执行被动运行状况检查以在客户端连接期间监控故障，并将导致一致故障的服务器标记为 DOWN。

被动运行状况检查可监控通过负载均衡器的客户端流量是否出现故障。例如，如果池成员发送 TCP 重置 (RST) 以响应客户端连接，则负载均衡器会检测到该故障。如果连续发生多次故障，则负载均衡器会将服务器池成员视为暂时不可用，并在一段时间内停止向该池成员发送连接请求。一段时间后，负载均衡器会发送连接请求以验证池成员是否已恢复。如果该连接成功，则将池成员视为正常。否则，负载均衡器会等待一段时间，然后重试。

被动运行状况检查将以下情况视为客户端流量故障。

- 对于与第 7 层虚拟服务器关联的服务器池，如果与池成员的连接失败。例如，如果池成员在负载均衡器尝试在负载均衡器与池成员之间连接或执行 SSL 握手失败时发送 TCP RST。
- 对于与第 4 层 TCP 虚拟服务器关联的服务器池，如果池成员发送 TCP RST 以响应客户端 TCP SYN 或完全不响应。
- 对于与第 4 层 UDP 虚拟服务器关联的服务器池，如果收到 ICMP 错误消息（端口或目标无法访问）以响应客户端 UDP 数据包。

对于与第 7 层虚拟服务器关联的服务器池，发生任何 TCP 连接错误（例如，TCP RST 发送数据失败或 SSL 握手失败）时，失败的连接计数将递增。

对于与第 4 层虚拟服务器关联的服务器池，如果未收到对发送给服务器池成员的 TCP SYN 的响应或收到 TCP RST 以响应 TCP SYN，则将服务器池成员视为 DOWN。失败计数将递增。

对于第 4 层 UDP 虚拟服务器，如果收到 ICMP 错误消息（例如，端口或目标无法访问）以响应客户端通信，则将其视为 DOWN。

注 可以为每个服务器池配置一个被动运行状况监控器。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择 **网络 > 负载均衡 > 监控器 > 被动 > 添加被动监控器**。
- 3 输入被动运行状况监控器的名称和描述。
- 4 配置用于监控服务池的值。

您也可以接受主动运行状况监控器的默认值。

选项	说明
失败检查计数	设置一个值，当连续失败的次数达到此值时，服务器被视为暂时不可用。
超时期限	设置在将服务器视为 DOWN 之前测试的次数。
标记	输入标记可使搜索变得更容易。 可以指定一个标记以设置标记的范围。

例如，当连续故障次数达到配置值 5 时，则将该成员视为在 5 秒内暂时不可用。在此期限过后，该成员会再次尝试建立新连接，以查看其是否可用。如果该连接成功，则将该成员视为可用，失败计数将设置为零。但是，如果该连接失败，则它不用于另一个 5 秒超时间隔。

后续步骤

将被动运行状况监控器与服务器池相关联。请参见[添加服务器池](#)。

添加服务器池

服务器池包含一个或多个已配置并运行相同应用程序的服务器。可以将单个池与第 4 层和第 7 层虚拟服务器相关联。

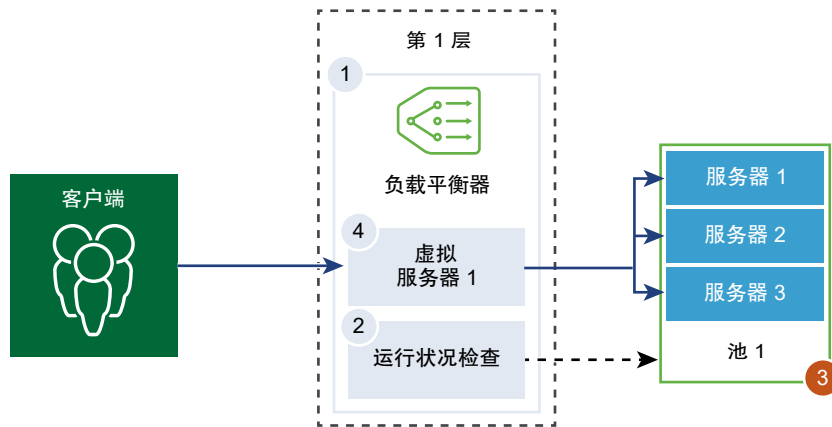
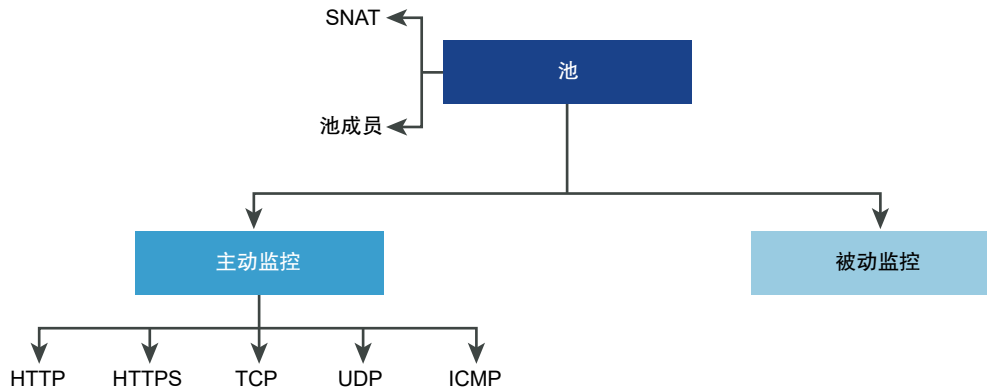


图 7-1. 服务器池参数配置



前提条件

- 如果使用动态池成员，则必须配置 NS 组。请参见[创建 NS 组](#)。
- 确认配置了被动运行状况监控器。请参见[添加被动监控器](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择网络 > 负载均衡 > 服务器池 > 添加服务器池。

3 输入负载均衡器服务器池的名称和说明。

您可以选择描述由服务器池管理的连接。

4 选择服务器池的算法平衡方法。

负载均衡算法控制如何在成员之间分发入站连接。可以直接在服务器池或服务器上使用该算法。

所有负载均衡算法均跳过满足以下任何条件的服务器：

- 管理状态设置为 **DISABLED**
- 管理状态设置为 **GRACEFUL_DISABLED** 且没有匹配的持久性条目
- 主动或被动运行状况检查状态为 **DOWN**
- 达到服务器池最大并发连接数的连接限制。

选项	说明
ROUND_ROBIN	在能够处理入站客户端请求的可用服务器列表中循环遍历请求。 忽略服务器池成员权重（即使已配置）。
WEIGHTED_ROUND_ROBIN	每个服务器都会分配到一个权重值，表示该服务器相对于池中其他服务器的性能。 该值决定了发送到某个服务器的客户端请求数量（与池中的其他服务器相比）。 此负载均衡算法侧重于在可用服务器资源之间公平地分发负载。
LEAST_CONNECTION	根据服务器上已存在的连接数将客户端请求分发到多个服务器。 新连接会被发送到连接数最少的服务器。忽略服务器池成员权重（即使已配置）。
WEIGHTED_LEAST_CONNECTION	每个服务器都会分配到一个权重值，表示该服务器相对于池中其他服务器的性能。 该值决定了发送到某个服务器的客户端请求数量（与池中的其他服务器相比）。 此负载均衡算法侧重于使用权重值在可用服务器资源之间分布负载。 默认情况下，如果未配置权重值且已启用启动缓慢，则权重值为 1。
IP-HASH	根据源 IP 地址的哈希值以及所有运行的服务器的总权重选择服务器。

5 选择服务器池成员。

服务器池由一个或多个池成员组成。

选项	说明
输入各个成员	<p>输入池成员名称、IP 地址和端口。</p> <p>可为每个服务器池成员配置一个权重，用于负载均衡算法。该权重表示给定池成员相对于同一池中其他成员的负载处理能力。</p> <p>您可以设置服务器池管理状态。默认情况下，此选项在添加服务器池成员时启用。</p> <p>如果禁用此选项，将处理活动连接，不会为新连接选择服务器池成员。新连接将被分配到池的其他成员。</p> <p>如果正常禁用，它允许您移除服务器以进行维护。在此状态下，与服务器池中成员的现有连接将继续得到处理。</p> <p>切换按钮可将池成员指定为备用成员，从而使用运行状况监控器提供主动-备用状态。如果活动成员未通过运行状况检查，则会对备用成员执行流量故障切换。在服务器选择期间将跳过备用成员。当服务器池处于非活动状态时，入站连接将仅发送到使用抱歉页面（指示应用程序不可用）配置的备用成员。</p> <p>最大并发连接值分配最大连接数，以便服务器池成员在服务器选择期间不会过载和跳过。如果未指定值，则连接数无限制。</p>
选择组	<p>选择预先配置的服务器池成员组。</p> <p>输入组名称和可选的说明。</p> <p>从现有列表设置计算成员或创建一个。您可以指定成员资格条件，选择组的成员，添加 IP 和 MAC 地址作为组成员，以及添加 Active Directory 组。通过身份成员与计算成员相交来定义组的成员资格。</p> <p>输入标记可使搜索变得更容易。可以指定一个标记以设置标记的范围。</p> <p>您可以选择定义最大组 IP 地址列表。</p>

6 从下拉菜单中选择服务器池的主动运行状况监控器。

负载均衡器向服务器定期发送 ICMP ping 以独立于数据流量验证运行状况。您只能为每个服务器池配置一个活动运行状况检查监控器。

7 选择“源 NAT (SNAT)”转换模式。

根据拓扑，可能需要 SNAT，以便负载均衡器接收从服务器发送到客户端的流量。可以针对每个服务器池启用 SNAT。

模式	说明
自动映射模式	<p>负载均衡器使用接口 IP 地址和临时端口继续与最初连接到服务器已建立的侦听端口之一的客户端进行通信。</p> <p>需要 SNAT。</p> <p>启用端口过载，这样如果元组（源 IP、源端口、目标 IP、目标端口和 IP 协议）在执行 SNAT 过程后是唯一的，则允许对多个连接使用相同的 SNAT IP 和端口。</p> <p>您还可以设置端口过载系数，以允许某个端口可同时用于多个连接的最大次数。</p>
禁用	禁用 SNAT 转换模式。
IP 池	<p>指定单个 IP 地址范围（例如，1.1.1.1-1.1.1.10），以便在连接到池中的任何服务器时用于 SNAT。</p> <p>默认情况下，对配置的所有 SNAT IP 地址使用端口范围 4000-64000。端口范围 1000-4000 是留给从 Linux 应用程序启动的运行状况检查和连接等用途的。如果存在多个 IP 地址，则以轮循方式选择这些地址。</p> <p>启用端口过载，这样如果元组（源 IP、源端口、目标 IP、目标端口和 IP 协议）在执行 SNAT 过程后是唯一的，则允许对多个连接使用相同的 SNAT IP 和端口。</p> <p>您还可以设置端口过载系数，以允许某个端口可同时用于多个连接的最大次数。</p>

8 切换按钮以启用 TCP 多路复用。

通过 TCP 多路复用，可以在负载均衡器和服务器之间使用相同的 TCP 连接，从而发送来自不同客户端 TCP 连接的多个客户端请求。

9 设置每个池为发送将来的客户端请求而保持活动状态的最大 TCP 多路复用连接数。

10 输入服务器池必须始终维护的最小活动成员数量。

11 从下拉菜单中选择服务器池的被动运行状况监控器。

12 输入标记可使搜索变得更容易。

可以指定一个标记以设置标记的范围。

设置虚拟服务器组件

您可以设置第 4 层和第 7 层虚拟服务器并配置多个虚拟服务器组件，例如应用程序配置文件、持久配置文件以及负载均衡器规则。

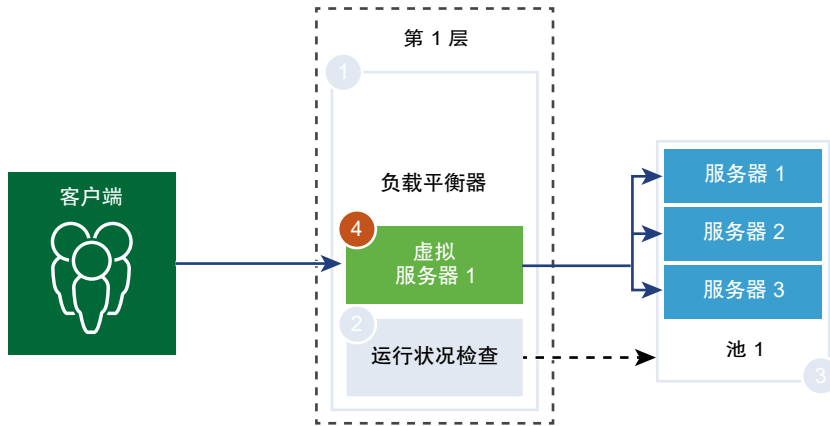
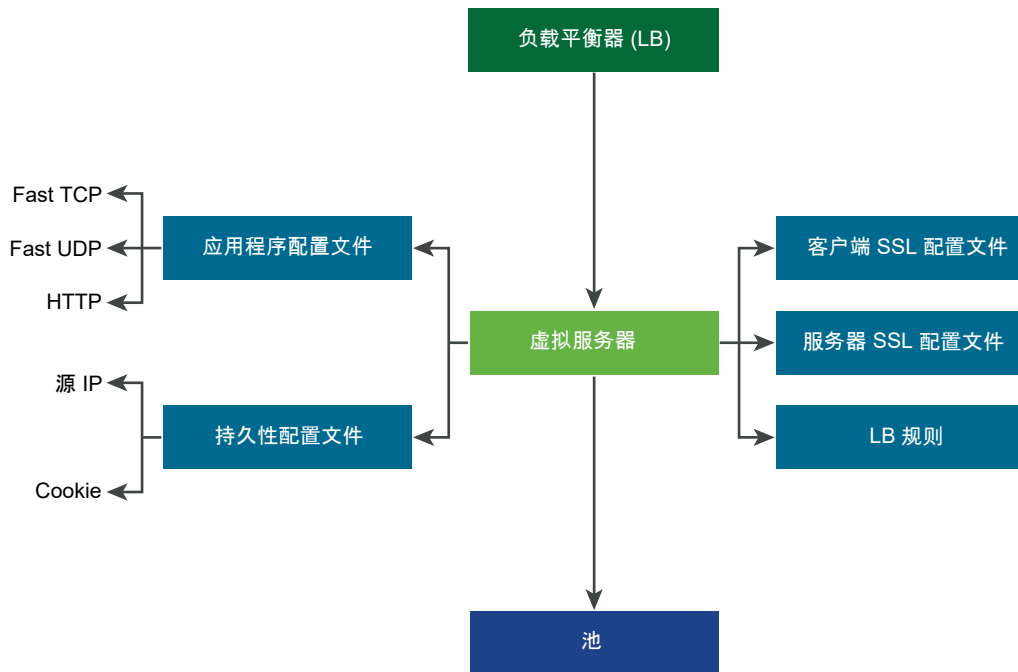


图 7-2. 虚拟服务器组件



添加应用程序配置文件

应用程序配置文件与虚拟服务器相关联，以增强负载均衡网络流量并简化流量管理任务。

应用程序配置文件定义特定网络流量类型的行为。关联的虚拟服务器会根据应用程序配置文件中指定的值处理网络流量。Fast TCP、Fast UDP 和 HTTP 应用程序配置文件是支持的配置文件类型。

默认情况下，如果没有应用程序配置文件与虚拟服务器关联，将使用 TCP 应用程序配置文件。如果应用程序基于 TCP 或 UDP 协议运行且不需要任何应用程序级负载均衡（例如，HTTP URL 负载均衡），将使用 TCP 和 UDP 应用程序配置文件。如果您只需要第 4 层负载均衡（此方法性能更高并支持连接镜像），也会使用这些配置文件。

如果负载均衡器必须根据第 7 层执行操作，例如，将所有映像请求负载均衡到某特定服务器池成员或停止 HTTPS 以从池成员卸载 SSL，则对 HTTP 和 HTTPS 应用程序使用 HTTP 应用程序配置文件。与 TCP 应用程序配置文件不同，在选择服务器池成员之前，HTTP 应用程序配置文件会停止客户端 TCP 连接。

图 7-3. 第 4 层 TCP 和 UDP 应用程序配置文件

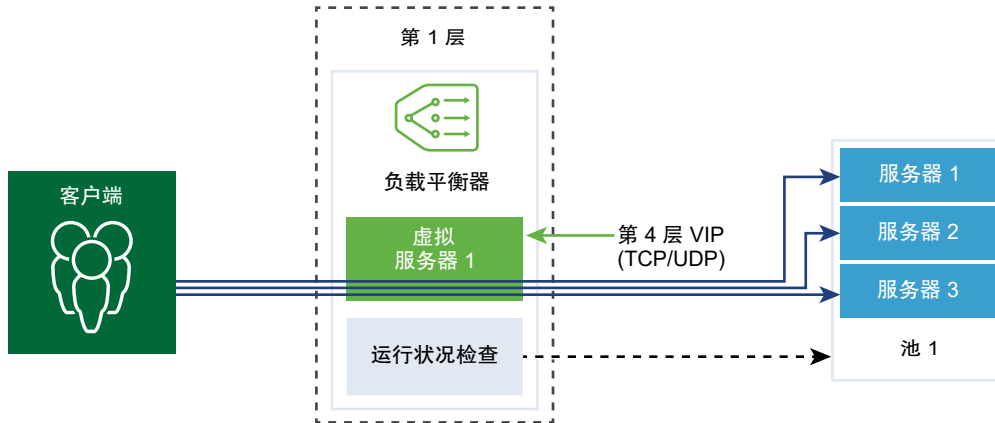
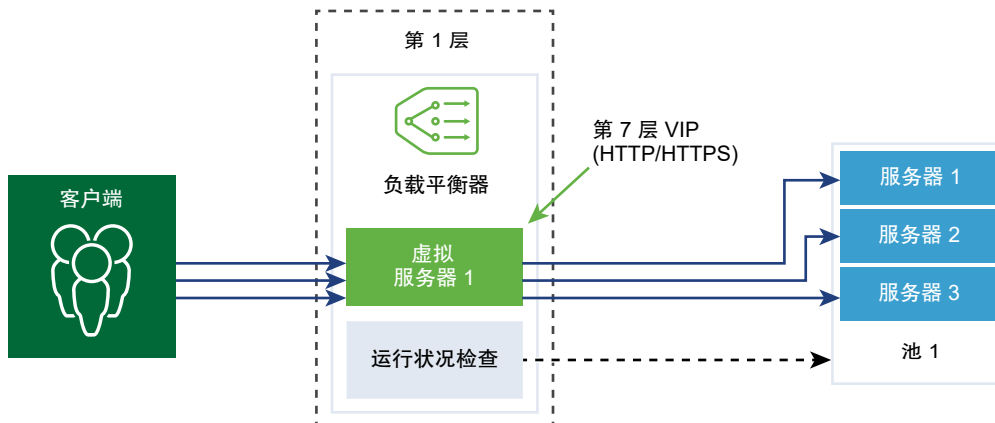


图 7-4. 第 7 层 HTTPS 应用程序配置文件



步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择网络 > 负载均衡 > 配置文件 > 应用程序 > 添加应用程序配置文件。
- 3 选择 **Fast TCP** 应用程序配置文件，然后输入配置文件详细信息。

您也可以接受 Fast TCP 配置文件的默认设置。

选项	说明
名称和说明	输入 Fast TCP 应用程序配置文件的名称和描述。
闲置超时	输入在建立 TCP 连接后服务器可以保持闲置的时长（秒）。 将空闲时间设置为实际应用程序空闲时间，再加几秒，以便负载均衡器不会先于应用程序关闭其连接。
HA 流量镜像	切换该按钮可将发往关联虚拟服务器的所有流量镜像到 HA 备用节点。

选项	说明
连接关闭超时	输入在关闭 TCP 连接之前 FIN 或 RST 必须为应用程序保持该连接的时间（秒）。支持较快的连接速率可能需要短暂的关闭超时。
标记	输入标记可使搜索变得更容易。 可以指定一个标记以设置标记的范围。

4 选择 **Fast UDP** 应用程序配置文件，然后输入配置文件详细信息。

您也可以接受 UDP 配置文件的默认设置。

选项	说明
名称和说明	输入 Fast UDP 应用程序配置文件的名称和描述。
闲置超时	输入在建立 UDP 连接后服务器可以保持闲置的时长（秒）。 UDP 是一个无连接协议。为实现负载均衡，在闲置超时期限内收到的流量签名（例如，源和目标 IP 地址或端口和 IP 协议）相同的所有 UDP 数据包均视为属于同一连接并发送到相同服务器。 如果在闲置超时期限内未收到任何数据包，则会关闭在流量签名与选定服务器之间创建关联的连接。
HA 流量镜像	切换该按钮可将发往关联虚拟服务器的所有流量镜像到 HA 备用节点。
标记	输入标记可使搜索变得更容易。 可以指定一个标记以设置标记的范围。

5 选择 **HTTP** 应用程序配置文件，然后输入配置文件详细信息。

您也可以接受 HTTP 配置文件的默认设置。

HTTP 应用程序配置文件用于 HTTP 和 HTTPS 应用程序。

选项	说明
名称和说明	输入 HTTP 应用程序配置文件的名称和描述。
闲置超时	输入 HTTP 应用程序可以保持闲置的时长（秒），而不是必须在 TCP 应用程序配置文件中配置的 TCP 套接字设置。
请求标头大小	指定用于存储 HTTP 请求标头的最大缓冲区大小（字节）。
X-Forwarded-For (XFF)	<ul style="list-style-type: none"> ■ 插入 - 如果入站请求中不存在 XFF HTTP 标头，则负载均衡器会插入一个带有客户端 IP 地址的新 XFF 标头。如果入站请求中存在 XFF HTTP 标头，则负载均衡器会在 XFF 标头中附加客户端 IP 地址。 ■ 替换 - 如果入站请求中存在 XFF HTTP 标头，则负载均衡器会替换该标头。 <p>Web 服务器会记录其处理的每个请求以及请求客户端 IP 地址。可使用这些日志进行调试和分析。如果部署拓扑需要在负载均衡器上进行 SNAT，则服务器会使用客户端 SNAT IP 地址，这违背了日志记录的目的。</p> <p>解决办法是，可以将负载均衡器配置为插入带有原始客户端 IP 地址的 XFF HTTP 标头。可以将服务器配置为记录 XFF 标头中的 IP 地址，而不是连接的源 IP 地址。</p>
请求正文大小	输入用于存储 HTTP 请求正文的缓冲区最大大小值。 如果未指定大小，则请求正文大小不受限制。

选项	说明
重定向	<ul style="list-style-type: none"> ■ 无 - 如果网站暂时关闭，用户将收到“未找到页面”错误消息。 ■ HTTP 重定向 - 如果网站暂时关闭或已移动，该虚拟服务器的入站请求可以暂时重定向到此处指定的 URL。仅支持静态重定向。 <p>例如，如果将“HTTP 重定向”设置为 <code>http://sitedown.abc.com/sorry.html</code>，无论实际请求如何（例如，<code>http://original_app.site.com/home.html</code> 或 <code>http://original_app.site.com/somepage.html</code>），当原始网站关闭时，入站请求都会重定向到指定 URL。</p> <ul style="list-style-type: none"> ■ HTTP 到 HTTPS 重定向 - 某些安全应用程序可能需要强制通过 SSL 进行通信，但是不拒绝非 SSL 连接，而是重定向客户端请求以使用 SSL。通过“HTTP 到 HTTPS 重定向”，您可以保留主机和 URI 路径并重定向客户端请求以使用 SSL。 <p>对于 HTTP 到 HTTPS 重定向，HTTPS 虚拟服务器必须具有端口 443，并且必须在同一负载均衡器上配置相同的虚拟服务器 IP 地址。</p> <p>例如，将针对 <code>http://app.com/path/page.html</code> 的客户端请求重定向到 <code>https://app.com/path/page.html</code>。如果在重定向（例如，重定向到 <code>https://secure.app.com/path/page.html</code>）时必须修改主机名或 URI，则必须使用负载均衡规则。</p>
NTLM 身份验证	<p>切换该按钮可使负载均衡器关闭 TCP 多路复用并启用 HTTP 保持活动状态。</p> <p>NTLM 身份验证协议可优先于 HTTP 使用。对于使用 NTLM 身份验证的负载均衡，必须为托管基于 NTLM 的应用程序的服务器池禁用 TCP 多路复用。否则，可能使用通过一个客户端的凭据建立的服务器端连接处理另一个客户端的请求。</p> <p>如果 NTLM 在配置文件中已启用并与虚拟服务器相关联，同时在服务器池启用了 TCP 多路复用，则 NTLM 优先。不会对该虚拟服务器执行 TCP 多路复用。但是，如果同一池与另一个非 NTLM 虚拟服务器相关联，则 TCP 多路复用可用于到该虚拟服务器的连接。</p> <p>如果客户端使用 HTTP/1.0，则负载均衡器将升级到 HTTP/1.1 协议并设置 HTTP 保持活动状态。基于同一客户端 TCP 连接接收的所有 HTTP 请求都通过单个 TCP 连接发送到相同服务器，以确保不需要重新授权。</p>
标记	<p>输入标记可使搜索变得更容易。</p> <p>可以指定一个标记以设置标记的范围。</p>

添加持久性配置文件

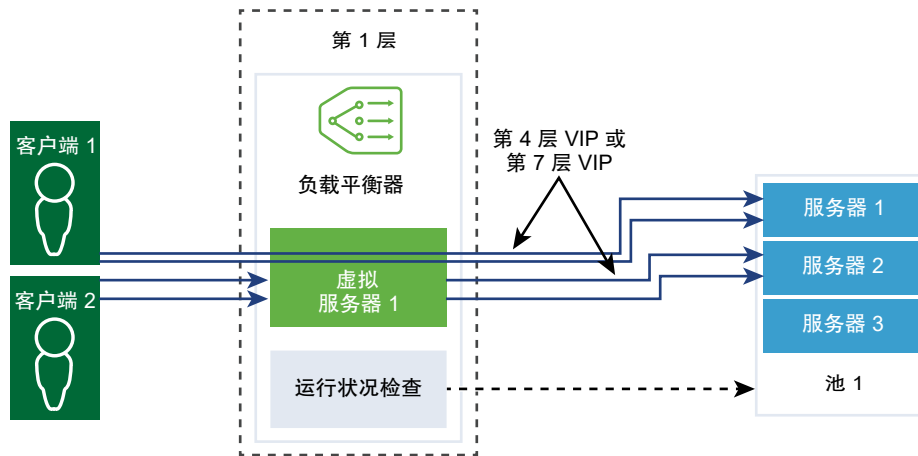
负载均衡器可实现持久性，将所有相关连接定向到同一服务器，从而确保有状态应用程序的稳定性。为了满足不同类型的应用程序需求，支持不同类型的持久性。

某些应用程序会保持服务器状态，如购物车。此类状态可能基于客户端并由客户端 IP 地址或根据 HTTP 会话标识。在处理来自同一客户端或 HTTP 会话的后续相关连接时，应用程序可能会访问或修改此状态。

源 IP 持久性配置文件基于源 IP 地址跟踪会话。客户端请求连接到支持源地址持久性的虚拟服务器时，负载均衡器将检查该客户端之前是否曾建立连接；如果是，则将客户端返回给同一服务器。否则，可以根据池负载均衡算法选择服务器池成员。源 IP 持久性配置文件由第 4 层和第 7 层虚拟服务器使用。

Cookie 持久性配置文件将插入唯一的 Cookie，以便在客户端首次访问站点时标识会话。客户端在后续请求中转发 HTTP Cookie，并且负载均衡器使用该信息提供 Cookie 持久性。第 7 层虚拟服务器只能使用 Cookie 持久性配置文件。请注意，不支持 Cookie 名称中存在空格。

通用持久性配置文件会根据 HTTP 请求中的 HTTP 标头、Cookie 或 URL 来支持持久性。因此，当会话 ID 是 URL 的一部分时，配置文件将支持应用程序会话持久性。该配置文件未直接与虚拟服务器关联。在配置用于请求转发和响应重写的负载均衡器规则时，可以指定该配置文件。



步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择网络 > 负载均衡 > 配置文件 > 持久性 > 添加持久性配置文件。
- 3 选择源 IP 以添加源 IP 持久性配置文件并输入配置文件详细信息。

您也可以接受默认源 IP 配置文件设置。

选项	说明
名称和说明	输入源 IP 持久性配置文件的名称和描述。
共享持久性	<p>切换该按钮以共享持久性，使与此配置文件关联的所有虚拟服务器均可共享持久性表。</p> <p>如果与虚拟服务器关联的“源 IP”持久性配置文件中未启用持久性共享，则与配置文件关联的每个虚拟服务器都将维护一个专用持久性表。</p>
持久性条目超时	<p>输入持久性到期时间（秒）。</p> <p>负载均衡器持久性表维护用来记录客户端请求被定向到同一服务器的条目。</p> <p>从新客户端 IP 首次连接时，将根据负载均衡算法选择池成员以均衡负载。NSX 会将该持久性条目存储在 LB 持久性表中，该表可通过以下 CLI 命令在托管活动 T1-LB 的 Edge 节点上查看：<code>get load-balancer <LB-UUID> persistence-tables</code>。</p> <ul style="list-style-type: none"> ■ 当存在从该客户端到 VIP 的连接时，将保留该持久性条目。 ■ 如果不再有从该客户端到 VIP 的连接，该持久性条目将启动在“持久性条目超时”值中指定的定时器倒计时。如果在定时器到期之前没有从该客户端到 VIP 的新连接，则会删除该客户端 IP 的持久性条目。如果该客户端在删除持久性条目后又重新连接，则会根据负载均衡算法重新选择池成员以均衡负载。
已满时清除条目	<p>如果流量很大，则较大的超时值可能会导致持久性表快速填满。如果启用此选项，则会删除最早的条目以接受最新条目。</p> <p>如果禁用此选项，则当源 IP 持久性表已满时，会拒绝新的客户端连接。</p>

选项	说明
HA 持久性镜像	切换该按钮以将持久性条目同步到 HA 对等项。如果启用 HA 持久性镜像，则在发生负载均衡器故障切换时，会保持客户端 IP 持久性。
标记	输入标记可使搜索变得更容易。 可以指定一个标记以设置标记的范围。

4 选择 Cookie 持久性配置文件，然后输入配置文件详细信息。

选项	说明
名称和说明	输入 Cookie 持久性配置文件的名称和描述。
共享持久性	切换该按钮以在与相同池成员关联的多个虚拟服务器之间共享持久性。 Cookie 持久性配置文件将插入格式为 <名称>.<配置文件 ID>.<池 ID> 的 Cookie。 如果与虚拟服务器关联的 Cookie 持久性配置文件中未启用持久性共享，则会使用每个虚拟服务器的专用 Cookie 持久性并由池成员对其进行限定。负载均衡器将插入格式为 <名称>.<虚拟服务器 ID>.<池 ID> 的 Cookie。
Cookie 模式	从下拉菜单中选择一个模式。 <ul style="list-style-type: none"> ■ INSERT - 添加唯一的 Cookie 以标识会话。 ■ PREFIX - 附加到现有 HTTP Cookie 信息。 ■ REWRITE - 重写现有 HTTP Cookie 信息。
Cookie 名称	输入 Cookie 名称。不支持 Cookie 名称中存在空格。
Cookie 域	输入域名。 HTTP Cookie 域只能在 INSERT 模式中配置。
Cookie 回退	切换该按钮，以便在 Cookie 指向处于 DISABLED 或 DOWN 状态的服务器时拒绝客户端请求。 如果 Cookie 指向处于 DISABLED 或 DOWN 状态的服务器，请选择一个新的服务器来处理客户端请求。
Cookie 路径	输入 Cookie URL 路径。 HTTP Cookie 路径只能在 INSERT 模式中设置。
Cookie 加密	切换该按钮以禁用加密。 禁用乱码时，Cookie 服务器 IP 地址和端口信息采用明文形式。加密 Cookie 服务器 IP 地址和端口信息。
Cookie 类型	从下拉菜单中选择 Cookie 类型。 会话 Cookie - 未存储。关闭浏览器后将丢失。 持久性 Cookie - 由浏览器存储。关闭浏览器时不会丢失。
最长空闲时间	输入 Cookie 过期之前 Cookie 类型可以处于空闲状态的时间（秒）。
最长 Cookie 保留时间	对于会话 Cookie 类型，请输入 Cookie 的可用时间（秒）。
标记	输入标记可使搜索变得更容易。 可以指定一个标记以设置标记的范围。

5 选择通用以添加通用持久性配置文件，然后输入配置文件详细信息。

选项	说明
名称和说明	输入源 IP 持久性配置文件的名称和描述。
共享持久性	切换该按钮以在虚拟服务器之间共享配置文件。
持久性条目超时	<p>输入持久性到期时间（秒）。</p> <p>负载均衡器持久性表维护用来记录客户端请求被定向到同一服务器的条目。</p> <p>从新客户端 IP 首次连接时，将根据负载均衡算法选择池成员以均衡负载。NSX 会将该持久性条目存储在 LB 持久性表中，该表可通过以下 CLI 命令在托管活动 T1-LB 的 Edge 节点上查看：get load-balancer <LB-UUID> persistence-tables。</p> <ul style="list-style-type: none"> ■ 当存在从该客户端到 VIP 的连接时，将保留该持久性条目。 ■ 如果不再有从该客户端到 VIP 的连接，该持久性条目将启动在“持久性条目超时”值中指定的定时器倒计时。如果在定时器到期之前没有从该客户端到 VIP 的新连接，则会删除该客户端 IP 的持久性条目。如果该客户端在删除持久性条目后又重新连接，则会根据负载均衡算法重新选择池成员以均衡负载。
HA 持久性镜像	切换该按钮以将持久性条目同步到 HA 对等项。
标记	<p>输入标记可使搜索变得更容易。</p> <p>可以指定一个标记以设置标记的范围。</p>

添加 SSL 配置文件

SSL 配置文件配置与应用程序无关的 SSL 属性（如密码列表）并在多个应用程序中重用这些列表。负载均衡器充当客户端和服务端时的 SSL 属性有所不同，因此支持使用单独的客户端和服务端 SSL 配置文件。

注 SSL 配置文件在 NSX-T Data Center Limited Export 版本中不受支持。

客户端 SSL 配置文件是指负载均衡器充当 SSL 服务器并停止客户端 SSL 连接。服务端 SSL 配置文件是指负载均衡器充当客户端并与服务器建立连接。

您可以在客户端和服务端 SSL 配置文件上指定密码列表。

通过 SSL 会话缓存，SSL 客户端和服务端可以重用先前商定的安全参数，避免在 SSL 握手期间发生开销很大的公钥操作。默认情况下，将在客户端和服务端禁用 SSL 会话缓存。

SSL 会话票证是另一种允许 SSL 客户端和服务端重用先前商定会话参数的机制。在 SSL 会话票证中，客户端和服务端商定是否在握手交换期间支持 SSL 会话票证。如果二者均支持，则服务器可以向客户端发送包含加密 SSL 会话参数的 SSL 票证。客户端可以在后续连接中使用该票证来重用会话。SSL 会话票证在客户端处于启用状态，但在服务端处于禁用状态。

图 7-5. SSL 卸载

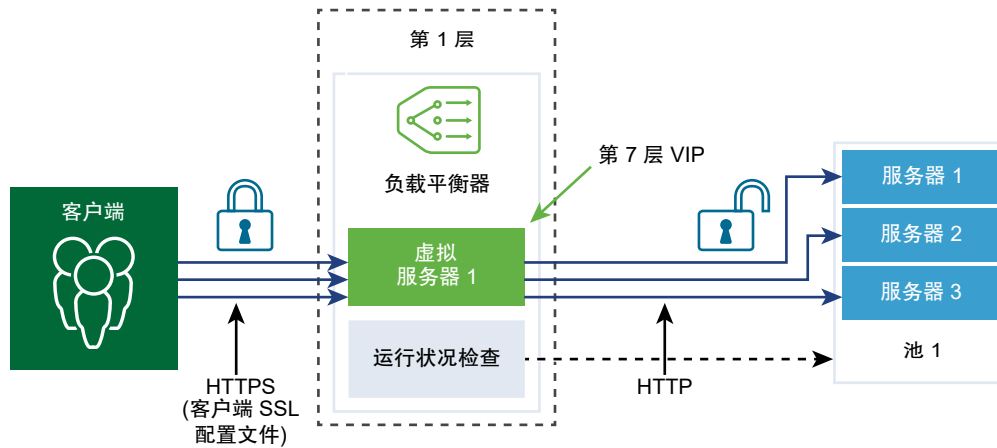
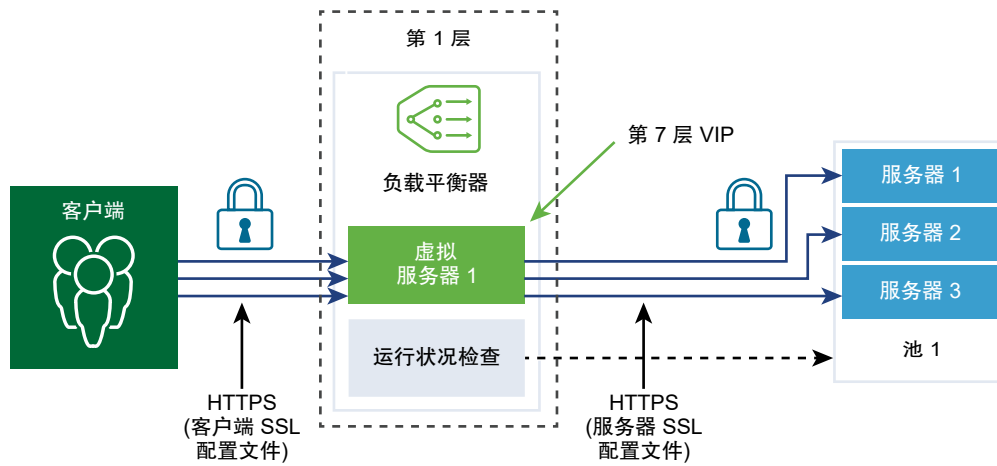


图 7-6. 端到端 SSL



步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 选择网络 > 负载均衡 > 配置文件 > SSL 配置文件。
- 3 选择客户端 SSL 配置文件，然后输入配置文件详细信息。

选项	说明
名称和说明	输入客户端 SSL 配置文件的名称和描述。
SSL Suite	从下拉菜单中选择 SSL 密码组，并填充将在客户端 SSL 配置文件中包含的可用 SSL 密码和 SSL 协议。 经过平衡的 SSL 密码组是默认选项。
会话缓存	切换该按钮，使 SSL 客户端和服务端可以重用先前商定的安全参数，避免在 SSL 握手期间发生开销很大的公钥操作。
标记	输入标记可使搜索变得更容易。 可以指定一个标记以设置标记的范围。

选项	说明
支持的 SSL 密码	根据 SSL Suite，在此处填充为您分配的支持的 SSL 密码。单击 查看更多 可查看整个列表。 如果选择 自定义 ，则必须从下拉菜单中选择 SSL 密码。
支持的 SSL 协议	根据 SSL Suite，在此处填充为您分配的支持的 SSL 协议。单击 查看更多 可查看整个列表。 如果选择 自定义 ，则必须从下拉菜单中选择 SSL 密码。
会话缓存条目超时	输入缓存超时（秒）以指定 SSL 会话参数必须保留并可重用的时长。
首选服务器密码	切换该按钮，使服务器可以从其支持的列表中选择第一个受支持的密码。 在 SSL 握手期间，客户端向服务器发送经过排序的受支持密码列表。

4 选择服务器 SSL 配置文件，然后输入配置文件详细信息。

选项	说明
名称和说明	输入服务器 SSL 配置文件的名称和描述。
SSL Suite	从下拉菜单中选择 SSL 密码组，并填充将在服务器 SSL 配置文件中包含的可用 SSL 密码和 SSL 协议。 经过平衡的 SSL 密码组是默认选项。
会话缓存	切换该按钮，使 SSL 客户端和服务器可以重用先前商定的安全参数，避免在 SSL 握手期间发生开销很大的公钥操作。
标记	输入标记可使搜索变得更容易。 可以指定一个标记以设置标记的范围。
支持的 SSL 密码	根据 SSL Suite，在此处填充为您分配的支持的 SSL 密码。单击 查看更多 可查看整个列表。 如果选择 自定义 ，则必须从下拉菜单中选择 SSL 密码。
支持的 SSL 协议	根据 SSL Suite，在此处填充为您分配的支持的 SSL 协议。单击 查看更多 可查看整个列表。 如果选择 自定义 ，则必须从下拉菜单中选择 SSL 密码。
会话缓存条目超时	输入缓存超时（秒）以指定 SSL 会话参数必须保留并可重用的时长。
首选服务器密码	切换该按钮，使服务器可以从其支持的列表中选择第一个受支持的密码。 在 SSL 握手期间，客户端向服务器发送经过排序的受支持密码列表。

添加第 4 层虚拟服务器

虚拟服务器接收所有客户端连接并在服务器之间进行分发。虚拟服务器具有 IP 地址、端口和协议。对于第 4 层虚拟服务器，可以指定端口范围列表，而不是单个 TCP 或 UDP 端口，以支持具有动态端口的复杂协议。

第 4 层虚拟服务器必须与主服务器池（也称为默认池）相关联。

如果虚拟服务器状态为已禁用，则会通过发送 TCP RST（对于 TCP 连接）或 ICMP 错误消息（对于 UDP）拒绝对虚拟服务器的任何新连接尝试。即使新连接存在匹配的持久性条目，也会拒绝这些连接。活动连接将继续进行处理。如果虚拟服务器从负载均衡器中删除或与负载均衡器解除关联，则到该虚拟服务器的活动连接将失败。

前提条件

- 确认应用程序配置文件可用。请参见[添加应用程序配置文件](#)。
- 确认持久配置文件可用。请参见[添加持久性配置文件](#)。
- 确认客户端和服务器的 SSL 配置文件可用。请参见[添加 SSL 配置文件](#)。
- 确认服务器池可用。请参见[添加服务器池](#)。
- 确认负载均衡器可用。请参见[添加负载均衡器](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**网络 > 负载均衡 > 虚拟服务器 > 添加虚拟服务器**。
- 3 选择 **L4 TCP** 协议，然后输入协议详细信息。

第 4 层虚拟服务器支持 Fast TCP 或 Fast UDP 协议，而不同时支持两者。

要在相同的 IP 地址和端口上支持 Fast TCP 或 Fast UDP 协议，例如 DNS，必须为每个协议创建一个虚拟服务器。

选项	说明
名称和说明	输入第 4 层虚拟服务器的名称和描述。
IP 地址	输入虚拟服务器的 IP 地址。
端口	输入虚拟服务器的端口号。
负载均衡器	从下拉菜单中选择要附加到该第 4 层虚拟服务器的现有负载均衡器。
服务器池	<p>从下拉菜单中选择现有服务器池。</p> <p>服务器池包含一个或多个配置类似并运行相同应用程序的服务器（也称为池成员）。</p> <p>您可以单击垂直省略号创建服务器池。</p>
应用程序配置文件	<p>根据协议类型，将自动填充现有应用程序配置文件。</p> <p>您可以单击垂直省略号创建应用程序配置文件。</p>
持久性	<p>从下拉菜单中选择现有持久性配置文件。</p> <p>可以在虚拟服务器上启用持久性配置文件，从而允许将源 IP 相关客户端连接发送到相同服务器。</p>
最大并发连接数	设置允许与虚拟服务器建立的最大并发连接，这样虚拟服务器就不会耗尽托管在同一负载均衡器上的其他应用程序的资源。
最大新连接速率	设置与服务器池成员的最大新连接，这样虚拟服务器就不会耗尽资源。
Sorry Server 池	<p>从下拉菜单中选择现有 Sorry Server 池。</p> <p>负载均衡器无法从默认池选择后端服务器来处理请求时，Sorry Server 池将处理请求。</p> <p>您可以单击垂直省略号创建服务器池。</p>

选项	说明
默认池成员端口	如果未定义虚拟服务器的池成员端口，请输入默认池成员端口。 例如，如果虚拟服务器通过端口范围 2000-2999 定义，并且默认池成员端口范围设置为 8000-8999，则将虚拟服务器端口 2500 的入站客户端连接发送到目标端口设置为 8500 的池成员。
管理状态	切换按钮以禁用第 4 层虚拟服务器的管理状态。
访问日志	切换按钮以启用第 4 层虚拟服务器的日志记录。
标记	输入标记可使搜索变得更容易。 可以指定一个标记以设置标记的范围。

4 选择 L4 UDP 协议，然后输入协议详细信息。

选项	说明
名称和说明	输入第 4 层虚拟服务器的名称和描述。
IP 地址	输入虚拟服务器的 IP 地址。
端口	输入虚拟服务器的端口号。
负载均衡器	从下拉菜单中选择要附加到该第 4 层虚拟服务器的现有负载均衡器。
服务器池	从下拉菜单中选择现有服务器池。 服务器池包含一个或多个配置类似并运行相同应用程序的服务器（也称为池成员）。 您可以单击垂直省略号创建服务器池。
应用程序配置文件	根据协议类型，将自动填充现有应用程序配置文件。 您可以单击垂直省略号创建应用程序配置文件。
持久性	从下拉菜单中选择现有持久性配置文件。 可以在虚拟服务器上启用持久性配置文件，从而允许将源 IP 相关客户端连接发送到相同服务器。
最大并发连接数	设置允许与虚拟服务器建立的最大并发连接，这样虚拟服务器就不会耗尽托管在同一负载均衡器上的其他应用程序的资源。
最大新连接速率	设置与服务器池成员的最大新连接，这样虚拟服务器就不会耗尽资源。
Sorry Server 池	从下拉菜单中选择现有 Sorry Server 池。 负载均衡器无法从默认池选择后端服务器来处理请求时，Sorry Server 池将处理请求。 您可以单击垂直省略号创建服务器池。
默认池成员端口	如果未定义虚拟服务器的池成员端口，请输入默认池成员端口。 例如，如果虚拟服务器通过端口范围 2000-2999 定义，并且默认池成员端口范围设置为 8000-8999，则将虚拟服务器端口 2500 的入站客户端连接发送到目标端口设置为 8500 的池成员。
管理状态	切换按钮以禁用第 4 层虚拟服务器的管理状态。
访问日志	切换按钮以启用第 4 层虚拟服务器的日志记录。
标记	输入标记可使搜索变得更容易。 可以指定一个标记以设置标记的范围。

添加第 7 层 HTTP 虚拟服务器

虚拟服务器接收所有客户端连接并在服务器之间进行分发。虚拟服务器具有 IP 地址、端口和协议 TCP。

仅具有 HTTP 应用程序配置文件的第 7 层虚拟服务器支持负载均衡器规则。不同的负载均衡器服务可以使用负载均衡器规则。

注 NSX-T Data Center 3.0 及更高版本支持第 7 层 SSL 直通。

每个负载均衡器规则由一个或多个匹配条件和单项或多项操作组成。如果未指定匹配条件，则负载均衡器规则始终匹配并用于定义默认规则。如果指定了多个匹配条件，则匹配策略确定必须匹配所有条件还是必须匹配任一条件，负载均衡器规则才会被视为匹配项。

每个负载均衡器规则在负载均衡处理的特定阶段实施：HTTP 请求重写、HTTP 请求转发和 HTTP 响应重写。并非所有匹配条件和操作都适用于每个阶段。

如果虚拟服务器状态为已禁用，则会通过发送 TCP RST（对于 TCP 连接）或 ICMP 错误消息（对于 UDP）拒绝对虚拟服务器的任何新连接尝试。即使新连接存在匹配的持久性条目，也会拒绝这些连接。活动连接将继续进行处理。如果虚拟服务器从负载均衡器中删除或与负载均衡器解除关联，则到该虚拟服务器的活动连接将失败。

注 SSL 配置文件在 NSX-T Data Center Limited Export 版本中不受支持。

如果在虚拟服务器上配置了客户端 SSL 配置文件绑定，而不是服务器端 SSL 配置文件绑定，则虚拟服务器在 SSL 终止模式下运行，该模式与客户端和服务器分别具有加密连接和明文连接。如果同时配置了客户端和服务器端 SSL 配置文件绑定，则虚拟服务器在 SSL 代理模式下运行，该模式与客户端和服务器具有加密连接。

目前不支持在不关联客户端 SSL 配置文件绑定的情况下关联服务器端 SSL 配置文件绑定。如果客户端和服务器端 SSL 配置文件绑定不与虚拟服务器相关联且应用程序基于 SSL，则虚拟服务器在 SSL 非感知模式下运行。在这种情况下，必须为第 4 层配置虚拟服务器。例如，虚拟服务器可与 Fast TCP 配置文件相关联。

前提条件

- 确认应用程序配置文件可用。请参见[添加应用程序配置文件](#)。
- 确认持久配置文件可用。请参见[添加持久性配置文件](#)。
- 确认客户端和服务器的 SSL 配置文件可用。请参见[添加 SSL 配置文件](#)。
- 确认服务器池可用。请参见[添加服务器池](#)。
- 确认 CA 和客户端证书可用。请参见[创建证书签名请求文件](#)。
- 确认证书吊销列表 (CRL) 可用。请参见[导入证书吊销列表](#)。
- 确认负载均衡器可用。请参见[添加负载均衡器](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择 **网络 > 负载均衡 > 虚拟服务器 > 添加虚拟服务器**。

3 选择 L7 HTTP 协议并输入协议详细信息。

第 7 层虚拟服务器支持 HTTP 和 HTTPS 协议。

选项	说明
名称和说明	输入第 7 层虚拟服务器的名称和说明。
IP 地址	输入虚拟服务器的 IP 地址。
端口	输入虚拟服务器的端口号。
负载均衡器	从下拉菜单中选择要附加到该第 4 层虚拟服务器的现有负载均衡器。
服务器池	从下拉菜单中选择现有服务器池。 服务器池包含一个或多个配置类似并运行相同应用程序的服务器（也称为池成员）。 您可以单击垂直省略号创建服务器池。
应用程序配置文件	根据协议类型，将自动填充现有应用程序配置文件。 您可以单击垂直省略号创建应用程序配置文件。
持久性	从下拉菜单中选择现有持久性配置文件。 可以在虚拟服务器上启用持久性配置文件，从而允许将源 IP 和 Cookie 相关客户端连接发送到相同服务器。

4 单击配置以设置第 7 层虚拟服务器 SSL。

您可以配置客户端 SSL 和服务器 SSL。

5 配置客户端 SSL。

选项	说明
客户端 SSL	切换按钮以启用配置文件。 客户端 SSL 配置文件绑定允许对要与同一虚拟服务器相关联的不同主机名使用多个证书。
默认证书	从下拉菜单中选择一个默认证书。 如果服务器不将多个主机名托管在同一 IP 地址上或客户端不支持服务器名称指示 (SNI) 扩展，则会使用此证书。
客户端 SSL 配置文件	从下拉菜单中选择客户端 SSL 配置文件。
SNI 证书	从下拉菜单中选择可用 SNI 证书。
受信任的 CA 证书	选择可用 CA 证书。
强制客户端身份验证	切换按钮以启用此菜单项。
证书链深度	设置证书链深度以验证服务器证书链深度。
证书吊销列表	选择可用 CRL 以禁止使用损坏的服务器证书。

6 配置服务器 SSL。

选项	说明
服务器 SSL	切换按钮以启用配置文件。
客户端证书	从下拉菜单中选择一个客户端证书。 如果服务器不将多个主机名托管在同一 IP 地址上或客户端不支持服务器名称指示 (SNI) 扩展，则会使用此证书。
服务器 SSL 配置文件	从下拉菜单中选择服务器端 SSL 配置文件。
受信任的 CA 证书	选择可用 CA 证书。
强制服务器身份验证	切换按钮以启用此菜单项。 服务器端 SSL 配置文件绑定指定是否必须验证在 SSL 握手期间提供给负载均衡器的服务器证书。启用验证后，服务器证书必须由其中一个可信 CA 签名，这些 CA 的自签名证书在同一服务器端 SSL 配置文件绑定中指定。
证书链深度	设置证书链深度以验证服务器证书链深度。
证书吊销列表	选择可用 CRL 以禁止使用损坏的服务器证书。 服务器端上不支持 OCSP 和 OCSP 装订 (OCSP stapling)。

7 配置其他第 7 层虚拟服务器属性。

选项	说明
最大并发连接数	设置允许与虚拟服务器建立的最大并发连接，这样虚拟服务器就不会耗尽托管在同一负载均衡器上的其他应用程序的资源。
最大新连接速率	设置与服务器池成员的最大新连接，这样虚拟服务器就不会耗尽资源。
Sorry Server 池	从下拉菜单中选择现有 Sorry Server 池。 负载均衡器无法从默认池选择后端服务器来处理请求时，Sorry Server 池将处理请求。 您可以单击垂直省略号创建服务器池。
默认池成员端口	如果未定义虚拟服务器的池成员端口，请输入默认池成员端口。 例如，如果虚拟服务器通过端口范围 2000-2999 定义，并且默认池成员端口范围设置为 8000-8999，则将虚拟服务器端口 2500 的入站客户端连接发送到目标端口设置为 8500 的池成员。
管理状态	切换按钮以禁用第 7 层虚拟服务器的管理状态。
访问日志	切换按钮以启用第 7 层虚拟服务器的日志记录。
标记	输入标记可使搜索变得更容易。 可以指定一个标记以设置标记的范围。

8 单击保存。

添加负载均衡器规则

通过第 7 层 HTTP 虚拟服务器，您可以选择配置负载均衡器规则并使用匹配或操作规则自定义负载均衡行为。

负载均衡器规则支持 REGEX 匹配类型。支持 PCRE 样式 REGEX 模式，但高级用例存在一些限制。在匹配条件中使用 REGEX 时，支持已命名捕获组。

REGEX 限制包括：

- 不支持字符并集和交集。例如，不要使用 `[a-z[0-9]]` 和 `[a-z&&[aeiou]]`，而要相应使用 `[a-z0-9]` 和 `[aeiou]`。
- 仅支持 9 个向后引用，可以使用 `\1` 到 `\9` 来引用它们。
- 请使用 `\Odd` 格式来匹配八进制数字，而不要使用 `\ddd` 格式。
- 顶层级别不支持嵌入式标记，嵌入式标记仅在组中受支持。例如，不要使用 “`Case (?i:s)ensitive`”，而要使用 “`Case ((?i:s)ensitive)`”。
- 不支持预处理操作 `\l`、`\u`、`\L` 和 `\U`。其中 `\l` 是将下一字符变为小写，`\u` 是将下一字符变为大写，`\L` 将后续直至 `\E` 的字符变为小写，`\U` 则将后续直至 `\E` 的字符变为大写。
- 不支持 `(?(condition)X)`、`(? {code})`、`(??{Code})` 和 `(?#comment)`。
- 不支持预定义的 Unicode 字符类 `\X`
- 不支持对 Unicode 字符使用已命名字符构造。例如，不要使用 `\N{name}`，而要使用 `\u2018`。

在匹配条件中使用 REGEX 时，支持已命名捕获组。例如，可以使用 REGEX 匹配模式 `/news/(?<year>\d+)-(?(<month>\d+)-(?(<day>\d+)/?(<article>.*))` 来匹配类似于 `/news/2018-06-15/news1234.html` 的 URI。

然后按如下所示设置变量：`$year = "2018" $month = "06" $day = "15" $article = "news1234.html"`。设置变量后，可以在负载均衡器规则操作中使用这些变量。例如，可以使用匹配的变量来重写 URI，例如 `/news.py?year=$year&month=$month&day=$day&article=$article`。该 URI 随后重写为 `/news.py?year=2018&month=06&day=15&article=news1234.html`。

重写操作可以使用已命名捕获组和内置变量的组合。例如，URI 可以重写为 `/news.py?year=$year&month=$month&day=$day&article=$article&user_ip=$_remote_addr`。该示例 URI 随后重写为 `/news.py?year=2018&month=06&day=15&article=news1234.html&user_ip=1.1.1.1`。

注 对于已命名捕获组，名称不能以字符 `_` 开头。

除了已命名捕获组之外，还可以在重写操作中使用以下内置变量。所有内置变量的名称均以 `_` 开头。

- `$_args` - 请求中的参数
- `$_arg_<name>` - 请求行中的参数 `<name>`
- `$_cookie_<name>` - `<name>` Cookie 的值
- `$_upstream_cookie_<name>` - 由 “Set-Cookie” 响应标头字段中的上游服务器发送的具有指定名称的 Cookie
- `$_upstream_http_<name>` - 任意响应标头字段，`<name>` 是字段名称，该字段名称将转换为小写，并且其中的短划线将替换为下划线
- `$_host` - 按优先级顺序，请求行中的主机名，或者 “Host” 请求标头字段中的主机名或与请求匹配的服务器名称
- `$_http_<name>` - 任意请求标头字段，`<name>` 是字段名称，该字段名称将转换为小写，并且其中的短划线将替换为下划线

- `$_https` - 如果连接在 SSL 模式下工作，为 "on"；否则为 ""
- `$_is_args` - 如果请求行包含参数，为 "?"；否则为 ""
- `$_query_string` - 与 `$_args` 相同
- `$_remote_addr` - 客户端地址
- `$_remote_port` - 客户端端口
- `$_request_uri` - 完整的原始请求 URI（包含参数）
- `$_scheme` - 请求方案 "http" 或 "https"
- `$_server_addr` - 接受请求的服务器的地址
- `$_server_name` - 接受请求的服务器的名称
- `$_server_port` - 接受请求的服务器的端口
- `$_server_protocol` - 请求协议，通常为 "HTTP/1.0" 或 "HTTP/1.1"
- （仅限 NSX-T Data Center 2.5.0）`$_ssl_client_cert` - 为已建立的 SSL 连接返回 PEM 格式的客户端证书，证书中除第一行以外的每一行开头均附加制表符字符。
- （NSX-T Data Center 2.5.1 和更高版本）`$_ssl_client_escaped_cert` - 为已建立的 SSL 连接返回 PEM 格式的客户端证书。
- `$_ssl_server_name` - 通过 SNI 返回请求的服务器名称
- `$_uri` - 请求中的 URI 路径
- `$_ssl_ciphers` - 返回客户端 SSL 密码
- `$_ssl_client_i_dn` - 根据 RFC 2253 返回建立的 SSL 连接的客户端证书的“颁发者 DN”字符串
- `$_ssl_client_s_dn` - 根据 RFC 2253 返回建立的 SSL 连接的客户端证书的“主体 DN”字符串
- `$_ssl_protocol` - 返回建立的 SSL 连接的协议
- `$_ssl_session_reused` - 如果重用 SSL 会话，则返回 "r"，否则，返回 "."

前提条件

确认第 7 层 HTTP 虚拟服务器可用。请参见[添加第 7 层 HTTP 虚拟服务器](#)。

步骤

- 1 打开第 7 层 HTTP 虚拟服务器。

- 2 在“负载均衡器规则”区域中，单击**设置 > 添加规则**以配置 HTTP 请求重写阶段的负载均衡器规则。支持的匹配类型是 REGEX、STARTS_WITH、ENDS_WITH 等，以及逆反选项。

支持的匹配条件	说明
HTTP 请求方法	与 HTTP 请求方法匹配。 http_request.method - 要匹配的值
HTTP 请求 URI	与不带查询参数的 HTTP 请求 URI 匹配。 http_request.uri - 要匹配的值
HTTP 请求 URI 参数	与 HTTP 请求 URI 查询参数匹配。 http_request.uri_arguments - 要匹配的值
HTTP 请求版本	与 HTTP 请求版本匹配。 http_request.version - 要匹配的值
HTTP 请求标头	与任何 HTTP 请求标头匹配。 http_request.header_name - 要匹配的标头名称 http_request.header_value - 要匹配的值
HTTP 请求 Cookie	与任何 HTTP 请求 cookie 匹配。 http_request.cookie_value - 要匹配的值
HTTP 请求正文	与 HTTP 请求正文内容匹配。 http_request.body_value - 要匹配的值
客户端 SSL	与客户端 SSL 配置文件 ID 匹配。 ssl_profile_id - 要匹配的值
TCP 标头端口	与 TCP 源或目标端口匹配。 tcp_header.source_port - 要匹配的源端口 tcp_header.destination_port - 要匹配的目标端口
IP 标头源	与 IP 源或目标地址匹配。 ip_header.source_address - 要匹配的源地址 ip_header.destination_address - 要匹配的目标地址
变量	创建一个变量并向该变量分配值。
区分大小写	设置区分大小写的标记进行 HTTP 标头值比较。

操作	说明
HTTP 请求 URI 重写	修改 URI。 http_request.uri - 要写入的 URI（不含查询参数） http_request.uri_args - 要写入的 URI 查询参数
HTTP 请求标头重写	修改 HTTP 标头的值。 http_request.header_name - 标头名称 http_request.header_value - 要写入的值
HTTP 请求标头删除	删除 HTTP 标头。 http_request.header_delete - 标头名称 http_request.header_delete - 要写入的值

3 单击 **请求转发 > 添加规则** 以配置 HTTP 请求转发的负载均衡器规则。

所有匹配值接受正则表达式。

支持的匹配条件	说明
HTTP 请求方法	与 HTTP 请求方法匹配。 http_request.method - 要匹配的值
HTTP 请求 URI	与 HTTP 请求 URI 匹配。 http_request.uri - 要匹配的值
HTTP 请求版本	与 HTTP 请求版本匹配。 http_request.version - 要匹配的值
HTTP 请求标头	与任何 HTTP 请求标头匹配。 http_request.header_name - 要匹配的标头名称 http_request.header_value - 要匹配的值
HTTP 请求 Cookie	与任何 HTTP 请求 cookie 匹配。 http_request.cookie_value - 要匹配的值
HTTP 请求正文	与 HTTP 请求正文内容匹配。 http_request.body_value - 要匹配的值
客户端 SSL	与客户端 SSL 配置文件 ID 匹配。 ssl_profile_id - 要匹配的值
TCP 标头端口	与 TCP 源或目标端口匹配。 tcp_header.source_port - 要匹配的源端口 tcp_header.destination_port - 要匹配的目标端口
IP 标头源	与 IP 源或目标地址匹配。 ip_header.source_address - 要匹配的源地址 ip_header.destination_address - 要匹配的目标地址
变量	创建一个变量并向该变量分配值。
区分大小写	设置区分大小写的标记进行 HTTP 标头值比较。
操作	说明
HTTP 拒绝	拒绝请求，例如，通过将状态设置为 5xx。 http_forward.reply_status - 用于拒绝的 HTTP 状态代码 http_forward.reply_message - HTTP 拒绝消息
HTTP 重定向	重定向请求。状态代码必须设置为 3xx。 http_forward.redirect_status - 用于重定向的 HTTP 状态代码 http_forward.redirect_url - HTTP 重定向 URL
选择池	将请求强制到特定服务器池。指定池成员的配置算法（预测器）用于在服务器池中 选择服务器。 http_forward.select_pool - 服务器池 UUID

操作	说明
变量持久性检测	选择通用持久性配置文件，然后输入变量名称。 您还可以启用 哈希变量 。如果变量值非常长，则对变量进行哈希处理可确保能将其正确存储到持久性表中。如果未启用 哈希变量 ，则当变量值非常长时，只会将变量值的固定前缀部分存储到持久性表中。因此，对于具有长变量值的两个不同请求，它们应发送到不同的后端服务器，但因为其变量值具有相同的前缀部分，可能会发送到同一个后端服务器。
应答状态	显示应答的状态。
应答消息	服务器使用应答消息来响应，其中包含确认的地址和配置。

4 单击**响应重写** > **添加规则**以配置 HTTP 响应重写的负载均衡器规则。

所有匹配值接受正则表达式。

支持的匹配条件	说明
HTTP 响应标头	与任何 HTTP 响应标头匹配。 http_response.header_name - 要匹配的标头名称 http_response.header_value - 要匹配的值
HTTP 响应方法	与 HTTP 响应方法匹配。 http_response.method - 要匹配的值
HTTP 响应 URI	与 HTTP 响应 URI 匹配。 http_response.uri - 要匹配的值
HTTP 响应 URI 参数	与 HTTP 响应 URI 参数匹配。 http_response.uri_args - 要匹配的值
HTTP 响应版本	与 HTTP 响应版本匹配。 http_response.version - 要匹配的值
HTTP 响应 Cookie	与任何 HTTP 响应 cookie 匹配。 http_response.cookie_value - 要匹配的值
客户端 SSL	与客户端 SSL 配置文件 ID 匹配。 ssl_profile_id - 要匹配的值
TCP 标头端口	与 TCP 源或目标端口匹配。 tcp_header.source_port - 要匹配的源端口 tcp_header.destination_port - 要匹配的目标端口
IP 标头源	与 IP 源或目标地址匹配。 ip_header.source_address - 要匹配的源地址 ip_header.destination_address - 要匹配的目标地址

支持的匹配条件	说明
变量	创建一个变量并向该变量分配值。
区分大小写	设置区分大小写的标记进行 HTTP 标头值比较。
操作	说明
HTTP 响应标头重写	修改 HTTP 响应标头的值。 http_response.header_name - 标头名称 http_response.header_value - 要写入的值
HTTP 响应标头删除	删除 HTTP 标头。 http_request.header_delete - 标头名称 http_request.header_delete - 要写入的值
变量持久性学习	选择通用持久性配置文件，然后输入变量名称。 您还可以启用 哈希变量 。如果变量值非常长，则对变量进行哈希处理可确保能将其正确存储到持久性表中。如果未启用 哈希变量 ，则当变量值非常长时，只会将变量值的固定前缀部分存储到持久性表中。因此，对于具有长变量值的两个不同请求，它们应发送到不同的后端服务器，但因为其变量值具有相同的前缀部分，可能会发送到同一个后端服务器。

为服务器池和虚拟服务器创建的组

NSX Manager 会自动为负载均衡器服务器池和 VIP 端口创建组。

负载均衡器创建的组显示在**清单 > 组**下。

创建的服务器池组具有名称为 NLB.PoolLB.*Pool_Name LB_Name*，并分配有组成员 IP 地址：

- 配置为无 LB-SNAT（透明）的池：0.0.0.0/0
- 配置为无 LB-SNAT 自动映射的池：T1-Uplink IP 100.64.x.y 和 T1-ServiceInterface IP
- 配置为无 LB-SNAT IP-Pool 的池：LB-SNAT IP-Pool

创建的 VIP 组具有名称 NLB.VIP.*virtual server name*，VIP 组成员 IP 地址为 VIP IP@。

对于服务器池组，您可以创建分布式防火墙规则以允许来自负载均衡器 (NLB.PoolLB.*Pool_Name LB_Name*) 的流量。对于 Tier-1 网关防火墙，您可以创建相应的规则来允许从客户端到 LB VIP NLB.VIP.*virtual server name* 的流量。

转发策略

8

此功能适用于 NSX Cloud。

转发策略或基于策略的路由 (Policy-Based Routing, PBR) 规则定义了 NSX-T 如何处理来自 NSX 管理的虚拟机的流量。可以将该流量定向到 NSX-T 覆盖网络，也可以通过云提供商的（底层）网络路由该流量。

注 有关如何使用 NSX-T Data Center 管理公有云工作负载虚拟机的详细信息，请参见第 22 章 使用 NSX Cloud。

在转换 VPC/VNet 上部署 PCG 或将计算 VPC/VNet 链接到转换 VPC/VNet 后，将自动设置三个默认转发策略。

- 1 一个**路由到底层网络策略**，用于在转换/计算 VPC/VNet 中寻址的所有流量
- 2 另一个**路由到底层网络策略**，用于传输到公有云的元数据服务的所有流量。
- 3 一个**路由到覆盖网络策略**，用于所有其他流量，例如，传输到转换/计算 VPC/VNet 外部的流量。这些流量通过 NSX-T 覆盖网络隧道路由到 PCG 并进一步路由到目标。

注 对于传输到相同 PCG 管理的另一个 VPC/VNet 的流量：流量通过 NSX-T 覆盖网络隧道从 NSX 管理的源 VPC/VNet 路由到 PCG，然后路由到目标 VPC/VNet。

对于传输到不同 PCG 管理的另一个 VPC/VNet 的流量：流量通过 NSX 覆盖网络隧道从一个 NSX 管理的 VPC/VNet 路由到源 VPC/VNet 的 PCG，然后转发到 NSX 管理的目标 VPC/VNet 的 PCG。

如果流量传输到 Internet，则 PCG 在 Internet 中将其路由到目标。

在路由到底层网络时进行微分段

即使是将流量路由到底层网络的工作负载虚拟机，也会实施微分段。

如果您具有从 NSX 管理的工作负载虚拟机到管理的 VPC/VNet 外部的目标的直接连接，并且要绕过 PCG，请设置转发策略以通过底层网络路由来自该虚拟机的流量。

在通过底层网络路由流量时，将绕过 PCG，因此，流量不会遇到南北向防火墙。不过，您仍然需要管理东西向或分布式防火墙 (DFW) 的规则，因为在流量到达 PCG 之前将在虚拟机级别应用这些规则。

支持的转发策略及其常见用例

您可能会在下拉菜单中看到一组转发策略，但在该版本中仅支持以下转发策略：

- 路由到底层网络
- 从底层网络路由
- 路由到覆盖网络

这些转发策略可以在以下常见场景中使用：

- **路由到底层网络：**从 NSX 管理的虚拟机中访问底层网络上的服务。例如，访问 AWS 底层网络上的 AWS S3 服务。
- **从底层网络路由：**从底层网络中访问 NSX 管理的虚拟机上托管的服务。例如，从 AWS ELB 中访问 NSX 管理的虚拟机。

本章讨论了以下主题：

- [添加或编辑转发策略](#)

添加或编辑转发策略

您可以编辑自动创建的转发策略或添加新策略。

例如，要使用公有云提供的服务，例如 AWS 的 S3，可以手动创建策略，以允许一组 IP 地址通过底层网络路由来访问此服务。

前提条件

您必须拥有在上面部署了 PCG 的 VPC 或 VNet。

步骤

- 1 单击**添加区域**。适当地命名该部分，例如 **AWS 服务**。
- 2 选中该区域旁边的复选框，然后单击**添加规则**。命名该规则，例如 **S3 规则**。
- 3 在**源**选项卡中，选择具有工作负载虚拟机（要提供对它们的服务访问权限）的 VPC 或 VNet，例如 AWS VPC。在这里，还可以创建**组**以包括匹配一个或多个条件的多个虚拟机。
- 4 在**目标**选项卡中，选择托管该服务的 VPC 或 VNet，例如包含 AWS 中 S3 服务的 IP 地址的**组**。
- 5 在**服务**选项卡中，从下拉菜单中选择服务。如果服务不存在，可添加该服务。还可以将此选择保留**任何**，因为您可以在**目标**下提供路由详细信息。
- 6 在**操作**选项卡中，选择您希望路由工作的方式，例如，如果为 AWS S3 服务设置此策略，请选择**路由到底层网络**。
- 7 单击**发布**以完成转发策略的设置。

IP 地址管理 (IPAM)

9

要管理 IP 地址，可以配置 DNS（域名系统）、DHCP（动态主机配置协议）、IP 地址池和 IP 地址块。

注 IP 段由 NSX Container Plug-in (NCP) 使用。有关 NCP 的详细信息，请参见《适用于 Kubernetes 和 Cloud Foundry 的 NSX Container Plug-in - 安装和管理指南》。

本章讨论了以下主题：

- 添加 DNS 区域
- 添加 DNS 转发器服务
- 添加 DHCP 服务器
- 为 Tier-0 或 Tier-1 网关配置 DHCP 中继服务器
- 添加 IP 地址池
- 添加 IP 地址块

添加 DNS 区域

可以为 DNS 服务配置 DNS 区域。DNS 区域是 DNS 中域名空间的独特部分。

在配置 DNS 区域时，您可以为 DNS 转发器指定一个源 IP，以在将 DNS 查询转发到上游 DNS 服务器时使用。如果未指定源 IP，则 DNS 查询数据包的源 IP 将是 DNS 转发器的侦听器 IP。如果侦听器 IP 是无法从外部上游 DNS 服务器访问的内部地址，则需要指定源 IP。要确保将 DNS 响应数据包路由回转发器，需要一个专用源 IP。或者，您也可以在逻辑路由器上配置 SNAT 以将侦听器 IP 转换为公共 IP。在这种情况下，您不需要指定源 IP。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择 **网络 > IP 地址管理 > DNS**。
- 3 单击 **DNS 区域** 选项卡。

- 4 要添加默认区域，请选择**添加 DNS 区域 > 添加默认区域**
 - a 输入名称和可选的说明。
 - b 输入最多三个 DNS 服务器的 IP 地址。
 - c （可选）在**源 IP** 字段中输入 IP 地址。
- 5 要添加 FQDN 区域，请选择**添加 DNS 区域 > 添加 FQDN 区域**
 - a 输入名称和可选的说明。
 - b 输入域的 FQDN。
 - c 输入最多三个 DNS 服务器的 IP 地址。
 - d （可选）在**源 IP** 字段中输入 IP 地址。
- 6 单击**保存**。

添加 DNS 转发器服务

您可以将 DNS 转发器配置为将 DNS 查询转发到外部 DNS 服务器。

在配置 DNS 转发器之前，必须配置一个默认的 DNS 区域。您可以选择性地配置一个或多个 FQDN DNS 区域。每个 DNS 区域最多与 3 个 DNS 服务器相关联。配置 FQDN DNS 区域时，可指定一个或多个域名。一个 DNS 转发器可以与一个默认 DNS 区域和最多 5 个 FQDN DNS 区域相关联。收到 DNS 查询后，DNS 转发器会将查询中的域名与 FQDN DNS 区域中的域名进行比较。如果找到了匹配项，则会将查询转发到在 FQDN DNS 区域中指定的 DNS 服务器。如果未找到匹配项，则会将查询转发到在默认 DNS 区域中指定的 DNS 服务器。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**网络 > IP 地址管理 > DNS**。
- 3 单击**添加 DNS 服务**。
- 4 输入名称和可选的说明。
- 5 选择 Tier-0 或 Tier-1 网关。
- 6 输入 DNS 服务的 IP 地址。
客户端会将 DNS 查询发送到此 IP 地址，该地址也称为 DNS 转发器的侦听器 IP。
- 7 选择默认 DNS 区域。
- 8 选择日志级别。
- 9 最多选择五个 FQDN 区域。
- 10 单击**管理状态**切换按钮以启用或禁用 DNS 服务。
- 11 单击**保存**。

添加 DHCP 服务器

通过使用 DHCP（动态主机配置协议），客户端可以从 DHCP 服务器中自动获取网络配置，例如，IP 地址、子网掩码、默认网关和 DNS 配置。您可以创建 DHCP 服务器以处理 DHCP 请求。

注 VLAN 支持的分段上不支持使用此过程创建的 DHCP 服务器。您必须使用**高级网络和安全**下的 DHCP 功能来创建在 VLAN 支持的逻辑交换机上受支持的 DHCP 服务器。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**网络 > IP 地址管理 > DHCP**。
- 3 单击**添加服务器**。
- 4 选择 **DHCP 服务器**以作为服务器类型。
- 5 输入该服务器的名称。
- 6 使用 CIDR 格式输入该服务器的 IP 地址。

该步骤将创建两个逻辑端口（一个用于逻辑接口，另一个用于 DHCP 服务器本身），并将 DHCP 服务器连接到特定的 DHCP 逻辑交换机。该接口将在 Tier-0 或 Tier-1 网关上显示为连接的接口，因此，请确保为要将 DHCP 服务器分配到的 Tier-1 或 Tier-0 网关选择不重叠的子网。您可以指定 **<IP address>/30** 以实现该目的。不会向连接的 Tier-0 网关通告此处使用的子网范围，但会在 Tier-1 网关的转发表中显示该范围。

- 7 输入租约时间。
- 8 选择一个 NSX Edge 群集。
- 9 单击**保存**。
- 10 要将 DHCP 服务器分配给 Tier-0 或 Tier-1 网关，请执行以下操作：
 - a 导航到**网络 > Tier-0 网关**或**网络 > Tier-1 网关**。
 - b 编辑一个现有的网关。
 - c 在 **IP 地址管理**字段中，单击**无 IP 分配**。
 - d 从“类型”下拉列表中选择 **DHCP 本地服务器**。
 - e 选择一个 DHCP 服务器。
 - f 单击**保存**。
 - g 单击**保存**。
- 11 要将 DHCP 服务器分配给一个分段，请执行以下操作：
 - a 导航到**网络 > 分段**。
 - b 添加或编辑一个分段。

该分段必须与一个 Tier-0 或 Tier-1 网关相关联。

- c 如果要添加新的分段，请单击**设置子网**，或单击**子网**下面的编号以添加或修改一个子网。
- d 输入相应的 DHCP 范围。
- e 单击**应用**。
- f 单击**保存**。

为 Tier-0 或 Tier-1 网关配置 DHCP 中继服务器

通过使用 DHCP（动态主机配置协议），客户端可以从 DHCP 服务器中自动获取网络配置，例如，IP 地址、子网掩码、默认网关和 DNS 配置。您可以创建 DHCP 中继服务器以将 DHCP 流量中继到外部 DHCP 服务器。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**网络 > IP 地址管理 > DHCP**。
- 3 单击**添加服务器**。
- 4 选择 **DHCP 中继**以作为服务器类型。
- 5 输入中继服务器的名称。
- 6 为该服务器输入一个或多个 IP 地址。
- 7 单击**保存**。
- 8 转到**网络 > Tier-0 网关**或**网络 > Tier-1 网关**，以便为网关配置 DHCP 中继服务器。
- 9 编辑相应的网关。
- 10 在 **IP 地址管理**字段中，单击**无 IP 分配**（对于 Tier-0 网关）或**未设置 IP 分配集**（对于 Tier-1 网关）。
- 11 在**类型**字段中，选择 **DHCP 中继**。
- 12 在 **DHCP 中继**字段中，选择之前创建的 DHCP 中继服务器。
- 13 单击**保存**。
- 14 对于已连接到将使用此 DHCP 中继服务的网关的每个分段，均必须指定 DHCP 范围才能使中继正常运行。
 - a 转到**网络 > 分段**。
 - b 添加或编辑一个分段。
 - c 如果要添加新的分段，请单击**设置子网**，或单击**子网**下面的编号以修改子网。
 - d 指定一个或多个 DHCP 范围。

这是为使中继正常运行而必须执行的操作。

- e 单击**应用**。
- f 单击**保存**。

添加 IP 地址池

可以配置 IP 地址池，以供 DHCP 等组件使用。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**网络 > IP 地址管理 > IP 地址池**。
- 3 单击**添加 IP 地址池**。
- 4 输入名称和可选的说明。
- 5 单击**子网**列中的**设置**以添加子网。
- 6 要指定地址块，请选择**添加子网 > IP 块**。
 - a 选择 IP 块。
 - b 指定大小。
 - c 单击**自动分配网关**切换开关以启用或禁用自动网关 IP 分配。
 - d 单击**添加**。
- 7 要指定 IP 范围，请选择 **添加子网 > IP 范围**。
 - a 输入 IPv4 或 IPv6 范围。
 - b 使用 CIDR 格式输入 IP 范围。
 - c 输入一个地址作为**网关 IP**。
 - d 单击**添加**。
- 8 单击**保存**。

添加 IP 地址块

您可以配置 IP 地址块供其他组件使用。

注 还可以通过导航到**高级网络 and 安全性 > 网络 > IPAM** 来添加 IP 地址块。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**网络 > IP 地址管理 > IP 地址池**。
- 3 单击 **IP 地址块**选项卡。
- 4 单击**添加 IP 地址块**。

- 5 输入名称和可选的说明。
- 6 使用 CIDR 格式输入一个 IP 块。
- 7 单击**保存**。

本节中的主题涵盖分布式防火墙规则、身份防火墙、网络侦测、网关防火墙和端点保护策略的南北向和东西向安全功能。

本章讨论了以下主题：

- 安全配置概述
- 安全术语
- 身份防火墙
- 第 7 层上下文配置文件
- 分布式防火墙
- 东西向网络安全 - 第三方服务链
- 配置网关防火墙
- 南北向网络安全 - 插入第三方服务
- 端点保护
- 安全配置文件

安全配置概述

可以为您的环境在预定义的类别下配置东西向和南北向防火墙策略。

分布式防火墙（东西向）和网关防火墙（南北向）提供了多组按类别划分的可配置规则。可以配置一个排除列表，其中包含要从防火墙实施中排除的逻辑交换机、逻辑端口或组。

安全策略按以下方式实施：

- 规则在类别中按从左到右的顺序进行处理。
- 规则是按从上到下的顺序处理的。
- 根据规则表中的最上面规则检查每个数据包，然后向下移到表中的后续规则。
- 强制实施表中与流量参数匹配的第一个规则。

无法强制实施后续规则，因为随后将停止为该数据包搜索规则。由于这种行为，始终建议将最精细的策略放在规则表顶部。这可确保这些规则将在更具体的规则之前加以实施。

安全术语

以下术语将在整个分布式防火墙中使用。

表 10-1. 与安全相关的术语

构造	定义
策略	安全策略包括防火墙规则和服务配置等各种安全元素。策略以前称为防火墙区域。
规则	作为流量评估依据和定义在匹配时所执行操作的一组参数。规则包括源和目标、服务、上下文配置文件、日志记录以及标记等参数。
组	组包括静态和动态添加的不同对象，可用作防火墙规则的源和目标字段。可以将组配置为包含虚拟机、IP 集、MAC 集、逻辑端口、逻辑交换机、AD 用户组和其他嵌套组的组合。可以基于标记、虚拟机名称、操作系统名称或计算机名称动态包含组。 创建组时，必须包括该组所属的域，默认情况下为默认域。 组以前称为 NS 组或安全组。
服务	定义端口和协议的组合。用于根据端口和协议对流量进行分类。可以在防火墙规则中使用预定义的服务和用户定义的服务。
上下文配置文件	定义上下文感知的属性，其中包括应用程序 ID 和域名。此外，还包括子属性，如应用程序版本或密码集。防火墙规则可以包含上下文配置文件以启用第 7 层防火墙规则。

身份防火墙

通过使用身份防火墙 (Identity Firewall, IDFW) 功能，NSX 管理员可以创建基于 Active Directory 用户的分布式防火墙 (DFW) 规则。

IDFW 可用于虚拟桌面 (VDI) 或远程桌面会话 (RDSH 支持)，从而允许多个用户同时登录，根据要求访问用户应用程序并且能够保持独立的用户环境。VDI 管理系统控制向哪些用户授予对 VDI 虚拟机的访问权限。NSX-T 从启用了 IDFW 的源虚拟机 (Virtual Machine, VM) 控制对目标服务器的访问。使用 RDSH，管理员在 Active Directory (AD) 中创建具有不同用户的安全组，并根据角色允许或拒绝这些用户访问应用程序服务器。例如，人力资源和工程部门可以连接到同一个 RDSH 服务器，并且可以访问该服务器中的不同应用程序。

IDFW 还可在具有受支持操作系统的虚拟机上使用。请参见[身份防火墙支持的配置](#)。

IDFW 配置 workflow 简要概述首先介绍了基础架构准备。准备工作包括管理员在每个保护的集群上安装主机准备组件和设置 Active Directory 同步，以便 NSX 可以使用 AD 用户和组。接下来，IDFW 必须知道 Active Directory 用户登录到的桌面才能应用 IDFW 规则。当用户生成网络事件时，在虚拟机上随 VMware Tools 一起安装的 Thin Agent 将收集和转发该信息，并将该信息发送到上下文引擎。该信息用于提供分布式防火墙的实施。

IDFW 仅在分布式防火墙规则中处理源中的用户身份。基于身份的组不能用作 DFW 规则中的目标。

注 IDFW 依赖于客户机操作系统的安全性和完整性。恶意本地管理员可以通过多种方法来伪造其身份以绕过防火墙规则。用户身份信息由客户机虚拟机中的 NSX Guest Introspection Thin Agent 提供。安全管理员必须确保已在每个客户机虚拟机中安装并运行 Thin Agent。已登录的用户不应具有移除或停止该代理的特权。

有关支持的 IDFW 配置，请参见[身份防火墙支持的配置](#)。

IDFW 工作流：

- 1 用户通过打开 Skype 或 Outlook 登录到虚拟机并启动网络连接。
- 2 Thin Agent 将检测用户登录事件，它会收集连接信息和身份信息，并将该信息发送到上下文引擎。
- 3 上下文引擎将该连接和身份信息转发到分布式防火墙实施任何适用的规则。

身份防火墙工作流

IDFW 允许基于用户身份的防火墙规则，从而对传统防火墙进行了增强。例如，管理员可以允许或禁止客户支持人员通过单个防火墙策略访问 HR 数据库。

基于身份的防火墙规则是由 Active Directory (AD) 组成员的成员资格确定的。请参见[身份防火墙支持的配置](#)。

IDFW 仅在分布式防火墙规则中处理源中的用户身份。基于身份的组不能用作 DFW 规则中的目标。

注 对于身份防火墙规则实施，应为所有使用 Active Directory 的虚拟机开启 Windows 时间服务。这会确保在 Active Directory 和虚拟机之间同步日期和时间。AD 组成员资格变化（包括启用和删除用户）不会立即对登录的用户生效。要使更改生效，用户必须注销，然后重新登录。在修改组成员资格时，AD 管理员应强制注销。此行为是 Active Directory 存在的一个限制。

前提条件

如果在虚拟机上启用了 Windows 自动登录，请转到[本地计算机策略 > 计算机配置 > 管理模板 > 系统 > 登录](#)，然后启用[计算机启动和登录时总是等待网络](#)。

有关支持的 IDFW 配置，请参见[身份防火墙支持的配置](#)。

步骤

- 1 启用 NSX 文件侦测驱动程序和 NSX 网络侦测驱动程序。默认情况下，执行 VMware Tools 完全安装时会添加这些驱动程序。
- 2 在集群或独立主机上启用 IDFW：[启用身份防火墙](#)。
- 3 配置 Active Directory 域：[添加 Active Directory](#)。
- 4 配置 Active Directory 同步操作：[同步 Active Directory](#)。
- 5 创建包含 Active Directory 组成员的安全组 (SG)：[添加组](#)。
- 6 将包含 AD 组成员的 SG 分配给分布式防火墙规则：[添加分布式防火墙](#)。

启用身份防火墙

必须启用身份防火墙，IDFW 防火墙规则才能生效。

步骤

- 1 选择[安全 > 分布式防火墙](#)。
- 2 在左侧角，单击[操作 > 常规设置](#)。

3 切换状态按钮以启用 IDFW。

还必须启用分布式防火墙以使 IDFW 正常工作。

4 要在独立主机或集群上启用 IDFW，请选择身份防火墙设置选项卡。

5 切换启用栏，然后选择独立主机，或选择必须启用 IDFW 主机的集群。

6 单击保存。

身份防火墙最佳做法

以下最佳做法有助于最大限度提高身份防火墙规则的成功率。

- IDFW 支持以下协议：
 - 单用户（VDI 或非 RDSH 服务器）用例支持 - TCP、UDP、ICMP
 - 多用户 (RDSH) 用例支持 - TCP、UDP
 - 。
- 单个基于 ID 的组只能在分布式防火墙规则中用作源。如果在源中需要使用基于 IP 和基于 ID 的组，请创建两个单独的防火墙规则。
- 对域进行的任何更改（包括域名更改）将触发与 Active Directory 之间的完全同步。由于完全同步可能需要很长的时间，我们建议在非高峰时间或非办公时间进行同步。
- 对于本地域控制器，将在 Active Directory 同步中使用默认 LDAP 端口 389 和 LDAPS 端口 636，不应编辑这些端口号以将其更改为非默认值。

身份防火墙支持的配置

虚拟机 (VM) 上的 IDFW 支持以下配置。不支持物理设备的 IDFW。

客户机操作系统	实施类型
Windows 8	桌面 - 支持桌面用户用例
Windows 10	桌面 - 支持桌面用户用例
Windows 2012	服务器 - 支持服务器用户用例
Windows 2012R2	服务器 - 支持服务器用户用例
Windows 2016	服务器 - 支持服务器用户用例
Windows 2012R2	RDSH - 支持远程桌面会话主机
Windows 2016	RDSH - 支持远程桌面会话主机

Active Directory 域控制器：

- Windows Server 2012
- Windows Server 2012R2
- Windows Server 2016
- Windows Server 2019

主机操作系统：ESXi

VMware Tools - 版本 11

- VMCI 驱动程序
- NSX 文件侦测驱动程序
- NSX 网络侦测驱动程序

第 7 层上下文配置文件

第 7 层应用程序 ID 已配置为上下文配置文件的一部分。

上下文配置文件可以指定一个或多个 **属性**，除此之外，该配置文件还可以包含子属性，以供在分布式防火墙 (DFW) 规则和网关防火墙规则中使用。定义子属性时，例如 TLS 版本 1.2，不支持多个应用程序标识属性。除了属性外，DFW 还支持使用可在上下文配置文件中指定的完全限定域名 (FQDN) 或 URL 来将 FQDN 加入白名单或黑名单。目前，支持预定义域列表。可以在一个上下文配置文件中将 FQDN 与属性一起配置，或者也可以在不同的上下文配置文件中分别对二者进行配置。定义上下文配置文件后，即可将其应用于一个或多个分布式防火墙规则。

目前，支持预定义域列表。在添加属性类型域名 (FQDN) 的新上下文配置文件时，您可以看到 FQDN 列表。此外，您还可以通过运行 API 调用 `/policy/api/v1/infra/context-profiles/attributes?attribute_key=DOMAIN_NAME` 来查看 FQDN 列表。

注

- 网关防火墙规则不支持在上下文配置文件中使用 FQDN 属性或其他子属性。
 - Tier-0 网关防火墙策略不支持上下文配置文件。网关防火墙规则不支持使用 FQDN 属性或其他子属性。
-

如果已在规则中使用某个上下文配置文件，则将根据基于 5 元组的规则表匹配来自虚拟机的任何流量。如果匹配流量的规则还包括第 7 层上下文配置文件，该数据包将被重定向到名为 vDPI 引擎的用户空间组件。会针对每个流量将后续的少量数据包推送到该 vDPI 引擎，确定应用程序 ID 后，此信息将存储在内核内的上下文表中。在该流量的下一个数据包进入时，会再次将上下文表中的信息与规则表进行比较，然后按 5 元组和第 7 层应用程序 ID 进行匹配。将采取在完全匹配规则中定义的相应措施，如果存在允许规则，将在内核中处理该流量的所有后续数据包，并根据连接表进行匹配。对于完全匹配的丢弃规则，会生成拒绝数据包。如果将该流量推送到 DPI，防火墙生成的日志将包含第 7 层应用程序 ID 和适用 URL。

入站数据包的规则处理：

- 1 在数据包进入 DFW 或网关筛选器后，将基于 5 元组在流量表中查找数据包。
- 2 如果找不到任何流量/状态，则会基于 5 元组将流量与规则表相匹配，并且会在流量表中创建一个条目。
- 3 如果流量与具有第 7 层服务对象的规则匹配，则流量表状态会被标记为“DPI 正在进行”。
- 4 之后，流量会被推送到 DPI 引擎。DPI 引擎将确定应用程序 ID。
- 5 在确定应用程序 ID 后，DPI 引擎会向下发送已插入到此流量上下文表中的属性。“DPI 正在进行”标记将被移除，并且流量不再被推送到 DPI 引擎。

- 6 流量（现在具有应用程序 ID）将针对匹配应用程序 ID 的所有规则重新进行评估，该过程从基于 5 元组匹配的原始规则开始，并会选择第一个完全匹配的 L4/L7 规则。将会执行适当的操作（允许/拒绝），并相应地更新流量表条目。

第 7 层防火墙规则 workflow

创建在分布式防火墙规则或网关防火墙规则中使用的上下文配置文件时，将使用第 7 层应用程序 ID。通过基于属性的规则实施，用户可以允许或拒绝在任何端口上运行应用程序。

NSX-T 为常见基础架构和企业应用程序提供内置 [属性](#)。应用程序 ID 包括版本（SSL/TLS 和 CIFS/SMB）和密码套件（SSL/TLS）。对于分布式防火墙，应用程序 ID 通过上下文配置文件在规则中使用，且可以与 FQDN 白名单和黑名单组合在一起。ESXi 和 KVM 主机上支持应用程序 ID。

注

- 网关防火墙规则不支持在上下文配置文件中使用 FQDN 属性或其他子属性。
 - Tier-0 网关防火墙策略不支持上下文配置文件。网关防火墙规则不支持使用 FQDN 属性或其他子属性。
-

支持的应用程序 ID 和 FQDN:

- 对于 FQDN，用户需要在端口 53 上为指定的 DNS 服务器配置一个具有 DNS 应用程序 ID 的高优先级规则。
- 对于 ALG 应用程序 ID（FTP、ORACLE、DCERPC、TFTP），需要为防火墙规则提供对应的 ALG 服务。
- 仅在标准端口上会检测到 SYSLOG 应用程序 ID。

KVM 支持的应用程序 ID 和 FQDN:

- KVM 不支持子属性。
- KVM 支持 FTP 和 TFTP ALG 应用程序 ID。

请注意，如果您结合使用第 7 层和 ICMP 或者任何其他协议，则需要最后放置第 7 层防火墙规则。将不会执行排在第 7 层任意/任意规则之前的任何规则。

步骤

- 1 创建自定义上下文配置文件：[添加上下文配置文件](#)。
- 2 在分布式防火墙规则或网关防火墙规则中使用上下文配置文件：[添加分布式防火墙](#) 或 [添加网关防火墙策略和规则](#)。

在将服务设置为任意的防火墙规则中可以使用多个应用程序 ID 上下文配置文件。对于 ALG 配置文件（FTP、ORACLE、DCERPC、TFTP），每个规则支持一个上下文配置文件。

属性

第 7 层属性（应用程序 ID）可识别特定的数据包或流量由哪个应用程序生成，而这一过程与所使用的端口无关。

通过基于应用程序 ID 的实施，用户可以允许或拒绝应用程序在任何端口上运行，或者强制应用程序在其标准端口上运行。vDPI 允许将数据包负载与定义的模式（通常称为签名）进行匹配。基于签名的标识和实施让客户不仅能够匹配流量所属的特定应用程序/协议，而且还能够匹配该协议的版本，例如 TLS 版本 1.0、TLS 版本 1.2 或 CIFS 流量的不同版本。这使客户能够了解或限制使用对数据中心内部署的所有应用程序及其东西向流量具有已知漏洞的协议。

第 7 层应用程序 ID 在分布式防火墙规则和网关防火墙规则的上下文配置文件中使用时，并且受 ESXi 和 KVM 主机支持。

注 NFS 第 4 版不是支持的属性。

注

- 网关防火墙规则不支持在上下文配置文件中使用时使用 FQDN 属性或其他子属性。
- Tier-0 网关防火墙策略不支持上下文配置文件。网关防火墙规则不支持使用 FQDN 属性或其他子属性。

支持的应用程序 ID 和 FQDN:

- 对于 FQDN，用户需要在端口 53 上为指定的 DNS 服务器配置一个具有 DNS 应用程序 ID 的高优先级规则。
- 对于 ALG 应用程序 ID（FTP、ORACLE、DCERPC、TFTP），需要为防火墙规则提供对应的 ALG 服务。
- 仅在标准端口上会检测到 SYSLOG 应用程序 ID。

KVM 支持的应用程序 ID 和 FQDN:

- KVM 不支持子属性。
- KVM 支持 FTP 和 TFTP ALG 应用程序 ID。

属性（应用程序 ID）	说明	类型
360ANTIV	360 安全卫士是由中国的 IT 公司奇虎 360 所开发的一款程序	Web 服务
ACTIVDIR	Microsoft Active Directory	网络
AMQP	高级消息队列协议是一种应用程序层协议，它支持应用程序或组织之间的业务消息通信	网络
AVAST	因浏览 Avast 防病毒软件下载的官方网站 Avast.com 而生成的流量	Web 服务
AVG	AVG 防病毒/安全软件下载和更新	文件传输
AVIRA	Avira 防病毒/安全软件下载和更新	文件传输
BLAST	一种远程访问协议，可在数据中心对计算体验进行压缩、加密和编码，然后跨 VMware Horizon 桌面的任何标准 IP 网络对其进行传输。	远程访问

属性（应用程序 ID）	说明	类型
BDEFENDER	BitDefender 防病毒/安全软件下载和更新	文件传输
CA_CERT	证书颁发机构 (CA) 颁发数字证书，以便对用于消息加密的公钥的所有权进行认证	网络
CIFS	CIFS（通用 Internet 文件系统）用于在网络上的节点之间提供对目录、文件、打印机和串行端口的共享访问及其他通信	文件传输
CLDAP	无连接轻量级目录访问协议是一种使用 UDP 在 Internet 协议 (IP) 网络上访问和维护分布式目录信息服务的应用程序协议。	网络
CTRXCGP	Citrix 通用网关协议是一种使用 UDP 在 Internet 协议 (IP) 网络上访问和维护分布式目录信息服务的应用程序协议。	数据库
CTRXCOTO	托管 Citrix GoToMeeting，或基于 GoToMeeting 平台的类似会话。包括语音、视频和有限的人群管理功能	协作
CTRICA	ICA（独立计算架构）是由 Citrix Systems 设计的一种用于应用程序服务器系统的专有协议	远程访问
DCERPC	分布式计算环境/远程过程调用，这是一种为分布式计算环境 (Distributed Computing Environment, DCE) 开发的远程过程调用系统	网络
DIAMETER	一种用于计算机网络的身份验证、授权和计帐协议	网络
DHCP	动态主机配置协议是用于管理网络内 IP 地址分发的协议	网络
DNS	通过 TCP 或 UDP 查询 DNS 服务器	网络
EPIC	Epic EMR 是一个电子病历应用程序，用于提供病患护理和医疗保健信息。	客户端服务器
ESET	Eset 防病毒/安全软件下载和更新	文件传输
FPROT	F-Prot 防病毒/安全软件下载和更新	文件传输
FTP	FTP（文件传输协议）用于将文件从文件服务器传输到本地计算机	文件传输
GITHUB	基于 Web 的 Git 或版本控制存储库和 Internet 托管服务	协作
HTTP	（超文本传输协议）万维网的主要传输协议	Web 服务
HTTP2	因浏览支持 HTTP 2.0 协议的网站而生成的流量	Web 服务
IMAP	IMAP（Internet 邮件访问协议）是一种用于访问远程服务器上的电子邮件的 Internet 标准协议	邮件
KASPRSKY	Kaspersky 防病毒/安全软件下载和更新	文件传输
KERBEROS	Kerberos 是一种网络身份验证协议，旨在通过使用密钥加密为客户端/服务器应用程序提供强身份验证	网络
LDAP	LDAP（轻量级目录访问协议）是一种用于读取和编辑 IP 网络上的目录的协议	数据库
MAXDB	对 MaxDB SQL 服务器进行的 SQL 连接和查询	数据库
MCAFEE	McAfee 防病毒/安全软件下载和更新	文件传输

属性（应用程序 ID）	说明	类型
MSSQL	Microsoft SQL Server 是一个关系型数据库。	数据库
NFS	允许客户端计算机上的用户以一种类似于访问本地存储的方式通过网络访问文件。 注 NFS 第 4 版不是支持的属性。	文件传输
NNTP	Internet 应用程序协议，用于在新闻服务器之间传输 Usenet 新闻文章 (netnews) 以及由最终用户客户端应用程序读取和发布文章。	文件传输
NTBIOSNS	NetBIOS 名称服务。要启动会话或分发数据报，应用程序必须使用该名称服务注册其 NetBIOS 名称	网络
NTP	NTP（网络时间协议）用于同步网络上计算机系统的时钟	网络
OCSP	一种 OCSP 响应程序，用于验证用户的私钥尚未被泄露或撤销	网络
ORACLE	由 Oracle 公司开发和销售的一种对象关系型数据库管理系统 (Object-Relational Database Management System, ORDBMS)。	数据库
PANDA	Panda 安全防病毒/安全软件下载和更新。	文件传输
PCOIP	一种远程访问协议，可在数据中心对计算体验进行压缩、加密和编码，然后跨任何标准 IP 网络对其进行传输。	远程访问
POP2	POP（邮局协议）是由本地电子邮件客户端用来从远程服务器检索电子邮件的一种协议。	邮件
POP3	Microsoft 实施的 NetBIOS 名称服务 (NetBIOS Name Service, NBNS)，它是一种用于 NetBIOS 计算机名称的名称服务器和服务。	邮件
RADIUS	提供集中式身份验证、授权和计帐 (Authentication, Authorization and Accounting, AAA) 管理，以使计算机连接和使用网络服务	网络
RDP	RDP（远程桌面协议）为用户提供另一台计算机的图形界面	远程访问
RTCP	RTCP（实时传输控制协议）是实时传输协议 (Real-time Transport Protocol, RTP) 的姊妹协议。RTCP 提供 RTP 流量的带外控制信息。	流媒体
RTP	RTP（实时传输协议）主要用于提供实时音频和视频	流媒体
RTSP	RTSP（实时流协议）用于建立和控制端点之间的媒体会话	流媒体
SIP	SIP（会话发起协议）是一种用于设置和控制语音和视频通话的通用控制协议	流媒体
SMTP	SMTP（简单邮件传输协议）是一种用于跨 Internet 协议 (Internet Protocol, IP) 网络传输电子邮件的 Internet 标准。	邮件
SNMP	SNMP（简单网络管理协议）是一种用于管理 IP 网络上的设备的 Internet 标准协议。	网络监控
SSH	SSH（安全 Shell）是一种网络协议，允许使用安全通道在两个联网设备之间交换数据。	远程访问
SSL	SSL（安全套接字层）是一种加密协议，可提供 Internet 上的安全性。	Web 服务
SYMUPDAT	Symantec LiveUpdate 流量，这包括间谍软件定义、防火墙规则、防病毒特征码文件和软件更新。	文件传输

属性（应用程序 ID）	说明	类型
SYSLOG	SYSLOG 是一种协议，它允许网络设备将事件消息发送到日志记录服务器。	网络监控
TELNET	在 Internet 或局域网上使用的一种网络协议，用于使用虚拟终端连接提供面向交互式文本的双向通信。	远程访问
TFTP	TFTP（普通文件传输协议）用于使用客户端（如 WinAgents TFTP 客户端）列出 TFTP 服务器（如 SolarWinds TFTP 服务器）上的文件，从该服务器下载文件，以及将文件上传到该服务器。	文件传输
VNC	虚拟网络计算的流量。	远程访问
WINS	Microsoft 实施的 NetBIOS 名称服务 (NBNS)，它是一种用于 NetBIOS 计算机名称的名称服务器和服务。	网络

分布式防火墙

分布式防火墙附带有防火墙规则的预定义类别。先从上到下，然后从左到右对规则进行评估。

表 10-2. 分布式防火墙规则类别

类别	说明
以太网	用于基于第 2 层的规则
紧急	用于隔离和允许规则
基础架构	定义对共享服务的访问。全局规则 - AD、DNS、NTP、DHCP、备份、管理服务器
环境	区域之间的规则 - 生产与开发，业务单位之间的规则
应用程序	应用程序、应用程序层之间的规则，或微服务之间的规则

防火墙草稿

草稿是一个包含策略部分和规则的完整分布式防火墙配置。草稿可以自动保存或手动保存，并且可以立即发布或先保存以供将来发布。

要手动保存防火墙配置草稿，请转到分布式防火墙屏幕的右上角，然后单击**操作 > 保存**。保存后，可以通过选择**操作 > 查看**来查看配置。默认情况下，自动草稿处于启用状态。通过转到**操作 > 常规设置**，可禁用自动草稿。启用自动草稿后，对防火墙配置进行的任何更改都会导致系统生成自动草稿。最多可保存 100 个自动草稿和 10 个手动草稿。可对自动草稿进行编辑并将其另存为手动草稿，以供立即发布或以后发布。为了防止多个用户打开和编辑草稿，可以锁定手动草稿。草稿发布后，当前配置将替换为草稿中的配置。

保存或查看防火墙草稿

草稿是一种已经发布或者已保存以供日后发布的分布式防火墙配置。草稿可以自动创建和手动创建。

可以编辑和保存手动草稿。可以克隆自动草稿并将其另存为手动草稿，然后进行编辑。可保存的最大草稿数量为 100 个自动草稿和 10 个手动草稿。

步骤

1 单击**安全 > 分布式防火墙**。

2 要手动保存防火墙配置，请转到**操作 > 保存**。

可以保存手动草稿，或对其进行编辑然后再保存。保存后，您可以恢复到原始配置。

3 **命名**配置。

4 为防止多个用户打开和编辑手动草稿，请**锁定**该配置，并添加注释。

5 单击**保存**。

6 要查看保存的配置，请单击**操作 > 查看**。

将打开一个时间轴，显示所有已保存的配置。要查看草稿名称、日期、时间和保存者等详细信息，请指向任何草稿的点图标或星形图标。已保存的配置可以按时间筛选，显示最近一天、一周、30 天或过去三个月的所有草稿。可以按自动草稿和我保存的草稿筛选这些草稿。也可以使用右上方的搜索工具按名称筛选这些草稿。

7 将鼠标悬停在草稿上可查看已保存配置的名称、日期和时间详细信息。单击名称可查看详细信息。

详细的草稿视图显示了为与此草稿同步而需要对当前防火墙配置所做的更改。如果发布此草稿，则此视图中显示的所有更改都将应用于当前配置。

单击向下箭头可展开每个部分，并且可以显示每个部分中已添加、修改和删除的更改。比较显示，已添加的规则在左侧方框中具有绿色条，已修改的元素（例如名称更改）具有黄色条，已删除的元素具有红色条。

8 要编辑所选草稿的名称或描述，请单击**查看草稿详细信息**窗口中的菜单图标（三个点），然后选择**编辑**。

可以锁定手动草稿。如果锁定，则必须为草稿提供相关注释。

有些角色（如企业管理员）具有完全访问凭据，无法锁定。请参见[基于角色的访问控制](#)。

9 也可以通过单击**克隆**来克隆和保存自动草稿和手动草稿。

在“保存的配置”窗口中，您可以接受默认名称，也可以对其进行编辑。您还可以锁定配置。如果锁定，则必须为草稿提供相关注释。

10 要保存已克隆的草稿配置版本，请单击**保存**。该草稿会立即显示在“保存的配置”部分中。

后续步骤

查看草稿后，您可以加载并发布该草稿。随后，它将成为活动的防火墙配置。

发布或恢复防火墙草稿

您可以加载并发布自动草稿和保存的手动草稿以成为活动配置。

在发布过程中，将创建新的自动草稿。可以发布此自动草稿以恢复到先前的配置。

步骤

- 1 要查看保存的配置，请单击**操作 > 查看**。

将打开一个时间轴，显示所有已保存的配置。要查看草稿名称、日期、时间和保存者等详细信息，请指向任何草稿的点图标。已保存的配置按时间筛选，显示在 1 天、1 周、30 天或过去 3 个月中创建的所有草稿。

- 2 单击草稿名称，此时将显示“查看草稿详细信息”窗口。

- 3 单击**加载**。主窗口中将显示新的防火墙配置。

注 如果正在使用防火墙筛选器，或者当前配置中存在未保存的更改，则无法加载草稿。

- 4 要提交草稿配置并使其处于活动状态，请单击**发布**。要返回到以前发布的配置，请单击**恢复**。

发布后，草稿中的更改将存在于活动配置中。

- 5 要在发布之前编辑所选草稿的内容，请在单击**加载**后，编辑配置。

- 6 要保存已编辑的草稿配置版本，请单击**操作 > 保存**。

手动草稿可以另存为新的配置或对现有配置的更新。自动草稿只能另存为新配置。

- 7 输入**名称**和可选的**说明**。您还可以**锁定**草稿。如果锁定，则必须为草稿提供相关注释。

- 8 单击**保存**。

- 9 要提交草稿配置并使其处于活动状态，请单击**发布**；或者要返回先前发布的配置，请单击**恢复**。

添加分布式防火墙

分布式防火墙 (DFW) 监控虚拟机上的所有东西向流量。

前提条件

要由 DFW 保护的客户机虚拟机必须将其 vNIC 连接到与传输区域关联的 N-VDS 逻辑交换机。

如果您要为身份防火墙创建规则，首先创建一个具有 Active Directory 成员的组。IDFW 仅支持基于 TCP 的防火墙规则。

注 对于身份防火墙规则实施，应为所有使用 Active Directory 的虚拟机开启 Windows 时间服务。这会确保在 Active Directory 和虚拟机之间同步日期和时间。AD 组成员资格变化（包括启用和删除用户）不会立即对登录的用户生效。要使更改生效，用户必须注销，然后重新登录。在修改组成员资格时，AD 管理员应强制注销。此行为是 Active Directory 存在的一个限制。

请注意，如果您结合使用第 7 层和 ICMP 或者任何其他协议，则需要最后放置第 7 层防火墙规则。将不会执行排在第 7 层任意/任意规则之前的任何规则。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。

- 2 从导航面板中选择**安全 > 分布式防火墙**。

- 3 通过选择**操作 > 常规设置**，然后切换“分布式防火墙状态”按钮，启用分布式防火墙。单击**保存**。

- 4 确保您处于正确的预定义类别，然后单击**添加策略**。有关类别的详细信息，请参见[分布式防火墙](#)。
- 5 输入新策略区域的**名称**。
- 6 （可选）要配置以下策略设置，请单击齿轮图标：

选项	说明
TCP 严格模式	<p>TCP 连接以三向握手（SYN、SYN-ACK、ACK）开始，通常以双向交换（FIN、ACK）结束。在某些情况下，分布式防火墙（DFW）可能看不到特定流的三向握手（由于非对称流量或在流存在时启用分布式防火墙）。默认情况下，分布式防火墙不强制要求看到三向握手，并选取已建立的会话。可以在每个区域启用“TCP 严格模式”，以禁止在会话中途提取数据，并实现三向握手要求。</p> <p>如果为特定 DFW 策略启用 TCP 严格模式，并使用默认“任意-任意”阻止规则，将丢弃该区域中不符合三向握手连接要求并与基于 TCP 的规则匹配的数据包。“严格模式”仅适用于有状态 TCP 规则，并在分布式防火墙策略级别启用。对于与默认“任意-任意”允许规则（没有指定任何 TCP 服务）匹配的数据包，不会强制采用 TCP 严格模式。</p>
有状态	有状态防火墙监控活动连接的状态，并使用此信息来确定允许哪些数据包通过防火墙。
已锁定	<p>可以锁定策略，以防止多个用户对相同区域进行编辑。锁定某个区域时，必须包含一条注释。</p> <p>有些角色（如企业管理员）具有完全访问凭据，无法锁定。请参见基于角色的访问控制。</p>

- 7 单击**发布**。可以添加多个策略，然后一起发布。
新策略将显示在屏幕上。
- 8 选择策略区域，然后单击**添加规则**。
- 9 输入规则的名称。
- 10 在**源**列中，单击编辑图标并选择规则的源。可以将具有 Active Directory 成员的组用作 IDFW 规则的源字段。有关详细信息，请参见[添加组](#)。
支持 IPv4、IPv6 和多播地址。
注意：IPv6 防火墙必须在已连接分段上启用 IPv6 IP 发现。有关详细信息，请参见[了解 IP 发现分段配置文件](#)。
- 11 在**目标**列中，单击编辑图标并选择规则的目标。如果未定义，目标将匹配**任意**。有关详细信息，请参见[添加组](#)。支持 IPv4、IPv6 和多播地址。
- 12 在**服务**列中，单击编辑图标并选择服务。如果未定义，服务将与**任意**匹配。

- 13 将规则添加到以太网类别时，此**配置文件**列不可用。对于所有其他规则类别，在**配置文件**列中，单击编辑图标并选择上下文配置文件，或单击**添加新的上下文配置文件**。请参见**添加上下文配置文件**。

上下文配置文件使用第 7 层应用程序 ID 属性用于分布式防火墙规则和网关防火墙规则。在将服务设置为**任意的**防火墙规则中可以使用多个应用程序 ID 上下文配置文件。对于 ALG 配置文件（FTP 和 TFTP），每个规则支持一个上下文配置文件。

- 14 单击**应用**以将上下文配置文件应用于规则。

- 15 默认情况下，**应用对象**列设置为 DFW，并且此规则应用于所有工作负载。您还可以将规则或策略应用于选定的组。**应用对象**按规则定义实施范围，主要用于 ESXi 和 KVM 主机上的优化或资源。这有助于为特定区域和租户定义目标策略，而不会干扰为其他租户和区域定义的其他策略。

不能在**应用对象**文本框中使用仅包含 IP 地址的组、仅包含 MAC 地址的组或 Active Directory 组。

- 16 在**操作**列中，选择一个操作。

选项	说明
允许	允许具有指定的源、目标和协议的所有 L3 或 L2 流量通过当前防火墙上下文。与规则匹配并接受的数据包将通过系统，就好像没有防火墙一样。
丢弃	丢弃具有指定的源、目标和协议的数据包。丢弃数据包是一个静默操作，不会向源或目标系统发送通知。丢弃数据包将导致重试连接，直到达到重试阈值。
拒绝	拒绝具有指定的源、目标和协议的数据包。拒绝数据包是一种较友好的数据包阻止方式，因为将向发送方发送“无法到达目标 (destination unreachable)”消息。如果协议是 TCP，则会发送 TCP RST 消息。对于 UDP、ICMP 和其他 IP 连接，发送包含管理上被禁止的代码的 ICMP 消息。使用“拒绝”的一个好处是，在仅尝试一次后，就会向发送应用程序通知无法建立连接。

- 17 单击状态切换按钮以启用或禁用规则。

- 18 （可选）单击齿轮图标以配置以下规则选项：

选项	说明
日志记录	默认情况下，将禁用日志记录。日志存储在 ESXi 和 KVM 主机上的 /var/log/dfwptlogs.log 文件中。
方向	指从目标对象角度来查看的流量方向。“入站”表示只检查流入对象的流量，“出站”表示只检查从对象流出的流量，“双向”表示检查两个方向的流量。
IP 协议	基于 IPv4、IPv6 或 IPv4-IPv6 实施规则。
日志标签	启用日志记录后，防火墙日志中将带有日志标签。

- 19 单击**发布**。可以添加多个规则，然后一起发布。

- 20 对于每个规则，单击**信息**图标以查看规则 ID 号和强制执行规则的位置。

在发布规则之前，此图标将呈灰显状态。您还可以在单击筛选器图标时指定规则 ID，以仅显示符合筛选标准的策略和规则。

- 21 在安全策略级别上增强了实现状态 API，以提供更多实现状态信息。可以通过指定查询参数 *include_enforced_status = true* 以及 *intent_path* 来实现此目的。进行以下 API 调用。

```
GET https://<nsx>/policy/api/v1/infra/realized-state/status?intent_path=/
infra/domains/default/security-policies/<security-policy-
id>&include_enforced_status=true
```

分布式防火墙数据包日志

如果为防火墙规则启用了日志记录，则可以通过查看防火墙数据包日志，对问题进行故障排除。

不管是 ESXi 还是 KVM 主机，该日志文件都是 `/var/log/dfwptlogs.log`。

以下是分布式防火墙规则的常规日志示例：

```
2018-07-03T19:44:09.749Z b6507827 INET match PASS mainrs/1024 IN 52 TCP 192.168.4.3/49627-
>192.168.4.4/49153 SEW

2018-07-03T19:46:02.338Z 7396c504 INET match DROP mainrs/1024 OUT 52 TCP 192.168.4.3/49676-
>192.168.4.4/135 SEW

2018-07-06T18:15:49.647Z 028cd586 INET match DROP mainrs/1027 IN 36 PROTO 2 0.0.0.0->224.0.0.1

2018-07-06T18:19:54.764Z 028cd586 INET6 match DROP mainrs/1027 OUT 143 UDP
fe80:0:0:0:68c2:8472:2364:9be/546->ff02:0:0:0:0:1:2/547
```

DFW 日志文件格式的元素包括以下内容（以空格分隔）：

- 时间戳：
- 接口的 VIF ID 的最后八位数字
- INET 类型（v4 或 v6）
- 原因（匹配）
- 操作（通过、丢弃、拒绝）
- 规则集名称/规则 ID
- 数据包方向（入站/出站）
- 数据包大小
- 协议（TCP、UDP 或 PROTO #）
- netx 规则命中的 SVM 方向
- 源 IP 地址/源端口 > 目标 IP 地址/目标端口
- TCP 标记 (SEW)

对于传递的 TCP 数据包，在会话结束时，会出现终止日志：

```
2018-07-03T19:44:30.585Z 7396c504 INET TERM mainrs/1024 OUT TCP RST 192.168.4.3/49627-
>192.168.4.4/49153 20/16 1718/76308
```

TCP 终止日志的元素包括以下内容（以空格分隔）：

- 时间戳：
- 接口的 VIF ID 的最后 8 位数字
- INET 类型（v4 或 v6）
- 操作（终止）
- 规则集名称/规则 ID
- 数据包方向（入站/出站）
- 协议（TCP、UDP 或 PROTO #）
- TCP RST 标记
- netx 规则命中的 SVM 方向
- 源 IP 地址/源端口 > 目标 IP 地址/目标端口
- 入站数据包计数/出站数据包计数（全部累计）
- 入站数据包大小/出站数据包大小

以下是分布式防火墙规则的 FQDN 日志文件示例：

```
2019-01-15T00:34:45.903Z 7c607b29 INET match PASS 1031 OUT 48 TCP 10.172.178.226/32808-
>23.72.199.234/80 S www.sway.com(034fe78d-5857-0680-81e4-d8da6b28d1b4)
```

FQDN 日志的元素包括以下内容（以空格分隔）：

- 时间戳：
- 接口的 VIF ID 的最后八位数字
- INET 类型（v4 或 v6）
- 原因（匹配）
- 操作（通过、丢弃、拒绝）
- 规则集名称/规则 ID
- 数据包方向（入站/出站）
- 数据包大小
- 协议（TCP、UDP 或 PROTO #）
- 源 IP 地址/源端口 > 目标 IP 地址/目标端口
- 域名/UUID，其中 UUID 是域名的二进制内部表示形式

以下是分布式防火墙规则的第 7 层日志文件示例：

```
2019-01-15T00:35:07.221Z 82f365ae INET match REJECT 1034 OUT 48 TCP 10.172.179.6/49818-
>23.214.173.202/80 S APP_HTTP

2019-01-15T00:34:46.486Z 7c607b29 INET match PASS 1030 OUT 48 UDP 10.172.178.226/42035-
>10.172.40.1/53 APP_DNS
```

第 7 层日志的元素包括以下内容（以空格分隔）：

- 时间戳：
- 接口的 VIF ID 的最后八位数字
- INET 类型（v4 或 v6）
- 原因（匹配）
- 操作（通过、丢弃、拒绝）
- 规则集名称/规则 ID
- 数据包方向（入站/出站）
- 数据包大小
- 协议（TCP、UDP 或 PROTO #）
- 源 IP 地址/源端口 > 目标 IP 地址/目标端口
- APP_XXX 是发现的应用程序

选择默认连接策略

您可以选择一个默认连接策略，以强制实施安全模型。

默认连接策略在其他防火墙规则基础上创建全部允许（黑名单）或全部拒绝（白名单）防火墙策略，而不是必须修改各个规则。要设置默认连接策略，请转到[分布式防火墙](#)。在页面顶部，单击连接状态以选择其他选项。

必须创建了防火墙策略和规则，才能更改默认选择的连接策略，并使其立即生效。如果没有创建策略或规则，则会保留默认的连接策略，直到创建了策略和规则为止。

可以使用以下选项：

- **黑名单(带或不带日志记录)：**这是默认选项，将在 DFW 上创建一个全部允许规则。
- **白名单(带或不带日志记录)：**创建全部拒绝流量防火墙规则。仅允许来自防火墙规则中定义的站点或应用程序的通信，并拒绝访问所有其他通信，包括 DHCP 流量。
- **无：**选择该选项以禁用防火墙规则黑名单和白名单。如果您有一组已使用先前版本的 NSX-T Data Center 配置的规则，它将非常有用。

管理防火墙排除列表

防火墙排除列表由可以根据组成员资格从防火墙规则中排除的组组成。

可以从防火墙规则中排除任何组，并且列表中最多可以包含 100 个组。不能将 IP 集、MAC 集和 AD 组作为成员包含在防火墙排除列表中使用的组中。

注 NSX-T Data Center 会自动将 NSX Manager 和 NSX Edge 节点虚拟机添加到防火墙排除列表中。

步骤

- 1 导航到**安全 > 分布式防火墙 > 操作 > 排除列表**。

此时将显示一个窗口，其中会列出可用的组。

- 2 要将组添加到排除列表，请单击任意组旁边的复选框。然后单击**应用**。
- 3 要创建组，请单击**添加组**。请参见**添加组**。
- 4 要编辑组，请单击组旁边的三个点菜单，然后选择**编辑**。
- 5 要删除组，请单击三点菜单，然后选择**删除**。
- 6 要显示组详细信息，请单击**全部展开**。

筛选特定域 (FQDN/URL)

设置分布式防火墙规则，以筛选使用 FQDN/URL 标识的特定域，例如 *.office365.com。

目前，支持预定义域列表。在添加属性类型域名 (FQDN) 的新上下文配置文件时，您可以看到 FQDN 列表。此外，您还可以通过运行 API 调用 `/policy/api/v1/infra/context-profiles/attributes?attribute_key=DOMAIN_NAME` 来查看 FQDN 列表。

您必须先设置一个 DNS 规则，然后在该规则下面设置 FQDN 允许列表或拒绝列表规则。NSX-T Data Center 使用 DNS 响应（从 DNS 服务器到虚拟机的响应）中的生存时间 (TTL)，来保留虚拟机 (VM) 的 DNS 到 IP 映射缓存条目。要使用 DNS 安全配置文件覆盖 DNS TTL，请参见**配置 DNS 安全**。要使 FQDN 筛选生效，虚拟机需要使用 DNS 服务器进行域解析（无静态 DNS 条目），并且还需要采用在 DNS 响应中收到的 TTL。NSX-T Data Center 使用 DNS 侦听获取 IP 地址和 FQDN 之间的映射。应在所有逻辑端口上的交换机中启用 SpoofGuard，以防止发生 DNS 欺骗攻击的风险。当恶意虚拟机可以插入欺骗性的 DNS 响应以将流量重定向到恶意端点或绕过防火墙时，即会出现 DNS 欺骗攻击。有关 SpoofGuard 的详细信息，请参见**了解 SpoofGuard 分段配置文件**。

此功能适用于第 7 层，不包含 ICMP。如果用户为 example.com 上的所有服务创建拒绝列表规则，则当 ping example.com 响应而 curl example.com 未响应时，此功能将正常使用。

最佳做法是选择通配符 FQDN，因为此类 FQDN 包含子域。例如，如果选择 *.example.com，则将包含 americas.example.com 和 emea.example.com 等子域。如果使用 example.com，则将不包含任何子域。

对 ESXi 主机执行 vMotion 操作期间，会一直保留基于 FQDN 的规则。

注 支持 ESXi 和 KVM 主机。KVM 主机仅支持 FQDN 允许列表。FQDN 筛选仅适用于 TCP 和 UDP 流量。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 导航到**安全 > 分布式防火墙**。
- 3 按照**添加分布式防火墙** 中的步骤添加防火墙策略区域。还可以使用现有的防火墙策略区域。
- 4 选择新的或现有的防火墙策略区域，然后单击**添加规则**首先创建 DNS 防火墙规则。
- 5 提供防火墙规则的名称，例如 **DNS 规则**，并提供以下详细信息：

选项	说明
服务	单击编辑图标，然后选择适用于环境的 DNS 或 DNS-UDP 服务。
配置文件	单击编辑图标并选择 DNS 上下文配置文件。这是预先创建的，默认情况下可用于您的部署。
应用对象	根据需要选择一个组。
操作	选择 允许 。

- 6 再次单击**添加规则**以设置 FQDN 允许列表或拒绝列表规则。
- 7 相应地命名规则，例如 **FQDN/URL 允许列表**。将此规则拖动到此策略区域下的 DNS 规则下。
- 8 提供以下详细信息：

选项	说明
服务	单击编辑图标并选择要与此规则关联的服务，例如 HTTP。
配置文件	单击编辑图标，然后单击 添加新的上下文配置文件 。单击名为 属性 的列，然后选择 域名 (FQDN) 。从预定义列表中选择属性名称/值列表。单击 添加 。请参见 添加上下文配置文件 以了解详细信息。
应用对象	根据需要选择 DFW 或一个组。
操作	选择 允许 、 丢弃 或 拒绝 。

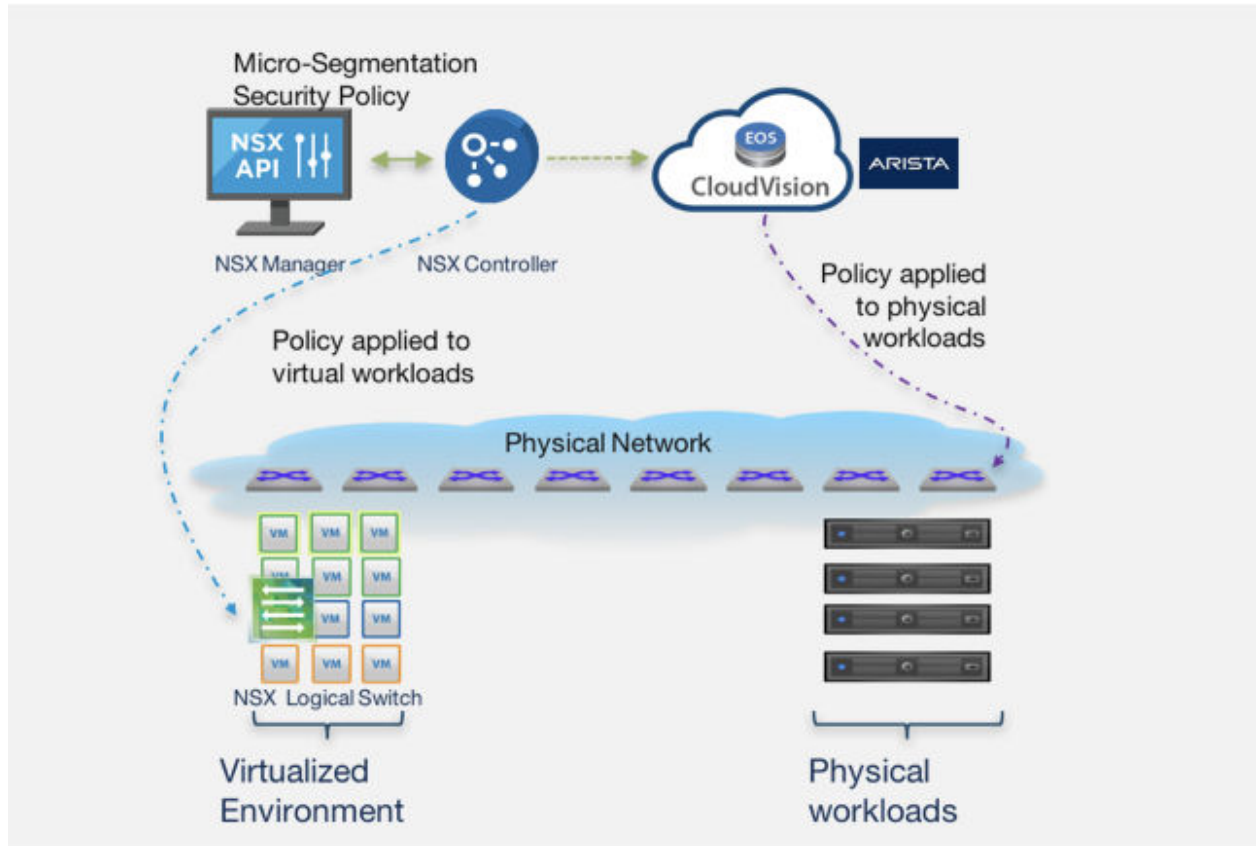
- 9 单击**发布**。

将安全策略扩展到物理工作负载

NSX-T Data Center 可以用作单个管理点，以同时管理虚拟工作负载和物理工作负载。

从 NSX-T Data Center 2.5.1 开始，支持与 Arista CloudVision eXchange (CVX) 集成。通过此集成，可在虚拟工作负载和物理工作负载之间提供一致的网络连接和安全服务，而不考虑您所使用的应用程序框架或物理网络基础架构。NSX-T Data Center 不会直接对物理网络交换机或路由器进行编程，而是会在物理 SDN 控制器级别进行集成，从而保留安全管理员和物理网络管理员的自主权。

从 NSX-T Data Center 2.5.1 开始，支持与 Arista EOS 4.22.1FX-PCS 及更高版本集成。



限制

- Arista 交换机需要先存在 ARP 流量，然后才会将防火墙规则应用于已连接到 Arista 交换机的终端主机。因此，在将防火墙规则配置为阻止流量之前，数据包可以通过交换机。
- 当交换机崩溃或重新加载时，允许的流量不会恢复。在交换机启动后，需要再次填充 ARP 表，才能在交换机上实施防火墙规则。
- 对于连接到已与 Arista 物理交换机相连接的 FTP 服务器的 FTP 被动客户端，无法对 Arista 物理交换机应用防火墙规则。
- 在使用 CVX 集群虚拟 IP 的 CVX HA 设置中，必须将 CVX 虚拟机的 DVPG 混杂模式和伪传输设置为“接受”。如果将这两个选项设置为默认值（“拒绝”），则将无法从 NSX Manager 访问 CVX HA 虚拟 IP。

配置 Arista CVX 以使其与 NSX-T Manager 交互

配置 NSX-T Data Center 后，请在 Arista CloudVision eXchange (CVX) 上完成相应的配置过程，以使 CVX 能够与 NSX-T Data Center 进行交互。

前提条件

NSX-T Data Center 已将 CVX 注册为一个实施点。

步骤

- 1 以 root 用户身份登录到 NSX Manager，然后运行以下命令以创建 CVX 与 NSX Manager 进行通信时所用的指纹。

```
openssl s_client -connect <IP address of nsx-manager>:443 | openssl x509 -pubkey -noout |
openssl rsa -pubin -outform der | openssl dgst -sha256 -binary | openssl base64
```

示例输出：

```
depth=0 C = US, ST = CA, L = Palo Alto, O = VMware Inc., OU = NSX, CN = nsx-mgr
verify error:num=18:self signed certificate
verify return:1
depth=0 C = US, ST = CA, L = Palo Alto, O = VMware Inc., OU = NSX, CN = nsx-mgr
verify return:1
writing RSA key
S+zwADluzeNf+dnffDpYvgs4YrS6QBgyeDry40bPgms=
```

- 2 在 CVX CLI 中运行以下命令：

```
cvx
no shutdown
service pcs
no shutdown
controller <IP address of nsx-manager>
username <NSX administrator user name>
password <NSX administrator password>
enforcement-point cvx-default-ep
pinned-public-key <thumbprint for CVX to communicate with NSX
                    Manager>
notification-id <notification ID created while registering CVX with NSX>
end
```

- 3 在 CVX CLI 中运行以下命令以检查配置：

```
show running-config
```

示例输出：

```
cvx
    no shutdown
    source-interface Management1
    !
    service hsc
        no shutdown

    !
    service pcs
        no shutdown
        controller 192.168.2.80
        username admin
```

```
password 7 046D26110E33491F482F2800131909556B
enforcement-point cvx-default-ep
pinned-public-key sha256//S+zwADluzeNf+dnffDpYvgs4YrS6QBgyeDry40bPgms=
notification-id a0286cb6-de4d-41de-99a0-294465345b80
```

- 4 在连接到物理服务器的物理交换机的以太网接口上配置 tag。在由 CVX 管理的物理交换机上运行以下命令。

```
configure terminal
interface ethernet 4
tag phy_app_server
end
copy running-config startup-config
Copy completed successfully.
```

- 5 运行以下命令以验证交换机的标记配置：

```
show running-config section tag
```

示例输出：

```
interface Ethernet4
description connected-to-7150s-3
switchport trunk allowed vlan 1-4093
switchport mode trunk
tag sx4_app_server
```

在标记的接口上使用 ARP 学习的 IP 地址将与 NSX-T Data Center 共享。

- 6 登录到 NSX Manager，以便为由 CVX 管理的物理工作负载创建并发布防火墙规则。有关创建规则的详细信息，请参见第 10 章 安全。例如：

	<input type="checkbox"/>	名称	源	目标	服务	配置文件	应用对象	操作	
⋮	<input type="checkbox"/>	Firewall_Services	(2)	应用对象	DFW				● 开启 ⓘ ⓘ ⓘ
⋮	<input type="checkbox"/>	vm_to_phy_server	① ⓘ vm	ⓘ phy_server	任意	无	DFW	● 允许 ▾	● ⓘ ⓘ ⓘ
⋮	<input type="checkbox"/>	phy_server_to_vm	① ⓘ phy_server	ⓘ vm	任意	无	DFW	● 允许 ▾	● ⓘ ⓘ ⓘ

NSX-T Data Center 中发布的 NSX-T Data Center 策略和规则在由 CVX 管理的物理交换机上显示为动态 ACL。

```
prmh-nsx-tor-7050sx-4#show ip access-lists dynamic
IP Access List et4.v4.in [dynamic]
 10 permit ip host 71.1.1.3 host 27.1.1.11

IP Access List et4.v4.out [dynamic]
 10 permit ip host 27.1.1.11 host 71.1.1.3
```

有关详细信息，请参见 [CVX HA 设置](#)、[CVX HA 虚拟 IP 设置](#)和[物理交换机 MLAG 设置](#)。

配置 NSX-T Data Center 以使其与 Arista CVX 交互

在 NSX-T Data Center 上完成相应的配置过程，以便可以将 CVX 添加为 NSX-T Data Center 中的实施点，并且 NSX-T Data Center 能够与 CVX 进行交互。

前提条件

获取 Arista CVX 集群的虚拟 IP 地址。

步骤

- 1 以 root 用户身份登录到 NSX Manager，然后运行以下命令以检索 CVX 的指纹：

```
openssl s_client -connect <virtual IP address of CVX cluster> | openssl x509 -noout
-fingerprint -sha256
```

示例输出：

```
depth=0 CN = self.signed
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = self.signed
verify return:1
SHA256
Fingerprint=35:C1:42:BC:7A:2A:57:46:E8:72:F4:C8:B8:31:E3:13:5F:41:95:EF:D8:1E:E9:3D:F0:CC:3
B:09:A2:FE:22:DE
```

- 2 编辑检索到的指纹，以仅使用小写字符并排除指纹中的任何冒号。

编辑后的 CVX 指纹的示例：

```
35c142bc7a2a5746e872f4c8b831e3135f4195efd81ee93df0cc3b09a2fe22de
```

- 3 调用 PATCH /policy/api/v1/infra/sites/default/enforcement-points API 并使用 CVX 指纹为 CVX 创建一个实施端点。例如：

```
PATCH https://<nsx-manager>/policy/api/v1/infra/sites/default/enforcement-points/cvx-
default-ep
{
  "auto_enforce": "false",
  "connection_info": {
    "enforcement_point_address": "<IP address of CVX>",
    "resource_type": "CvxConnectionInfo",
    "username": "cvpadmin",
    "password": "1q2w3e4rT",
    "thumbprint": "65a9785e88b784f54269e908175ada662be55f156a2dc5f3a1b0c339cea5e343"
  }
}
```

- 4 调用 GET /policy/api/v1/infra/sites/default/enforcement-points API 以检索该端点信息。例如：

```
https://<nsx-manager>/policy/api/v1/infra/sites/default/enforcement-points/cvx-default-ep
{
```

```

"auto_enforce": "false",
"connection_info": {
  "enforcement_point_address": "<IP address of CVX>",
  "resource_type": "CvxConnectionInfo",
  "username": "admin",
  "password": "1q2w3e4rT",
  "thumbprint": "35c142bc7a2a5746e872f4c8b831e3135f4195efd81ee93df0cc3b09a2fe22de"
}
}

```

示例输出:

```

{
  "connection_info": {
    "thumbprint": "35c142bc7a2a5746e872f4c8b831e3135f4195efd81ee93df0cc3b09a2fe22de",
    "enforcement_point_address": "192.168.2.198",
    "resource_type": "CvxConnectionInfo"
  },
  "auto_enforce": false,
  "resource_type": "EnforcementPoint",
  "id": "cvx-default-ep",
  "display_name": "cvx-default-ep",
  "path": "/infra/sites/default/enforcement-points/cvx-default-ep",
  "relative_path": "cvx-default-ep",
  "parent_path": "/infra/sites/default",
  "marked_for_delete": false,
  "_system_owned": false,
  "_create_user": "admin",
  "_create_time": 1564036461953,
  "_last_modified_user": "admin",
  "_last_modified_time": 1564036461953,
  "_protection": "NOT_PROTECTED",
  "_revision": 0
}

```

- 5 调用 POST `/api/v1/notification-watchers/` API 并使用 CVX 指纹创建一个通知 ID。例如:

```

POST https://<nsx-manager>/api/v1/notification-watchers/
{
  "server": "<virtual IP address of CVX cluster>",
  "method": "POST",
  "uri": "/pcs/v1/nsgroup/notification",
  "use_https": true,
  "certificate_sha256_thumbprint":
    "35c142bc7a2a5746e872f4c8b831e3135f4195efd81ee93df0cc3b09a2fe22de",
  "authentication_scheme": {
    "scheme_name": "BASIC_AUTH",
    "username": "cvpadmin",
    "password": "1q2w3e4rT"
  }
}

```

- 6 调用 GET /api/v1/notification-watchers/ 以检索该通知 ID。

示例输出：

```
{
  "id": "a0286cb6-de4d-41de-99a0-294465345b80",
  "server": "192.168.2.198",
  "port": 443,
  "use_https": true,
  "certificate_sha256_thumbprint":
"35c142bc7a2a5746e872f4c8b831e3135f4195efd81ee93df0cc3b09a2fe22de",
  "method": "POST",
  "uri": "/pcs/v1/nsgroup/notification",
  "authentication_scheme": {
    "scheme_name": "BASIC_AUTH",
    "username": "cvpadmin"
  },
  "send_timeout": 30,
  "max_send_uri_count": 5000,
  "resource_type": "NotificationWatcher",
  "display_name": "a0286cb6-de4d-41de-99a0-294465345b80",
  "_create_user": "admin",
  "_create_time": 1564038044780,
  "_last_modified_user": "admin",
  "_last_modified_time": 1564038044780,
  "_system_owned": false,
  "_protection": "NOT_PROTECTED",
  "_revision": 0
}
```

- 7 调用 PATCH /policy/api/v1/infra/domains/default/domain-deployment-maps/cvx-default-dmap API 以创建一个 CVX 域部署映射。例如：

```
PATCH https://<nsx-manager>/policy/api/v1/infra/domains/default/domain-deployment-maps/cvx-
default-dmap
{

  "display_name": "cvx-deployment-map",

  "id": "cvx-default-dmap",

  "enforcement_point_path": "/infra/sites/default/enforcement-points/cvx-default-ep"

}
```

- 8 调用 GET /policy/api/v1/infra/domains/default/domain-deployment-maps API 以检索该部署映射信息。

共享地址集

可以在分布式防火墙规则的**应用对象**文本框中创建并使用基于动态或逻辑对象的安全组。

由于地址集是根据虚拟机名称或标签动态填充的，并且必须针对每个筛选器进行更新，因此它们可能用完了主机上可用于存储 DFW 规则和 IP 地址集的堆内存量。

在 NSX-T Data Center 版本 2.5 及更高版本中，称为“全局”或“共享地址集”的功能可以在所有筛选器之间共享地址集。虽然每个筛选器可以具有不同的规则（取决于**应用对象**），但是地址集成员在所有筛选器中都是固定的。默认情况下，已启用此功能，这可以减少堆内存使用量。无法禁用此功能。

在 NSX-T Data Center 版本 2.4 及更低版本中，已禁用全局或共享地址集，并且包含大量分布式防火墙规则的环境可能会遇到 VSIP 堆内存耗尽的情况。

东西向网络安全 - 第三方服务链

合作伙伴在 NSX-T Data Center 中注册网络服务（如入侵检测系统或入侵防御系统 (IPS/IDS)）后，作为管理员，您可以配置网络服务以自检在内部部署数据中心的虚拟机之间流动的东西向流量。

前提条件

- 合作伙伴必须在 NSX-T Data Center 中注册服务。
- 必须使用传输节点配置文件准备 ESXi 主机以作为 NSX-T Data Center 传输节点。

注

- 仅在 ESXi 主机上支持服务虚拟机，在 KVM 主机上不支持服务虚拟机。
- NSX-T Data Center 仅保护在 ESXi 主机上运行的客户机虚拟机。
- NSX-T Data Center 不保护在 KVM 主机上运行的客户机虚拟机。

网络保护（东西向）的重要概念

在内部部署数据中心的客户机虚拟机之间流动的流量由合作伙伴提供的第三方服务进行保护。下面几个概念有助于您了解 workflow。

- **服务：**合作伙伴在 NSX-T Data Center 中注册服务。服务表示合作伙伴提供的安全功能，包含服务部署详细信息，例如服务虚拟机的 OVF URL、连接服务的服务点、服务的状态。
- **供应商模板：**包含服务可在网络流量上执行的功能。合作伙伴定义供应商模板。例如，供应商模板可以提供网络操作服务，如通过隧道与 IPSec 服务进行连接。
- **服务配置文件：**供应商模板的一个实例。NSX-T Data Center 管理员可以创建服务虚拟机要使用的服务配置文件。
- **客户机虚拟机：**网络中流量的源或目标。入站或出站流量由为运行东西向网络服务的规则定义的服务链自检。
- **服务虚拟机：**运行服务指定的 OVA 或 OVF 设备的虚拟机。它通过服务层面进行连接以接收重定向的流量。

- **服务实例：**在主机上部署服务时创建。每个服务实例具有一个相应的服务虚拟机。
- **服务分段：**与传输区域关联的服务层面的一个分段。每个服务连接都与其他服务连接以及 NSX-T 提供的常规 L2 或 L3 网络分段分开。服务层面管理服务连接。
- **Service Manager：**指向一组服务的合作伙伴 Service Manager。
- **服务链：**管理员定义的服务配置文件的逻辑序列。服务配置文件按服务链中定义的顺序自检网络流量。例如，第一个服务配置文件是防火墙，第二个服务配置文件是监控器，依此类推。服务链可以为不同的流量方向（输入/输出）指定不同的服务配置文件序列。
- **重定向策略：**确保为特定服务链分类的流量重定向到该服务链。它基于与 NSX-T Data Center 安全组和服务链相匹配的流量模式。与模式匹配的所有流量重都沿服务链重定向。
- **服务路径：**实施服务链的服务配置文件的服务虚拟机序列。管理员定义服务链，其中包含服务配置文件的预定义顺序。NSX-T Data Center 从基于客户机虚拟机和服务虚拟机的数量及位置从服务链生成多个服务路径。它会为要进行自检的流量流选择最佳的服务路径。每个服务路径通过服务路径索引 (SPI) 进行标识，并且路径上的每个跃点具有唯一的服务索引 (SI)。

NSX-T Data Center 对东西向流量的要求

在 NSX-T Data Center 部署中，您需要确保存在覆盖网络传输区域和支持覆盖网络的逻辑交换机。

东西向服务插入将应用于整个 NSX-T 部署。您无法在集群级别或主机级别部署该服务。

所有传输节点的类型必须为“覆盖网络”，因为该服务会发送支持 GENEVE 或支持覆盖网络的逻辑交换机上的流量。支持覆盖网络（支持 GENEVE）的逻辑交换机是在内部置备的，在用户界面上不可见。

即使您计划仅使用支持 VLAN 的逻辑交换机进行部署，东西向流量仍会通过覆盖网络传输区域和支持覆盖网络的逻辑交换机。因此，请确保创建覆盖网络传输区域和支持 GENEVE 的逻辑交换机。如果不满足这些要求，则在执行 vMotion 期间，主机上的客户机虚拟机将无法迁移到其他传输节点。客户机虚拟机会进入“已断开连接”状态，从而导致东西向服务中出现配置错误。

东西向网络安全的高级别任务

请按照以下步骤设置东西向流量的网络安全。

表 10-3. 配置东西向网络侦测的任务列表

工作流程任务	用户配置	实施
注册服务	合作伙伴	仅 API
注册供应商模板	合作伙伴	仅 API
注册 Service Manager	合作伙伴	仅 API
为东西向流量自检部署服务	管理员	API 和 NSX Manager UI
添加服务配置文件	管理员	API 和 NSX Manager UI

表 10-3. 配置东西向网络侦测的任务列表（续）

workflows 任务	用户配置	实施
添加服务链	管理员	API 和 NSX Manager UI
为东西向流量添加重定向规则	管理员	API 和 NSX Manager UI

为东西向流量自检部署服务

合作伙伴注册服务后，作为管理员，您必须在群集的成员主机上部署服务的实例。

在群集中的所有 NSX-T Data Center 主机上部署运行合作伙伴安全引擎的合作伙伴服务虚拟机。部署 SVM 后，可以创建 SVM 用于保护客户机虚拟机的策略规则。

前提条件

- 所有主机都由一个 vCenter Server 管理。
- 合作伙伴服务必须已在 NSX-T Data Center 中注册并准备好进行部署。
- NSX-T Data Center 管理员可以访问合作伙伴服务和供应商模板。
- 服务虚拟机和合作伙伴 Service Manager（控制台）必须能够在管理网络级别相互通信。
- 基于主机的服务部署：在每个主机上部署服务虚拟机之前，请先应用传输节点配置文件以为群集的每个主机配置 NSX-T Data Center。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择 **系统 > 服务部署 > 部署 > 部署服务**。
- 3 从“合作伙伴服务”字段中，选择合作伙伴服务。
- 4 输入服务部署名称。
- 5 在“计算管理器”字段中，选择 vCenter Server 以部署服务。
- 6 在“群集”字段中，选择需要部署服务的群集。
- 7 在“数据存储”下拉菜单中，选择一个数据存储作为服务虚拟机的存储库。
- 8 在“网络”列中，单击 **设置** 并通过选择 DHCP 或静态 IP 地址类型和数据网络输入管理网络接口。
- 9 在“服务分段”字段中，从列表中选择服务分段，或单击“操作”图标添加或编辑服务分段。将为连接到服务分段的客户机虚拟机提供东西向网络流量保护。
- 10 在“部署类型”字段中，选择以下部署选项之一。根据由合作伙伴注册的服务，可以在单个服务虚拟机中部署多个服务。
 - 群集：在属于专用于托管服务虚拟机的群集的一个或多个主机上部署服务。
 - 基于主机：在群集中的所有主机上部署服务。
- 11 在“部署模板”字段中，选择可提供用于保护要在客户机虚拟机组上运行的工作负载的属性的模板。

12 （仅限基于群集的部署）在“群集部署计数”中，输入要在群集上部署的服务虚拟机数量。vCenter Server 决定在哪个主机上部署服务虚拟机。

13 单击**保存**。

结果

服务部署后，合作伙伴 Service Manager 将收到更新通知。

后续步骤

了解有关在主机上部署的服务实例的部署详细信息和运行状况。请参见[添加服务配置文件](#)。

添加服务配置文件

服务配置文件是合作伙伴供应商模板的一个实例。管理员可以自定义供应商模板的属性以创建模板实例。

注 您可以为单个供应商创建多个服务配置文件。例如，为正向路径设置的服务配置文件提供 IDS 保护，而为反向路径设置的服务配置文件支持 IPS 保护。但是，可以同时为正向路径和反向路径设置同一个服务配置文件。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 导航到 **安全 > 东西向安全 > 网络自检 > 服务配置文件**。
- 3 从“合作伙伴服务”下拉字段中选择一项服务。您可以为选择的服务创建服务配置文件。
- 4 输入服务配置文件名称，然后选择供应商模板。
- 5 “重定向操作”字段将继承供应商模板的功能。例如，如果供应商模板提供的功能是“复制”，则在创建服务配置文件时，重定向操作默认为“复制”。
- 6 （可选）定义要用于筛选出和管理服务配置文件的标记。
- 7 单击**保存**。

结果

此时将为合作伙伴服务创建一个新的服务配置文件。

后续步骤

添加服务链。请参见[添加服务链](#)。

添加服务链

服务链是网络管理员定义的服务配置文件的逻辑序列。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**安全 > 东西向安全 > 网络自检 > 服务链 > 添加链**。

- 3 输入服务链名称。
- 4 在“服务分段”字段中，选择要应用服务链的服务分段。服务分段是连接覆盖网络传输区域的多个服务虚拟机的服务层面的一个分段。服务链中的每个服务虚拟机都与其他服务虚拟机分开，且 L2 和 L3 网络分段由 NSX-T Data Center 运行。服务层面控制对服务虚拟机的访问。
- 5 要设置正向路径，请单击**设置正向路径**字段，然后单击**按顺序添加配置文件**。
- 6 在服务链中添加第一个配置文件，然后单击**添加**。
- 7 要指定下一个服务配置文件，请单击**按顺序添加配置文件**，然后输入详细信息。也可以使用向上和向下箭头图标重新排列配置文件的顺序。
- 8 单击**保存**以完成添加服务链的正向路径。
- 9 在“反向路径”列中，选择**反转正向路径**，以使服务层使用您为正向路径设置的服务配置文件。
- 10 要为反向路径设置新的服务配置文件，请单击**设置反向路径**，然后添加服务配置文件。
- 11 单击**保存**以完成添加服务链的反向路径。
- 12 在“故障策略”字段中，
 - 选择**允许**以在服务虚拟机出现故障时将流量发送到目标虚拟机。可通过活跃度检测机制检测服务虚拟机故障，该机制只能由合作伙伴启用。
 - 选择**阻止**以在服务虚拟机出现故障时不将流量发送到目标虚拟机。
- 13 单击**保存**。

结果

添加服务链后，合作伙伴 Service Manager 将收到更新通知。

后续步骤

创建重定向规则，以便自检东西向网络流量。请参见[为东西向流量添加重定向规则](#)。

为东西向流量添加重定向规则

可添加用于重定向东西向流量以进行网络自检的规则。

在策略中定义规则。策略的概念类似于防火墙区域的概念。在添加策略时，请选择服务链以通过服务链的服务配置文件重定向流量以进行自检。


规则定义包含流量的源和目标、自检服务、要应用规则的 NSX-T Data Center 对象和流量重定向策略。发布规则后，找到匹配的流量模式时，NSX Manager 便触发规则。规则开始自检流量。例如，NSX Manager 对必须进行自检的流量流进行分类时，不会将其转发到常规的分布式防火墙，而是沿着在策略中指定的服务链重定向该流量。服务链中定义的服务配置文件将自检合作伙伴提供的网络服务的流量。如果某服务配置文件完成自检时未检测到流量中存在任何安全问题，则流量将转发到服务链中的下一个服务配置文件。服务链结束时，流量将转发到目标。

将向合作伙伴 Service Manager 和 NSX-T Data Center 发送所有通知。

前提条件

可使用服务链重定向流量以进行网络自检。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 安全 > 东西向安全 > 网络自检 > 规则 > 添加策略。
策略区域类似于在其中定义了确定流量如何流动的规则的防火墙区域。
- 3 选择一个服务链。
- 4 要添加策略，请单击**发布**。
- 5 单击区域中的  垂直省略号，然后单击**添加规则**。
- 6 编辑**源**字段以通过定义成员资格条件、静态成员、IP/MAC 地址或 Active Directory 组添加组。
 - a 使用以下某个实体定义成员资格条件：
 - 虚拟机
 - 逻辑交换机
 - 逻辑端口
 - IP 集
 - b 使用以下某个实体定义静态成员列表：
 - 组
 - 分段
 - 分段端口
 - 虚拟网络接口
 - 虚拟机
- 7 单击**保存**。
- 8 要添加目标组，请编辑**目标**字段。
- 9 在“应用对象”字段中，可以执行以下操作之一：
 - 选择 **DFW** 以将规则应用于连接到逻辑交换机的所有虚拟网卡。
 - 选择**虚拟机组**以将规则应用于组中成员虚拟机的虚拟网卡。可以从静态列表或基于动态条件选择成员。支持的 NSX-T Data Center 对象包括：虚拟机、逻辑交换机、逻辑端口、IP 集等。
- 10 在“操作”字段中，选择**重定向**以沿服务链重定向流量；或选择**不重定向**，不对流量应用网络自检。
- 11 单击**发布**。
- 12 要恢复已发布的规则，选择一个规则，然后单击**恢复**。
- 13 要添加策略，请单击 **+** **添加策略**。

- 14 要克隆策略或规则，选择策略或规则，然后单击**克隆**。
- 15 要启用规则，请启用“启用/禁用”图标，或选择规则，然后从菜单中单击**启用 > 启用规则**。
- 16 启用或禁用规则后，请单击**发布**以实施规则。

结果

传输到源的流量将重定向到服务链以进行网络自检。链中的服务配置文件对流量自检后，流量将传送到目标。

在部署期间，可以更改某特定策略的虚拟机组成员资格。NSX-T Data Center 将向合作伙伴 Service Manager 发送有关这些更新的通知。

配置网关防火墙

网关防火墙表示在边界防火墙应用的规则。

所有共享规则视图下有预定义类别，在该视图中，可以查看跨所有网关的规则。先从上到下，然后从左到右对规则进行评估。可以使用 **API** 更改类别名称。

表 10-4. 网关防火墙规则类别

规则类别	用途
紧急	用于隔离。还可用于“允许”规则。
系统	这些规则由 NSX-T Data Center 自动生成且特定于内部控制层面流量，如 BFD 规则、VPN 规则等。 注 请勿编辑系统规则。
共享的预规则	这些规则跨网关全局应用。
本地网关	这些规则特定于特定网关。
自动服务规则	这些是应用于数据层面的自动联结规则。可以根据需要编辑这些规则。
默认	这些规则定义默认网关防火墙行为。

添加网关防火墙策略和规则

可以通过将网关防火墙规则添加到属于预定义类别的防火墙策略区域下实施这些规则。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**安全 > 南北向安全 > 网关防火墙**。
- 3 要启用网关防火墙，请选择**操作 > 常规设置**，然后切换状态按钮。单击**保存**。
- 4 单击**添加策略**，有关类别的详细信息，请参见[配置网关防火墙](#)。
- 5 输入新策略区域的**名称**。

6 选择策略目标。

7 单击齿轮图标以配置以下策略设置：

设置	说明
TCP 严格模式	TCP 连接以三向握手（SYN、SYN-ACK、ACK）开始，通常以双向交换（FIN、ACK）结束。在某些情况下，防火墙可能看不到特定流量的三向握手（例如由于非对称流量）。默认情况下，防火墙不强制要求看到三向握手，而是选取已建立的会话。可以在每个区域启用“TCP 严格模式”，以禁止在会话中途提取数据，并实现三向握手要求。如果为特定防火墙策略启用 TCP 严格模式，并使用默认“任意-任意”阻止规则，将丢弃该策略区域中不符合三向握手连接要求并与基于 TCP 的规则匹配的数据包。“严格模式”仅适用于有状态 TCP 规则，并在网关防火墙策略级别启用。对于与默认“任意-任意”允许规则（没有指定任何 TCP 服务）匹配的数据包，不会强制采用 TCP 严格模式。
有状态	有状态防火墙监控活动连接的状态，并使用此信息来确定允许哪些数据包通过防火墙。
已锁定	可以锁定策略，以防止多个用户对相同区域进行更改。锁定某个区域时，必须包含一条注释。

8 单击**发布**。可以添加多个策略，然后一起发布。

新策略将显示在屏幕上。

9 选择策略区域，然后单击**添加规则**。

10 输入规则的名称。支持 IPv4、IPv6 和多播地址。

11 在**源**列中，单击编辑图标并选择规则的源。有关详细信息，请参见[添加组](#)。

12 在**目标**列中，单击编辑图标并选择规则的目标。如果未定义，目标将与任何内容匹配。有关详细信息，请参见[添加组](#)。

13 在**服务**列中，单击铅笔图标并选择服务。如果未定义，服务将与任何内容匹配。

14 在**配置文件**列中，单击编辑图标并选择上下文配置文件，或单击**添加新的上下文配置文件**。请参见[添加上下文配置文件](#)。

- Tier-0 网关防火墙策略不支持上下文配置文件。
- 网关防火墙规则不支持具有 FQDN 属性或其他子属性的上下文配置文件。

上下文配置文件使用第 7 层应用程序 ID 属性用于分布式防火墙规则和网关防火墙规则。在将服务设置为任意的防火墙规则中可以使用多个应用程序 ID 上下文配置文件。对于 ALG 配置文件（FTP 和 TFTP），每个规则支持一个上下文配置文件。

15 单击**应用**。

16 **应用对象**列定义每个规则的实施范围，允许用户有选择地将规则应用于一个或多个上行链路接口或服务接口。默认情况下，网关防火墙规则将应用于选定网关上的所有可用上行链路和服务接口。

- 17 在**操作**列中，选择一个操作。

选项	说明
允许	允许具有指定的源、目标和协议的所有流量通过当前防火墙上文。与规则匹配并接受的数据包将通过系统，就好像没有防火墙一样。
丢弃	丢弃具有指定的源、目标和协议的数据包。丢弃数据包是一个静默操作，不会向源或目标系统发送通知。丢弃数据包将导致重试连接，直到达到重试阈值。
拒绝	拒绝具有指定的源、目标和协议的数据包。拒绝数据包将向发送方发送“目标无法访问 (destination unreachable)”消息。如果协议是 TCP，则会发送 TCP RST 消息。对于 UDP、ICMP 和其他 IP 连接，发送包含管理上被禁止的代码的 ICMP 消息。在尝试一次后，会向发送应用程序通知无法建立连接。

- 18 单击状态切换按钮以启用或禁用规则。

- 19 单击齿轮图标以设置日志记录、方向、IP 协议、标记和备注。

选项	说明
日志记录	可以禁用或启用日志记录。日志存储在 Edge 上的 /var/log/syslog 中。
方向	选项包括 入站 、 出站 和 入站/出站 。默认选项为 入站/出站 。此字段指从目标对象角度来看的流量方向。 入站 意味着只检查流入对象的流量， 出站 意味着只检查从对象流出的流量， 入站/出站 意味着检查两个方向的流量。
IP 协议	选项包括 IPv4 、 IPv6 和 IPv4_IPv6 。默认选项为 IPv4_IPv6 。
标记	已添加到规则的标记。

注 单击图形图标可查看防火墙规则的流量统计信息。可以查看字节数、数据包计数和会话数等信息。

- 20 单击**发布**。可以添加多个规则，然后一起发布。
- 21 对于每个策略区域，单击**信息**图标以查看推送到 Edge 节点的 Edge 防火墙规则的当前状态。还会显示在将规则推送到 Edge 节点时生成的所有警报。
- 22 要查看应用于 Edge 节点的策略规则的合并状态，请进行 API 调用。

```
GET https://<policy-mgr>/policy/api/v1/infra/realized-state/status?
intent_path=/infra/domains/default/gateway-policies/
<GatewayPolicy_ID>&include_enforced_status=true
```

南北向网络安全 - 插入第三方服务

NSX-T Data Center 提供了在数据中心插入 Tier-0 或 Tier-1 路由器第三方服务以将流量重定向到第三方服务进行自检的功能。仅支持使用 ESXi 主机部署南北向服务虚拟机。不支持 KVM 主机。

南北向网络安全的高级别任务

请按照以下步骤设置南北向流量的网络安全。

表 10-5. 配置南北向网络自检的任务列表

workflow任务	用户配置	实施
在 NSX-T Data Center 中注册服务	合作伙伴	仅 API
为南北向流量自检部署服务	管理员	API 和 NSX Manager UI
配置流量重定向	管理员	API 和 NSX Manager UI

为南北向流量自检部署服务

注册服务后，必须部署服务实例，该服务才会开始处理网络流量。

在用作物理环境和 vCenter Server 上逻辑网络之间网关的 Tier-0 或 Tier-1 逻辑路由器上部署合作伙伴服务虚拟机。将 SVM 部署为独立服务实例或活动-备用服务实例后，可以创建重定向规则，将流量重定向到 SVM 以进行网络自检。

前提条件

- 所有主机都由一个 vCenter Server 管理。
- 合作伙伴服务已在 NSX-T Data Center 中注册并准备好进行部署。
- NSX-T Data Center 管理员可以访问合作伙伴服务。
- 逻辑路由器的高可用性模式必须为活动-备用模式。
- 启用 Distributed Resource Scheduler 实用程序。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**高级网络和安全** > **合作伙伴服务** > **服务实例** > **目录**。
- 3 “目录”选项卡显示已注册的服务。
- 4 选择在 OVF 规格中显示的服务，然后单击**部署**以开始部署服务实例。
- 5 在“合作伙伴服务插入”窗口中，单击**继续**。
- 6 在“合作伙伴服务”窗口中，输入详细信息。

表 10-6. 合作伙伴服务详细信息

字段	说明
实例名称	输入用来标识服务实例的名称。
说明	关于服务实例的描述。

表 10-6. 合作伙伴服务详细信息（续）

字段	说明
合作伙伴服务	选择已在 NSX-T Data Center 中注册的合作伙伴服务。
部署规范	选择要部署的规格。
逻辑路由器	选择必须部署服务实例的 Tier-O 逻辑路由器。

7 单击**下一步**。

8 在“实例配置”窗口中，输入详细信息。

表 10-7. 服务实例详细信息

字段	说明
部署模式	选择 独立 可在 Tier-O 逻辑路由器部署单个服务实例。 选择 高可用性 可在 Tier-O 逻辑路由器以活动-备用模式部署多个服务实例。
故障策略	选择 允许 或 阻止 。
服务实例 IP 地址	输入服务实例要使用的 IP 地址。
网关	输入网关地址。
子网掩码	输入子网掩码。
网络 ID	输入要连接管理网络的逻辑交换机的网络 ID。
计算管理器	选择已注册的 vCenter Server。
资源池	选择提供资源来部署服务实例的资源池。
数据存储	选择用于存储服务实例数据的存储库。

9 单击**下一步**。

10 在“高级配置”窗口中，输入详细信息。

表 10-8.

字段	说明
部署模板	选择要在服务实例部署过程中使用的模板。
许可证	输入模板的许可证。

11 单击**完成**。

结果

“服务实例”选项卡显示部署进度。完成部署可能需要几分钟时间。验证部署状态，以确保服务实例已成功部署在 Tier-O 逻辑路由器。

或者，转到 vCenter Server 并验证部署状态。

后续步骤

配置规则以将流量重定向到在 Tier-O 路由器上部署的服务实例。请参见[配置流量重定向](#)

配置流量重定向

在部署服务实例后，请配置路由器重定向到该服务的流量类型。配置流量重定向与配置防火墙类似。

有关配置防火墙的信息，请参见[防火墙区域和防火墙规则](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**高级网络和安全 > 合作伙伴服务 > 服务实例**。
- 3 单击服务实例。
- 4 单击**流量重定向**选项卡。
- 5 要添加区域，请选择一个现有的区域，然后单击**添加区域**。
 - ◆ 从菜单中，选择**在上方添加区域**或**在下方添加区域**。

将创建一个新区域。要重定向的流量类型设置为 **L3 重定向**，服务类型为**无状态**，**应用对象**字段与主机上配置的 Tier-O 逻辑路由器相关联。在定义规则后，将自动填充**规则**字段。

- 6 单击**发布**以永久保存该区域的配置详细信息。
- 7 要在该区域中添加规则，请选择该区域，然后单击**添加规则**。
- 8 在规则行中，输入以下详细信息：
 - a 输入规则名称。
 - b 输入 L3 流量的源和目标。在将从源传输的流量重定向到目标虚拟机之前，合作伙伴服务虚拟机将对流量进行自检。
 - c 在**应用对象**字段中，选择 Tier-O 路由器的上行链路。
 - d 如果服务虚拟机需要对流量进行自检，请在**操作**字段中选择**重定向**；如果不需要对流量进行南北向自检，请选择**不重定向**。
- 9 可以单独启用每个规则。在启用规则后，它将应用于与该规则匹配的流量。
- 10 单击“高级设置”以配置流量方向和启用日志记录。
- 11 在包含规则的区域末尾，单击**发布**以永久保存该区域中的规则，或单击**恢复**以取消该操作。

结果

流量将发送到网络自检规则，其中的策略规则将应用于流量。

后续步骤

请参见[为南北向流量添加重定向规则](#)。


为南北向流量添加重定向规则

可以使用**高级网络和安全** UI 设置南北向重定向规则。仅在 Tier-0 路由器中插入的服务发生流量重定向。按照**配置流量重定向**的说明进行操作。

前提条件

- 在 NSX-T 上注册并部署第三方服务。
- 配置 Tier-0 路由器。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 安全 > 南北向防火墙 > 网络自检 (南北向) > 添加策略。
策略区域类似于在其中定义了确定流量如何流动的规则的防火墙区域。
- 3 将**重定向到**设置为在 NSX-T 中注册的服务实例，以执行在源和目标实体之间传输的流量的网络自检。
- 4 要添加策略，请单击**发布**。
- 5 单击区域中的  垂直省略号，然后单击**添加规则**。
- 6 编辑**源**字段以通过定义成员资格条件、静态成员、IP/MAC 地址或 Active Directory 组添加组。可以从以下类型之一定义成员资格条件：虚拟机、逻辑交换机、逻辑端口、IP 集。可以从以下类别之一选择静态成员：组、分段、分段端口、虚拟网络接口或虚拟机。
- 7 单击**保存**。
- 8 要添加目标组，请编辑**目标**字段。
- 9 在“应用对象”字段中，可以执行以下操作之一：
 - 选择 **DFW** 以将规则应用于连接到逻辑交换机的所有虚拟网卡。
 - 选择**虚拟机组**以将规则应用于组中成员虚拟机的虚拟网卡。可以从静态列表或基于动态条件选择成员。支持的 NSX-T Data Center 对象包括：虚拟机、逻辑交换机、逻辑端口、IP 集等。
- 10 在“操作”字段中，选择**重定向**以沿服务实例重定向流量；或选择**不重定向**，而不将网络自检应用于流量。
- 11 单击**发布**。
- 12 要恢复已发布的规则，选择一个规则，然后单击**恢复**。
- 13 要添加策略，请单击 **+ 添加策略**。
- 14 要克隆策略或规则，选择策略或规则，然后单击**克隆**。
- 15 要启用规则，请启用“启用/禁用”图标，或选择规则，然后从菜单中单击**启用 > 启用规则**。
- 16 启用或禁用规则后，请单击**发布**以实施规则。

结果

根据设置的操作，南北向流量将重定向到服务实例以进行网络自检。

监控流量重定向

部署服务实例并配置流量重定向后，可以监控传入和传出服务实例的流量。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 选择**高级网络和安全 > 合作伙伴服务 > 服务实例**。
- 3 单击服务实例的名称。

概览选项卡将显示服务实例的配置和状态。

- 4 单击**统计信息**选项卡。
将显示有关传入/传出服务实例的数据包数和数据量的信息。
- 5 单击**刷新**以更新统计信息。

端点保护

NSX-T Data Center 允许您插入第三方合作伙伴服务，作为提供端点保护服务的单独服务虚拟机。合作伙伴服务虚拟机会根据 NSX-T Data Center 管理员应用的端点保护策略规则来处理客户机虚拟机中的文件、进程和注册表活动。

了解端点保护

了解端点保护的用例、工作流和重要概念。

端点保护用例

在虚拟环境中，可使用客户机侦测平台为客户机虚拟机提供防病毒和防恶意软件保护。

作为 NSX 管理员，您可以实施已部署为服务虚拟机（服务 VM 或 SVM）的防病毒和防恶意软件解决方案来监控客户机虚拟机上的文件、网络或进程活动。每当访问文件时，如尝试打开文件时，将通知防恶意软件服务虚拟机该事件。然后，服务虚拟机将确定如何响应事件。例如，检查文件中是否有病毒签名。

- 如果服务虚拟机确定该文件不包含病毒，则允许打开文件的操作成功执行。
- 如果服务虚拟机在文件中检测到病毒，则会请求客户机虚拟机上的 Thin Agent 执行以下任一操作：
 - 删除受感染的文件或拒绝对该文件的访问。
 - 可以通过 NSX 为已感染的虚拟机分配标记。此外，您可以定义一个规则，以将带有此类标记的客户机虚拟机自动移到一个专门用于放置受感染虚拟机的隔离安全组，从而对这些虚拟机进行进一步的扫描并将其从网络中隔离出来，直到完全消除感染为止。

使用客户机侦测平台保护客户机虚拟机端点具有以下好处：

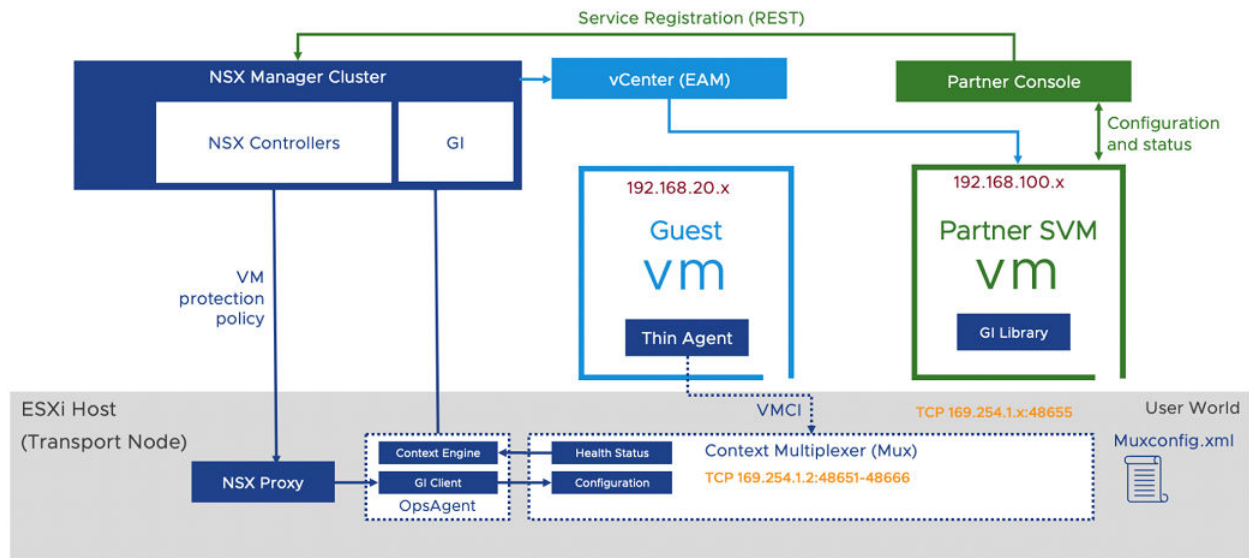
- **减少计算资源的消耗：**客户机侦测会将主机上每个端点中的病毒特征码和安全扫描逻辑卸载到该主机上的第三方合作伙伴服务虚拟机中。由于病毒扫描仅在服务虚拟机上进行，因此，无需在客户机虚拟机上耗费计算资源来运行病毒扫描。

- 改善管理：将病毒扫描卸载到服务虚拟机后，只需要将病毒特征码更新到每个主机上的一个对象。这种机制优于基于代理的解决方案，因为在后者中，需要在所有客户机虚拟机上更新同一个病毒特征码。
- 提供持续不断的防病毒和防恶意软件保护：因为服务虚拟机会持续运行，因此客户机虚拟机无需运行最新的病毒特征码。例如，快照虚拟机可能运行的是较旧版本的病毒特征码，这使传统的端点保护方式很容易受到攻击。而在客户机侦测平台中，服务虚拟机会持续运行最新版本的病毒和恶意软件特征码，从而可确保新添加的虚拟机也会得到最新版本的病毒特征码的保护。
- 将病毒特征码卸载到服务虚拟机：病毒数据库生命周期超出了客户机虚拟机生命周期，因此服务虚拟机不会受客户机虚拟机中断的影响。

客户机侦测架构

了解 NSX-T Data Center 中的服务插入和客户机侦测组件的架构。

图 10-1. 客户机侦测架构



重要概念：

- 合作伙伴控制台：由安全供应商提供的与客户机侦测平台配合使用的 Web 应用程序。
- NSX Manager：NSX 的管理平面设备，可为客户和合作伙伴提供用于配置网络和安全策略的 API 和图形用户界面。对于客户机侦测，NSX Manager 还会提供用于部署和管理合作伙伴设备的 API 和 GUI。
- 客户机侦测 SDK：VMware 提供的供安全供应商使用的库。
- 服务虚拟机：由安全供应商提供的需使用 VMware 提供的客户机侦测 SDK 的虚拟机。该虚拟机包含用于扫描文件或进程活动以在客户机上检测病毒或恶意软件的逻辑。扫描请求后，它会针对客户机虚拟机对请求所采取的操作返回结论或通知。
- 客户机侦测主机代理（上下文多路复用器）：用于处理端点保护策略的配置。还会多路复用受保护的虚拟机中的消息并将其转发到服务虚拟机。它会报告客户机侦测平台的运行状况，并在 muxconfig.xml 文件中维护服务虚拟机配置的记录。

- 操作代理（上下文引擎和客户机侦测客户端）：可将客户机侦测配置转发到客户机侦测主机代理（上下文多路复用器）。还可以将解决方案的运行状况转发到 NSX Manager。
- EAM：NSX Manager 可使用 ESXi Agent Manager 在配置了保护方案的集群的每个主机上部署合作伙伴服务虚拟机。
- Thin Agent：在客户机虚拟机中运行的文件或网络侦测代理。还会截获通过主机代理转发到服务虚拟机的文件和网络活动。此代理是 VMware Tools 的一部分。它取代了由防病毒或防恶意软件安全方案供应商提供的传统代理。它是一种通用的轻量级代理，有助于将用于扫描的文件和进程卸载到供应商提供的服务虚拟机。

端点保护的重要概念

端点保护工作流程需要合作伙伴在 NSX-T Data Center 中注册他们的服务，需要管理员使用这些服务。下面几个概念有助于您了解工作流程。

- 服务定义：合作伙伴使用以下属性定义服务：名称、说明、支持的规格、包含网络接口的部署属性以及 SVM 要使用的设备 OVF 软件包位置。
- 服务插入：NSX 提供了服务插入框架，它允许合作伙伴将网络和安全解决方案与 NSX 平台相集成。客户机侦测解决方案是服务插入的一种形式。
- 服务配置文件和供应商模板：合作伙伴注册供应商模板，以公开策略的保护级别。例如，保护级别可以分为黄金级、白银级或白金级。可以从供应商模板创建服务配置文件，这使得 NSX 管理员可以根据自己的偏好来命名供应商模板。对于除客户机侦测以外的服务，可以使用属性进行进一步自定义服务配置文件。然后，可以在端点保护策略规则中使用服务配置文件为 NSX 中定义的虚拟机组配置保护。作为管理员，您可以根据虚拟机名称、标记或标识符创建组。可以选择从单个供应商模板创建多个服务配置文件。
- 端点保护策略：策略是一组规则。当具有多个策略，请按运行顺序对它们进行排序。这一点同样适用于在策略中定义的规则。例如，策略 A 具有三个规则，策略 B 具有四个规则，这些规则按策略 A 先于策略 B 的顺序排列。当客户机侦测开始运行策略时，将先运行策略 A 中的规则，然后运行策略 B 中的规则。
- 端点保护规则：作为 NSX 管理员，您可以创建规则来指定要保护的虚拟机组，并通过为每个规则指定服务配置文件来选择这些组的保护级别。
- 服务实例：它指的是主机上的服务虚拟机。vCenter 将服务虚拟机视为特殊的虚拟机，这些虚拟机在任何客户机虚拟机打开电源之前启动，并在所有客户机虚拟机关闭电源后停止。每个主机的每个服务都具有一个服务实例。

重要事项 服务实例数等于服务运行主机的主机数。例如，如果一个集群中有八个主机，并在两个集群上部署了合作伙伴服务，则运行的服务实例总数为 16 个 SVM。

- 服务部署：作为 admin，您可以通过 NSX-T 在每个集群上部署合作伙伴服务虚拟机。部署是在集群级别进行管理的，因此在将任何主机添加到集群时，EAM 会在这些主机上自动部署服务虚拟机。

自动部署 SVM 非常重要，因为如果在 vCenter 集群上配置了 Distributed Resource Scheduler (DRS) 服务，则 vCenter 可以在新主机上部署和启动 SVM 后，重新均衡现有虚拟机，或将现有虚拟机分发到添加到集群的任何新主机。由于合作伙伴服务虚拟机需要使用 NSX-T 平台为客户机虚拟机提供安全保护，因此必须将主机准备好作为传输节点。

重要事项 一个服务部署指的是 vCenter Server 上一个用于部署和配置一个合作伙伴服务的集群。

- 文件侦测驱动程序：安装在客户机虚拟机上，会拦截客户机虚拟机上的文件活动。
- 网络侦测驱动程序：安装在客户机虚拟机上，可拦截客户机虚拟机上的网络流量、进程和用户活动。

端点保护的高级别任务

在 NSX-T Data Center 中注册包含安全扫描逻辑的第三方合作伙伴服务以保护客户机虚拟机。当 NSX 管理员部署已注册的服务并对客户机虚拟机组应用端点保护策略时，将强制实施合作伙伴服务。

用于端点保护用例的客户机侦测工作流程如下所示：

图 10-2. 端点保护 workflow

工作流程任务	角色/用户配置	实施
在 NSX-T Data Center 中注册服务	合作伙伴管理员	合作伙伴控制台
在 NSX-T Data Center 中注册服务	合作伙伴管理员	合作伙伴控制台
在 NSX-T Data Center 中注册服务	合作伙伴管理员	合作伙伴控制台
部署服务	NSX 管理员	API 和 NSX Manager UI
查看服务实例详细信息	NSX 管理员	API 和 NSX Manager UI
启动服务实例	NSX 管理员	API 和 NSX Manager UI
添加服务配置文件	NSX 管理员	API 和 NSX Manager UI
使用客户机侦测策略	NSX 管理员	API 和 NSX Manager UI
添加并发布端点保护规则	NSX 管理员	API 和 NSX Manager UI
监控端点保护状态	NSX 管理员	API 和 NSX Manager UI

配置端点保护

可使用第三方合作伙伴安全服务保护在 NSX-T Data Center 环境中运行的客户机虚拟机。

配置端点保护策略的概要步骤如下：

- 1 在客户机虚拟机上配置端点保护之前，请确保满足配置端点保护的必备条件。
- 2 受支持的软件。请参见[支持的软件](#)。
- 3 安装适用于 Linux 虚拟机的文件侦测驱动程序。请参见在[Linux 虚拟机上安装客户机侦测瘦代理](#)。
- 4 安装适用于 Windows 虚拟机的文件侦测驱动程序。请参见在[Linux 虚拟机上安装客户机侦测瘦代理](#)。
- 5 安装适用于 Linux 虚拟机的网络侦测驱动程序。请参见[为网络侦测安装 Linux Thin Agent](#)。

- 6 创建具有客户机侦测合作伙伴管理员角色的用户请参见[创建具有客户机侦测合作伙伴管理员角色的用户](#)。
- 7 在 NSX-T Data Center 中注册合作伙伴服务。请参考“合作伙伴”文档。
- 8 部署服务。请参见[部署服务](#)。
- 9 使用客户机侦测策略。请参见[使用客户机侦测策略](#)。
- 10 添加并发布端点保护规则。请参见[添加并发布端点保护规则](#)。
- 11 监控端点保护规则。请参见[监控端点保护状态](#)。

配置端点保护的必备条件

在为客户机虚拟机配置端点保护之前，请确保满足以下必备条件。

前提条件

- 已在所有主机上安装 NSX Manager。
- 通过应用传输节点配置文件，准备 NSX-T Data Center 集群并将其配置为传输节点。将主机配置为传输节点后，安装客户机侦测组件。请参见《NSX-T Data Center 安装指南》。
- 已安装并配置合作伙伴控制台以在 NSX-T Data Center 中注册服务。
- 确保客户机虚拟机运行虚拟机硬件配置文件版本 9 或更高版本。
- 配置 VMware Tools 并安装 Thin Agent。
 - 请参见在 [Linux 虚拟机上安装客户机侦测瘦代理](#)。
 - 请参见在 [Windows 虚拟机上安装客户机侦测瘦代理](#)。
 - 请参见为网络侦测安装 [Linux Thin Agent](#)。

在 Linux 虚拟机上安装客户机侦测瘦代理

在 Linux 中，客户机侦测支持仅用于防病毒保护的文件侦测。要使用客户机侦测安全解决方案保护 Linux 虚拟机，您必须安装客户机侦测瘦代理。

Linux Thin Agent 是作为操作系统特定软件包 (OSP) 的一部分提供的。这些软件包托管在 VMware 软件包门户上。企业或安全管理员（非 NSX 管理员）可以在 NSX 外部的客户机虚拟机上安装该代理。

不需要安装 VMware Tools。

根据您的 Linux 操作系统，请通过根权限执行以下步骤：

前提条件

- 确保客户机虚拟机安装了支持的 Linux 版本。
 - Red Hat Enterprise Linux (RHEL) 7.4（64 位）GA
 - SUSE Linux Enterprise Server (SLES) 12（64 位）GA
 - Ubuntu 16.04.5 LTS（64 位）GA
 - CentOS 7.4 GA

- 确认在 Linux 虚拟机上安装了 GLib 2.0。

步骤

1 对于 Ubuntu 系统

- a 使用以下命令获取并导入 VMware 包装公钥。

```
curl -O https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
apt-key add VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- b 在 /etc/apt/sources.list.d 下新建一个名为 vmware.list 的文件。
- c 编辑文件使其包含以下内容：

```
deb [arch=amd64] https://packages.vmware.com/packages/nsx-gi/latest/ubuntu/ xenial main
```

- d 安装该软件包。

```
apt-get update
apt-get install vmware-nsx-gi-file
```

2 对于 RHEL7 系统

- a 使用以下命令获取并导入 VMware 包装公钥。

```
curl -O https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
rpm --import VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- b 在 /etc/yum.repos.d 下新建一个名为 vmware.repo 的文件。
- c 编辑文件使其包含以下内容：

```
[vmware]
name = VMware
baseurl = https://packages.vmware.com/packages/nsx-gi/latest/rhel7/x86_64
enabled = 1
gpgcheck = 1
metadata_expire = 86400
ui_repoid_vars = basearch
```

3 安装该软件包。

```
yum install vmware-nsx-gi-file
```

4 对于 SLES 系统

- a 使用以下命令获取并导入 VMware 包装公钥。

```
curl -O https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-
RSA-KEY.pub
rpm --import VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- b 添加以下存储库：

```
zypper ar -f "https://packages.vmware.com/packages/nsx-gi/latest/sle12/x86_64/" VMware
```

- c 安装该软件包。

```
zypper install vmware-nsx-gi-file
```

5 对于 CentOS 系统

- a 使用以下命令获取并导入 VMware 包装公钥。

```
curl -O https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-
RSA-KEY.pub
rpm --import VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- b 在 /etc/yum.repos.d 下新建一个名为 vmware.repo 的文件。

- c 编辑文件使其包含以下内容：

```
[vmware]
name = VMware
baseurl = https://packages.vmware.com/packages/nsx-gi/latest/centos7/x86_64
enabled = 1
gpgcheck = 1
metadata_expire = 86400
ui_repoid_vars = basearch
```

后续步骤

使用服务 `vsepd status` 命令和管理特权验证 Thin Agent 是否正在运行。状态必须为正在运行。

为网络侦测安装 Linux Thin Agent

安装 Linux Thin Agent 以自检网络流量。

重要事项 为防止客户机虚拟机使用防病毒软件，您无需为网络侦测安装 Linux Thin Agent。

用于自检网络流量的 Linux Thin Agent 驱动程序依赖于开源驱动程序。

前提条件

安装以下软件包：

- glib2

- libnetfilter-contrack3/ libnetfilter-contrack
- libnetfilter-queue1/ libnetfilter-queue
- iptables

步骤

1 安装客户机侦测提供的开源驱动程序。

- a 添加以下 URL 作为操作系统的基本 URL。

```
deb [arch=amd64] https://packages.vmware.com/guest-introspection-for-vmware-nsx/latest/
```

- b 导入 VMware 包装密钥。

```
https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- c 更新存储库并安装开源驱动程序。

```
apt-get install Guest-Introspection-for-VMware-NSX
```

2 安装用于自检文件和/或网络流量的 Linux Thin Agent。

- 要安装文件和网络侦测软件包，请在步骤 c 中选择 vmware-nsx 软件包。
 - 要安装网络侦测软件包，请在步骤 c 中选择 vmware-nsx-gi-net 软件包。
- a 添加以下 URL 作为操作系统的基本 URL。

```
deb [arch=amd64] https://packages.vmware.com/packages/nsx-gi/latest
```

- b 导入 VMware 包装密钥。

```
https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- c 安装其中一个驱动程序。

```
vmware-nsx-gi
vmware-nsx-gi-net
```

在 Windows 虚拟机上安装客户机侦测瘦代理

要使用客户机侦测安全解决方案保护虚拟机，您必须在虚拟机上安装客户机侦测瘦代理（也称为客户机侦测驱动程序）。客户机侦测驱动程序是随适用于 Windows 的 VMware Tools 提供的，但不是默认安装的一部分。要在 Windows 虚拟机上安装客户机侦测，您必须执行自定义安装并选择这些驱动程序。

在安装了该安全解决方案的 ESXi 主机上启动已安装客户机侦测驱动程序的 Windows 虚拟机时，将会自动保护这些虚拟机。在关机并重新启动后，仍会对保护的虚拟机进行安全保护，即使在通过 vMotion 移动到另一个安装了该安全解决方案的 ESXi 主机后也是如此。

- 如果您使用的是 vSphere 6.0，请参见以下有关安装 VMware Tools 的说明：[在 Windows 虚拟机中手动安装或升级 VMware Tools](#)。
- 如果使用的是 vSphere 6.5，请参见以下说明以安装 VMware Tools：<https://docs.vmware.com/cn/VMware-Tools/index.html>。

前提条件

确保客户机虚拟机安装了支持的 Windows 版本。NSX 客户机侦测支持以下 Windows 操作系统：

- Windows XP SP3 及更高版本（32 位）
- Windows Vista（32 位）
- Windows 7（32/64 位）
- Windows 8（32/64 位）
- Windows 8.1 (32/64)（vSphere 6.0 及更高版本）
- Windows 10
- Windows 2003 SP2 及更高版本（32/64 位）
- Windows 2003 R2（32/64 位）
- Windows 2008（32/64 位）
- Windows 2008 R2（64 位）
- Win2012 (64)
- Win2012 R2 (64)（vSphere 6.0 及更高版本）
- Windows Server 2016
- Windows Server 2019

步骤

- 1 按照针对您的 vSphere 版本的说明开始安装 VMware Tools。选择**自定义安装**。
- 2 展开“VMCI 驱动程序”部分。

可用的选项因 VMware Tools 版本而异。

3 选择要在虚拟机上安装的驱动程序。

驱动程序	说明
vShield Endpoint 驱动程序	安装文件侦测 (vsepflt) 和网络侦测 (vnetflt) 驱动程序。
客户机侦测驱动程序	安装文件侦测 (vsepflt) 和网络侦测 (vnetflt) 驱动程序。
NSX 文件侦测驱动程序和 NSX 网络侦测驱动程序	选择 NSX 文件侦测驱动程序以安装 vsepflt。 (可选) 选择 NSX 网络侦测驱动程序以安装 vnetflt (Windows 10 或更高版本上为 vnetWFP)。
注 只有在使用身份防火墙或端点监控功能时, 才应选择 NSX 网络侦测驱动程序。	

4 在要添加的驱动程序旁边的下拉菜单中, 选择此功能将安装在本地硬盘上。

5 按照此过程中的剩余步骤进行操作。

后续步骤

使用 fltmc 命令和管理特权验证 Thin Agent 是否正在运行。输出中的“筛选器名称”列将列出具有条目 vsepflt 的瘦代理。

支持的软件

客户机侦测可以与特定版本的软件进行互操作。

VMware Tools

支持 VMware Tool 10.3.10 版本。

检查 VMware Tools 和 NSX-T 之间的互操作性。请参见 [VMware 产品互操作性列表](#)。

支持的操作系统

- Windows 7
- Windows 8/8.1
- Windows 10
- Windows 2008 Server R2
- Windows 2012 Server R2
- Windows 2016 Server
- CentOS 7.4 GA
- RHEL 7.4 GA
- Ubuntu 16.04.5 LTS (64 位)
- SLES 12 GA

支持的主机

有关支持的 ESXi 主机, 请参见 [VMware 产品互操作性列表](#)。

创建具有客户机侦测合作伙伴管理员角色的用户

为用户分配 NSX-T Data Center 中提供的客户机侦测合作伙伴管理员角色。

注意：建议与客户机侦测合作伙伴管理员角色相关联的用户注册合作伙伴服务，以避免出现任何安全问题。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择系统 → 用户 → 角色分配。
- 3 单击添加。
- 4 选择用户，并为该用户分配 **GI 合作伙伴管理员** 角色。

后续步骤

在 NSX-T Data Center 中注册服务。请参见在 [NSX-T Data Center 中注册服务](#)。

在 NSX-T Data Center 中注册服务

在 NSX-T Data Center 中注册第三方安全服务。

前提条件

- 确保满足必备条件。请参见[配置端点保护的必备条件](#)。
- 确保为 vIDM 用户分配了 GI 合作伙伴管理员角色。将使用此角色来在 NSX-T Data Center 中注册服务。

步骤

- 1 使用 GI 合作伙伴管理员特权登录到合作伙伴控制台。
- 2 在 NSX-T Data Center 中注册服务、供应商模板以及配置合作伙伴解决方案。请参见合作伙伴文档。

后续步骤

查看合作伙伴服务目录。请参见[查看合作伙伴服务目录](#)。

查看合作伙伴服务目录

目录页面显示所有合作伙伴及其在 NSX-T Data Center 中注册的服务。

前提条件

- 合作伙伴已在 NSX-T Data Center 中注册服务。
- 服务部署在集群上。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。

2 选择**系统 > 服务部署 > 目录**。

3 在某服务上单击**查看**。“部署”页面将显示有关该服务的详细信息，如部署状态、网络详细信息、集群详细信息等。

后续步骤

升级合作伙伴服务虚拟机。

部署服务

注册服务后，必须部署服务实例，该服务才会开始处理网络流量。

在集群中的所有 NSX-T Data Center 主机上部署运行合作伙伴安全引擎的合作伙伴服务虚拟机。使用 vSphere ESX Agency Manager (EAM) 服务在每个主机上部署合作伙伴服务虚拟机。部署 SVM 后，可以创建 SVM 用于保护客户机虚拟机的策略规则。

前提条件

- 所有主机都由一个 vCenter Server 管理。
- 合作伙伴服务已在 NSX-T Data Center 中注册并准备好进行部署。
- NSX-T Data Center 管理员可以访问合作伙伴服务和供应商模板。
- 服务虚拟机和合作伙伴 Service Manager（控制台）必须能够在管理网络级别相互通信。
- 将主机准备好作为 NSX-T Data Center 传输节点：
 - 创建传输区域。
 - 创建 IP 池以分配隧道端点 IP 地址。
 - 创建上行链路配置文件。
 - 添加传输节点配置文件，为自动部署 NSX-T Data Center 传输节点准备好集群。
 - 配置独立或受管主机。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 转到**系统**选项卡，然后单击**服务部署**。
- 3 从“合作伙伴服务”下拉列表中，选择要部署的服务。
- 4 单击**部署**，然后单击**部署服务**。
- 5 输入服务部署名称。
- 6 在“计算管理器”字段中，选择 vCenter Server 上的计算资源以部署服务。
- 7 在“集群”字段中，选择需要部署服务的集群。

- 8 在“数据存储”下拉菜单中，您可以：
 - a 选择一个数据存储作为服务虚拟机的存储库。
 - b 选择**已在主机上指定**。该设置意味着无需在此向导中选择数据存储和端口组。可以直接在 vCenter Server 中的 EAM 上将代理设置配置为指向用于服务部署的特定数据存储和端口组。

要了解如何配置 EAM，请参阅 vSphere 文档。
- 9 在“网络”列中，单击**设置**。
- 10 将“管理网络接口”设为**已在主机上指定**或 **DVPG**。
- 11 将网络类型设为 DHCP 或静态 IP 池。如果将网络类型设置为静态 IP 池，请从可用的 IP 池列表中进行选择。
- 12 在“部署规范”字段中，选择基于主机的部署以在所有主机上部署服务。根据由合作伙伴注册的服务，可以在单个服务虚拟机中部署多个服务。
- 13 在“部署模板”字段中，选择已注册的部署模板。
- 14 单击**保存**。

结果

新主机添加到集群时，EAM 将自动在新主机上部署服务虚拟机。部署过程可能需要一些时间，具体取决于供应商的实施。可以在 NSX Manager 用户界面中查看状态。状态变为部署成功时，表明服务已在主机上成功部署。

要从集群中移除主机，请先将其移至维护模式。然后，选择将客户机虚拟机迁移到另一个主机的选项以完成迁移。

后续步骤

了解有关在主机上部署的服务实例的部署详细信息和运行状况。请参见[查看服务实例详细信息](#)。

查看服务实例详细信息

了解有关在集群的成员主机上所部署服务实例的部署详细信息和运行状况。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**系统 > 服务部署 > 服务实例**。
- 3 从“合作伙伴服务”下拉菜单中，选择合作伙伴服务以查看与服务实例相关的详细信息。

表 10-9.

字段	说明
服务实例名称	标识特定主机上服务实例的唯一 ID。
服务部署名称	部署服务时输入的名称。
部署位置	主机 IP 地址或 FQDN

表 10-9. (续)

字段	说明
部署模式	集群或独立
部署状态	“开启”状态确定部署成功
运行状况	<p>部署服务实例时，运行状况为就绪。要将运行状况从就绪更改为已启动，请对配置进行所需的更改。请参见启动服务实例。</p> <p>在 NSX-T Data Center 成功实现以下参数后，运行状况将从就绪更改为已启动。</p> <ul style="list-style-type: none"> ■ 解决方案状态：开启 ■ NSX-T Data Center 客户机侦测代理和 NSX-T Data Center Ops 代理之间的连接：已连接 ■ 收到运行状况的时间：<天，日期，时间>

后续步骤

启动服务实例。请参见[启动服务实例](#)。

启动服务实例

部署服务实例后，需要在 NSX-T Data Center 中实现某些参数，以使运行状况保持正常运行状态。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**系统 > 服务部署 > 服务实例**。
- 3 从“合作伙伴服务”下拉菜单中，选择合作伙伴服务以查看与服务实例相关的详细信息。
- 4 “运行状况”列显示服务实例的状态为就绪。它表示已准备好使用“端点保护策略规则”配置“服务实例”以保护虚拟机。
- 5 要使运行状况更改为开启，必须在 NSX-T Data Center 中实现以下参数。
 - 客户机虚拟机必须在主机上可用。
 - 必须打开虚拟机的电源。
 - 端点保护规则必须应用于客户机虚拟机。
 - 必须使用支持的 VMtools 和文件侦测驱动程序版本配置客户机虚拟机。

后续步骤

添加服务配置文件。请参见[添加服务配置文件](#)。

添加服务配置文件

仅当服务配置文件在 NSX-T Data Center 中可用时，才实施客户机侦测策略。通过合作伙伴提供的模板创建服务配置文件。服务配置文件是管理员通过选择供应商提供的模板为虚拟机选择保护级别（黄金级、白银级和白金级策略）的一种方法。

例如，供应商可以提供黄金、白金和白银策略级别。创建的每个配置文件可服务于不同类型的工作负载。黄金级服务配置文件为 PCI 类型的工作负载提供完整的防恶意软件，而白银级服务配置文件仅为常规工作负载提供基本的防恶意软件保护。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 选择 **安全 > 端点保护 > 端点保护规则 > 服务配置文件**。
- 3 从“合作伙伴服务”字段中，选择要为其创建服务配置文件的服务。
- 4 单击 **添加服务配置文件**。
- 5 输入服务配置文件名称，然后选择供应商模板。（可选）添加描述和标记。
- 6 单击 **保存**。

用于创建服务配置文件的供应商模板 ID 将传送到合作伙伴控制台。合作伙伴将存储供应商模板 ID 以跟踪受这些供应商模板保护的客户机虚拟机的使用情况。

结果

创建服务配置文件后，NSX admin 可创建规则以在发布策略规则之前将服务配置文件关联到一组虚拟机。

后续步骤

对需要防御恶意软件的客户机虚拟机组应用端点保护策略。请参见[使用客户机侦测策略](#)。

使用客户机侦测策略

可以通过创建规则，将服务配置文件与虚拟机组相关联，以便在虚拟机组上实施策略。将规则应用于虚拟机组后，便立即开始提供保护。

端点保护策略是一种由合作伙伴提供的保护服务，可通过在客户机虚拟机上实施服务配置文件保护客户机虚拟机免受恶意软件的攻击。将规则应用于虚拟机组后，该组中的所有客户机虚拟机都将受该服务配置文件的保护。在客户机虚拟机上发生文件访问事件时，GI 精简代理（在每个客户机虚拟机上运行）将收集文件的上下文（文件属性、文件句柄和其他上下文详细信息），并向 SVM 通知事件。如果 SVM 要扫描文件内容，它将使用 EPSec API 库请求详细信息。SVM 给出文件未受感染结论后，GI 精简代理允许用户访问该文件。如果 SVM 报告文件已受感染，GI 精简代理将拒绝用户访问此文件。

要在虚拟机组上执行安全服务，您需要：

步骤

- 1 定义策略和规则。
- 2 定义成员资格条件以建立虚拟机组。

- 3 为虚拟机组定义规则。
- 4 发布规则。

添加并发布端点保护规则

将策略规则发布到虚拟机组意味着将需要保护的虚拟机组与特定的服务配置文件相关联。

步骤

- 1 在“策略区域”中，选择一个策略。
- 2 单击**添加** -> **添加规则**。
- 3 在新规则中，输入规则名称。
- 4 在“选择组”字段中，单击“编辑”图标。
- 5 在“设置组”窗口中，从现有组列表选择一个组或添加一个新组。
 - a 要添加新组，请单击**添加组**，输入相关详细信息，然后单击**保存**。
请参见[添加组](#)。
- 6 在“组”列中，选择虚拟机组。
- 7 在“服务配置文件”列中，选择为组中的客户机虚拟机提供所需保护级别的服务配置文件。
 - a 要添加新的服务配置文件，请单击**添加服务配置文件**，输入相关详细信息，然后单击**保存**。
请参见[添加服务配置文件](#)。
- 8 单击**发布**。

结果

端点保护策略将保护虚拟机组。

后续步骤

您可能希望根据不同虚拟机组所需的保护类型更改规则顺序。请参见[客户机侦测如何运行端点保护策略](#)

监控端点保护状态

监控受保护虚拟机和不受保护虚拟机的配置状态、主机代理和服务虚拟机问题，以及配置有文件侦测驱动程序（在 VMtools 安装过程中安装）的虚拟机。

您可以查看：

- 查看服务部署状态。
- 查看端点保护的配置状态。
- 查看为端点保护设置的容量状态。

查看服务部署状态

可在监控仪表板上查看服务部署详细信息。

查看系统范围内的 EPP 策略状态。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 导航到 **主页 > 监控 - 仪表板**。
- 3 从下拉菜单中单击 **监控 - 系统**。
- 4 要查看系统中集群之间的部署状态，请导航到“端点保护”小组件，单击圆环图以查看成功或不成功的部署。

“服务部署”页面将显示部署详细信息。

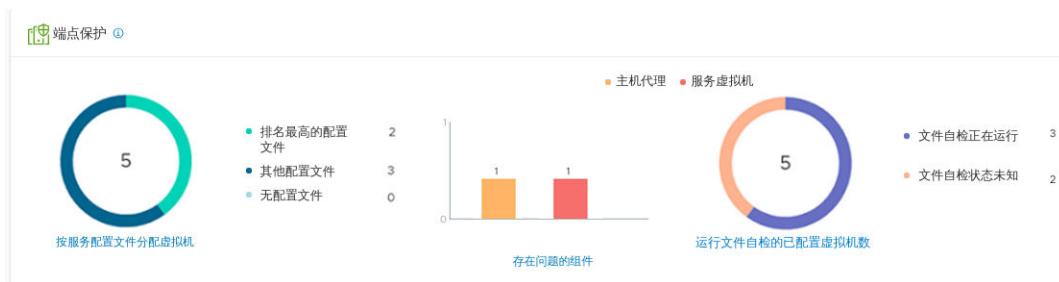
查看端点保护的配置状态

查看端点保护服务的配置状态。

查看系统范围内的 EPP 策略状态。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 导航到 **主页 > 安全 > 安全概览**。
- 3 要查看集群上 EPP 的状态，请单击“安全”小组件。
- 4 在“安全概览”页面中，单击**配置**。



- 5 在“端点保护”部分中，查看：
 - a 显示“按服务配置文件分配虚拟机”小组件：
 - 1 受排名最高的配置文件保护的虚拟机数量。排名最高的配置文件表示保护集群上最多数量虚拟机的配置文件。
 - 2 受其余服务配置文件保护的虚拟机被归类为“其他配置文件”。
 - 3 未受保护的虚拟机被归类为“无配置文件”。

“端点保护规则”页面会显示受端点保护策略保护的虚拟机。

b 显示“存在问题的组件”小组件：

- 1 主机：与上下文多路复用器相关的问题。
- 2 SVM：与服务虚拟机相关的问题。例如，如果 SVM 状态为关闭，则与客户机虚拟机的 SVM 连接会关闭。

“部署”页面上的“状态”列会显示运行状况问题。

c 显示“运行文件侦测的配置虚拟机”小组件：

- 1 受文件侦测驱动程序保护的虚拟机。
- 2 文件侦测驱动程序状态为未知的虚拟机。

ESXi Agency Manager (EAM) 尝试解决与主机、SVM 和配置错误相关的一些问题。请参见[解决合作伙伴服务问题](#)。

查看为端点保护设置的容量状态

查看端点保护服务的容量状态。

查看 EPP 策略的容量状态。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 导航到主页 > 监控 - 仪表板。
- 3 从下拉菜单中单击 **监控 - 网络和安全**。
- 4 要查看集群上 EPP 的状态，请单击“安全”小组件。
- 5 在“安全概览”页面中，单击**容量**，然后查看以下参数的容量状态。

限制	最大容量	当前清单 (已实现)	警告警示	严重警示
分布式防火墙规则	100,000	2	0%	70% 100%
系统范围的防火墙区域	10,000	5	0.05%	70% 100%

- a **已启用端点保护的系统范围的主机：**如果受保护的主机数量达到阈值限制，则当达到相应的阈值限制时，NSX Manager 会发出警告警示或严重警示通知。
- b **已启用端点保护的系统范围的虚拟机：**如果受保护的虚拟机数量达到阈值限制，则当达到相应的阈值限制时，NSX Manager 会发出警告警示或严重警示通知。

注 您可以为这些参数设置阈值限制、查看状态，并在这些参数达到设定的阈值限制时接收警示。

管理端点保护

解决策略冲突、服务虚拟机的运行状况问题，并了解端点保护策略的运行方式。

解决合作伙伴服务问题

如果合作伙伴服务虚拟机未正常运行，则客户机虚拟机不会受到保护以抵御恶意软件的攻击。

在每个主机上，确认以下服务或进程已启动并正在运行：

- ESXi Agency Manager (EAM) 服务必须启动并正在运行。必须可访问以下 URL。

```
https://<vCenter_Server_IP_Address>/eam/mob
```

确认 ESXi Agency Manager 处于联机状态。

```
root> service-control --status vmware-eam
```

- 不能删除 SVM 的端口组，因为需要这些端口组来确保 SVM 持续保护客户机虚拟机。

```
https://<vCenter_Server_IP_Address>/ui
```

- 在 vCenter Server 中，转到虚拟机，单击**网络**选项卡，然后检查是否列出了 **vmervice-vshield-pg**。
- 上下文多路复用器 (MUX) 服务启动并正在运行。检查 **nsx-context-mux** VIB 在主机上已启动并正在运行。
- NSX-T Data Center 与合作伙伴服务控制台通信的管理接口必须已启动。
- 在 MUX 和 SVM 之间启用通信的控制接口必须已启动。必须创建将 MUX 与 SVM 连接的端口组。合作伙伴服务要正常运行，需要此接口和端口组。

ESXi Agency Manager 问题

下表列出了可以使用 NSX Manager 用户界面上的“解决”按钮解决的 ESXi Agency Manager 问题。它会向 NSX Manager 通知错误详细信息。

表 10-10. ESXi Agency Manager 问题

问题	类别	说明	解决方案
无法访问代理 OVF	虚拟机未部署	需要在主机上部署代理虚拟机，但由于 ESXi Agent Manager 无法访问代理的 OVF 软件包，无法部署代理虚拟机。发生这种情况可能是因为，提供 OVF 软件包的 Web 服务器已关闭。该 Web 服务器通常位于创建代理机构的解决方案内部。	ESXi Agency Manager (EAM) 服务会重试 OVF 下载操作。检查合作伙伴管理控制台状态。单击 解决 。
主机版本不兼容	虚拟机未部署	需要在主机上部署代理虚拟机。但是，由于兼容性问题，未在主机上部署代理。	升级主机或解决方案以使代理与主机兼容。检查 SVM 的兼容性。单击 解决 。

表 10-10. ESXi Agency Manager 问题（续）

资源不足	虚拟机未部署	需要在主机上部署代理虚拟机。但是，由于主机的 CPU 或内存资源较少，ESXi Agency Manager (EAM) 服务未部署代理虚拟机。	ESXi Agency Manager (EAM) 服务会尝试重新部署虚拟机。确保 CPU 和内存资源可用。检查主机并释放一些资源。单击 解决 。
空间不足	虚拟机未部署	需要在主机上部署代理虚拟机。但是，由于主机上的代理数据存储没有足够的可用空间，未部署代理虚拟机。	ESXi Agency Manager (EAM) 服务会尝试重新部署虚拟机。释放数据存储上的一些空间。单击 解决 。
无代理虚拟机网络	虚拟机未部署	需要在主机上部署代理虚拟机，但由于未在主机上配置代理网络，无法部署代理。	将 customAgentVmNetwork 中列出的某个网络添加到主机。在数据存储可用后，该问题会自动解决。
OVF 格式无效	虚拟机未部署	需要在主机上置备代理虚拟机，但由于 OVF 软件包置备失败，无法执行该操作。在升级或修补提供 OVF 软件包的解决方案以提供代理虚拟机的有效 OVF 软件包之后，置备才有可能成功。	ESXi Agency Manager (EAM) 服务会尝试重新部署 SVM。请查看合作伙伴解决方案文档或升级合作伙伴解决方案以获取有效的 OVF 软件包。单击 解决 。
缺少代理 IP 池	虚拟机已关闭电源	需要打开代理虚拟机电源，但由于在代理的虚拟机网络上没有定义任何 IP 地址，代理虚拟机已关闭电源。	在虚拟机网络上定义 IP 地址。单击 解决 。
无代理虚拟机数据存储	虚拟机已关闭电源	需要在主机上部署代理虚拟机，但由于未在主机上配置代理数据存储，无法部署代理。	将 customAgentVmDatastore 中列出的某个数据存储添加到主机。在数据存储可用后，该问题会自动解决。
无自定义代理虚拟机网络	无代理虚拟机网络	需要在主机上部署代理虚拟机，但由于未在主机上配置代理网络，无法部署代理。	将主机添加到自定义代理虚拟机网络中列出的某个网络中。在自定义虚拟机网络可用后，该问题会自动解决。
无自定义代理虚拟机数据存储	无代理虚拟机数据存储	需要在主机上部署代理虚拟机，但由于未在主机上配置代理数据存储，无法部署代理。	将主机添加到自定义代理虚拟机数据存储中列出的某个数据存储中。该问题会自动解决。
孤立代理机构	代理机构问题	在 vCenter Server 中不再注册创建代理机构的解决方案。	在 vCenter Server 中注册解决方案。
孤立的 DvFilter 交换机	主机问题	在主机上存在 dvFilter 交换机，但主机上的代理均不依赖于 dvFilter。如果在更改代理机构配置时主机断开连接，会发生这种情况。	单击 解决 。在更新代理机构配置之前，ESXi Agency Manager (EAM) 服务会尝试连接主机。
代理虚拟机未知	主机问题	在 vCenter Server 清单中找到不属于该 vSphere ESX Agent Manager 服务器实例中的任何代理机构的代理虚拟机。	单击 解决 。ESXi Agency Manager (EAM) 服务会尝试将虚拟机置于其所属的清单中。

表 10-10. ESXi Agency Manager 问题（续）

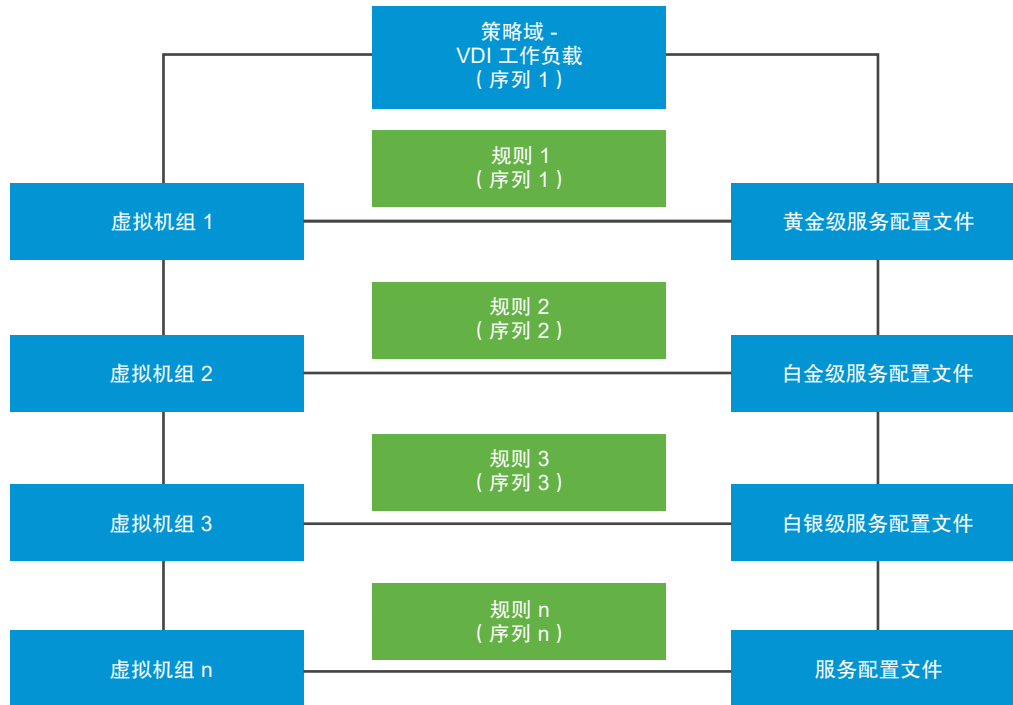
OVF 属性无效	虚拟机问题	必须打开代理虚拟机电源，但缺少 OVF 属性或具有无效的值。	单击 解决 。ESXi Agency Manager (EAM) 服务会尝试重新配置正确的 OVF 属性。
虚拟机已损坏	虚拟机问题	代理虚拟机已损坏。	单击 解决 。ESXi Agency Manager (EAM) 服务会尝试修复虚拟机。
虚拟机已孤立	虚拟机问题	代理虚拟机存在于主机上，但主机不再是代理机构范围的一部分。如果在更改代理机构配置时主机断开连接，会发生这种情况。	单击 解决 。ESXi Agency Manager (EAM) 服务会尝试将主机重新连接到代理机构配置。
虚拟机已部署	虚拟机问题	需要从主机中移除代理虚拟机，但并未移除代理虚拟机。vSphere ESX Agent Manager 无法移除代理虚拟机的原因很具体，例如，主机处于维护模式、已关闭电源或处于待机模式。	单击 解决 。ESXi Agency Manager (EAM) 服务会尝试从主机中移除代理虚拟机。
虚拟机已关闭电源	虚拟机问题	需要打开代理虚拟机电源，但已关闭代理虚拟机电源。	单击 解决 。ESXi Agency Manager (EAM) 服务会尝试打开虚拟机的电源。
虚拟机已打开电源	虚拟机问题	需要关闭代理虚拟机电源，但已打开代理虚拟机电源。	单击 解决 。ESXi Agency Manager (EAM) 服务会尝试关闭虚拟机的电源。
虚拟机已挂起	虚拟机问题	需要打开代理虚拟机电源，但代理虚拟机已挂起。	单击 解决 。ESXi Agency Manager (EAM) 服务会尝试打开虚拟机的电源。
虚拟机文件夹错误	虚拟机问题	代理虚拟机需要位于指定的代理虚拟机文件夹中，但位于其他文件夹中。	单击 解决 。ESXi Agency Manager (EAM) 服务会尝试将代理虚拟机置于指定的文件夹中。
虚拟机资源池错误	虚拟机问题	代理虚拟机需要位于指定的代理虚拟机资源池中，但位于其他资源池中。	单击 解决 。ESXi Agency Manager (EAM) 服务会尝试将代理虚拟机置于指定的资源池。
虚拟机未部署	代理问题	需要在主机上部署代理虚拟机，但并未部署代理虚拟机。ESXi Agent Manager 无法部署代理的原因很具体，例如，无法访问代理的 OVF 软件包或缺少主机配置。如果从主机中明确删除代理虚拟机，则也会出现该问题。	单击 解决 以部署该代理虚拟机。

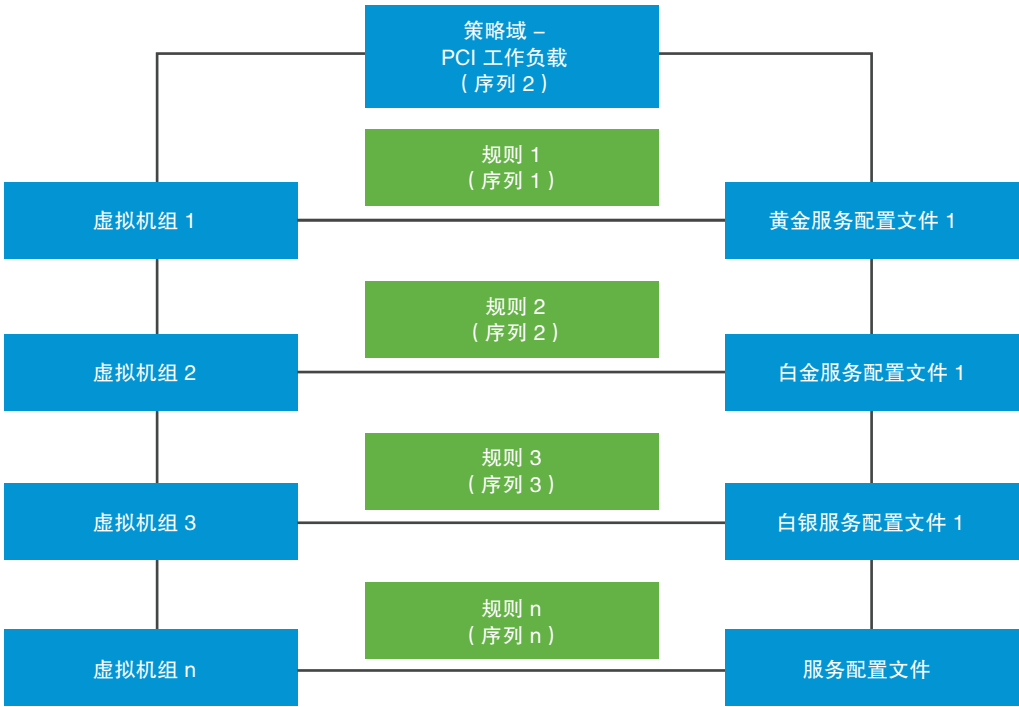
接下来，为虚拟机组配置端点保护。请参见[端点保护](#)。

客户机侦测如何运行端点保护策略

端点保护策略按特定顺序实施。设计策略时，请考虑与规则相关联的序列号和托管规则的域。

场景：您的组织中运行许多工作负载，为便于演示，我们只考虑其中两种类型的工作负载 - 运行虚拟桌面基础架构 (VDI) 的虚拟机和运行支付卡行业数据安全标准 (PCI-DSS) 工作负载的虚拟机。组织中的一部分员工需要远程桌面访问，从而形成了虚拟桌面基础架构 (VDI) 工作负载。根据组织规定的合规性规则，这些 VDI 工作负载可能需要黄金保护策略级别。而 PCI-DSS 工作负载需要最高级别的保护：白金级保护。





由于有两种工作负载类型，需要创建两个策略，分别用于 VDI 工作负载和服务器工作负载。在每个策略或区域中，定义一个域来反映工作负载类型，并在该区域中为该工作负载定义规则。发布规则以在客户机虚拟机上启动 GI 服务。GI 在内部使用两个序列号：策略序列号和规则序列号，用于确定要运行的规则的完整序列。每个规则都有两种用途：确定要保护的虚拟机和为保护虚拟机而必须应用的保护策略。

要更改序列顺序，请通过在 NSX-T Policy Manager UI 拖动规则来更改其序列顺序。或者，也可以使用 API 为规则明确分配序列号。

另外，还可以执行 NSX-T Data Center API 调用，通过将服务配置文件与虚拟机组关联手动定义规则并声明规则的序列号。有关 API 和参数的详细信息，请参见《NSX-T Data Center API 指南》。执行服务配置 API 调用，以将配置文件应用于虚拟机组等实体。

表 10-11. 用于定义将服务配置文件应用于虚拟机组的规则 NSX-T Data Center API

API	详细信息
获取所有服务配置详细信息。	<div>GET /api/v1/service-configs</div> <div>此服务配置 API 返回以下详细信息：应用于虚拟机组的服务配置文件、受保护的虚拟机组以及决定规则优先级的序列号或优先级编号。</div>
创建服务配置。	<div>POST /api/v1/service-configs</div> <div>此服务配置 API 接受以下项的输入参数：服务配置文件、要保护的虚拟机组以及必须应用于规则的顺序号或优先级编号。</div>
删除服务配置。	<div>DELETE /api/v1/service-configs/<config-set-id></div> <div>此服务配置 API 删除应用于虚拟机组的配置。</div>

表 10-11. 用于定义将服务配置文件应用于虚拟机组的规则 NSX-T Data Center API（续）

API	详细信息
获取特定配置的详细信息。	<pre>GET /api/v1/service-configs/ <config-set-id></pre> <p>获取特定配置的详细信息。</p>
更新服务配置。	<pre>PUT /api/v1/service-configs/ <config-set-id></pre> <p>更新服务配置。</p>
获取有效的配置文件。	<pre>GET /api/v1/service-configs/ effective-profiles?resource_id=<resource-id> &resource_type=<resource-type></pre> <p>此服务配置 API 仅返回应用于特定虚拟机组的配置文件。</p>

通过遵循以下建议高效管理规则：

- 为必须先运行的规则所在的策略设置更高的序列号。从 UI 中，可以拖动策略更改其优先级。
- 同样，为每个策略内的规则设置更高的序列号。
- 根据所需的规则数量，可以将规则按 2、3、4 或甚至 10 的倍数分开放置。因此，两个相隔 10 个位置的连续规则可以更灵活地对规则重新排序，而不必更改所有规则的序列顺序。例如，如果您不打算定义许多规则，可以选择以 10 个位置为间隔放置规则。因此，规则 1 获取序列号 1，规则 2 获取序列号 10，规则 3 获取序列号 20，依此类推。此建议可灵活地高效管理规则，无需对所有规则重新排序。

在内部，客户机侦测以下列方式对这些策略规则排序。

```
Policy 1 ↔ Sequence Number 1 (1000)

- Rule 1 : Group 1 ↔ Service Profile ↔ Sequence Number 1 (1001)

- Rule 2 : Group 1 ↔ Service Profile ↔ Sequence Number 10 (1010)

- Rule 3 : Group 1 ↔ Service Profile ↔ Sequence Number 20 (1020)

- Rule 4 : Group 1 ↔ Service Profile ↔ Sequence Number 30 (1030)

Policy 2 ↔ Sequence Number 2 (2000)

- Rule 1 : Group 1 ↔ Service Profile ↔ Sequence Number 1 (2001)

- Rule 2 : Group 1 ↔ Service Profile ↔ Sequence Number 10 (2010)

- Rule 3 : Group 1 ↔ Service Profile ↔ Sequence Number 20 (2020)

- Rule 4 : Group 1 ↔ Service Profile ↔ Sequence Number 30 (2030)
```

根据以上序列号，GI 先运行策略 1 的规则，再运行策略 2 的规则。

但在某些情况下，预期规则不应用于虚拟机组或虚拟机。需要解决这些冲突才可应用所需的策略保护级别。

解决端点策略冲突

我们以这样一种场景为例：存在两个策略域，且每个策略域均包含多个规则。作为 **admin** 用户，您并不能始终确定哪些虚拟机最终可以获得组的成员资格，因为虚拟机根据动态成员资格条件（例如，操作系统名称、计算机名称、用户、标记）与组相关联。

在以下情况下会出现冲突：

- 一个虚拟机属于两个组，其中每个组由不同的配置文件进行保护。
- 一个合作伙伴服务虚拟机与多个服务配置文件相关联。
- 意外规则在客户机虚拟机上运行，或规则不在虚拟机组上运行。
- 序列号未分配给策略规则或域。

表 10-12. 解决策略冲突

场景	预期端点保护流程	解决方案
一个虚拟机获得多个组的成员资格时。而且，每个组由不同类型的服务配置文件进行保护。 未对虚拟机应用预期保护。	<p>基于组成员资格条件创建的虚拟机组意味着将虚拟机动态添加到该组。在这种情况下，同一虚拟机可以属于多个组。由于成员资格条件将虚拟机动态填充到组，因此无法预先确定虚拟机将属于哪个组。</p> <p>假设虚拟机 1 属于组 1 和组 2。</p> <ul style="list-style-type: none"> ■ 规则 1：对组 1（按操作系统名称）应用黄金级（服务配置文件），且序列号为 1 ■ 规则 2：对组 2（按标记）应用白金级，且序列号为 10 <p>端点保护策略在虚拟机 1 上运行黄金级服务配置文件，但不在虚拟机 1 上运行白金级服务配置文件。</p>	<p>更改规则 2 的序列号，使其在规则 1 之前运行。</p> <ul style="list-style-type: none"> ■ 在 NSX-T Policy Manager UI 上的规则列表中，将规则 2 拖动到规则 1 之前。 ■ 使用 NSX-T Policy Manager API，手动为规则 2 添加更高的序列号。
当规则与同一个服务配置文件相关联以保护两个虚拟机组时。 端点保护不在第二个虚拟机组上运行该规则。	<p>端点保护仅在虚拟机上运行第一个服务配置文件，因为同一个服务配置文件不能跨策略或域再次应用于任何其他规则。</p> <p>假设虚拟机 1 属于组 1 和组 2。</p> <p>规则 1：对组 1（按操作系统名称）应用黄金级（服务配置文件）</p> <p>规则 2：对组 2（按标记）应用黄金级（服务配置文件）</p>	<ul style="list-style-type: none"> ■ 将组 2 添加到规则 1。（规则 1：对组 1、组 2 应用配置文件 1）

隔离虚拟机

基于合作伙伴设置的保护级别和标记将规则应用于虚拟机后，可能会有虚拟机被标识为已受到感染，需要隔离。

合作伙伴使用 API 和标记 `virus_found=true` 来标记受到感染的虚拟机。受影响的虚拟机在连接时将使用 `virus_found=true` 标记。

作为管理员，您可以基于带 `virus_found=true` 值的标记创建预定义隔离组，以便在标记受感染的虚拟机后将其填充到组中。作为 **admin**，您可以选择为隔离组设置特定的防火墙规则。您可以为隔离组设置防火墙规则。例如，您可以选择阻止隔离组的所有入站和出站流量。

确认服务实例的运行状况

服务实例的运行状况状态取决于诸多因素：合作伙伴解决方案的状态、客户机侦测代理（上下文多路复用器）和上下文引擎（Ops 代理）之间的连接、客户机侦测代理信息的可用性以及 NSX Manager 的 SVM 协议信息。

步骤


- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 选择 **系统 > 服务部署 > 服务实例**。
- 3 在“运行状况”列中，单击  了解服务实例的运行状况。

表 10-13. 第三方服务实例的运行状况

参数	说明
收到运行状况的时间	NSX Manager 收到服务实例的运行状况详细信息时的最新时间戳。
解决方案状态	在 SVM 上运行的合作伙伴解决方案的状态。状态“正常”指示合作伙伴解决方案正常运行。
NSX-T Data Center 客户机侦测代理和 NSX-T Data Center Ops 代理之间的连接	当 NSX-T Data Center 客户机侦测代理（上下文多路复用器）与 Ops 代理（包括上下文引擎）连接在一起时，状态为“正常”。上下文多路复用器将 SVM 的运行状况信息转发到上下文引擎。它们还相互之间共享 SVM-VM 配置，以了解哪些客户机虚拟机受到 SVM 的保护。
服务虚拟机协议版本	内部用于对问题进行故障排除的传输协议版本。
NSX-T Data Center 客户机侦测代理信息	表示 NSX-T Data Center 客户机侦测代理和 SVM 之间的协议版本兼容性。

- 4 如果运行状况为正常（显示为绿色的状态）并且合作伙伴控制台显示所有客户机虚拟机均受到保护，则服务实例的运行状况为正常。
- 5 如果运行状况为正常（显示为绿色的状态）但是合作伙伴控制台显示客户机虚拟机处于不受保护状态，请执行以下步骤：
 - a 与 VMware 技术支持联系以解决问题。服务实例的运行状况可能为“关闭”，未能正确反映在 NSX Manager 用户界面上。

- 6 如果运行状况为关闭（显示为红色的状态），那么确定服务实例运行状况的一个或多个因素已停止运行。

表 10-14. 对运行状况进行故障排除

运行状况详细信息	解决方案
解决方案状态为关闭或不可用。	<ol style="list-style-type: none"> 1 确认服务部署状态为正常（绿色）。如果遇到错误，请参见解决合作伙伴服务问题。 2 确保受影响主机中至少一个客户机虚拟机受到端点保护策略保护。 3 从合作伙伴控制台中，确认解决方案服务是否正在主机上的 SVM 上运行。请参见合作伙伴文档了解更多详细信息。 4 如果上述步骤无法解决此问题，请与 VMware 技术支持联系。
NSX-T Data Center 客户机侦测代理和 NSX-T Data Center Ops 代理之间的连接处于关闭状态。	<ol style="list-style-type: none"> 1 确认服务部署状态为正常（绿色）。如果遇到错误，请参见解决合作伙伴服务问题。 2 确保受影响主机中至少一个客户机虚拟机受到端点保护策略保护。 3 从合作伙伴控制台中，确认解决方案服务是否正在主机上的 SVM 上运行。请参见合作伙伴文档了解更多详细信息。 4 如果上述步骤无法解决此问题，请与 VMware 技术支持联系。
服务虚拟机协议版本不可用。	<ol style="list-style-type: none"> 1 确认服务部署状态为正常（绿色）。如果遇到错误，请参见解决合作伙伴服务问题。 2 确保受影响主机中至少一个客户机虚拟机受到端点保护策略保护。 3 从合作伙伴控制台中，确认解决方案服务是否正在主机上的 SVM 上运行。请参见合作伙伴文档了解更多详细信息。 4 如果上述步骤无法解决此问题，请与 VMware 技术支持联系。
NSX-T Data Center 客户机侦测代理信息不可用。	与 VMware 技术支持联系。

删除合作伙伴服务

要删除合作伙伴服务，请执行 API 调用。执行 API 调用以删除在主机上部署的合作伙伴服务或 SVM 之前，需要从 NSX Manager 用户界面执行以下操作。

要删除合作伙伴服务，请执行以下操作：

步骤

- 1 移除对在主机上运行的虚拟机组应用的 EPP 规则。
- 2 移除对虚拟机组应用的服务配置文件保护。

- 3 要移除与合作伙伴 Service Manager 绑定的解决方案 SVM，请执行以下 API 调用。

```
/DEL https://<NSX_Manager_IPaddress>/api/v1/serviceinsertion/services/{{service_id}}/
solution-configs/<solution-config-id>
```

- 4 要删除服务部署，请执行以下 API 调用。

```
/DEL https://<NSX_Manager_IPaddress>/api/v1/serviceinsertion/services/<service-id>/service-
deployments/<service-deployment-id>
```

有关 API 参数的详细信息，请参阅《NSX-T Data Center API 指南》。

安全配置文件

本节包含用于微调防火墙操作的配置文件：会话定时器、泛洪保护和 DNS 安全

创建会话定时器

会话定时器定义会话闲置后在防火墙中保留的时间。

协议的会话超时过期后，会话会关闭。在防火墙上，可以为 TCP、UDP 和 ICMP 会话指定一些超时以应用于用户定义的组或者 Tier-0 或 Tier-1 网关。可以根据您的网络需要修改默认会话值。请注意，如果将值设置得太低，可能会导致频繁超时；如果将值设置得太高，可能会延迟故障检测。

步骤

- 1 导航到 **安全 > 设置 > 安全配置文件 > 会话定时器**。
- 2 单击**添加配置文件**。
此时将显示**配置文件**屏幕，并将填充默认值。
- 3 输入定时器配置文件的**名称**和**描述**（可选）。
- 4 单击**设置**以选择要应用定时器配置文件的 Tier-0 或 Tier-1 网关或组。
- 5 选择协议。接受默认值或输入您自己的值。

TCP 变量	说明
First Packet	发送第一个数据包之后连接的超时值。默认为 120 秒。
Opening	传输第二个数据包之后连接的超时值。默认为 30 秒。
Established	完全建立连接之后连接的超时值。
CLOSING	发送第一个 FIN 之后连接的超时值。默认为 120 秒。
FIN WAIT	交换 FIN 并且连接已关闭之后，连接的超时值。默认为 45 秒。
CLOSED	一个端点发送 RST 之后，连接的超时值。默认为 20 秒。

UDP 变量	说明
First Packet	发送第一个数据包之后连接的超时值。这是新 UDP 流的初始超时。默认为 60 秒。
SINGLE	源主机发送多个数据包，而目标主机没有发送回数据包时连接的超时值。默认为 30 秒。
MULTIPLE	两个主机都发送了数据包时连接的超时值。默认为 60 秒。
ICMP 变量	说明
First Packet	发送第一个数据包之后连接的超时值。这是新 ICMP 流量的初始超时。默认为 20 秒。
错误回复	为响应 ICMP 数据包而返回 ICMP 错误之后连接的超时值。默认为 10 秒。

6 单击保存。

后续步骤

保存后，单击[管理组到配置文件的优先级](#)，以管理组到配置文件的绑定优先级。

默认会话定时器值

会话定时器配置文件会将超时值应用于 Tier-0 或 Tier-1 路由器接口或者包含分段的组。超时值可决定协议会话在关闭后保持活动状态的时长。

会话定时器值

- 使用 API 和 UI 显示的默认定时器配置文件仅应用于分布式防火墙 (DFW)。
- 网关防火墙 (Gateway Firewall, GFW) 默认会话定时器与使用 API 和 UI 时看到的默认配置文件定时器不同。GFW 默认会话定时器针对南北向流量进行了优化，默认情况下，该定时器较低。
- 可以使用 API 和 UI 更改 DFW 和 GFW 的防火墙会话定时器。
- 如果需要，可以将相同的非默认定时器配置文件应用于 DFW 和 GFW。

如果未自定义定时器值，则网关将采用默认值。网关防火墙默认定时器值：

定时器属性	Edge 默认值（秒）	最小值（秒）	最大值（秒）
ICMP Error Reply	6	10	4320000
ICMP First Packet	6	10	4320000
TCP Closed	2	10	4320000
TCP Closing	900	10	4320000
TCP Established	7200	120	4320000
TCP Fin-wait	4	10	4320000
TCP First Packet	120	10	4320000
TCP Opening	30	10	4320000
UDP First Packet	30	10	4320000

定时器属性	Edge 默认值 (秒)	最小值 (秒)	最大值 (秒)
UDP Multiple	30	10	4320000
UDP Single	30	10	4320000

分布式防火墙默认会话定时器值：

定时器属性	DFW 默认值 (秒)	最小值 (秒)	最大值 (秒)
ICMP Error Reply	10	10	4320000
ICMP First Packet	20	10	4320000
TCP Closed	20	10	4320000
TCP Closing	120	10	4320000
TCP Established	43200	120	4320000
TCP Fin-wait	45	10	4320000
TCP First Packet	120	10	4320000
TCP Opening	30	10	4320000
UDP First Packet	60	10	4320000
UDP Multiple	60	10	4320000
UDP Single	30	10	4320000

泛洪保护

泛洪保护有助于防御“拒绝服务”(Denial of Service, DDoS) 攻击。

DDoS 攻击的目的在于向服务器发送大量请求以消耗服务器的所有可用资源，进而使合法流量无法访问服务器。创建泛洪保护配置文件可对 ICMP、UDP 和半开放式 TCP 流量施加活动会话数量限制。分布式防火墙可以缓存处于 SYN_SENT 和 SYN_RECEIVED 状态的流量条目，并在从启动器收到 ACK 后将每个条目升级到 TCP 状态，从而完成三向握手。

步骤

- 1 导航到 **安全 > 安全配置文件 > 泛洪保护**。
- 2 单击 **添加配置文件**，然后选择 **添加 Edge 网关配置文件** 或 **添加防火墙配置文件**。

3 填写泛洪保护配置文件参数：

表 10-15. 防火墙配置文件和 Edge 网关配置文件的参数

参数	最小值和最大值	默认	
TCP 半开连接限制 - 通过限制防火墙允许的处于活动状态但未完全建立的 TCP 流量数量来防止 TCP SYN 泛洪攻击。	1-1,000,000	防火墙 - 无 Edge 网关 - 1,000,000	设置此文本框以限制活动的 TCP 半打开连接数量。如果此文本框为空，则将在 ESX 节点上禁用此限制，并将其设置为 Edge 网关的默认值。
UDP 活动流限制 - 通过限制防火墙允许的活动的 UDP 流量数量来防止 UDP 泛洪攻击。达到设置的 UDP 流限制后，则会丢弃后面的可建立新流量的 UDP 数据包。	1-1,000,000	防火墙 - 无 Edge 网关 - 1,000,000	设置此文本框以限制活动的 UDP 连接数量。如果此文本框为空，则将在 ESX 节点上禁用此限制，并将其设置为 Edge 网关的默认值。
ICMP 活动流限制 - 通过限制防火墙允许的活动的 ICMP 流量数量来防止 ICMP 泛洪攻击。达到设置的流限制后，则会丢弃后面的可建立新流量的 ICMP 数据包。	1-1,000,000	防火墙 - 无 Edge 网关 - 10,000	设置此文本框以限制活动的 ICMP 打开连接数量。如果此文本框为空，则将在 ESX 节点上禁用此限制，并将其设置为 Edge 网关的默认值。
其他活动连接限制	1-1,000,000	防火墙 - 无 Edge 网关 - 10,000	设置此文本框以限制除 ICMP、TCP 和 UDP 半打开连接之外的其他活动连接的数量。如果此文本框为空，则将在 ESX 节点上禁用此限制，并将其设置为 Edge 网关的默认值。
SYN 缓存 - 在已同时配置 TCP 半开连接限制的情况下使用 SYN 缓存。可通过维护未完全建立的 TCP 会话的 SYN 缓存来强制限制活动的半打开连接数量。此缓存用于维护处于 SYN_SENT 和 SYN_RECEIVED 状态的流量条目。从启动器收到 ACK 后，会将每个 SYN 缓存条目升级为完整的 TCP 状态条目，从而完成三向握手。		仅适用于防火墙配置文件。	可打开和关闭。仅当配置了 TCP 半开连接限制时，启用 SYN 缓存才有效。
RST 欺骗 - 从 SYN 缓存清除半打开状态时，生成到服务器的欺骗性 RST。允许服务器清理与 SYN 泛洪相关联的状态（半打开状态）。		仅适用于防火墙配置文件。	可打开和关闭。必须选择“SYN 缓存”此选项才可用，

4 要将配置文件应用到 Edge 网关和防火墙组，请单击**设置**。

5 单击**保存**。

后续步骤

保存后，单击[管理组到配置文件的优先级](#)，以管理组到配置文件的绑定优先级。

配置 DNS 安全配置文件

创建 DNS 安全配置文件有助于防御与 DNS 相关的攻击。

在设置 DNS 安全配置文件后，您可以执行以下操作：

- 侦听传输节点上一个或一组虚拟机的 DNS 响应，以将 FQDN 与 IP 地址相关联。
- 添加全局和默认 DNS 服务器信息，并将其应用于使用 DFW 规则的所有虚拟机。
- 为所选虚拟机指定选定的 DNS 服务器信息。
- 将 DNS 配置文件应用于组。

注 当前版本仅支持 ESXi。

步骤

- 1 导航到 **安全 > 设置 > 安全配置文件 > DNS 安全**。
- 2 单击**添加配置文件**。
- 3 输入以下值：

选项	说明
配置文件名称	提供配置文件名称。
TTL	<p>此字段可捕获 DNS 缓存条目的活动时间（以秒为单位）。您可以选择以下选项：</p> <p>TTL 0 - 缓存条目永不过期。</p> <p>TTL 1 至 3599 - 无效</p> <p>TTL 3600 至 864000 - 有效</p> <p>TTL 留空 - 在 DNS 响应数据包中设置的自动 TTL。</p> <p>注 DNS 安全配置文件的默认 DNS 缓存超时为 24 小时。</p>
应用对象	<p>您可以根据任意条件选择要将 DNS 安全配置文件应用到的组。</p> <p>注 对一个虚拟机，只会应用一个 DNS 服务器配置文件。</p>
标记	<p>可选。为 DNS 配置文件分配标记和范围，以便于进行搜索。有关详细信息，请参见将标记添加到对象。</p>

- 4 单击**保存**。

后续步骤

保存后，单击[管理组到配置文件的优先级](#)，以管理组到配置文件的绑定优先级。

管理组到配置文件的优先级

您可以将多个组绑定到一个安全配置文件。NSX-T Data Center 将安全配置文件应用于优先级别最高的组。

如果将安全配置文件绑定到多个组，NSX-T Data Center 会将最高级别的优先级分配给该列表中的最新组。但是，您可以更改组的优先级。

要为组分配优先级，请执行以下操作：

前提条件

- 会话定时器组只能包含分段、分段端口和虚拟机作为成员。不支持其他类别类型。
- DNS 安全组只能包含虚拟机作为成员。不支持其他类别类型。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 导航到 **安全 > 安全配置文件**。
- 3 单击 **管理组到配置文件的优先级**。
- 4 要为组分配最高级别的优先级，请将其移动到列表的顶部。
- 5 单击 **关闭**。

结果

安全配置文件将应用于优先级最高的组。

您可以为 NSX-T Data Center 清单配置服务、组、上下文配置文件和虚拟机。

单击**清单**选项卡时，将显示清单对象的概述，其中会显示清单中的组、服务、虚拟机和上下文配置文件的数量。此外，还会显示有关组的以下信息：

- 已在策略中使用的组数
- 未在策略中使用的组数
- 具有成员的组数
- 没有成员的组数
- 身份组数
- 已在策略中使用的身份组数
- 未在策略中使用的身份组数

本章讨论了以下主题：

- [添加服务](#)
- [添加组](#)
- [添加上下文配置文件](#)

添加服务

可以配置服务并指定用于匹配网络流量的参数，例如，端口和协议对。

也可以使用服务在防火墙规则中允许或阻止某些类型的流量。创建服务后，无法更改类型。某些服务是预定义的，无法修改或删除。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**清单 > 服务**。
- 3 单击**添加新服务**。
- 4 输入名称。
- 5 单击**设置服务条目**。单击**添加新服务条目**。

6 对于新服务，请选择服务类型，并指定其他属性。

可用的类型包括 IP、IGMP、ICMPv4、ICMPv6、ALG、TCP、UDP 和以太网。

7 单击**保存**。

8 （可选）添加一个或多个标记。

9 （可选）输入说明。

10 单击**保存**。

添加组

组包括以静态和动态方式添加的不同对象，可用作防火墙规则的源和目标。

可以将组配置为包含虚拟机、IP 集、MAC 集、分段端口、分段、AD 用户组和其他组的组合。可以基于标记、虚拟机名称、操作系统名称或计算机名称动态包含组。无法在分布式防火墙规则的“应用对象”字段中使用基于动态或逻辑对象的组。

NSX 中的标记区分大小写，但是基于标记的组“不区分大小写”。例如，如果动态分组成员资格条件为 `vm Tag Equals 'quarantine'`，则该组将包括所有包含标记“quarantine”或“QUARANTINE”的虚拟机。

还可以从防火墙规则中排除任何组，并且列表中最多可以包含 100 个组。对于已经包含在防火墙排除列表中的组，不能包含 IP 集、MAC 集和 AD 组作为其成员。有关详细信息，请参见[管理防火墙排除列表](#)。

NSX Cloud 说明 如果使用的是 NSX Cloud，请参见[使用 NSX-T Data Center 和公有云标记对虚拟机分组](#)，以了解有关如何使用公有云标记对 NSX Manager 中的工作负载虚拟机进行分组的信息。

单个基于 ID 的组只能在分布式防火墙规则中用作源。如果在源中需要使用基于 IP 和基于 ID 的组，请创建两个单独的防火墙规则。

不能在**应用对象**文本框中使用仅包含 IP 地址的组、仅包含 MAC 地址的组或 Active Directory 组。

注 在 vCenter Server 中添加或移除主机时，主机上的虚拟机的外部 ID 将发生变化。如果虚拟机是一个组的静态成员，并且虚拟机的外部 ID 发生变化，则 NSX Manager UI 不再将虚拟机显示为该组的成员。不过，列出组的 API 仍显示该组包含虚拟机，并且虚拟机具有原始外部 ID。如果将虚拟机添加为一个组的静态成员，并且虚拟机的外部 ID 发生变化，您必须使用新的外部 ID 重新添加虚拟机。您也可以使用动态成员资格条件以避免该问题。

步骤

1 从导航面板中选择**清单 > 组**。

2 单击**添加组**。

3 输入组名称。

4 （可选）单击**设置成员**。

对于每个成员资格条件，最多可以指定五个规则，且这些规则可与逻辑 **AND** 运算符结合使用。可用成员条件可应用于以下各项：

- **分段端口** - 可指定标记和可选范围。
- **分段** - 可指定标记和可选范围。
- **虚拟机** - 可指定名称、标记、计算机操作系统名称或计算机名称（等于、包含、开头为、结尾为或不等于特定字符串）。
- **IP 集** - 可指定标记和可选范围。

5 （可选）单击**成员**以选择成员。

可用成员类型包括：

- **组**
- **分段**
- **分段端口**
- **虚拟网络接口**
- **虚拟机**

6 （可选）单击 **IP/MAC 地址** 以将 IP 和 MAC 地址添加为组成员。

支持 IPv4、IPv6 和多播地址。

7 （可选）单击 **AD 组** 以添加 Active Directory 组。可以在身份防火墙的分布式防火墙规则的源字段中使用具有 Active Directory 成员的组。组可以同时包含 AD 成员和计算成员。

8 （可选）输入说明和标记。

9 单击**应用**。

将列出组，并提供用于查看成员及组使用位置的选项。

添加上下文配置文件

通过上下文配置文件，可以创建属性键值对，例如第 7 层应用程序 ID 和域名。定义上下文配置文件之后，可将其用于一个或多个分布式防火墙规则和网关防火墙规则。

有两个属性可在上下文配置文件中使用的：应用程序 ID 和域名 (FQDN)。选择应用程序 ID 可以具有一个或多个子属性，如 TLS_Version 和 CIPHER_SUITE。可以在单个上下文配置文件中同时使用应用程序 ID 和域名。可以在同一个配置文件中多个应用程序 ID。可以使用一个具有子属性的应用程序 ID - 在单个配置文件中多个应用程序 ID 属性时，将清除子属性。

目前，支持预定义域列表。在添加属性类型域名 (FQDN) 的新上下文配置文件时，您可以看到 FQDN 列表。此外，您还可以通过运行 API 调用 `/policy/api/v1/infra/context-profiles/attributes?attribute_key=DOMAIN_NAME` 来查看 FQDN 列表。

注

- 网关防火墙规则不支持在上下文配置文件中 **使用 FQDN 属性或其他子属性**。
 - Tier-0 网关防火墙策略不支持上下文配置文件。网关防火墙规则不支持 **使用 FQDN 属性或其他子属性**。
-

步骤

- 1 选择**清单 > 上下文配置文件**。
- 2 单击**添加新的上下文配置文件**。
- 3 输入**配置文件名称**。
- 4 在“属性”列中，单击**设置**。
- 5 选择一个属性，或单击**添加属性**，然后选择 **应用程序 ID** 或**域名 (FQDN)**。
- 6 选择一个或多个属性。
- 7 （可选）如果选择了具有子属性（如 **SSL** 或 **CIFS**）的属性，请在“子属性/值”列中单击**设置**。
 - a 单击**添加子属性**，然后从下拉菜单中选择子属性类别。
 - b 选择一个或多个子属性。
 - c 单击**添加**。可以通过单击**添加子属性**添加其他子属性。
 - d 单击**应用**。
- 8 单击**添加**。
- 9 （可选）要添加其他类型的属性，请再次单击**添加属性**。
- 10 单击**应用**。
- 11 （可选）输入说明。
- 12 （可选）输入标记。
- 13 单击**保存**。

后续步骤

将此上下文配置文件应用于第 7 层分布式防火墙规则（适用于第 7 层或域名）或网关防火墙规则（适用于第 7 层）。

可以通过多种方式监控 NSX-T 环境及网络流量。

本章讨论了以下主题：

- 添加防火墙 IPFIX 配置文件
- 添加交换机 IPFIX 配置文件
- 添加 IPFIX 收集器
- 添加端口镜像配置文件
- 简单网络管理协议 (SNMP)
- 使用 vRealize Log Insight 监控系统
- 使用 vRealize Operations Manager 监控系统
- 使用 vRealize Network Insight Cloud 监控系统
- 高级监控工具

添加防火墙 IPFIX 配置文件

您可以为防火墙配置 IPFIX 配置文件。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**安全规划和故障排除 > IPFIX**。
- 3 单击**防火墙 IPFIX 配置文件**选项卡。
- 4 单击**添加防火墙 IPFIX 配置文件**。

5 填写以下详细信息。

设置	说明
名称和说明	输入名称和可选的说明。 注 如果要创建全局配置文件，请将配置文件命名为 Global 。无法从 UI 中编辑或删除全局配置文件，但可以使用 NSX-T Data Center API 执行此操作。
活动流导出超时 (分钟)	在这段时间过后，即使收到与流量关联的更多数据包，流量也会超时。默认值为 1。
观察域 ID	此参数标识网络流量所源自的观察域。默认值为 0，表示没有特定的观察域。
收集器配置	从下拉菜单中选择一个收集器。
应用对象	单击 设置 并选择要将筛选器应用到的组，或创建一个新组。
优先级	当多个配置文件适用时，此参数可解决冲突。IPFIX 导出程序仅使用具有最高优先级的配置文件。较低的值意味着更高的优先级。

6 单击 **保存**，然后单击 **是** 以继续配置配置文件。

7 单击 **保存**。

添加交换机 IPFIX 配置文件

您可以配置交换机（也称为分段）的 IPFIX 配置文件。

通过基于流量的网络监控，网络管理员可以深入了解通过网络的流量。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择 **安全规划和故障排除 > IPFIX**。
- 3 单击 **交换机 IPFIX 配置文件** 选项卡。
- 4 单击 **添加交换机 IPFIX 配置文件**。
- 5 输入以下详细信息：

设置	说明
名称和说明	输入名称和可选的说明。 注 如果要创建全局配置文件，请将配置文件命名为 Global 。无法从 UI 中编辑或删除全局配置文件，但可以使用 NSX-T Data Center API 执行此操作。
活动超时 (秒)	在这段时间过后，即使收到与流量关联的更多数据包，流量也会超时。默认值为 300。
空闲超时 (秒)	在这段时间过后，如果没有收到与流量关联的更多数据包，流量将会超时（仅限 ESXi，KVM 根据活动超时确定所有流量是否超时）。默认值为 300。
数据包采样概率 (%)	将采样的数据包比例（大致）。如果增加该设置，可能会影响 Hypervisor 和收集器的性能。如果所有 Hypervisor 将更多 IPFIX 数据包发送到收集器，收集器可能无法收集所有数据包。如果将概率设置为默认值 0.1%，则会将性能影响降到较低的程度。

设置	说明
收集器配置	从下拉菜单中选择一个收集器：
应用对象	选择类别：分段、分段端口或组。IPFIX 配置文件将应用于所选对象。
优先级	当多个配置文件适用时，此参数可解决冲突。IPFIX 导出程序仅使用具有最高优先级的配置文件。较低的值意味着更高的优先级。
最大流量	在网桥上缓存的最大流量数（仅限 KVM，无法在 ESXi 上配置）。默认值为 16384。
观察域 ID	观察域 ID 标识网络流量所源自的观察域。输入 0 表示没有特定的观察域。
导出覆盖网络流量	此参数定义是否对上行链路和隧道端口上的覆盖流量进行采样和导出。样本中将同时包含 vNIC 流量和覆盖流量。默认值为 已启用 。如果禁用，将仅对 vNIC 流量进行采样和导出。
标记	输入标记可使搜索变得更容易。

6 单击**保存**，然后单击**是**以继续配置配置文件。

7 单击**应用对象**以将配置文件应用于对象。

选择一个或多个对象。

8 单击**保存**。

添加 IPFIX 收集器

可以为防火墙和交换机配置 IPFIX 收集器。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**安全规划和故障排除 > IPFIX**。
- 3 单击**收集器**选项卡。
- 4 选择**添加新收集器 > IPFIX 交换机**或**添加新收集器 > IPFIX 防火墙**。
- 5 输入名称。
- 6 输入最多四个收集器的 IP 地址和端口。支持 IPv4 和 IPv6 地址。
- 7 单击**保存**。

添加端口镜像配置文件

可以为端口镜像会话配置端口镜像配置文件。

请注意，仅覆盖网络分段支持逻辑 SPAN，而 VLAN 分段则不支持。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**安全规划和故障排除 > 端口镜像**

- 3 选择**添加配置文件 > 远程 L3 SPAN** 或**添加配置文件 > 逻辑 SPAN**。
- 4 输入名称和可选的说明。
- 5 填写以下配置文件详细信息。

会话类型	参数
远程 L3 SPAN	<ul style="list-style-type: none"> ■ 方向 - 选择双向、输入或输出。 ■ 截断长度 - 指定要从数据包捕获的字节数。 ■ 封装类型 - 选择 GRE、ERSPAN II 或 ERSPAN III。 ■ GRE 密钥 - 如果封装类型为 GRE，则指定一个 GRE 密钥。 ■ ERSPAN ID - 如果封装类型为 ERSPAN II 或 ERSPAN III，则指定一个 ERSPAN ID。
逻辑 SPAN	<ul style="list-style-type: none"> ■ 方向 - 选择双向、输入或输出。 ■ 截断长度 - 指定要从数据包捕获的字节数。

- 6 单击**源**列中的**设置**以设置源。
 对于逻辑 SPAN，可用的源为**分段端口**、**虚拟机组**和**虚拟网络接口组**。
 对于远程 L3 SPAN，可用的源为**分段**、**分段端口**、**虚拟机组**和**虚拟网络接口组**。
- 7 单击**目标**列中的**设置**以设置目标。
- 8 单击**保存**。

简单网络管理协议 (SNMP)

您可以使用简单网络管理协议 (SNMP) 监控 NSX-T Data Center 组件。安装后，默认情况下不会启动 SNMP 服务。

步骤

- 1 登录到 NSX Manager CLI 或 NSX Edge CLI。
- 2 运行以下命令

- 对于 SNMPv1/SNMPv2:

```
set snmp community <community-string>
start service snmp
```

community-string 的字符数量上限为 64。

- 对于 SNMPv3

```
set snmp v3-users <user_name> auth-password <auth_password> priv-password
<priv_password>

start service snmp
```

user_name 的字符数量上限为 32。确保密码符合 PAM 限制条件。如果要更改默认引擎 ID，请使用以下命令：

```
set snmp v3-engine-id <v3-engine-id>

start service snmp
```

v3-engine-id 是一个长度为 10 到 64 个字符的十六进制字符串。

NSX-T Data Center 支持将 SHA1 和 AES128 用作身份验证和隐私协议。您还可以使用 API 调用来设置 SNMPv3。有关详细信息，请参阅《NSX-T Data Center API 指南》。

示例：

使用 vRealize Log Insight 监控系统

您可以使用 Log Insight NSX-T 内容包监控 NSX-T Data Center 环境。

此内容包中具有以下警示：

警示名称	说明
SysCpuUsage	CPU 使用率高于 95% 的时间超过 10 分钟。
SysMemUsage	内存使用率高于 95% 的时间超过 10 分钟。
SysDiskUsage	一个或多个分区的磁盘使用率高于 89% 的时间超过 10 分钟。
PasswordExpiry	设备用户帐户的密码即将过期或已过期。
CertificateExpiry	一个或多个 CA 签名证书已过期。
ClusterNodeStatus	本地 Edge 集群节点已关闭。
BackupFailure	NSX 计划的备份操作失败。
VipLeadership	NSX 管理集群 VIP 已关闭。
ApiRateLimit	客户端 API 已达到配置的阈值。
CorfuQuorumLost	集群中有两个节点已关闭，并丢失了 corfu 仲裁。
DfwHeapMem	DFW 堆内存已超出配置的阈值。
ProcessStatus	关键流程状态已更改。
ClusterFailoverStatus	SR 高可用性状态已更改或活动/备用服务进行故障切换。
DhcpPoolUsageOverloadedEvent	DHCP 池已达到配置的使用量阈值。
FabricCryptoStatus	由于未通过 Known_Answer_Tests (KAT)，Edge 加密 mux 驱动程序已关闭。
VpnTunnelState	VPN 隧道已关闭。
BfdTunnelStatus	BFD 隧道状态已更改。
RoutingBgpNeighborStatus	BGP 邻居处于关闭状态。
VpnL2SessionStatus	L2 VPN 会话已关闭。
VpnIkeSessionStatus	IKE 会话已关闭。

警示名称	说明
RoutingStatus	路由 (BGP/BFD) 已关闭。
DnsForwarderStatus	DNS 转发器运行状态为“已关闭”。
TnConnDown_15min	传输节点与控制器/管理器的连接已断开至少 15 分钟。
TnConnDown_5min	传输节点与控制器/管理器的连接已断开至少 5 分钟。
ServiceDown	一个或多个服务已关闭。
IpNotAvailableInPool	池中沒有可用的 IP 或已达到配置的阈值。
LoadBalancerError	NSX 负载均衡器服务处于错误状态
LoadBalancerDown	NSX 负载均衡器服务处于关闭状态
LoadBalancerVsDown	VS 状态：所有池成员均已关闭。
LoadBalancerPoolDown	池状态：所有池成员均已关闭。
ProcessCrash	进程或守护进程在数据路径或其他 LB 进程（如 Dispatcher 等）中崩溃。

使用 vRealize Operations Manager 监控系统

您可以使用 vRealize Operations Manager 监控 NSX-T Data Center 环境。

表 12-1. NSX-T 管理包中的警示

警示	说明	建议
NSX-T 管理服务失败	以下情况下触发：NSX-T Data Center 主机上的管理服务未运行。	请登录到 NSX-T Manager，然后重新启动失败的管理服务。
逻辑交换机的管理状态为未启动	以下情况下触发：逻辑交换机上禁用了管理状态。	请登录到 NSX-T，然后根据需 要启用管理状态。
Edge 节点控制器/管理器连接未启动	以下情况下触发：NSX-T Data Center 中的 Edge 节点连接状态为已断开。	请检查控制器集群和管理器集群的 Edge 节点连接状态，并修复已断开的连接。
Edge 主机节点处于失败/错误状态	以下情况下触发：由于以下原因之一，NSX-T Data Center 中的主机节点处于错误或失败状态： <ul style="list-style-type: none"> ■ Edge 配置错误 ■ 安装失败 ■ 卸载失败 ■ 升级失败 ■ 虚拟机部署失败 ■ 虚拟机关闭电源失败 ■ 虚拟机打开电源失败 ■ 虚拟机取消部署失败 	Edge 主机节点处于失败/错误状态，请检查主机节点状态并修复该问题。
BFD 服务已禁用	以下情况下触发：未在逻辑路由器上启用 BFD 服务。	即使配置了邻居，也未启用 Tier-0 路由器的 BFD 服务。如果需要，请启用 BFD 服务。
未配置 NAT 规则	以下情况下触发：未在逻辑路由器上配置 NAT 规则。	请登录到 NSX-T Manager，然后为逻辑路由器添加 NAT 规则。

表 12-1. NSX-T 管理包中的警示 （续）

警示	说明	建议
未配置静态路由	以下情况下触发：未在逻辑路由器上配置静态路由。	请登录到 NSX-T Manager ，如果需要，请为逻辑路由器添加静态路由。
路由通告服务已禁用	以下情况下触发：未在逻辑路由器上启用路由通告服务。	即使配置了路由通告，也未启用 Tier-1 路由器的路由通告服务，请登录到 NSX-T Manager 并启用该服务。
路由重新分发服务已禁用	以下情况下触发：未在逻辑路由器上启用路由重新分发服务。	即使配置了路由重新分发规则，也未启用 Tier-0 路由器的路由重新分发服务，请登录到 NSX-T Manager 并启用该服务。
已为逻辑路由器禁用 ECMP 服务	以下情况下触发：未在逻辑路由器上启用 ECMP 服务。	即使配置了邻居，也未启用 Tier-0 路由器的 BGP ECMP 服务，请登录到 NSX-T Manager 并启用该服务。
控制器节点连接已断开	以下情况下触发： NSX-T Data Center 中的控制器节点连接状态为已断开。	请登录到 NSX-T Manager ，检查控制器节点与管理节点和控制器集群的连接并解决断开连接状态。
部署的控制器节点少于 3 个	以下情况下触发： NSX-T Data Center 服务器的控制器节点少于三个。	在集群中部署至少 3 个控制器节点。
控制器集群状态不稳定	以下情况下触发： NSX-T Data Center 中的所有控制器节点都已关闭。	请检查控制器集群的状态。
管理状态不稳定	以下情况下触发：管理集群上的任一节点的状态均为已关闭。	请检查管理集群的状态。
文件系统使用率超过 85%	以下情况下触发：控制器虚拟机的客户机文件系统使用率超过 85%。	文件系统使用率超过 85%，请检查并清理文件系统以腾出更多空间。
文件系统使用率超过 75%	以下情况下触发：控制器虚拟机的客户机文件系统使用率超过 75%。	文件系统使用率超过 75%，请检查并清理文件系统以腾出更多空间。
文件系统使用率超过 70%	以下情况下触发：控制器虚拟机的客户机文件系统使用率超过 70%。	文件系统使用率超过 70%，请检查并清理文件系统以腾出更多空间。
Edge 集群的状态为已关闭	以下情况下触发： Edge 集群的状态为已关闭。	请检查 Edge 集群状态，如果需要，请按照 NSX-T 文档和 VMware 文档中建议的标准故障排除步骤进行操作。
逻辑交换机的状态为失败	以下情况下触发：逻辑交换机的状态为失败。	请检查逻辑交换机状态，如果需要，请按照 NSX-T 文档和 VMware 文档中建议的标准故障排除步骤进行操作。

表 12-1. NSX-T 管理包中的警示（续）

警示	说明	建议
负载均衡器服务的运行状态为已关闭	以下情况下触发：负载均衡器服务的运行状态为已关闭。	请检查负载均衡器服务的运行状态，如果需要，请按照 NSX-T 文档和 VMware 文档中建议的标准故障排除步骤进行操作。
负载均衡器服务的运行状态为错误	以下情况下触发：负载均衡器服务的运行状态包含错误。	请检查负载均衡器服务的运行状态，如果需要，请按照 NSX-T 文档和 VMware 文档中建议的标准故障排除步骤进行操作。
负载均衡器虚拟服务器的运行状态为已关闭	以下情况下触发：负载均衡器虚拟服务器的运行状态为已关闭。	请检查负载均衡器虚拟服务器的运行状态，如果需要，请按照 NSX-T 文档和 VMware 文档中建议的标准故障排除步骤进行操作。
负载均衡器虚拟服务器的运行状态为已分离	以下情况下触发：负载均衡器虚拟服务器的运行状态为已分离。	请检查负载均衡器虚拟服务器的运行状态，如果需要，请按照 NSX-T 文档和 VMware 文档中建议的标准故障排除步骤进行操作。
Edge 节点的配置状态为失败	以下情况下触发：Edge 节点的配置状态为失败。	请检查 Edge 节点的配置状态，如果需要，请按照 NSX-T 文档和 VMware 文档中建议的标准故障排除步骤进行操作。
管理服务的监控运行时状态为失败	以下情况下触发：管理服务的监控运行时状态停止运行。	请登录到 NSX-T Manager VA，然后重新启动失败的管理服务。
管理集群的管理状态不稳定	以下情况下触发：管理集群的管理状态不稳定。	请检查管理集群的状态。
部署的管理器节点少于 3 个	以下情况下触发：NSX-T 服务器部署的管理器节点少于三个。	在集群中部署至少 3 个管理器节点。
管理器节点连接已断开	以下情况下触发：管理器节点的管理器连接状态为已断开。	请登录到 NSX-T Manager，检查管理器节点的管理器连接，并按照 NSX-T 文档和 VMware 文档中建议的标准故障排除步骤进行操作。
管理器节点的文件系统使用率超过 85%	以下情况下触发：管理器节点的客户机文件系统使用率超过 85%。	文件系统使用率超过 85%，请检查并清理文件系统以腾出更多空间。
管理器节点的文件系统使用率超过 75%	以下情况下触发：管理器节点的客户机文件系统使用率超过 75%。	文件系统使用率超过 75%，请检查并清理文件系统以腾出更多空间。
管理器节点的文件系统使用率超过 70%	以下情况下触发：管理器节点的客户机文件系统使用率超过 70%。	文件系统使用率超过 70%，请检查并清理文件系统以腾出更多空间。

使用 vRealize Network Insight Cloud 监控系统

您可以使用 vRealize Network Insight Cloud 监控 NSX-T Data Center 环境。

表 12-2. 通过 vRealize Network Insight 计算的 NSX-T 事件

OID	事件名称	默认严重性	UI 名称	说明
1.3.6.1.4.1.6876.100.1.0.80205	NSXTNoUplinkConnectivityEvent	警告	“NSX-T Tier-1 逻辑路由器断开连接”事件	已从 Tier-O 路由器断开连接 NSX-T Tier-1 逻辑路由器。无法从外部访问此路由器下的网络，反之亦然。
1.3.6.1.4.1.6876.100.1.0.80206	NSXTRoutingAdvertisementEvent	警告	路由通告已禁用	已对 NSX-T Tier-1 逻辑路由器禁用路由通告。无法从外部访问此路由器下的网络。
1.3.6.1.4.1.6876.100.1.0.80207	NSXTManagerConnectivityDownEvent	严重	NSX-T Edge 节点未连接管理器	NSX-T Edge 节点已断开与管理器的连接。
1.3.6.1.4.1.6876.100.1.0.80208	NSXTControllerConnectivityDegradedEvent	警告	NSX-T Edge 节点的控制器连接已降级	NSX-T Edge 节点无法与一个或多个控制器通信。
1.3.6.1.4.1.6876.100.1.0.80209	NSXTControllerConnectivityDownEvent	严重	NSX-T Edge 节点未连接控制器	NSX-T Edge 节点无法与任何控制器通信。
1.3.6.1.4.1.6876.100.1.0.80210	NSXTMtumismatchEvent	警告	NSX-T Tier-0 与上行链路交换机/路由器之间的 MTU 不匹配	在 Tier-0 逻辑路由器的接口上配置的 MTU 与同一 L2 网络中上行链路交换机/路由器的接口不匹配。这可能会影响网络性能。
1.3.6.1.4.1.6876.100.1.0.80211	NSXTExcludedVmFlowEvent	信息	NSX-T DFW 防火墙中排除了一个或多个虚拟机。	一个或多个虚拟机未受到 NSX-T DFW 防火墙的保护。vRealize Network Insight 将不会收到这些虚拟机的 IPFIX 流。
1.3.6.1.4.1.6876.100.1.0.80212	NSXTDoubleVlanTaggingEvent	警告	上行链路 Vlan 配置错误	通信中断，因为 Tier 0 路由器上行链路端口上的 VLAN 与外部网关上的 VLAN 不同。
1.3.6.1.4.1.6876.100.1.0.80213	NSXTNoTzAttachedOnTnEvent	警告	传输节点上未连接任何传输区域。	没有任何传输区域连接到传输节点。由于此原因，虚拟机可能会断开连接。
1.3.6.1.4.1.6876.100.1.0.80214	NSXTVtepDeleteEvent	警告	传输节点上没有可用的 VTEP。	将从传输节点中删除所有 VTEP。由于此原因，虚拟机可能会断开连接。

表 12-2. 通过 vRealize Network Insight 计算的 NSX-T 事件（续）

OID	事件名称	默认严重性	UI 名称	说明
1.3.6.1.4.1.6876.100.1.0.80225	NSXTControllerNodeToControlClusterConnectivityEvent	严重	NSX-T Controller 节点没有控制集群连接	NSX-T Controller 节点已断开控制集群连接。
1.3.6.1.4.1.6876.100.1.0.80226	NSXTControllerNodeToMgmtPlaneConnectivityEvent	严重	NSX-T Controller 节点没有管理平面连接	NSX-T Controller 节点已断开管理平面连接。
1.3.6.1.4.1.6876.100.1.0.80227	NSXTMPNodeToMgmtClusterConnectivityEvent	严重	NSX-T 管理节点没有管理集群连接	NSX-T 管理节点已断开管理集群连接。
1.3.6.1.4.1.6876.100.1.0.80246	NSXTHostNodeMgmtConnectivityStatusDownEvent	警告	NSX-T 主机节点未连接管理器	NSX Manager 与主机传输节点的连接状态之间不同步
1.3.6.1.4.1.6876.100.1.0.80247	NSXTEdgeNodeCtrlConnectivityStatusUnknownEvent	严重	NSX-T Edge 节点的控制器连接处于“未知”状态。	NSX-T Edge 节点控制器连接处于“未知”状态。
1.3.6.1.4.1.6876.100.1.0.80248	NSXTHostNodeCtrlConnectivityStatusDownEvent	警告	NSX-T 主机节点未连接控制器	NSX-T 主机节点无法与任何控制器通信。
1.3.6.1.4.1.6876.100.1.0.80249	NSXTHostNodeCtrlConnectivityStatusDegradedEvent	警告	NSX-T 主机节点的控制器连接已降级	NSX-T 主机节点无法与一个或多个控制器通信。
1.3.6.1.4.1.6876.100.1.0.80250	NSXTHostNodeCtrlConnectivityStatusUnknownEvent	警告	NSX-T 主机节点的控制器连接处于“未知”状态。	NSX-T 主机节点控制器连接处于“未知”状态。
1.3.6.1.4.1.6876.100.1.0.80228	NSXTHostNodePnicStatusDownEvent	警告	NSX-T 主机传输节点 Pnic 状态为“关闭”。	NSX-T 主机传输节点 Pnic 状态为“关闭”。
1.3.6.1.4.1.6876.100.1.0.80229	NSXTHostNodePnicStatusDegradedEvent	警告	NSX-T 主机传输节点 Pnic 状态为“已降级”。	NSX-T 主机传输节点 Pnic 状态为“已降级”。
1.3.6.1.4.1.6876.100.1.0.80230	NSXTHostNodePnicStatusUnknownEvent	警告	NSX-T 主机传输节点 Pnic 状态为“未知”。	NSX-T 主机传输节点 Pnic 状态为“未知”。
1.3.6.1.4.1.6876.100.1.0.80237	NSXTEdgeNodePnicStatusDownEvent	严重	NSX-T Edge 传输节点 Pnic 状态为“关闭”。	NSX-T Edge 传输节点 Pnic 状态为“关闭”。
1.3.6.1.4.1.6876.100.1.0.80238	NSXTEdgeNodePnicStatusDegradedEvent	严重	NSX-T Edge 传输节点 Pnic 状态为“已降级”。	NSX-T Edge 传输节点 Pnic 状态为“已降级”。
1.3.6.1.4.1.6876.100.1.0.80239	NSXTEdgeNodePnicStatusUnknownEvent	严重	NSX-T Edge 传输节点 Pnic 状态为“未知”。	NSX-T Edge 传输节点 Pnic 状态为“未知”。
1.3.6.1.4.1.6876.100.1.0.80231	NSXTHostNodeTunnelStatusDownEvent	警告	NSX-T 主机传输节点隧道状态为“关闭”。	NSX-T 主机传输节点隧道状态为“关闭”。
1.3.6.1.4.1.6876.100.1.0.80232	NSXTHostNodeTunnelStatusDegradedEvent	警告	NSX-T 主机传输节点隧道状态为“已降级”。	NSX-T 主机传输节点隧道状态为“已降级”。

表 12-2. 通过 vRealize Network Insight 计算的 NSX-T 事件（续）

OID	事件名称	默认严重性	UI 名称	说明
1.3.6.1.4.1.6876.100.1.0.80233	NSXTHostNodeTunnelStatusUnknownEvent	警告	NSX-T 主机传输节点隧道状态为“未知”。	NSX-T 主机传输节点隧道状态为“未知”。
1.3.6.1.4.1.6876.100.1.0.80240	NSXTEdgeNodeTunnelStatusDownEvent	严重	NSX-T Edge 传输节点隧道状态为“关闭”。	NSX-T Edge 传输节点隧道状态为“关闭”。
1.3.6.1.4.1.6876.100.1.0.80241	NSXTEdgeNodeTunnelStatusDegradeEvent	严重	NSX-T Edge 传输节点隧道状态为“已降级”。	NSX-T Edge 传输节点隧道状态为“已降级”。
1.3.6.1.4.1.6876.100.1.0.80242	NSXTEdgeNodeTunnelStatusUnknownEvent	严重	NSX-T Edge 传输节点隧道状态为“未知”。	NSX-T Edge 传输节点隧道状态为“未知”。
1.3.6.1.4.1.6876.100.1.0.80234	NSXTHostNodeStatusDownEvent	警告	NSX-T 主机传输节点状态为“关闭”。	NSX-T 主机传输节点状态为“关闭”。
1.3.6.1.4.1.6876.100.1.0.80235	NSXTHostNodeStatusDegradedEvent	警告	NSX-T 主机传输节点状态为“已降级”。	NSX-T 主机传输节点状态为“已降级”。
1.3.6.1.4.1.6876.100.1.0.80236	NSXTHostNodeStatusUnknownEvent	警告	NSX-T 主机传输节点状态为“未知”。	NSX-T 主机传输节点状态为“未知”。
1.3.6.1.4.1.6876.100.1.0.80243	NSXTEdgeNodeStatusDownEvent	严重	NSX-T Edge 传输节点状态为“关闭”。	NSX-T Edge 传输节点状态为“关闭”。
1.3.6.1.4.1.6876.100.1.0.80244	NSXTEdgeNodeStatusDegradedEvent	严重	NSX-T Edge 传输节点状态为“已降级”。	NSX-T Edge 传输节点状态为“已降级”。
1.3.6.1.4.1.6876.100.1.0.80245	NSXTEdgeNodeStatusUnknownEvent	严重	NSX-T Edge 传输节点状态为“未知”。	NSX-T Edge 传输节点状态为“未知”。
1.3.6.1.4.1.6876.100.1.0.80252	NSXTLogicalSwitchAdminStatusDownEvent	警告	NSX-T 逻辑交换机管理状态为“关闭”	NSX-T 逻辑交换机管理状态为“关闭”
1.3.6.1.4.1.6876.100.1.0.80253	NSXTLogicalPortOperationalStatusDownEvent	严重	NSX-T 逻辑端口运行状态为“关闭”	NSX-T 逻辑端口运行状态为“关闭”。此状态可能会导致连接到同一逻辑交换机的两个虚拟接口 (VIF) 之间出现通信故障，例如，无法从一个虚拟机 ping 另一个虚拟机。
1.3.6.1.4.1.6876.100.1.0.80254	NSXTLogicalPortOperationalStatusUnknownEvent	警告	NSX-T 逻辑端口运行状态为“未知”	NSX-T 逻辑端口运行状态为“未知”。此状态可能会导致连接到同一逻辑交换机的两个虚拟接口 (VIF) 之间出现通信故障，例如，无法从一个虚拟机 ping 另一个虚拟机。

表 12-2. 通过 vRealize Network Insight 计算的 NSX-T 事件（续）

OID	事件名称	默认严重性	UI 名称	说明
1.3.6.1.4.1.6876.100.1.0.80255	NSXTComputeManagerConnectionStatusNotUpEvent	警告	NSX-T 计算管理器连接状态为“未启动”	NSX-T 计算管理器连接状态为“未启动”
1.3.6.1.4.1.6876.100.1.0.80256	NSXTClusterBackUpDisabledEvent	警告	未调度 NSX-T Manager 备份。	未调度 NSX-T Manager 备份
1.3.6.1.4.1.6876.100.1.0.80257	NSXTDFWFirewallDisabledEvent	严重	NSX-T DFW 防火墙已禁用。	NSX-T Manager 中已禁用分布式防火墙
1.3.6.1.4.1.6876.100.1.0.80258	NSXTLogicalPortReceivedPacketDropEvent	警告	NSX-T 逻辑端口接收的数据包将被丢弃。	NSX-T 逻辑端口上接收的数据包将被丢弃，关联实体可能会受到影响
1.3.6.1.4.1.6876.100.1.0.80259	NSXTLogicalPortTransmittedPacketDropEvent	警告	NSX-T 逻辑端口传输的数据包将被丢弃。	NSX-T 逻辑端口上传输的数据包将被丢弃，关联实体可能会受到影响
1.3.6.1.4.1.6876.100.1.0.80260	NSXTLogicalSwitchReceivedPacketDropEvent	警告	NSX-T 逻辑交换机接收的数据包将被丢弃	NSX-T 逻辑交换机上接收的数据包将被丢弃，关联实体可能会受到影响
1.3.6.1.4.1.6876.100.1.0.80261	NSXTLogicalSwitchTransmittedPacketDropEvent	警告	NSX-T 逻辑交换机传输的数据包将被丢弃	NSX-T 逻辑交换机上传输的数据包将被丢弃，关联实体可能会受到影响
1.3.6.1.4.1.6876.100.1.0.80262	NSXTRxPacketDropOnMPNicEvent	警告	NSX-T 管理节点的网络接口上接收的数据包将被丢弃	NSX-T 管理节点的网络接口上接收的数据包将被丢弃。这可能会影响与 NSX-T 管理集群相关的网络流量。
1.3.6.1.4.1.6876.100.1.0.80263	NSXTRxPacketDropOnEdgeTnNicEvent	严重	NSX-T Edge 节点的网络接口上接收的数据包将被丢弃	NSX-T Edge 节点的网络接口上接收的数据包将被丢弃。这可能会影响 Edge 集群的网络流量。
1.3.6.1.4.1.6876.100.1.0.80264	NSXTRxPacketDropOnHostTnNicEvent	警告	NSX-T 主机节点的网络接口上接收的数据包将被丢弃	NSX-T 主机节点的网络接口上接收的数据包将被丢弃。这可能会影响 ESXi 主机上的网络流量。
1.3.6.1.4.1.6876.100.1.0.80265	NSXTTxPacketDropOnMPNicEvent	警告	NSX-T 管理节点的网络接口上传输的数据包将被丢弃	NSX-T 管理节点的网络接口上传输的数据包将被丢弃。这可能会影响与 NSX-T 管理集群相关的网络流量。

表 12-2. 通过 vRealize Network Insight 计算的 NSX-T 事件（续）

OID	事件名称	默认严重性	UI 名称	说明
1.3.6.1.4.1.6876.100.1.0.80266	NSXTTxPacketDropOnEdgeTnNicEvent	严重	NSX-T Edge 节点的网络接口上传输的数据包将被丢弃	NSX-T Edge 节点的网络接口上传输的数据包将被丢弃。这可能会影响 Edge 集群的网络流量。
1.3.6.1.4.1.6876.100.1.0.80267	NSXTTxPacketDropOnHostTnNicEvent	警告	NSX-T 主机节点的网络接口上传输的数据包将被丢弃	NSX-T 主机节点的网络接口上传输的数据包将被丢弃。这可能会影响 ESXi 主机上的网络流量。
1.3.6.1.4.1.6876.100.1.0.80402	NSXTMPNodeServiceCmlInventoryStatusEvent	警告	CM 清单服务已停止运行	CM 清单服务状态变成“已停止”。
1.3.6.1.4.1.6876.100.1.0.80403	NSXTMPNodeServiceControllerStatusEvent	警告	控制器服务已停止运行。	控制器服务状态变成“已停止”。
1.3.6.1.4.1.6876.100.1.0.80404	NSXTMPNodeServiceDataStoreStatusEvent	警告	数据存储服务已停止运行。	数据存储服务状态变成“已停止”。
1.3.6.1.4.1.6876.100.1.0.80405	NSXTMPNodeServiceHttpStatusEvent	警告	HTTP 服务已停止运行。	HTTP 服务状态变成“已停止”。
1.3.6.1.4.1.6876.100.1.0.80406	NSXTMPNodeServiceInstallUpgradeEvent	警告	安装升级服务已停止运行。	安装升级服务状态变成“已停止”。
1.3.6.1.4.1.6876.100.1.0.80407	NSXTMPNodeServiceLiagentStatusEvent	警告	LI 代理服务已停止运行。	LI 代理服务状态变成“已停止”。
1.3.6.1.4.1.6876.100.1.0.80408	NSXTMPNodeServiceManagerStatusEvent	警告	Manager Service 已停止运行。	Manager Service 状态变成“已停止”。
1.3.6.1.4.1.6876.100.1.0.80409	NSXTMPNodeServiceMgmtPlaneBusStatusEvent	警告	管理平面服务已停止运行。	管理服务状态变成“已停止”。
1.3.6.1.4.1.6876.100.1.0.80410	NSXTMPNodeServiceMigrationCoordinatorStatusEvent	警告	迁移协调器服务已停止运行。	迁移协调器服务状态变成“已停止”。
1.3.6.1.4.1.6876.100.1.0.80411	NSXTMPNodeServiceNodeMgmtStatusEvent	警告	节点管理服务已停止运行。	节点管理服务状态变成“已停止”。
1.3.6.1.4.1.6876.100.1.0.80412	NSXTMPNodeServiceNodeStatsStatusEvent	警告	节点统计信息服务已停止运行。	节点统计信息服务状态变成“已停止”。
1.3.6.1.4.1.6876.100.1.0.80413	NSXTMPNodeServiceNSXMessageBusStatusEvent	警告	消息总线服务已停止运行。	消息总线客户端服务状态变成“已停止”。
1.3.6.1.4.1.6876.100.1.0.80414	NSXTMPNodeServiceNSXPlatformClientStatusEvent	警告	平台客户端服务已停止运行。	平台客户端服务状态变成“已停止”。

表 12-2. 通过 vRealize Network Insight 计算的 NSX-T 事件（续）

OID	事件名称	默认严重性	UI 名称	说明
1.3.6.1.4.1.6876.100.1.0.80415	NSXTMPNodeService NSXUpgradeAgentStatusEvent	警告	升级代理服务已停止运行。	升级服务状态变成“已停止”。
1.3.6.1.4.1.6876.100.1.0.80416	NSXTMPNodeService NTPStatusEvent	警告	NTP 服务已停止运行。	NTP 服务状态变成“已停止”。
1.3.6.1.4.1.6876.100.1.0.80417	NSXTMPNodeService PolicyStatusEvent	警告	策略服务已停止运行。	策略服务状态变成“已停止”。
1.3.6.1.4.1.6876.100.1.0.80418	NSXTMPNodeService SearchStatusEvent	警告	搜索服务已停止运行。	搜索服务状态变成“已停止”。
1.3.6.1.4.1.6876.100.1.0.80419	NSXTMPNodeService SNMPStatusEvent	警告	SNMP 服务已停止运行。	SNMP 服务状态变成“已停止”。
1.3.6.1.4.1.6876.100.1.0.80420	NSXTMPNodeService SSHStatusEvent	警告	SSH 服务已停止运行。	SSH 服务状态变成“已停止”。
1.3.6.1.4.1.6876.100.1.0.80421	NSXTMPNodeService SyslogStatusEvent	警告	Syslog 服务已停止运行。	Syslog 服务状态变成“已停止”。
1.3.6.1.4.1.6876.100.1.0.80422	NSXTMPNodeService TelemetryStatusEvent	警告	遥测服务已停止运行。	遥测服务状态变成“已停止”。
1.3.6.1.4.1.6876.100.1.0.80423	NSXTMPNodeService UIServiceStatusEvent	警告	UI 服务已停止运行。	UI 服务状态变成“已停止”。
1.3.6.1.4.1.6876.100.1.0.80402	NSXTMPNodeService CmlInventoryStatusEvent	严重	CM 清单服务已停止	NSX-T 管理节点的服务之一 (CM 清单服务) 已停止运行。
1.3.6.1.4.1.6876.100.1.0.80403	NSXTMPNodeService ControllerStatusEvent	严重	控制器服务已停止	NSX-T 管理节点的服务之一 (控制器服务) 已停止运行。
1.3.6.1.4.1.6876.100.1.0.80404	NSXTMPNodeService DataStoreStatusEvent	严重	数据存储服务已停止	NSX-T 管理节点的服务之一 (数据存储服务) 已停止运行。
1.3.6.1.4.1.6876.100.1.0.80405	NSXTMPNodeService HttpStatusEvent	严重	HTTP 服务已停止	NSX-T 管理节点的服务之一 (HTTP 服务) 已停止运行。
1.3.6.1.4.1.6876.100.1.0.80406	NSXTMPNodeService InstallUpgradeEvent	警告	安装升级服务已停止	NSX-T 管理节点的服务之一 (安装升级服务) 已停止运行。
1.3.6.1.4.1.6876.100.1.0.80407	NSXTMPNodeService LiagentStatusEvent	警告	LI 代理服务已停止	NSX-T 管理节点的服务之一 (LI 代理服务) 已停止运行。
1.3.6.1.4.1.6876.100.1.0.80408	NSXTMPNodeService ManagerStatusEvent	严重	Manager Service 已停止	NSX-T 管理节点的服务之一 (Manager Service) 已停止运行。

表 12-2. 通过 vRealize Network Insight 计算的 NSX-T 事件（续）

OID	事件名称	默认严重性	UI 名称	说明
1.3.6.1.4.1.6876.100.1.0.80409	NSXTMPNodeServiceMgmtPlaneBusStatusEvent	警告	管理平面服务已停止	NSX-T 管理节点的服务之一 (管理平面服务) 已停止运行。
1.3.6.1.4.1.6876.100.1.0.80410	NSXTMPNodeServiceMigrationCoordinatorStatusEvent	警告	迁移协调器服务已停止	NSX-T 管理节点的服务之一 (迁移协调器服务) 已停止运行。
1.3.6.1.4.1.6876.100.1.0.80411	NSXTMPNodeServiceNodeMgmtStatusEvent	严重	节点管理服务已停止	NSX-T 管理节点的服务之一 (节点管理服务) 已停止运行。
1.3.6.1.4.1.6876.100.1.0.80412	NSXTMPNodeServiceNodeStatsStatusEvent	严重	节点统计信息服务已停止	NSX-T 管理节点的服务之一 (节点统计信息服务) 已停止运行。
1.3.6.1.4.1.6876.100.1.0.80413	NSXTMPNodeServiceNSXMessageBusStatusEvent	警告	消息总线服务已停止	NSX-T 管理节点的服务之一 (消息总线服务) 已停止运行。
1.3.6.1.4.1.6876.100.1.0.80414	NSXTMPNodeServiceNSXPlatformClientStatusEvent	严重	平台客户端服务已停止	NSX-T 管理节点的服务之一 (平台客户端服务) 已停止运行。
1.3.6.1.4.1.6876.100.1.0.80415	NSXTMPNodeServiceNSXUpgradeAgentStatusEvent	警告	升级代理服务已停止	NSX-T 管理节点的服务之一 (升级代理服务) 已停止运行。
1.3.6.1.4.1.6876.100.1.0.80416	NSXTMPNodeServiceNTPStatusEvent	严重	NTP 服务已停止	NSX-T 管理节点的服务之一 (NTP 服务) 已停止运行。
1.3.6.1.4.1.6876.100.1.0.80417	NSXTMPNodeServicePolicyStatusEvent	严重	策略服务已停止	NSX-T 管理节点的服务之一 (策略服务) 已停止运行。
1.3.6.1.4.1.6876.100.1.0.80418	NSXTMPNodeServiceSearchStatusEvent	严重	搜索服务已停止	NSX-T 管理节点的服务之一 (搜索服务) 已停止运行。
1.3.6.1.4.1.6876.100.1.0.80419	NSXTMPNodeServiceSNMPStatusEvent	警告	SNMP 服务已停止	NSX-T 管理节点的服务之一 (SNMP 服务) 已停止运行。
1.3.6.1.4.1.6876.100.1.0.80420	NSXTMPNodeServiceSSHStatusEvent	严重	SSH 服务已停止	NSX-T 管理节点的服务之一 (SSH 服务) 已停止运行。
1.3.6.1.4.1.6876.100.1.0.80421	NSXTMPNodeServiceSyslogStatusEvent	严重	Syslog 服务已停止	NSX-T 管理节点的服务之一 (Syslog 服务) 已停止运行。
1.3.6.1.4.1.6876.100.1.0.80422	NSXTMPNodeServiceTelemetryStatusEvent	警告	遥测服务已停止	NSX-T 管理节点的服务之一 (遥测服务) 已停止运行。

表 12-2. 通过 vRealize Network Insight 计算的 NSX-T 事件（续）

OID	事件名称	默认严重性	UI 名称	说明
1.3.6.1.4.1.6876.100.1.0.80423	NSXTMPNodeService UIServiceStatusEvent	严重	UI 服务已停止	NSX-T 管理节点的服务之一 (UI 服务) 已停止运行。
1.3.6.1.4.1.6876.100.1.0.80424	NSXTMPNodeService ClusterManagerStatusEvent	严重	集群管理器服务已停止	NSX-T 管理节点的服务之一 (集群管理器服务) 已停止运行。

NSX-T 系统事件

以下是 vRealize Network Insight 中支持的 NSX-T 2.2-2.5 事件列表。所有这些 NSX-T 系统事件的对象 ID (Object ID, OID) 均为 1.3.6.1.4.1.6876.100.1.0.80203。

表 12-3. NSX-T 系统事件

事件名称	说明
vmwNSXPlatformSysCpuUsage	管理器和 Edge 设备上的 CPU 使用情况 (NSX-T 2.2)。
vmwNSXPlatformSysDiskUsage	管理器和 Edge 设备上 /var/log 分区的磁盘空间使用情况 (NSX-T 2.2)。
vmwNSXPlatformSysMemUsage	管理器和 Edge 设备上的内存使用情况 (NSX-T 2.2)。
vmwNSXPlatformSysConfigDiskUsage	管理器和 Edge 设备上 /config 分区的磁盘使用情况 (NSX-T 2.4)。
vmwNSXPlatformSysVarDumpDiskUsage	管理器和 Edge 设备上 /var/dump 分区的磁盘使用情况 (NSX-T 2.5)。
vmwNSXPlatformSysRepositoryDiskUsage	管理器和 Edge 设备上 /repository 分区的磁盘使用情况 (NSX-T 2.5)。
vmwNSXPlatformSysRootDiskUsage	管理器和 Edge 设备上根分区的磁盘使用情况 (NSX-T 2.5)。
vmwNSXPlatformSysTmpDiskUsage	管理器和 Edge 设备上 tmp 分区的磁盘使用情况 (NSX-T 2.5)。
vmwNSXPlatformSysImageDiskUsage	管理器和 Edge 设备上 /image 分区的磁盘使用情况 (NSX-T 2.5)。
vmwNSXDhcpPoolUsageOverloadedEvent	DHCP 池过载/正常 (NSX-T 2.5)。
vmwNSXDhcpPoolLeaseAllocationFailedEvent	DHCP 池租约分配失败/成功 (NSX-T 2.5)。
vmwNSXPlatformPasswordExpiryStatus	管理器密码过期 (NSX-T 2.4)。
vmwNSXPlatformCertificateExpiryStatus	管理器证书过期 (NSX-T 2.4)。
vmwNSXRoutingBgpNeighborStatus	BGP 邻居状态 (NSX-T 2.2)。
vmwNSXVpnTunnelState	VPN 隧道启动/关闭 (NSX-T 2.2)。
vmwNSXVpnL2TunnelStatus	L2 VPN 会话启动/关闭 (NSX-T 2.2)。

表 12-3. NSX-T 系统事件（续）

事件名称	说明
vmwNSXVpnIkeSessionStatus	IKE 会话启动/关闭 (NSX-T 2.2)。
vmwNSXDnsForwarderStatus	DNS 转发器状态 (NSX-T 2.4)。
vmwNSXClusterNodeStatus	集群节点状态 (NSX-T 2.4)。
vmwNSXFabricCryptoStatus	Edge 加密 mux 驱动程序未通过/通过 Known_Answer_Tests (KAT) (NSX-T 2.4)。
管理器磁盘利用率不正常	
BGP 邻居已关闭	BGP 邻居关闭时需要警示。
BGP 邻居已启动	邻居启动时清除警报。
存储使用情况超过 X	针对所有设备虚拟机 (MP、CCP) 或传输节点 (Edge、主机) 发出“存储超过 X - 事件”警报。
内存使用情况超过 X	针对所有设备虚拟机 (MP、CCP) 或传输节点 (Edge、主机) 发出“内存超过 X - 事件”警报。
CPU 使用情况超过 X	针对所有设备虚拟机 (MP、CCP) 或传输节点 (Edge、主机) 发出“CPU 超过 X - 事件”警报。

高级监控工具

NSX-T 支持高级监控方法，包括查看端口连接、跟踪流、端口镜像和活动监控等。

查看端口连接信息

您可以使用端口连接工具快速可视化两个虚拟机之间的连接和进行故障排除。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 从导航面板中选择**高级网络和安全 > 工具 > 端口连接**。
- 3 从**源虚拟机**下拉菜单中选择一个虚拟机。
- 4 从**目标虚拟机**下拉菜单中选择一个虚拟机。
- 5 单击**查看**。

将显示端口连接拓扑的可视图表。您可以单击可视输出中的任何组件以显示有关该组件的详细信息。

跟踪流

通过使用跟踪流，您可以将一个数据包注入网络，然后监控该数据包在网络中的传输情况。这样，您就可以监控网络，并找出瓶颈或中断等问题。

通过使用跟踪流，您可以确定数据包到达目标所经过的一个或多个路径，或者反过来沿这些路径查找丢弃数据包的位置。每个实体都会报告输入和输出上的数据包处理，因此您可以确定接收数据包或转发数据包时是否出现问题。

跟踪流与客户机虚拟机堆栈之间传输的 ping 请求/响应不同。跟踪流观察标记的数据包在通过覆盖网络时的情况，并监控每个数据包通过覆盖网络时的情况，直至其到达目标客户机虚拟机或 Edge 上行链路。请注意，绝不会将注入的标记的数据包实际传输到目标客户机虚拟机。

可以在传输节点上使用跟踪流，它支持 IPv4 和 IPv6 协议，其中包括：ICMP、TCP、UDP、DHCP、DNS 和 ARP/NDP。

您可以使用自定义标头字段和数据包大小构造数据包。跟踪流的源或目标可以是逻辑交换机端口、逻辑路由器上行链路端口、CSP 或 DHCP 端口。目标端点可以是 NSX 覆盖或底层中的任何设备。不过，您无法选择 NSX Edge 节点北面的目标。目标必须位于相同的子网上，或者必须能够通过 NSX 分布式逻辑路由器达到目标。

如果配置了 NSX 桥接，则包含未知目标 MAC 地址的数据包将始终发送到网桥。通常，网桥会将这些数据包转发到 VLAN 并将跟踪流数据包报告为“已传送”。报告为“已递送”的数据包不一定表示跟踪数据包已传送到指定的目标。

跟踪流观察可能包括广播的跟踪流数据包观察。如果不知道目标主机的 MAC 地址，ESXi 主机将广播跟踪流数据包。对于广播流量，源为虚拟机的 vNIC。广播流量的第 2 层目标 MAC 地址为 FF:FF:FF:FF:FF:FF。要为防火墙检测创建有效的数据包，广播跟踪流操作需要子网前缀长度。子网掩码使 NSX 可以计算数据包的 IP 网络地址。

使用跟踪流跟踪数据包路径

可使用跟踪流检查数据包的路径。跟踪流跟踪数据包的传输节点级别路径。跟踪数据包通过逻辑交换机覆盖网络，但对于连接到逻辑交换机的接口不可见。也就是说，不会将数据包实际传送到测试数据包的预期接收方。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**高级网络和安全 > 工具 > 跟踪流**。
- 3 选择 IPv4 或 IPv6 地址类型。
- 4 选择一种流量类型。

对于 IPv4 地址，流量类型选项为“单播”、“多播”和“广播”。对于 IPv6 地址，流量类型选项为“单播”或“多播”。

注意：VMware Cloud (VMC) 环境中不支持多播和广播。

5 根据流量类型，指定源和目标信息。

流量类型	源	目标
单播	<p>选择虚拟机或逻辑端口。对于虚拟机：</p> <ul style="list-style-type: none"> ■ 从下拉列表选择一个虚拟机。 ■ 选择虚拟接口。 ■ 如果在虚拟机中安装了 VMtools，或者使用 OpenStack 插件部署了虚拟机，则会显示 IP 地址和 MAC 地址（在这种情况下，将使用地址绑定）。如果虚拟机具有多个 IP 地址，请从下拉列表选择一个地址。 ■ 如果未显示 IP 地址和 MAC 地址，请在文本框中输入 IP 地址和 MAC 地址。 <p>对于逻辑端口：</p> <ul style="list-style-type: none"> ■ 选择连接类型：VIF、DHCP、Edge 上行链路或 Edge 集中式服务。 ■ 选择端口。 	<p>选择虚拟机、逻辑端口或 IP-MAC。对于虚拟机：</p> <ul style="list-style-type: none"> ■ 从下拉列表选择一个虚拟机。 ■ 选择虚拟接口。 ■ 如果在虚拟机中安装了 VMtools，或者使用 OpenStack 插件部署了虚拟机，则会显示 IP 地址和 MAC 地址（在这种情况下，将使用地址绑定）。如果虚拟机具有多个 IP 地址，请从下拉列表选择一个地址。 ■ 如果未显示 IP 地址和 MAC 地址，请在文本框中输入 IP 地址和 MAC 地址。 <p>对于逻辑端口：</p> <ul style="list-style-type: none"> ■ 选择连接类型：VIF、DHCP、Edge 上行链路或 Edge 集中式服务。 ■ 选择端口。 <p>对于 IP-MAC：</p> <ul style="list-style-type: none"> ■ 选择跟踪类型（第 2 层或第 3 层）。对于第 2 层，输入一个 IP 地址和 MAC 地址。对于第 3 层，输入一个 IP 地址。
多播	同上。	输入一个 IP 地址。它必须是 224.0.0.0-239.255.255.255 范围内的多播地址。
广播	同上。	输入一个子网前缀长度。

6 （可选）单击**高级**以查看高级选项。

7 （可选）在左侧的列中，输入以下字段所需的值或输入：

选项	说明
帧大小	默认值为 128。
TTL	默认值为 64。
超时 (毫秒)	默认值为 10000。
EtherType	默认值为 2048。
负载类型	选择 Base64、十六进制、纯文本、二进制或十进制 。
负载数据	根据所选类型设置负载格式。

8 （可选）选择一种协议并提供相关信息。

协议	参数
TCP	指定源端口、目标端口和 TCP 标记。
UDP	指定源端口和目标端口。
ICMPv6	指定 ICMP ID 和序列。

协议	参数
ICMP	指定 ICMP ID 和序列。
DHCPv6	选择 DHCP 消息类型： 要求、通告、请求或应答 。
DHCP	选择 DHCP OP 代码： 引导请求或引导应答 。
DNS	指定地址并选择消息类型： 查询或响应 。

9 单击跟踪。

将显示有关连接、组件和层的信息。如果选择单播和逻辑交换机作为目标，输出将包含一个表，其中列出了观察类型（已传送、已丢弃、已接收、已转发）、传输节点和组件以及拓扑图表。您可以为显示的观察应用一个筛选器（**全部、已传送、已丢弃**）。如果具有丢弃的观察，则默认应用**已丢弃**筛选器。否则，将应用**全部**筛选器。该图表显示了底板和路由器链接。请注意，不显示桥接信息。

监控端口镜像会话

您可以监控端口镜像会话以进行故障排除和用于其他用途。

请注意，仅覆盖网络逻辑交换机支持逻辑 SPAN，而 VLAN 逻辑交换机则不支持。

NSX Cloud 说明 如果使用 NSX Cloud，请参见 [NSX Cloud 支持的 NSX-T Data Center 功能](#) 以查看自动生成的逻辑实体、支持的功能以及 NSX Cloud 所需的配置的列表。

该功能具有以下限制：

- 源镜像端口不能位于多个镜像会话中。
- 通过使用 KVM，可以将多个网卡连接到同一 OVS 端口。镜像是在 OVS 上行链路端口上进行的，这意味着将镜像连接到 OVS 端口的所有 pNIC 上的流量。
- 对于本地 SPAN 会话，镜像会话源和目标端口必须位于同一主机 vSwitch 上。因此，如果通过 vMotion 将具有源或目标端口的虚拟机移到另一个主机，则无法再镜像该端口上的流量。
- 在 ESXi 上，如果在上行链路上启用了镜像，则 VDL2 使用 Geneve 协议将原始生产 TCP 数据包封装为 UDP 数据包。支持 TSO（TCP 分段卸载）的物理网卡可以更改这些数据包，并使用 MUST_TSO 标记来标记这些数据包。在具有 VMXNET3 或 E1000 vNIC 的监控虚拟机上，该驱动程序将数据包视为常规 UDP 数据包，而无法处理 MUST_TSO 标记并丢弃这些数据包。

如果将大量流量镜像到一个监控虚拟机，则驱动程序的缓冲区环可能会变满并丢弃数据包。为了缓解该问题，您可以采取下面的一个或多个措施：

- 增加接收缓冲区环大小。
- 为虚拟机分配更多 CPU 资源。

- 使用数据平面开发工具包 (Data Plane Development Kit, DPDK) 提高数据包处理性能。

注 确保监控虚拟机的 MTU 设置以及管理程序的虚拟网卡设备的 MTU 设置（对于 KVM）足够大以处理数据包。这对于封装的数据包特别重要，因为封装增加了数据包大小。否则，可能会丢弃数据包。具有 VMXNET3 网卡的 ESXi 虚拟机不会出现该问题，但 ESXi 和 KVM 虚拟机上的其他类型的网卡可能会出现该问题。

注 在涉及 KVM 主机上的虚拟机的 L3 端口镜像会话中，您必须设置足够大的 MTU 以处理封装所需的额外字节。镜像流量经由 OVS 接口和 OVS 上行链路。您必须将 OVS 接口的 MTU 设置为比原始数据包大小（在封装和镜像之前）至少大 100 字节。如果您看到丢弃的数据包，请增加主机的虚拟网卡和 OVS 接口的 MTU 设置。可以使用以下命令设置 OVS 接口的 MTU：

```
ovs-vsctl -- set interface <ovs_Interface> mtu_request=<MTU>
```

注 在监控虚拟机的逻辑端口以及虚拟机所在的主机的上行链路端口时，根据主机是 ESXi 还是 KVM，将会看到不同的行为。对于 ESXi，将使用相同的 VLAN ID 标记逻辑端口镜像数据包和上行链路镜像数据包，它们在监控虚拟机中显示为相同的数据包。对于 KVM，不使用 VLAN ID 标记逻辑端口镜像数据包，但标记上行链路镜像数据包，它们在监控虚拟机中显示为不同的数据包。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 3 选择**高级网络和安全 > 工具 > 端口镜像会话**。
- 4 单击**添加**并选择会话类型。
可用类型为**本地 SPAN**、**远程 SPAN**、**远程 L3 SPAN** 和**逻辑 SPAN**。
- 5 输入会话名称和可选描述。
- 6 提供其他参数。

会话类型	参数
本地 SPAN	<ul style="list-style-type: none"> ■ 传输节点 - 选择一个传输节点。 ■ 方向 - 选择双向、输入或输出。 ■ 数据包截断 - 选择一个数据包截断值。
远程 SPAN	<ul style="list-style-type: none"> ■ 会话类型 - 选择 RSPAN 源会话或 RSPAN 目标会话。 ■ 传输节点 - 选择一个传输节点。 ■ 方向 - 选择双向、输入或输出。 ■ 数据包截断 - 选择一个数据包截断值。 ■ 封装 VLAN ID - 指定一个封装 VLAN ID。 ■ 保留原始 VLAN - 选择是否保留原始 VLAN ID。

会话类型	参数
远程 L3 SPAN	<ul style="list-style-type: none"> ■ 封装 - 选择 GRE、ERSPAN II 或 ERSPAN III。 ■ GRE 密钥 - 如果封装为 GRE，则指定一个 GRE 密钥。ERSPAN ID - 如果封装为 ERSPAN II 或 ERSPAN III，则指定一个 ERSPAN ID。 ■ 方向 - 选择双向、输入或输出。 ■ 数据包截断 - 选择一个数据包截断值。
逻辑 SPAN	<ul style="list-style-type: none"> ■ 逻辑交换机 - 选择一个逻辑交换机。 ■ 方向 - 选择双向、输入或输出。 ■ 数据包截断 - 选择一个数据包截断值。

7 单击**下一步**。

8 提供源信息。

会话类型	参数
本地 SPAN	<ul style="list-style-type: none"> ■ 选择一个 N-VDS。 ■ 选择物理接口。 ■ 启用或禁用封装数据包。 ■ 选择虚拟机。 ■ 选择虚拟接口。
远程 SPAN	<ul style="list-style-type: none"> ■ 选择虚拟机。 ■ 选择虚拟接口。
远程 L3 SPAN	<ul style="list-style-type: none"> ■ 选择虚拟机。 ■ 选择虚拟接口。 ■ 选择逻辑交换机。
逻辑 SPAN	<ul style="list-style-type: none"> ■ 选择逻辑端口。

9 单击**下一步**。

10 提供目标信息。

会话类型	参数
本地 SPAN	<ul style="list-style-type: none"> ■ 选择虚拟机。 ■ 选择虚拟接口。
远程 SPAN	<ul style="list-style-type: none"> ■ 选择一个 N-VDS。 ■ 选择物理接口。
远程 L3 SPAN	<ul style="list-style-type: none"> ■ 指定一个 IPv4 地址。
逻辑 SPAN	<ul style="list-style-type: none"> ■ 选择逻辑端口。

11 单击**保存**。

保存端口镜像会话后，无法更改源或目标。

为端口镜像会话配置筛选器

您可以为端口镜像会话配置筛选器，以便限制镜像的数据量。

该功能具有以下功能和限制：

- 仅支持 ESXi 和 KVM 主机传输节点。
- 支持源和目标的 IP 地址、IP 前缀和 IP 范围。
- 不支持源或目标的 IPSet。
- 不支持 ESXi 或 KVM 上的镜像统计信息。

您必须使用 API 配置筛选器。不支持使用 NSX Manager UI。有关端口镜像 API 和 PortMirroringFilter 架构的详细信息，请参见《NSX-T Data Center API 参考》。

步骤

- 1 使用 NSX Manager UI 或 API 配置端口镜像会话。
- 2 调用 GET /api/v1/mirror-sessions API 以获取有关端口镜像会话的信息。
- 3 调用 GET /api/v1/mirror-sessions/<mirror-session-id> API 以添加一个或多个筛选器。例如，

```
PUT https://<nsx-mgr>/api/v1/mirror-sessions/e57e8b2d-3047-4550-b230-dd1ee0e10b49
{
  "resource_type": "PortMirroringSession",
  "id": "e57e8b2d-3047-4550-b230-dd1ee0e10b49",
  "display_name": "port-mirror-session-1",
  "description": "Pnic port mirror session 1",
  "mirror_sources": [
    {
      "resource_type": "LogicalPortMirrorSource",
      "port_ids": [
        "6a361832-43e4-430d-a48a-b84a6cba73c3"
      ]
    }
  ],
  "mirror_destination": {
    "resource_type": "LogicalPortMirrorDestination",
    "port_ids": [
      "3e42e8b2d-3047-4550-b230-dd1ee0e10b34"
    ]
  },
  "port_mirroring_filters": [
    {
      "filter_action": "MIRROR",
      "src_ips": {
        "ip-addresses": [
          "192.168.175.250",
          "2001:bd6::c:2957:160:126"
        ]
      },
      "dst_ips": {
```

```

        "ip-addresses": [
            "192.168.160.126",
            "2001:bd6::c:2957:175:250"
        ]
    }
}
"session_type": "LogicalPortMirrorSession",
"preserve_original_vlan": false,
"direction": "BIDIRECTIONAL",
"_revision": 0
}

```

- 4 （可选）您可以调用 `get mirroring-session <session-number>` CLI 命令以显示端口镜像会话的属性，包括筛选器。

配置 IPFIX

IPFIX（Internet 协议流量信息导出）是一个网络流量信息格式和导出标准。您可以为交换机和防火墙配置 IPFIX。对于交换机，将导出 VIF（虚拟接口）和 pNIC（物理网卡）中的网络流量。对于防火墙，将导出分布式防火墙组件管理的网络流量。

NSX Cloud 说明 如果使用 NSX Cloud，请参见 [NSX Cloud 支持的 NSX-T Data Center 功能](#) 以查看自动生成的逻辑实体、支持的功能以及 NSX Cloud 所需的配置的列表。

此功能符合 RFC 7011 和 RFC 7012 中指定的标准。

在启用 IPFIX 时，所有配置的主机传输节点使用端口 4739 将 IPFIX 消息发送到 IPFIX 收集器。对于 ESXi，NSX-T Data Center 自动打开端口 4739。对于 KVM，如果未启用防火墙，则会打开端口 4739，但如果启用了防火墙，您必须确保打开该端口，因为 NSX-T Data Center 不会自动打开该端口。

ESXi 和 KVM 上的 IPFIX 使用不同的方法对隧道数据包进行采样。在 ESXi 上，隧道数据包将采样为两个记录：

- 具有一些内部数据包信息的外部数据包记录
 - SrcAddr、DstAddr、SrcPort、DstPort 和 Protocol 指的是外部数据包。
 - 包含一些企业条目以描述内部数据包。
- 内部数据包记录
 - SrcAddr、DstAddr、SrcPort、DstPort 和 Protocol 指的是内部数据包。

在 KVM 上，隧道数据包将采样为一个记录：

- 具有一些外部隧道信息的内部数据包记录
 - SrcAddr、DstAddr、SrcPort、DstPort 和 Protocol 指的是内部数据包。
 - 包含一些企业条目以描述外部数据包。

配置交换机 IPFIX 收集器

您可以为交换机配置 IPFIX 收集器。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 选择 **高级网络和安全 > 工具 > IPFIX**
- 3 单击 **交换机 IPFIX 收集器** 选项卡。
- 4 单击 **添加** 以添加一个收集器。
- 5 输入名称和可选的说明。
- 6 单击 **添加**，然后输入收集器的 IP 地址和端口。
您最多可以添加 4 个收集器。
- 7 单击 **添加**。

配置交换机 IPFIX 配置文件

您可以为交换机配置 IPFIX 配置文件。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 选择 **高级网络和安全 > 工具 > IPFIX**
- 3 单击 **交换机 IPFIX 配置文件** 选项卡。
- 4 单击 **添加** 以添加一个配置文件。

设置	说明
名称和说明	输入名称和可选的说明。 注 如果要创建全局配置文件，请将配置文件命名为 Global 。无法从 UI 中编辑或删除全局配置文件，但可以使用 NSX-T Data Center API 执行此操作。
活动超时 (秒)	在这段时间过后，即使收到与流量关联的更多数据包，流量也会超时。默认值为 300。
空闲超时 (秒)	在这段时间过后，如果没有收到与流量关联的更多数据包，流量将会超时（仅限 ESXi，KVM 根据活动超时确定所有流量是否超时）。默认值为 300。
最大流量	在网桥上缓存的最大流量数（仅限 KVM，无法在 ESXi 上配置）。默认值为 16384。
导出覆盖网络流量	用于控制样本结果是否包含覆盖网络流量信息的设置。
采样概率 (%)	将采样的数据包比例（大致）。如果增加该设置，可能会影响管理程序和收集器的性能。如果所有管理程序将更多 IPFIX 数据包发送到收集器，收集器可能无法收集所有数据包。如果将概率设置为默认值 0.1%，则会将性能影响降到较低的程度。
观察域 ID	观察域 ID 标识网络流量所源自的观察域。输入 0 表示没有特定的观察域。

设置	说明
收集器配置文件	选择您在上一步中配置的交换机 IPFIX 收集器。
优先级	当多个配置文件适用时，此参数可解决冲突。IPFIX 导出程序仅使用具有最高优先级的配置文件。较低的值意味着更高的优先级。

5 单击添加。

配置防火墙 IPFIX 收集器

您可以为防火墙配置 IPFIX 收集器。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**高级网络和安全 > 工具 > IPFIX**
- 3 单击**防火墙 IPFIX 收集器**选项卡。
- 4 单击**添加**以添加一个收集器。
- 5 输入名称和可选的说明。
- 6 单击**添加**，然后输入收集器的 IP 地址和端口。
您最多可以添加 4 个收集器。
- 7 单击**添加**。

配置防火墙 IPFIX 配置文件

您可以为防火墙配置 IPFIX 配置文件。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**高级网络和安全 > 工具 > IPFIX**
- 3 单击**防火墙 IPFIX 配置文件**选项卡。
- 4 单击**添加**以添加一个配置文件。

设置	说明
名称和说明	输入名称和可选的说明。 注 如果要创建全局配置文件，请将配置文件命名为 Global 。无法从 UI 中编辑或删除全局配置文件，但可以使用 NSX-T Data Center API 执行此操作。
收集器配置	从下拉列表选择一个收集器。
活动流导出超时 (分钟)	在这段时间过后，即使收到与流量关联的更多数据包，流量也会超时。默认值为 1。

设置	说明
优先级	当多个配置文件适用时，此参数可解决冲突。 IPFIX 导出程序仅使用具有最高优先级的配置文件。较低的值意味着更高的优先级。
观察域 ID	此参数标识网络流量所源自的观察域。默认值为 0，表示没有特定的观察域。

5 单击添加。

ESXi IPFIX 模板

一个 ESXi 主机传输节点可支持八个逻辑交换机 IPFIX 流量模板和两个分布式防火墙 IPFIX 流量模板。

下表列出了逻辑交换机 IPFIX 数据包中的 VMware 特定的元素。

元素 ID	参数名称	数据类型	单元
880	tenantProtocol	unsigned8	1 个字节
881	tenantSourceIPv4	ipv4Address	4 个字节
882	tenantDestIPv4	ipv4Address	4 个字节
883	tenantSourceIPv6	ipv6Address	16 个字节
884	tenantDestIPv6	ipv6Address	16 个字节
886	tenantSourcePort	unsigned16	2 个字节
887	tenantDestPort	unsigned16	2 个字节
888	egressInterfaceAttr	unsigned16	2 个字节
889	vxlانExportRole	unsigned8	1 个字节
890	ingressInterfaceAttr	unsigned16	2 个字节
898	virtualObsID	string	可变长度

下表列出了分布式防火墙 IPFIX 数据包中的 VMware 特定的元素。

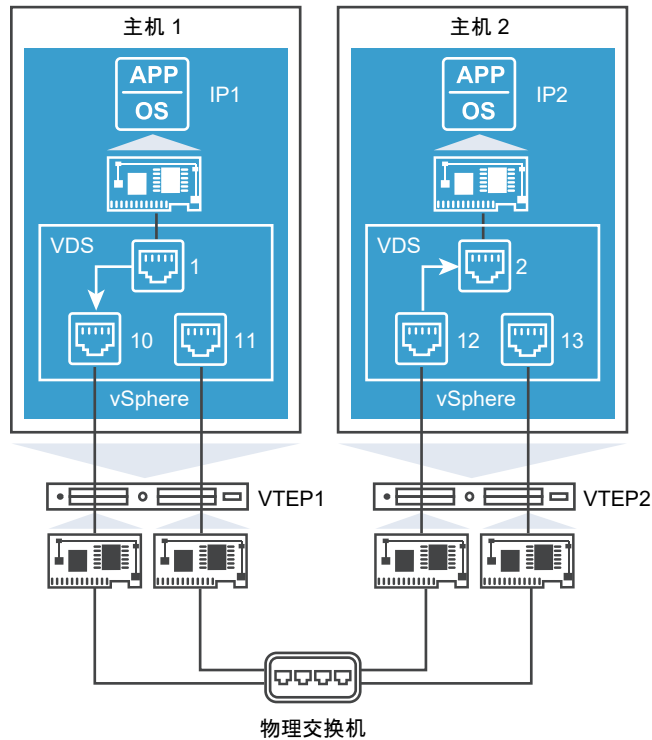
元素 ID	参数名称	数据类型	单元
950	ruleId	unsigned32	4 个字节
951	vmUuid	string	16 个字节
952	vnidIndex	unsigned32	4 个字节
953	sessionFlags	unsigned8	1 个字节
954	flowDirection	unsigned8	1 个字节
955	algControlFlowId	unsigned64	8 个字节
956	algType	unsigned8	1 个字节

元素 ID	参数名称	数据类型	单元
957	algFlowType	unsigned8	1 个字节
958	averageLatency	unsigned32	4 个字节
959	retransmissionCount	unsigned32	4 个字节
960	vifUuid	octetArray	16 个字节
961	vifId	string	可变长度

ESXi 逻辑交换机 IPFIX 模板

一个 ESXi 主机传输节点可支持八个逻辑交换机 IPFIX 流量模板。

下图显示了连接到 ESXi 主机的虚拟机之间受 IPFIX 功能监控的流量流：



IPv4 封装模板将具有以下元素：

- 标准元素
- SrcAddr: VTEP1
- DstAddr: VTEP2
- tenantSourceIPv4: IP1
- tenantDestIPv4: IP2
- tenantSourcePort: 10000

- tenantDestPort: 80
- tenantProtocol: TCP
- ingressInterfaceAttr: 0x03（隧道端口）
- egressInterfaceAttr: 0x01
- encapExportRole: 01
- virtualObsID: 89fd5032-2dc9-4fc3-993a-9bb4b616de54（逻辑端口 ID）

IPv4 模板

模板 ID: 256

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
// Specify the Interface port- Uplink Port, Access port,N.A
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()
```

IPv4 封装模板

模板 ID: 257

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4_ENCAP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
```

```

IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv4, 4)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestIPv4, 4)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourcePort, 2)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestPort, 2)
IPFIX_VMW_TEMPLATE_FIELD(tenantProtocol, 1)
// Specify the Interface port - Uplink Port, Access port, N.A
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
// TUNNEL-GW or no.
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_END()

```

IPv4 ICMP 模板

模板 ID: 258

```

IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4_ICMP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(encapId, 8)
// Specify the Interface port - Uplink Port, Access Port, or NA.
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 2)
IPFIX_TEMPLATE_END()

```

IPv4 ICMP 封装模板

模板 ID: 259

```

IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4_ICMP_ENCAP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)

```

```

IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv4, 4)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestIPv4, 4)
IPFIX_VMW_TEMPLATE_FIELD(tenantProtocol, 1)
// Specify the Interface port- Uplink Port, Access port,N.A
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
// TUNNEL-GW or no.
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()

```

IPv6 模板

模板 ID: 260

```

IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv6)
IPFIX_TEMPLATE_FIELD(sourceIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(destinationIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv6TOS,1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
// Specify the Interface port - Uplink Port, Access Port, or NA.
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()

```

IPv6 封装模板

模板 ID: 261

```

IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv6_ENCAP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv6TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
//ENCAP specific
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv6, 16)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestIPv6, 16)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourcePort, 2)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestPort, 2)
IPFIX_VMW_TEMPLATE_FIELD(tenantProtocol, 1)
// Specify the Interface port - Uplink Port, Access Port, or NA
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
// TUNNEL-GW or no.
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_END()

```

IPv6 ICMP 模板

模板 ID: 262

```

IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv6_ICMP)
IPFIX_TEMPLATE_FIELD(sourceIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(destinationIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(IPv6TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(encapId, 8)

```



```
// Specify the Interface port - Uplink Port, Access Port, or NA.
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 2)
IPFIX_TEMPLATE_END()
```

IPv6 ICMP 封装模板

模板 ID: 263

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv6_ICMP_ENCAP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_VMW_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_VMW_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(IPv6TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
//ENCAP Specific
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv6, 16)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestIPv6, 16)
IPFIX_VMW_TEMPLATE_FIELD(tenantProtocol, 1)
// Specify the Interface port - Uplink Port, Access Port, or NA
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
// TUNNEL-GW or no.
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()
```

ESXi 分布式防火墙 IPFIX 模板

ESXi 主机传输节点支持两个分布式防火墙 IPFIX 流量模板。

IPv4 模板

模板 ID: 288

```
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(icmpTypeIPv4, 1)
```

```

IPFIX_TEMPLATE_FIELD(icmpCodeIPv4,1)
IPFIX_TEMPLATE_FIELD(flowStartSeconds,4)
IPFIX_TEMPLATE_FIELD(flowEndSeconds,4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount,8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount,8)
IPFIX_TEMPLATE_FIELD(firewallEvent,1)
IPFIX_TEMPLATE_FIELD(direction,1)
IPFIX_TEMPLATE_FIELD(ruleId,4)
IPFIX_TEMPLATE_FIELD(vifUuid,16)
IPFIX_TEMPLATE_FIELD(sessionFlags,1)
IPFIX_TEMPLATE_FIELD(flowDirection,1)
IPFIX_TEMPLATE_FIELD(flowId,8)
IPFIX_TEMPLATE_FIELD(algControlFlowId,8)
IPFIX_TEMPLATE_FIELD(algType,1)
IPFIX_TEMPLATE_FIELD(algFlowType,1)
IPFIX_TEMPLATE_FIELD(averageLatency,4)
IPFIX_TEMPLATE_FIELD(retransmissionCount,4)

```

IPv6 模板

模板 ID: 289

```

IPFIX_TEMPLATE_FIELD(sourceIPv6Address,16)
IPFIX_TEMPLATE_FIELD(destinationIPv6Address,16)
IPFIX_TEMPLATE_FIELD(sourceTransportPort,2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort,2)
IPFIX_TEMPLATE_FIELD(protocolIdentifier,1)
IPFIX_TEMPLATE_FIELD(icmpTypeIPv6,1)
IPFIX_TEMPLATE_FIELD(icmpCodeIPv6,1)
IPFIX_TEMPLATE_FIELD(flowStartSeconds,4)
IPFIX_TEMPLATE_FIELD(flowEndSeconds,4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount,8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount,8)
IPFIX_TEMPLATE_FIELD(firewallEvent,1)
IPFIX_TEMPLATE_FIELD(direction,1)
IPFIX_TEMPLATE_FIELD(ruleId,4)
IPFIX_TEMPLATE_FIELD(vifUuid,16)
IPFIX_TEMPLATE_FIELD(sessionFlags,1)
IPFIX_TEMPLATE_FIELD(flowDirection,1)
IPFIX_TEMPLATE_FIELD(flowId,8)
IPFIX_TEMPLATE_FIELD(algControlFlowId,8)
IPFIX_TEMPLATE_FIELD(algType,1)
IPFIX_TEMPLATE_FIELD(algFlowType,1)
IPFIX_TEMPLATE_FIELD(averageLatency,4)
IPFIX_TEMPLATE_FIELD(retransmissionCount,4)

```

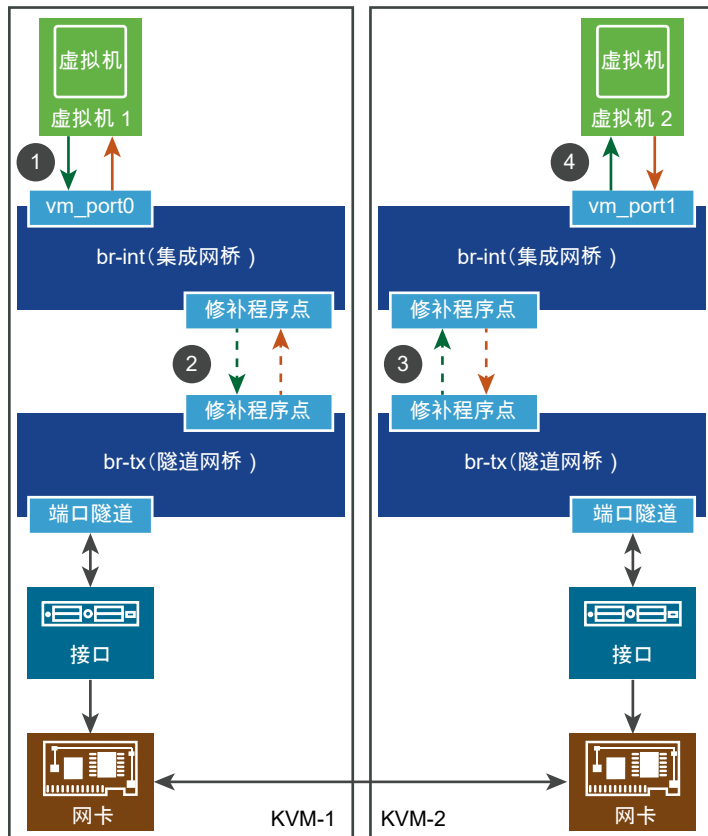
KVM IPFIX 模板

一个 KVM 主机传输节点支持 88 个 IPFIX 流量模板和 1 个选项模板。

下表列出了 KVM IPFIX 数据包中的 VMware 特定的元素。

元素 ID	参数名称	数据类型	单元
891	tunnelType	unsigned8	1 个字节
892	tunnelKey	字节数	可变长度
893	tunnelSourceIPv4Address	unsigned32	4 个字节
894	tunnelDestinationIPv4Address	unsigned32	4 个字节
895	tunnelProtocolIdentifier	unsigned8	1 个字节
896	tunnelSourceTransportPort	unsigned16	2 个字节
897	tunnelDestinationTransportPort	unsigned16	2 个字节
898	virtualObsID	string	可变长度

下图显示了连接到 KVM 主机的虚拟机之间受 IPFIX 功能监控的流量流：



KVM IPv4 IPFIX 输入模板将具有以下元素：

- 标准元素
- virtualObsID: 6d876a1c-e0ac-4bcf-85ee-bdd42fa7ba34 (逻辑端口 ID)

KVM 以太网 IPFIX 模板

有四个 KVM 以太网 IPFIX 模板：输入、输出、使用隧道的输入和使用隧道的输出。

以太网输入

模板 ID：256。字段计数：27。

字段包括：

- observationPointId（长度：4）
- DIRECTION（长度：1）
- SRC_MAC（长度：6）
- DESTINATION_MAC（长度：6）
- ethernetType（长度：2）
- ethernetHeaderLength（长度：1）
- INPUT_SNMP（长度：4）
- Unknown(368)（长度：4）
- IF_NAME（长度：变量）
- IF_DESC（长度：变量）
- 898（长度：变量，PEN：VMware Inc. (6876)）
- flowStartDeltaMicroseconds（长度：4）
- flowEndDeltaMicroseconds（长度：4）
- DROPPED_PACKETS（长度：8）
- DROPPED_PACKETS_TOTAL（长度：8）
- PKTS（长度：8）
- PACKETS_TOTAL（长度：8）
- Unknown(354)（长度：8）
- Unknown(355)（长度：8）
- Unknown(356)（长度：8）
- Unknown(357)（长度：8）
- Unknown(358)（长度：8）
- MUL_DPKTS（长度：8）
- postMCastPacketTotalCount（长度：8）
- Unknown(352)（长度：8）
- Unknown(353)（长度：8）

- flowEndReason (长度: 1)

以太网输出

模板 ID: 257。字段计数: 31。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- OUTPUT_SNMP (长度: 4)
- Unknown(369) (长度: 8)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)

- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)

使用隧道的以太网输入

模板 ID: 258。字段计数: 34。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)

- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)

使用隧道的以太网输出

模板 ID: 259。字段计数: 38。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- OUTPUT_SNMP (长度: 4)
- Unknown(369) (长度: 8)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))

- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)

KVM IPv4 IPFIX 模板

有四个 KVM IPv4 IPFIX 模板: 输入、输出、使用隧道的输入和使用隧道的输出。

IPv4 输入

模板 ID: 276。字段计数: 45。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)

- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)

- BYTES（长度：8）
- BYTES_TOTAL（长度：8）
- BYTES_SQUARED（长度：8）
- BYTES_SQUARED_PERMANENT（长度：8）
- IP_LENGTH_MINIMUM（长度：8）
- IP_LENGTH_MAXIMUM（长度：8）
- MUL_DOCTETS（长度：8）
- postMCastOctetTotalCount（长度：8）

IPv4 输出

模板 ID：277。字段计数：49。

字段包括：

- observationPointId（长度：4）
- DIRECTION（长度：1）
- SRC_MAC（长度：6）
- DESTINATION_MAC（长度：6）
- ethernetType（长度：2）
- ethernetHeaderLength（长度：1）
- INPUT_SNMP（长度：4）
- Unknown(368)（长度：4）
- IF_NAME（长度：变量）
- IF_DESC（长度：变量）
- OUTPUT_SNMP（长度：4）
- Unknown(369)（长度：4）
- IF_NAME（长度：变量）
- IF_DESC（长度：变量）
- IP_PROTOCOL_VERSION（长度：1）
- IP_TTL（长度：1）
- PROTOCOL（长度：1）
- IP_DSCP（长度：1）
- IP_PRECEDENCE（长度：1）
- IP_TOS（长度：1）

- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

使用隧道的 IPv4 输入

模板 ID: 278。字段计数: 52。

字段包括：

- observationPointId（长度：4）
- DIRECTION（长度：1）
- SRC_MAC（长度：6）
- DESTINATION_MAC（长度：6）
- ethernetType（长度：2）
- ethernetHeaderLength（长度：1）
- INPUT_SNMP（长度：4）
- Unknown(368)（长度：4）
- IF_NAME（长度：变量）
- IF_DESC（长度：变量）
- IP_PROTOCOL_VERSION（长度：1）
- IP_TTL（长度：1）
- PROTOCOL（长度：1）
- IP_DSCP（长度：1）
- IP_PRECEDENCE（长度：1）
- IP_TOS（长度：1）
- IP_SRC_ADDR（长度：4）
- IP_DST_ADDR（长度：4）
- 893（长度：4，PEN：VMware Inc. (6876)）
- 894（长度：4，PEN：VMware Inc. (6876)）
- 895（长度：1，PEN：VMware Inc. (6876)）
- 896（长度：2，PEN：VMware Inc. (6876)）
- 897（长度：2，PEN：VMware Inc. (6876)）
- 891（长度：1，PEN：VMware Inc. (6876)）
- 892（长度：变量，PEN：VMware Inc. (6876)）
- 898（长度：变量，PEN：VMware Inc. (6876)）
- flowStartDeltaMicroseconds（长度：4）
- flowEndDeltaMicroseconds（长度：4）
- DROPPED_PACKETS（长度：8）
- DROPPED_PACKETS_TOTAL（长度：8）

- PKTS（长度：8）
- PACKETS_TOTAL（长度：8）
- Unknown(354)（长度：8）
- Unknown(355)（长度：8）
- Unknown(356)（长度：8）
- Unknown(357)（长度：8）
- Unknown(358)（长度：8）
- MUL_DPKTS（长度：8）
- postMCastPacketTotalCount（长度：8）
- Unknown(352)（长度：8）
- Unknown(353)（长度：8）
- flowEndReason（长度：1）
- DROPPED_BYTES（长度：8）
- DROPPED_BYTES_TOTAL（长度：8）
- BYTES（长度：8）
- BYTES_TOTAL（长度：8）
- BYTES_SQUARED（长度：8）
- BYTES_SQUARED_PERMANENT（长度：8）
- IP_LENGTH_MINIMUM（长度：8）
- IP_LENGTH_MAXIMUM（长度：8）
- MUL_DOCTETS（长度：8）
- postMCastOctetTotalCount（长度：8）

使用隧道的 IPv4 输出

模板 ID：279。字段计数：56。

字段包括：

- observationPointId（长度：4）
- DIRECTION（长度：1）
- SRC_MAC（长度：6）
- DESTINATION_MAC（长度：6）
- ethernetType（长度：2）
- ethernetHeaderLength（长度：1）

- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- OUTPUT_SNMP (长度: 4)
- Unknown(369) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)

- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

KVM TCP over IPv4 IPFIX 模板

有四个 KVM TCP over IPv4 IPFIX 模板：输入、输出、使用隧道的输入和使用隧道的输出。

TCP over IPv4 输入

模板 ID: 280。字段计数: 53。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)

- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)

- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMcastOctetTotalCount (长度: 8)
- tcpAckTotalCount (长度: 8)
- tcpFinTotalCount (长度: 8)
- tcpPshTotalCount (长度: 8)
- tcpRstTotalCount (长度: 8)
- tcpSynTotalCount (长度: 8)
- tcpUrgTotalCount (长度: 8)

TCP over IPv4 输出

模板 ID: 281。字段计数: 57。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- OUTPUT_SNMP (长度: 4)
- Unknown(369) (长度: 4)
- IF_NAME (长度: 变量)

- IF_DESC (长度: 变量)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)

- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMcastOctetTotalCount (长度: 8)
- tcpAckTotalCount (长度: 8)
- tcpFinTotalCount (长度: 8)
- tcpPshTotalCount (长度: 8)
- tcpRstTotalCount (长度: 8)
- tcpSynTotalCount (长度: 8)
- tcpUrgTotalCount (长度: 8)

使用隧道的 TCP over IPv4 输入

模板 ID: 282。字段计数: 60。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)

- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)
- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMcastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)

- BYTES（长度：8）
- BYTES_TOTAL（长度：8）
- BYTES_SQUARED（长度：8）
- BYTES_SQUARED_PERMANENT（长度：8）
- IP_LENGTH_MINIMUM（长度：8）
- IP_LENGTH_MAXIMUM（长度：8）
- MUL_DOCTETS（长度：8）
- postMcastOctetTotalCount（长度：8）
- tcpAckTotalCount（长度：8）
- tcpFinTotalCount（长度：8）
- tcpPshTotalCount（长度：8）
- tcpRstTotalCount（长度：8）
- tcpSynTotalCount（长度：8）
- tcpUrgTotalCount（长度：8）

使用隧道的 TCP over IPv4 输出

模板 ID：283。字段计数：64。

字段包括：

- observationPointId（长度：4）
- DIRECTION（长度：1）
- SRC_MAC（长度：6）
- DESTINATION_MAC（长度：6）
- ethernetType（长度：2）
- ethernetHeaderLength（长度：1）
- INPUT_SNMP（长度：4）
- Unknown(368)（长度：4）
- IF_NAME（长度：变量）
- IF_DESC（长度：变量）
- OUTPUT_SNMP（长度：4）
- Unknown(369)（长度：4）
- IF_NAME（长度：变量）
- IF_DESC（长度：变量）

- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)
- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)

- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMcastOctetTotalCount (长度: 8)
- tcpAckTotalCount (长度: 8)
- tcpFinTotalCount (长度: 8)
- tcpPshTotalCount (长度: 8)
- tcpRstTotalCount (长度: 8)
- tcpSynTotalCount (长度: 8)
- tcpUrgTotalCount (长度: 8)

KVM UDP over IPv4 IPFIX 模板

有四个 KVM UDP over IPv4 IPFIX 模板: 输入、输出、使用隧道的输入和使用隧道的输出。

UDP over IPv4 输入

模板 ID: 284。字段计数: 47。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)

- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)

- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMcastOctetTotalCount (长度: 8)

UDP over IPv4 输出

模板 ID: 285。字段计数: 51。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- OUTPUT_SNMP (长度: 4)
- Unknown(369) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)

- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)

- postMCastOctetTotalCount (长度: 8)

使用隧道的 UDP over IPv4 输入

模板 ID: 286。字段计数: 54。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)
- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))

- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

使用隧道的 UDP over IPv4 输出

模板 ID: 287。字段计数: 58。

字段包括:

- observationPointId (长度: 4)

- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- OUTPUT_SNMP (长度: 4)
- Unknown(369) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)
- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))

- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP LENGTH MINIMUM (长度: 8)
- IP LENGTH MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

KVM SCTP over IPv4 IPFIX 模板

有四个 KVM SCTP over IPv4 IPFIX 模板: 输入、输出、使用隧道的输入和使用隧道的输出。

SCTP over IPv4 输入

模板 ID: 288。字段计数: 47。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)

- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

SCTP over IPv4 输出

模板 ID: 289。字段计数: 51。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- OUTPUT_SNMP (长度: 4)

- Unknown(369) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)

- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

使用隧道的 SCTP over IPv4 输入

模板 ID: 290。字段计数: 54。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- L4_SRC_PORT (长度: 2)

- L4_DST_PORT (长度: 2)
- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)

- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

使用隧道的 SCTP over IPv4 输出

模板 ID: 291。字段计数: 58。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- OUTPUT_SNMP (长度: 4)
- Unknown(369) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)

- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP LENGTH MINIMUM (长度: 8)

- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

KVM ICMPv4 IPFIX 模板

有四个 KVM ICMPv4 IPFIX 模板: 输入、输出、使用隧道的输入和使用隧道的输出。

ICMPv4 输入

模板 ID: 292。字段计数: 47。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- ICMP_IPv4_TYPE (长度: 1)
- ICMP_IPv4_CODE (长度: 1)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)

- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

ICMPv4 输出

模板 ID: 293。字段计数: 51。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)

- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- OUTPUT_SNMP (长度: 4)
- Unknown(369) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- ICMP_IPv4_TYPE (长度: 1)
- ICMP_IPv4_CODE (长度: 1)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)

- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMcastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMcastOctetTotalCount (长度: 8)

使用隧道的 ICMPv4 输入

模板 ID: 294。字段计数: 54。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)

- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- ICMP_IPv4_TYPE (长度: 1)
- ICMP_IPv4_CODE (长度: 1)
- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)

- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

使用隧道的 ICMPv4 输出

模板 ID: 295。字段计数: 58。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- OUTPUT_SNMP (长度: 4)
- Unknown(369) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)

- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- ICMP_IPv4_TYPE (长度: 1)
- ICMP_IPv4_CODE (长度: 1)
- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)

- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

KVM IPv6 IPFIX 模板

有四个 KVM IPv6 IPFIX 模板: 输入、输出、使用隧道的输入和使用隧道的输出。

IPv6 输入

模板 ID: 296。字段计数: 46。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)

- IPV6_SRC_ADDR (长度: 4)
- IPV6_DST_ADDR (长度: 4)
- FLOW_LABEL (长度: 4)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

IPv6 输出

模板 ID: 297。字段计数: 50。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- OUTPUT_SNMP (长度: 4)
- Unknown(369) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IPV6_SRC_ADDR (长度: 4)
- IPV6_DST_ADDR (长度: 4)
- FLOW_LABEL (长度: 4)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)

- PKTS（长度：8）
- PACKETS_TOTAL（长度：8）
- Unknown(354)（长度：8）
- Unknown(355)（长度：8）
- Unknown(356)（长度：8）
- Unknown(357)（长度：8）
- Unknown(358)（长度：8）
- MUL_DPKTS（长度：8）
- postMCastPacketTotalCount（长度：8）
- Unknown(352)（长度：8）
- Unknown(353)（长度：8）
- flowEndReason（长度：1）
- DROPPED_BYTES（长度：8）
- DROPPED_BYTES_TOTAL（长度：8）
- BYTES（长度：8）
- BYTES_TOTAL（长度：8）
- BYTES_SQUARED（长度：8）
- BYTES_SQUARED_PERMANENT（长度：8）
- IP_LENGTH_MINIMUM（长度：8）
- IP_LENGTH_MAXIMUM（长度：8）
- MUL_DOCTETS（长度：8）
- postMCastOctetTotalCount（长度：8）

使用隧道的 IPv6 输入

模板 ID：298。字段计数：53。

字段包括：

- observationPointId（长度：4）
- DIRECTION（长度：1）
- SRC_MAC（长度：6）
- DESTINATION_MAC（长度：6）
- ethernetType（长度：2）
- ethernetHeaderLength（长度：1）

- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IPV6_SRC_ADDR (长度: 4)
- IPV6_DST_ADDR (长度: 4)
- FLOW_LABEL (长度: 4)
- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)

- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMcastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMcastOctetTotalCount (长度: 8)

使用隧道的 IPv6 输出

模板 ID: 299。字段计数: 57。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- OUTPUT_SNMP (长度: 4)
- Unknown(369) (长度: 4)

- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IPV6_SRC_ADDR (长度: 4)
- IPV6_DST_ADDR (长度: 4)
- FLOW_LABEL (长度: 4)
- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)

- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

KVM TCP over IPv6 IPFIX 模板

有四个 KVM TCP over IPv6 IPFIX 模板：输入、输出、使用隧道的输入和使用隧道的输出。

TCP over IPv6 输入

模板 ID: 300。字段计数: 54。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)

- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IPV6_SRC_ADDR (长度: 4)
- IPV6_DST_ADDR (长度: 4)
- FLOW_LABEL (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)

- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMcastOctetTotalCount (长度: 8)
- tcpAckTotalCount (长度: 8)
- tcpFinTotalCount (长度: 8)
- tcpPshTotalCount (长度: 8)
- tcpRstTotalCount (长度: 8)
- tcpSynTotalCount (长度: 8)
- tcpUrgTotalCount (长度: 8)

TCP over IPv6 输出

模板 ID: 301。字段计数: 58。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- OUTPUT_SNMP (长度: 4)
- Unknown(369) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)

- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IPV6_SRC_ADDR (长度: 4)
- IPV6_DST_ADDR (长度: 4)
- FLOW_LABEL (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)

- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)
- tcpAckTotalCount (长度: 8)
- tcpFinTotalCount (长度: 8)
- tcpPshTotalCount (长度: 8)
- tcpRstTotalCount (长度: 8)
- tcpSynTotalCount (长度: 8)
- tcpUrgTotalCount (长度: 8)

使用隧道的 TCP over IPv6 输入

模板 ID: 302。字段计数: 61。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IPV6_SRC_ADDR (长度: 4)
- IPV6_DST_ADDR (长度: 4)

- FLOW_LABEL (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)
- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)

- BYTES_SQUARED（长度：8）
- BYTES_SQUARED_PERMANENT（长度：8）
- IP_LENGTH_MINIMUM（长度：8）
- IP_LENGTH_MAXIMUM（长度：8）
- MUL_DOCTETS（长度：8）
- postMCastOctetTotalCount（长度：8）
- tcpAckTotalCount（长度：8）
- tcpFinTotalCount（长度：8）
- tcpPshTotalCount（长度：8）
- tcpRstTotalCount（长度：8）
- tcpSynTotalCount（长度：8）
- tcpUrgTotalCount（长度：8）

使用隧道的 TCP over IPv6 输出

模板 ID：303。字段计数：65。

字段包括：

- observationPointId（长度：4）
- DIRECTION（长度：1）
- SRC_MAC（长度：6）
- DESTINATION_MAC（长度：6）
- ethernetType（长度：2）
- ethernetHeaderLength（长度：1）
- INPUT_SNMP（长度：4）
- Unknown(368)（长度：4）
- IF_NAME（长度：变量）
- IF_DESC（长度：变量）
- OUTPUT_SNMP（长度：4）
- Unknown(369)（长度：4）
- IF_NAME（长度：变量）
- IF_DESC（长度：变量）
- IP_PROTOCOL_VERSION（长度：1）
- IP_TTL（长度：1）

- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IPV6_SRC_ADDR (长度: 4)
- IPV6_DST_ADDR (长度: 4)
- FLOW_LABEL (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)
- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)

- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMcastOctetTotalCount (长度: 8)
- tcpAckTotalCount (长度: 8)
- tcpFinTotalCount (长度: 8)
- tcpPshTotalCount (长度: 8)
- tcpRstTotalCount (长度: 8)
- tcpSynTotalCount (长度: 8)
- tcpUrgTotalCount (长度: 8)

KVM UDP over IPv6 IPFIX 模板

有四个 KVM UDP over IPv6 IPFIX 模板: 输入、输出、使用隧道的输入和使用隧道的输出。

UDP over IPv6 输入

模板 ID: 304。字段计数: 48。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)

- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IPV6_SRC_ADDR (长度: 4)
- IPV6_DST_ADDR (长度: 4)
- FLOW_LABEL (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)

- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

UDP over IPv6 输出

模板 ID: 305。字段计数: 52。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- OUTPUT_SNMP (长度: 4)
- Unknown(369) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)

- IP_TOS (长度: 1)
- IPV6_SRC_ADDR (长度: 4)
- IPV6_DST_ADDR (长度: 4)
- FLOW_LABEL (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)

- MUL_DOCTETS（长度：8）
- postMCastOctetTotalCount（长度：8）

使用隧道的 UDP over IPv6 输入

模板 ID：306。字段计数：55。

字段包括：

- observationPointId（长度：4）
- DIRECTION（长度：1）
- SRC_MAC（长度：6）
- DESTINATION_MAC（长度：6）
- ethernetType（长度：2）
- ethernetHeaderLength（长度：1）
- INPUT_SNMP（长度：4）
- Unknown(368)（长度：4）
- IF_NAME（长度：变量）
- IF_DESC（长度：变量）
- IP_PROTOCOL_VERSION（长度：1）
- IP_TTL（长度：1）
- PROTOCOL（长度：1）
- IP_DSCP（长度：1）
- IP_PRECEDENCE（长度：1）
- IP_TOS（长度：1）
- IPV6_SRC_ADDR（长度：4）
- IPV6_DST_ADDR（长度：4）
- FLOW_LABEL（长度：4）
- L4_SRC_PORT（长度：2）
- L4_DST_PORT（长度：2）
- 893（长度：4，PEN：VMware Inc. (6876)）
- 894（长度：4，PEN：VMware Inc. (6876)）
- 895（长度：1，PEN：VMware Inc. (6876)）
- 896（长度：2，PEN：VMware Inc. (6876)）
- 897（长度：2，PEN：VMware Inc. (6876)）

- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

使用隧道的 UDP over IPv6 输出

模板 ID: 307。字段计数: 59。

字段包括：

- observationPointId（长度：4）
- DIRECTION（长度：1）
- SRC_MAC（长度：6）
- DESTINATION_MAC（长度：6）
- ethernetType（长度：2）
- ethernetHeaderLength（长度：1）
- INPUT_SNMP（长度：4）
- Unknown(368)（长度：4）
- IF_NAME（长度：变量）
- IF_DESC（长度：变量）
- OUTPUT_SNMP（长度：4）
- Unknown(369)（长度：4）
- IF_NAME（长度：变量）
- IF_DESC（长度：变量）
- IP_PROTOCOL_VERSION（长度：1）
- IP_TTL（长度：1）
- PROTOCOL（长度：1）
- IP_DSCP（长度：1）
- IP_PRECEDENCE（长度：1）
- IP_TOS（长度：1）
- IPV6_SRC_ADDR（长度：4）
- IPV6_DST_ADDR（长度：4）
- FLOW_LABEL（长度：4）
- L4_SRC_PORT（长度：2）
- L4_DST_PORT（长度：2）
- 893（长度：4，PEN：VMware Inc. (6876)）
- 894（长度：4，PEN：VMware Inc. (6876)）
- 895（长度：1，PEN：VMware Inc. (6876)）
- 896（长度：2，PEN：VMware Inc. (6876)）
- 897（长度：2，PEN：VMware Inc. (6876)）

- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

KVM SCTP over IPv6 IPFIX 模板

有四个 KVM SCTP over IPv6 IPFIX 模板：输入、输出、使用隧道的输入和使用隧道的输出。

SCTP over IPv6 输入

模板 ID：308。字段计数：48。

字段包括：

- observationPointId（长度：4）
- DIRECTION（长度：1）
- SRC_MAC（长度：6）
- DESTINATION_MAC（长度：6）
- ethernetType（长度：2）
- ethernetHeaderLength（长度：1）
- INPUT_SNMP（长度：4）
- Unknown(368)（长度：4）
- IF_NAME（长度：变量）
- IF_DESC（长度：变量）
- IP_PROTOCOL_VERSION（长度：1）
- IP_TTL（长度：1）
- PROTOCOL（长度：1）
- IP_DSCP（长度：1）
- IP_PRECEDENCE（长度：1）
- IP_TOS（长度：1）
- IPV6_SRC_ADDR（长度：4）
- IPV6_DST_ADDR（长度：4）
- FLOW_LABEL（长度：4）
- L4_SRC_PORT（长度：2）
- L4_DST_PORT（长度：2）
- 898（长度：变量，PEN：VMware Inc. (6876)）
- flowStartDeltaMicroseconds（长度：4）
- flowEndDeltaMicroseconds（长度：4）
- DROPPED_PACKETS（长度：8）
- DROPPED_PACKETS_TOTAL（长度：8）

- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

SCTP over IPv6 输出

模板 ID: 309。字段计数: 52。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)

- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- OUTPUT_SNMP (长度: 4)
- Unknown(369) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IPV6_SRC_ADDR (长度: 4)
- IPV6_DST_ADDR (长度: 4)
- FLOW_LABEL (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)

- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

使用隧道的 SCTP over IPv6 输入

模板 ID: 310。字段计数: 55。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)

- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IPV6_SRC_ADDR (长度: 4)
- IPV6_DST_ADDR (长度: 4)
- FLOW_LABEL (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)
- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)

- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMcastOctetTotalCount (长度: 8)

使用隧道的 SCTP over IPv6 输出

模板 ID: 311。字段计数: 59。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- OUTPUT_SNMP (长度: 4)
- Unknown(369) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)

- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IPV6_SRC_ADDR (长度: 4)
- IPV6_DST_ADDR (长度: 4)
- FLOW_LABEL (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)
- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)

- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

KVM ICMPv6 IPFIX 模板

有四个 KVM ICMPv6 IPFIX 模板: 输入、输出、使用隧道的输入和使用隧道的输出。

ICMPv6 输入

模板 ID: 312。字段计数: 48。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)

- IP_TOS (长度: 1)
- IPV6_SRC_ADDR (长度: 4)
- IPV6_DST_ADDR (长度: 4)
- FLOW_LABEL (长度: 4)
- ICMP_IPv6_TYPE (长度: 1)
- ICMP_IPv6_CODE (长度: 1)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)

- MUL_DOCTETS（长度：8）
- postMCastOctetTotalCount（长度：8）

ICMPv6 输出

模板 ID：313。字段计数：52。

字段包括：

- observationPointId（长度：4）
- DIRECTION（长度：1）
- SRC_MAC（长度：6）
- DESTINATION_MAC（长度：6）
- ethernetType（长度：2）
- ethernetHeaderLength（长度：1）
- INPUT_SNMP（长度：4）
- Unknown(368)（长度：4）
- IF_NAME（长度：变量）
- IF_DESC（长度：变量）
- OUTPUT_SNMP（长度：4）
- Unknown(369)（长度：4）
- IF_NAME（长度：变量）
- IF_DESC（长度：变量）
- IP_PROTOCOL_VERSION（长度：1）
- IP_TTL（长度：1）
- PROTOCOL（长度：1）
- IP_DSCP（长度：1）
- IP_PRECEDENCE（长度：1）
- IP_TOS（长度：1）
- IPV6_SRC_ADDR（长度：4）
- IPV6_DST_ADDR（长度：4）
- FLOW_LABEL（长度：4）
- ICMP_IPv6_TYPE（长度：1）
- ICMP_IPv6_CODE（长度：1）
- 898（长度：变量，PEN：VMware Inc. (6876)）

- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

使用隧道的 ICMPv6 输入

模板 ID: 314。字段计数: 55。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)

- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IPV6_SRC_ADDR (长度: 4)
- IPV6_DST_ADDR (长度: 4)
- FLOW_LABEL (长度: 4)
- ICMP_IPv6_TYPE (长度: 1)
- ICMP_IPv6_CODE (长度: 1)
- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)

- PKTS（长度：8）
- PACKETS_TOTAL（长度：8）
- Unknown(354)（长度：8）
- Unknown(355)（长度：8）
- Unknown(356)（长度：8）
- Unknown(357)（长度：8）
- Unknown(358)（长度：8）
- MUL_DPKTS（长度：8）
- postMCastPacketTotalCount（长度：8）
- Unknown(352)（长度：8）
- Unknown(353)（长度：8）
- flowEndReason（长度：1）
- DROPPED_BYTES（长度：8）
- DROPPED_BYTES_TOTAL（长度：8）
- BYTES（长度：8）
- BYTES_TOTAL（长度：8）
- BYTES_SQUARED（长度：8）
- BYTES_SQUARED_PERMANENT（长度：8）
- IP_LENGTH_MINIMUM（长度：8）
- IP_LENGTH_MAXIMUM（长度：8）
- MUL_DOCTETS（长度：8）
- postMCastOctetTotalCount（长度：8）

使用隧道的 ICMPv6 输出

模板 ID：315。字段计数：59。

字段包括：

- observationPointId（长度：4）
- DIRECTION（长度：1）
- SRC_MAC（长度：6）
- DESTINATION_MAC（长度：6）
- ethernetType（长度：2）
- ethernetHeaderLength（长度：1）

- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- OUTPUT_SNMP (长度: 4)
- Unknown(369) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IPV6_SRC_ADDR (长度: 4)
- IPV6_DST_ADDR (长度: 4)
- FLOW_LABEL (长度: 4)
- ICMP_IPv6_TYPE (长度: 1)
- ICMP_IPv6_CODE (长度: 1)
- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)

- PKTS（长度：8）
- PACKETS_TOTAL（长度：8）
- Unknown(354)（长度：8）
- Unknown(355)（长度：8）
- Unknown(356)（长度：8）
- Unknown(357)（长度：8）
- Unknown(358)（长度：8）
- MUL_DPKTS（长度：8）
- postMCastPacketTotalCount（长度：8）
- Unknown(352)（长度：8）
- Unknown(353)（长度：8）
- flowEndReason（长度：1）
- DROPPED_BYTES（长度：8）
- DROPPED_BYTES_TOTAL（长度：8）
- BYTES（长度：8）
- BYTES_TOTAL（长度：8）
- BYTES_SQUARED（长度：8）
- BYTES_SQUARED_PERMANENT（长度：8）
- IP_LENGTH_MINIMUM（长度：8）
- IP_LENGTH_MAXIMUM（长度：8）
- MUL_DOCTETS（长度：8）
- postMCastOctetTotalCount（长度：8）

KVM 以太网 VLAN IPFIX 模板

有四个 KVM 以太网 VLAN IPFIX 模板：输入、输出、使用隧道的输入和使用隧道的输出。

以太网 VLAN 输入

模板 ID：316。字段计数：30。

字段包括：

- observationPointId（长度：4）
- DIRECTION（长度：1）
- SRC_MAC（长度：6）
- DESTINATION_MAC（长度：6）

- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)

以太网 VLAN 输出

模板 ID: 317。字段计数: 34。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)

- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- OUTPUT_SNMP (长度: 4)
- Unknown(369) (长度: 8)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)

- flowEndReason (长度: 1)

使用隧道的以太网 VLAN 输入

模板 ID: 318。字段计数: 37。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)

- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)

使用隧道的以太网 VLAN 输出

模板 ID: 319。字段计数: 41。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- OUTPUT_SNMP (长度: 4)
- Unknown(369) (长度: 8)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- 893 (长度: 4, PEN: VMware Inc. (6876))

- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)

KVM IPv4 VLAN IPFIX 模板

有四个 KVM IPv4 VLAN IPFIX 模板: 输入、输出、使用隧道的输入和使用隧道的输出。

IPv4 VLAN 输入

模板 ID: 336。字段计数: 48。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)

- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)

- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

IPv4 VLAN 输出

模板 ID: 337。字段计数: 52。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- OUTPUT_SNMP (长度: 4)
- Unknown(369) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)

- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)

- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

使用隧道的 IPv4 VLAN 输入

模板 ID: 338。字段计数: 55。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)

- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP LENGTH MINIMUM (长度: 8)

- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

使用隧道的 IPv4 VLAN 输出

模板 ID: 339。字段计数: 59。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- OUTPUT_SNMP (长度: 4)
- Unknown(369) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)

- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP LENGTH MINIMUM (长度: 8)

- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

KVM TCP over IPv4 VLAN IPFIX 模板

有四个 KVM TCP over IPv4 VLAN IPFIX 模板: 输入、输出、使用隧道的输入和使用隧道的输出。

TCP over IPv4 VLAN 输入

模板 ID: 340。字段计数: 56。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)

- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)
- tcpAckTotalCount (长度: 8)
- tcpFinTotalCount (长度: 8)
- tcpPshTotalCount (长度: 8)
- tcpRstTotalCount (长度: 8)

- tcpSynTotalCount (长度: 8)
- tcpUrgTotalCount (长度: 8)

TCP over IPv4 VLAN 输出

模板 ID: 341。字段计数: 60。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- OUTPUT_SNMP (长度: 4)
- Unknown(369) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- L4_SRC_PORT (长度: 2)

- L4_DST_PORT (长度: 2)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)
- tcpAckTotalCount (长度: 8)
- tcpFinTotalCount (长度: 8)
- tcpPshTotalCount (长度: 8)

- tcpRstTotalCount (长度: 8)
- tcpSynTotalCount (长度: 8)
- tcpUrgTotalCount (长度: 8)

使用隧道的 TCP over IPv4 VLAN 输入

模板 ID: 342。字段计数: 63。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)
- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))

- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)

- postMCastOctetTotalCount (长度: 8)
- tcpAckTotalCount (长度: 8)
- tcpFinTotalCount (长度: 8)
- tcpPshTotalCount (长度: 8)
- tcpRstTotalCount (长度: 8)
- tcpSynTotalCount (长度: 8)
- tcpUrgTotalCount (长度: 8)

使用隧道的 TCP over IPv4 VLAN 输出

模板 ID: 343。字段计数: 67。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- OUTPUT_SNMP (长度: 4)
- Unknown(369) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)

- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)
- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)

- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMcastOctetTotalCount (长度: 8)
- tcpAckTotalCount (长度: 8)
- tcpFinTotalCount (长度: 8)
- tcpPshTotalCount (长度: 8)
- tcpRstTotalCount (长度: 8)
- tcpSynTotalCount (长度: 8)
- tcpUrgTotalCount (长度: 8)

KVM UDP over IPv4 VLAN IPFIX 模板

有四个 KVM UDP over IPv4 VLAN IPFIX 模板：输入、输出、使用隧道的输入和使用隧道的输出。

UDP over IPv4 VLAN 输入

模板 ID: 344。字段计数: 50。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)

- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMcastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)

- BYTES（长度：8）
- BYTES_TOTAL（长度：8）
- BYTES_SQUARED（长度：8）
- BYTES_SQUARED_PERMANENT（长度：8）
- IP_LENGTH_MINIMUM（长度：8）
- IP_LENGTH_MAXIMUM（长度：8）
- MUL_DOCTETS（长度：8）
- postMCastOctetTotalCount（长度：8）

UDP over IPv4 VLAN 输出

模板 ID：345。字段计数：54。

字段包括：

- observationPointId（长度：4）
- DIRECTION（长度：1）
- SRC_MAC（长度：6）
- DESTINATION_MAC（长度：6）
- ethernetType（长度：2）
- ethernetHeaderLength（长度：1）
- INPUT_SNMP（长度：4）
- Unknown(368)（长度：4）
- IF_NAME（长度：变量）
- IF_DESC（长度：变量）
- OUTPUT_SNMP（长度：4）
- Unknown(369)（长度：4）
- IF_NAME（长度：变量）
- IF_DESC（长度：变量）
- SRC_VLAN（长度：2）
- dot1qVlanId（长度：2）
- dot1qPriority（长度：1）
- IP_PROTOCOL_VERSION（长度：1）
- IP_TTL（长度：1）
- PROTOCOL（长度：1）

- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)

- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

使用隧道的 UDP over IPv4 VLAN 输入

模板 ID: 346。字段计数: 57。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)
- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))

- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)

- postMCastOctetTotalCount (长度: 8)

使用隧道的 UDP over IPv4 VLAN 输出

模板 ID: 347。字段计数: 61。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- OUTPUT_SNMP (长度: 4)
- Unknown(369) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)

- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP LENGTH MINIMUM (长度: 8)

- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

KVM SCTP over IPv4 VLAN IPFIX 模板

有四个 KVM SCTP over IPv4 VLAN IPFIX 模板: 输入、输出、使用隧道的输入和使用隧道的输出。

SCTP over IPv4 VLAN 输入

模板 ID: 348。字段计数: 50。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)

- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

SCTP over IPv4 VLAN 输出

模板 ID: 349。字段计数: 54。

字段包括:

- observationPointId (长度: 4)

- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- OUTPUT_SNMP (长度: 4)
- Unknown(369) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)

- PKTS（长度：8）
- PACKETS_TOTAL（长度：8）
- Unknown(354)（长度：8）
- Unknown(355)（长度：8）
- Unknown(356)（长度：8）
- Unknown(357)（长度：8）
- Unknown(358)（长度：8）
- MUL_DPKTS（长度：8）
- postMCastPacketTotalCount（长度：8）
- Unknown(352)（长度：8）
- Unknown(353)（长度：8）
- flowEndReason（长度：1）
- DROPPED_BYTES（长度：8）
- DROPPED_BYTES_TOTAL（长度：8）
- BYTES（长度：8）
- BYTES_TOTAL（长度：8）
- BYTES_SQUARED（长度：8）
- BYTES_SQUARED_PERMANENT（长度：8）
- IP_LENGTH_MINIMUM（长度：8）
- IP_LENGTH_MAXIMUM（长度：8）
- MUL_DOCTETS（长度：8）
- postMCastOctetTotalCount（长度：8）

使用隧道的 SCTP over IPv4 VLAN 输入

模板 ID：350。字段计数：57。

字段包括：

- observationPointId（长度：4）
- DIRECTION（长度：1）
- SRC_MAC（长度：6）
- DESTINATION_MAC（长度：6）
- ethernetType（长度：2）
- ethernetHeaderLength（长度：1）

- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)
- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)

- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

使用隧道的 SCTP over IPv4 VLAN 输出

模板 ID: 351。字段计数: 61。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)

- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- OUTPUT_SNMP (长度: 4)
- Unknown(369) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)
- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)

- PKTS（长度：8）
- PACKETS_TOTAL（长度：8）
- Unknown(354)（长度：8）
- Unknown(355)（长度：8）
- Unknown(356)（长度：8）
- Unknown(357)（长度：8）
- Unknown(358)（长度：8）
- MUL_DPKTS（长度：8）
- postMCastPacketTotalCount（长度：8）
- Unknown(352)（长度：8）
- Unknown(353)（长度：8）
- flowEndReason（长度：1）
- DROPPED_BYTES（长度：8）
- DROPPED_BYTES_TOTAL（长度：8）
- BYTES（长度：8）
- BYTES_TOTAL（长度：8）
- BYTES_SQUARED（长度：8）
- BYTES_SQUARED_PERMANENT（长度：8）
- IP_LENGTH_MINIMUM（长度：8）
- IP_LENGTH_MAXIMUM（长度：8）
- MUL_DOCTETS（长度：8）
- postMCastOctetTotalCount（长度：8）

KVM ICMPv4 VLAN IPFIX 模板

有四个 KVM ICMPv4 VLAN IPFIX 模板：输入、输出、使用隧道的输入和使用隧道的输出。

ICMPv4 VLAN 输入

模板 ID：352。字段计数：50。

字段包括：

- observationPointId（长度：4）
- DIRECTION（长度：1）
- SRC_MAC（长度：6）
- DESTINATION_MAC（长度：6）

- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- ICMP_IPv4_TYPE (长度: 1)
- ICMP_IPv4_CODE (长度: 1)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)

- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

ICMPv4 VLAN 输出

模板 ID: 353。字段计数: 54。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- OUTPUT_SNMP (长度: 4)
- Unknown(369) (长度: 4)
- IF_NAME (长度: 变量)

- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- ICMP_IPv4_TYPE (长度: 1)
- ICMP_IPv4_CODE (长度: 1)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)

- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

使用隧道的 ICMPv4 VLAN 输入

模板 ID: 354。字段计数: 57。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)

- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- ICMP_IPv4_TYPE (长度: 1)
- ICMP_IPv4_CODE (长度: 1)
- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMcastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)

- BYTES（长度：8）
- BYTES_TOTAL（长度：8）
- BYTES_SQUARED（长度：8）
- BYTES_SQUARED_PERMANENT（长度：8）
- IP_LENGTH_MINIMUM（长度：8）
- IP_LENGTH_MAXIMUM（长度：8）
- MUL_DOCTETS（长度：8）
- postMCastOctetTotalCount（长度：8）

使用隧道的 ICMPv4 VLAN 输出

模板 ID：355。字段计数：61。

字段包括：

- observationPointId（长度：4）
- DIRECTION（长度：1）
- SRC_MAC（长度：6）
- DESTINATION_MAC（长度：6）
- ethernetType（长度：2）
- ethernetHeaderLength（长度：1）
- INPUT_SNMP（长度：4）
- Unknown(368)（长度：4）
- IF_NAME（长度：变量）
- IF_DESC（长度：变量）
- OUTPUT_SNMP（长度：4）
- Unknown(369)（长度：4）
- IF_NAME（长度：变量）
- IF_DESC（长度：变量）
- SRC_VLAN（长度：2）
- dot1qVlanId（长度：2）
- dot1qPriority（长度：1）
- IP_PROTOCOL_VERSION（长度：1）
- IP_TTL（长度：1）
- PROTOCOL（长度：1）

- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IP_SRC_ADDR (长度: 4)
- IP_DST_ADDR (长度: 4)
- ICMP_IPv4_TYPE (长度: 1)
- ICMP_IPv4_CODE (长度: 1)
- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)

- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

KVM IPv6 VLAN IPFIX 模板

有四个 KVM IPv6 VLAN IPFIX 模板: 输入、输出、使用隧道的输入和使用隧道的输出。

IPv6 VLAN 输入

模板 ID: 356。字段计数: 49。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)

- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IPV6_SRC_ADDR (长度: 4)
- IPV6_DST_ADDR (长度: 4)
- FLOW_LABEL (长度: 4)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)

- MUL_DOCTETS（长度：8）
- postMCastOctetTotalCount（长度：8）

IPv6 VLAN 输出

模板 ID：357。字段计数：53。

字段包括：

- observationPointId（长度：4）
- DIRECTION（长度：1）
- SRC_MAC（长度：6）
- DESTINATION_MAC（长度：6）
- ethernetType（长度：2）
- ethernetHeaderLength（长度：1）
- INPUT_SNMP（长度：4）
- Unknown(368)（长度：4）
- IF_NAME（长度：变量）
- IF_DESC（长度：变量）
- OUTPUT_SNMP（长度：4）
- Unknown(369)（长度：4）
- IF_NAME（长度：变量）
- IF_DESC（长度：变量）
- SRC_VLAN（长度：2）
- dot1qVlanId（长度：2）
- dot1qPriority（长度：1）
- IP_PROTOCOL_VERSION（长度：1）
- IP_TTL（长度：1）
- PROTOCOL（长度：1）
- IP_DSCP（长度：1）
- IP_PRECEDENCE（长度：1）
- IP_TOS（长度：1）
- IPV6_SRC_ADDR（长度：4）
- IPV6_DST_ADDR（长度：4）
- FLOW_LABEL（长度：4）

- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

使用隧道的 IPv6 VLAN 输入

模板 ID: 358。字段计数: 56。

字段包括:

- observationPointId (长度: 4)

- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IPV6_SRC_ADDR (长度: 4)
- IPV6_DST_ADDR (长度: 4)
- FLOW_LABEL (长度: 4)
- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)

- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

使用隧道的 IPv6 VLAN 输出

模板 ID: 359。字段计数: 60。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)

- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- OUTPUT_SNMP (长度: 4)
- Unknown(369) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IPV6_SRC_ADDR (长度: 4)
- IPV6_DST_ADDR (长度: 4)
- FLOW_LABEL (长度: 4)
- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)

- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

KVM TCP over IPv6 VLAN IPFIX 模板

有四个 KVM TCP over IPv6 VLAN IPFIX 模板：输入、输出、使用隧道的输入和使用隧道的输出。

TCP over IPv6 VLAN 输入

模板 ID: 360。字段计数: 57。

字段包括:

- observationPointId (长度: 4)

- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IPV6_SRC_ADDR (长度: 4)
- IPV6_DST_ADDR (长度: 4)
- FLOW_LABEL (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)

- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP LENGTH MINIMUM (长度: 8)
- IP LENGTH MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)
- tcpAckTotalCount (长度: 8)
- tcpFinTotalCount (长度: 8)
- tcpPshTotalCount (长度: 8)
- tcpRstTotalCount (长度: 8)
- tcpSynTotalCount (长度: 8)
- tcpUrgTotalCount (长度: 8)

TCP over IPv6 VLAN 输出

模板 ID: 361。字段计数: 61。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)

- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- OUTPUT_SNMP (长度: 4)
- Unknown(369) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IPV6_SRC_ADDR (长度: 4)
- IPV6_DST_ADDR (长度: 4)
- FLOW_LABEL (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)

- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)
- tcpAckTotalCount (长度: 8)
- tcpFinTotalCount (长度: 8)
- tcpPshTotalCount (长度: 8)
- tcpRstTotalCount (长度: 8)
- tcpSynTotalCount (长度: 8)
- tcpUrgTotalCount (长度: 8)

使用隧道的 TCP over IPv6 VLAN 输入

模板 ID: 362。字段计数: 64。

字段包括:

- observationPointId (长度: 4)

- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IPV6_SRC_ADDR (长度: 4)
- IPV6_DST_ADDR (长度: 4)
- FLOW_LABEL (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)
- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))

- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMcastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMcastOctetTotalCount (长度: 8)
- tcpAckTotalCount (长度: 8)
- tcpFinTotalCount (长度: 8)
- tcpPshTotalCount (长度: 8)
- tcpRstTotalCount (长度: 8)
- tcpSynTotalCount (长度: 8)

- tcpUrgTotalCount (长度: 8)

使用隧道的 TCP over IPv6 VLAN 输出

模板 ID: 363。字段计数: 68。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- OUTPUT_SNMP (长度: 4)
- Unknown(369) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IPV6_SRC_ADDR (长度: 4)
- IPV6_DST_ADDR (长度: 4)
- FLOW_LABEL (长度: 4)
- L4_SRC_PORT (长度: 2)

- L4_DST_PORT (长度: 2)
- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)

- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)
- tcpAckTotalCount (长度: 8)
- tcpFinTotalCount (长度: 8)
- tcpPshTotalCount (长度: 8)
- tcpRstTotalCount (长度: 8)
- tcpSynTotalCount (长度: 8)
- tcpUrgTotalCount (长度: 8)

KVM UDP over IPv6 VLAN IPFIX 模板

有四个 KVM UDP over IPv6 VLAN IPFIX 模板: 输入、输出、使用隧道的输入和使用隧道的输出。

UDP over IPv6 VLAN 输入

模板 ID: 364。字段计数: 51。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)

- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IPV6_SRC_ADDR (长度: 4)
- IPV6_DST_ADDR (长度: 4)
- FLOW_LABEL (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMcastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)

- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

UDP over IPv6 VLAN 输出

模板 ID: 365。字段计数: 55。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- OUTPUT_SNMP (长度: 4)
- Unknown(369) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IPV6_SRC_ADDR (长度: 4)

- IPV6_DST_ADDR (长度: 4)
- FLOW_LABEL (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

使用隧道的 UDP over IPv6 VLAN 输入

模板 ID: 366。字段计数: 58。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IPV6_SRC_ADDR (长度: 4)
- IPV6_DST_ADDR (长度: 4)
- FLOW_LABEL (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)
- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))

- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

使用隧道的 UDP over IPv6 VLAN 输出

模板 ID: 367。字段计数: 62。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- OUTPUT_SNMP (长度: 4)
- Unknown(369) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IPV6_SRC_ADDR (长度: 4)
- IPV6_DST_ADDR (长度: 4)
- FLOW_LABEL (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)

- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP LENGTH MINIMUM (长度: 8)

- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

KVM SCTP over IPv6 VLAN IPFIX 模板

有四个 KVM SCTP over IPv6 VLAN IPFIX 模板: 输入、输出、使用隧道的输入和使用隧道的输出。

SCTP over IPv6 VLAN 输入

模板 ID: 368。字段计数: 51。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IPV6_SRC_ADDR (长度: 4)
- IPV6_DST_ADDR (长度: 4)
- FLOW_LABEL (长度: 4)
- L4_SRC_PORT (长度: 2)

- L4_DST_PORT (长度: 2)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

SCTP over IPv6 VLAN 输出

模板 ID: 369。字段计数: 55。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- OUTPUT_SNMP (长度: 4)
- Unknown(369) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IPV6_SRC_ADDR (长度: 4)
- IPV6_DST_ADDR (长度: 4)
- FLOW_LABEL (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)

- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

使用隧道的 SCTP over IPv6 VLAN 输入

模板 ID: 370。字段计数: 58。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)

- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IPV6_SRC_ADDR (长度: 4)
- IPV6_DST_ADDR (长度: 4)
- FLOW_LABEL (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)
- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)

- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

使用隧道的 SCTP over IPv6 VLAN 输出

模板 ID: 371。字段计数: 62。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)

- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- OUTPUT_SNMP (长度: 4)
- Unknown(369) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IPV6_SRC_ADDR (长度: 4)
- IPV6_DST_ADDR (长度: 4)
- FLOW_LABEL (长度: 4)
- L4_SRC_PORT (长度: 2)
- L4_DST_PORT (长度: 2)
- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))

- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

KVM ICMPv6 VLAN IPFIX 模板

有四个 KVM ICMPv6 IPFIX 模板: 输入、输出、使用隧道的输入和使用隧道的输出。

ICMPv6 输入

模板 ID: 372。字段计数: 51。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IPV6_SRC_ADDR (长度: 4)
- IPV6_DST_ADDR (长度: 4)
- FLOW_LABEL (长度: 4)
- ICMP_IPv6_TYPE (长度: 1)
- ICMP_IPv6_CODE (长度: 1)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)

- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

ICMPv6 输出

模板 ID: 373。字段计数: 55。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)

- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- OUTPUT_SNMP (长度: 4)
- Unknown(369) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IPV6_SRC_ADDR (长度: 4)
- IPV6_DST_ADDR (长度: 4)
- FLOW_LABEL (长度: 4)
- ICMP_IPv6_TYPE (长度: 1)
- ICMP_IPv6_CODE (长度: 1)
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)

- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

使用隧道的 ICMPv6 输入

模板 ID: 374。字段计数: 58。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)

- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IPV6_SRC_ADDR (长度: 4)
- IPV6_DST_ADDR (长度: 4)
- FLOW_LABEL (长度: 4)
- ICMP_IPv6_TYPE (长度: 1)
- ICMP_IPv6_CODE (长度: 1)
- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)
- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)

- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMcastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMcastOctetTotalCount (长度: 8)

使用隧道的 ICMPv6 输出

模板 ID: 375。字段计数: 62。

字段包括:

- observationPointId (长度: 4)
- DIRECTION (长度: 1)
- SRC_MAC (长度: 6)
- DESTINATION_MAC (长度: 6)
- ethernetType (长度: 2)
- ethernetHeaderLength (长度: 1)
- INPUT_SNMP (长度: 4)
- Unknown(368) (长度: 4)
- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- OUTPUT_SNMP (长度: 4)
- Unknown(369) (长度: 4)

- IF_NAME (长度: 变量)
- IF_DESC (长度: 变量)
- SRC_VLAN (长度: 2)
- dot1qVlanId (长度: 2)
- dot1qPriority (长度: 1)
- IP_PROTOCOL_VERSION (长度: 1)
- IP_TTL (长度: 1)
- PROTOCOL (长度: 1)
- IP_DSCP (长度: 1)
- IP_PRECEDENCE (长度: 1)
- IP_TOS (长度: 1)
- IPV6_SRC_ADDR (长度: 4)
- IPV6_DST_ADDR (长度: 4)
- FLOW_LABEL (长度: 4)
- ICMP_IPv6_TYPE (长度: 1)
- ICMP_IPv6_CODE (长度: 1)
- 893 (长度: 4, PEN: VMware Inc. (6876))
- 894 (长度: 4, PEN: VMware Inc. (6876))
- 895 (长度: 1, PEN: VMware Inc. (6876))
- 896 (长度: 2, PEN: VMware Inc. (6876))
- 897 (长度: 2, PEN: VMware Inc. (6876))
- 891 (长度: 1, PEN: VMware Inc. (6876))
- 892 (长度: 变量, PEN: VMware Inc. (6876))
- 898 (长度: 变量, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (长度: 4)
- flowEndDeltaMicroseconds (长度: 4)
- DROPPED_PACKETS (长度: 8)
- DROPPED_PACKETS_TOTAL (长度: 8)
- PKTS (长度: 8)
- PACKETS_TOTAL (长度: 8)
- Unknown(354) (长度: 8)

- Unknown(355) (长度: 8)
- Unknown(356) (长度: 8)
- Unknown(357) (长度: 8)
- Unknown(358) (长度: 8)
- MUL_DPKTS (长度: 8)
- postMCastPacketTotalCount (长度: 8)
- Unknown(352) (长度: 8)
- Unknown(353) (长度: 8)
- flowEndReason (长度: 1)
- DROPPED_BYTES (长度: 8)
- DROPPED_BYTES_TOTAL (长度: 8)
- BYTES (长度: 8)
- BYTES_TOTAL (长度: 8)
- BYTES_SQUARED (长度: 8)
- BYTES_SQUARED_PERMANENT (长度: 8)
- IP_LENGTH_MINIMUM (长度: 8)
- IP_LENGTH_MAXIMUM (长度: 8)
- MUL_DOCTETS (长度: 8)
- postMCastOctetTotalCount (长度: 8)

KVM 选项 IPFIX 模板

根据 IETF RFC 7011 中的第 3.4.2 节, 有一个 KVM 选项模板。

选项模板

模板 ID: 462。范围计数: 1。数据计数: 1。

监控逻辑交换机端口活动

例如, 您可以监控逻辑端口活动以解决网络拥塞和数据包丢弃问题。

前提条件

确认配置了一个逻辑交换机端口。请参见[将虚拟机连接到逻辑交换机](#)。

步骤

- 1 从浏览器中, 使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择 **高级网络和安全 > 网络 > 交换 > 端口**

3 单击端口的名称。

4 单击**监控**选项卡。

此时将显示端口状态和统计信息。

5 要下载主机已发现的 MAC 地址的 CSV 文件，请单击**下载 MAC 表**。

6 要监控端口上的活动，请单击**开始跟踪**。

此时将打开端口跟踪页面。您可以查看双向端口流量并确定丢弃的数据包。端口跟踪器页面还会列出与逻辑交换机端口关联的交换配置文件。

结果

如果注意到因网络拥塞而丢弃的数据包，可以为逻辑交换机端口配置 QoS 交换配置文件，以防止首选数据包上的数据丢失。请参见[了解 QoS 交换配置文件](#)。

您可以从**高级网络和安全**选项卡中配置逻辑交换机和相关的对象。逻辑交换机在脱离底层硬件的虚拟环境中再现交换功能（广播、未知单播、多播 (BUM) 流量）。

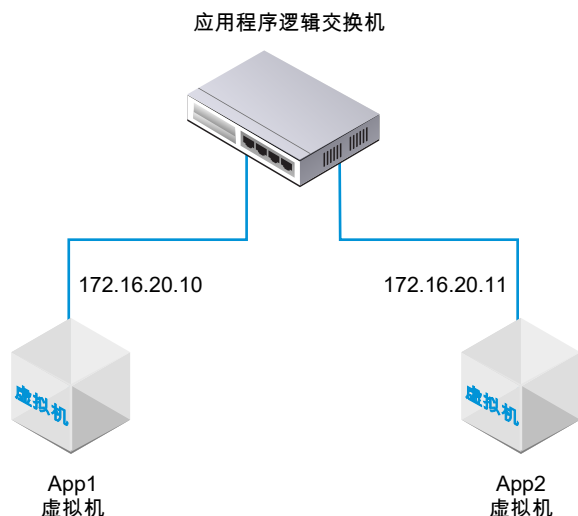
注 如果使用**高级网络和安全**用户界面来修政策“略界”面中创建的对象，则某些设置可能无法配置。这些只读设置的旁边有此图标：⊖。有关详细信息，请参见第 1 章 **NSX Manager 概览**。

逻辑交换机在提供可连接虚拟机的网络连接方式上类似于 VLAN。如果虚拟机连接到同一逻辑交换机，则虚拟机可以通过管理程序之间的隧道相互通信。每个逻辑交换机具有一个虚拟网络标识符 (Virtual Network Identifier, VNI)，与 VLAN ID 类似。与 VLAN 不同的是，VNI 远远超出 VLAN ID 的限制。

要查看并编辑 VNI 池的值，请登录到 NSX Manager，导航到 **Fabric > 配置文件**，然后单击**配置**选项卡。请注意，如果将池设置得太小，则所有 VNI 值都在使用中时创建逻辑交换机将失败。如果您删除逻辑交换机，VNI 值将在 6 小时后被重新使用。

在添加逻辑交换机时，请务必规划要构建的拓扑。

图 13-1. 逻辑交换机拓扑



例如，上面的拓扑显示连接到两个虚拟机的单个逻辑交换机。两个虚拟机可以位于不同主机集群或同一主机集群中的不同主机或同一主机上。由于示例中的虚拟机位于同一虚拟网络上，因此，在虚拟机上配置的基础 IP 地址必须位于同一子网中。

NSX Cloud 说明 如果使用 NSX Cloud，请参见 [NSX Cloud 支持的 NSX-T Data Center 功能](#) 以查看自动生成的逻辑实体、支持的功能以及 NSX Cloud 所需的配置的列表。

本章讨论了以下主题：

- [了解 BUM 帧复制模式](#)
- [创建逻辑交换机](#)
- [将虚拟机连接到逻辑交换机](#)
- [创建逻辑交换机端口](#)
- [测试第 2 层连接](#)
- [为 NSX Edge 上行链路创建 VLAN 逻辑交换机](#)
- [逻辑交换机和逻辑端口的交换配置文件](#)
- [增强型网络堆栈](#)
- [第 2 层桥接](#)

了解 BUM 帧复制模式

每个主机传输节点是一个隧道端点。每个隧道端点具有一个 IP 地址。这些 IP 地址可以位于同一子网中，也可以位于不同的子网中，具体取决于传输节点的 IP 池或 DHCP 配置。

在不同主机上的两个虚拟机直接通信时，将在与两个 Hypervisor 关联的两个隧道端点 IP 地址之间传输单播封装流量，而无需进行泛洪。

不过，与任何第 2 层网络一样，虚拟机发出的流量有时需要进行泛洪，这意味着需要将其发送到属于同一逻辑交换机的所有其他虚拟机。第 2 层广播、未知单播和多播流量（BUM 流量）就属于这种情况。回想一下，单个 NSX-T Data Center 逻辑交换机可以跨多个 Hypervisor。需要将给定 Hypervisor 上的虚拟机发出的 BUM 流量复制到远程 Hypervisor，这些 Hypervisor 托管连接到同一逻辑交换机的其他虚拟机。要启用这种泛洪，NSX-T Data Center 支持两种不同的复制模式：

- 分层双层（有时称为 MTEP）
- 头（有时称为源）

以下示例说明了分层式双层复制模式。假设主机 A 具有连接到虚拟网络标识符 (VNI) 5000、5001 和 5002 的虚拟机。请将 VNI 视为与 VLAN 类似，但每个逻辑交换机具有单个关联的 VNI。因此，有时可以将术语 VNI 和逻辑交换机换用。在我们说到主机位于 VNI 上时，我们的意思是主机的虚拟机连接到具有该 VNI 的逻辑交换机。

隧道端点表显示主机到 VNI 的连接。主机 A 检查 VNI 5000 的隧道端点表，并确定 VNI 5000 上的其他主机的隧道端点 IP 地址。

其中的一些 VNI 连接位于与主机 A 上的隧道端点相同的 IP 子网（也称为 IP 分段）上。对于其中的每个连接，主机 A 创建每个 BUM 帧的单独副本，并将该副本直接发送到每个主机。

其他主机的隧道端点位于不同的子网或 IP 分段上。对于具有多个隧道端点的每个分段，主机 A 将其中的一个端点提名为复制程序。

复制程序从主机 A 中接收 VNI 5000 的每个 BUM 帧的一个副本。该副本在封装标头中标记为本地复制。主机 A 不会将副本发送到与复制程序相同的 IP 分段中的其他主机。由复制程序负责为它了解的每个主机（位于 VNI 5000 上与复制程序主机相同的 IP 分段中）创建 BUM 帧副本。

将为 VNI 5001 和 5002 重复该过程。对于不同的 VNI，隧道端点列表和产生的复制程序可能是不同的。

头复制也称为头端复制，这种复制没有复制程序。主机 A 直接为 VNI 5000 上它了解的每个隧道端点创建每个 BUM 帧的副本并发送该副本。

如果所有主机隧道端点位于同一子网上，选择复制模式不会产生任何差异，因为这些行为是相同的。如果主机隧道端点位于不同的子网上，分层式双层复制有助于在多个主机之间分摊负载。分层双层是默认模式。

创建逻辑交换机

逻辑交换机连接到网络中的一个或多个虚拟机。连接到逻辑交换机的虚拟机可以使用管理程序之间的隧道互相通信。

前提条件

- 确认配置了一个传输区域。请参见 NSX-T Data Center 安装指南。
- 确认结构层节点已成功连接到 NSX-T Data Center 管理层面代理 (MPA) 和 NSX-T Data Center 本地控制层面 (LCP)。

在 GET `https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/state` API 调用中，state 必须为 success。请参见 NSX-T Data Center 安装指南。

- 确认传输节点已添加到传输区域中。请参见 NSX-T Data Center 安装指南。
- 确认管理程序已添加到 NSX-T Data Center 结构层中，并且在这些管理程序上托管了虚拟机。
- 熟悉逻辑交换机拓扑和 BUM 帧复制概念。请参见第 13 章 逻辑交换机和了解 BUM 帧复制模式。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 选择**高级网络和安全 > 网络 > 交换 > 交换机 > 添加**。
- 3 输入逻辑交换机的名称和可选描述。
- 4 为逻辑交换机选择一个传输区域。
连接到位于同一传输区域中的逻辑交换机的虚拟机可以相互通信。
- 5 输入上行链路绑定策略的名称。
- 6 将**管理状态**设置为**开启**或**关闭**。

7 为逻辑交换机择一种复制模式。

覆盖网络逻辑交换机需要使用复制模式（分层双层或头），但基于 VLAN 的逻辑交换机不需要使用复制模式。

复制模式	说明
分层双层	复制程序是一个主机，它将 BUM 流量复制到同一 VNI 中的其他主机。 每个主机将每个 VNI 中的一个主机隧道端点提名为复制程序。将为每个 VNI 完成该操作。
HEAD	主机创建每个 BUM 帧的副本，并将该副本发送到每个 VNI 中它了解的每个隧道端点。

8 （可选）指定一个 VLAN ID 或 VLAN ID 范围以用于 VLAN 标记。

要支持连接到该交换机的虚拟机的客户机 VLAN 标记，必须指定 VLAN ID 范围（也称为中继 VLAN ID 范围）。逻辑端口将根据中继 VLAN ID 范围过滤数据包，而客户机虚拟机可以根据中继 VLAN ID 范围使用自己的 VLAN ID 标记其数据包。

9 （可选）单击**交换配置文件**选项卡，然后选择交换配置文件。

10 单击**保存**。

在 NSX Manager UI 中，新逻辑交换机是一个可单击的链接。

后续步骤

将虚拟机连接到逻辑交换机。请参见[将虚拟机连接到逻辑交换机](#)。

将虚拟机连接到逻辑交换机

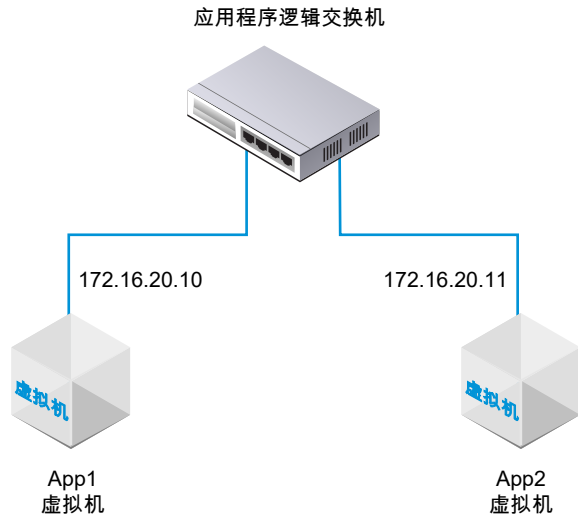
根据您的主机，将虚拟机连接到逻辑交换机的配置可能会有所不同。

可以连接到逻辑交换机的支持的主机是：在 vCenter Server 中管理的 ESXi 主机、单独的 ESXi 主机以及 KVM 主机。

将 vCenter Server 上托管的虚拟机连接到 NSX-T Data Center 逻辑交换机

如果在 vCenter Server 中管理某个 ESXi 主机，您可以通过基于 Web 的 vSphere Web Client 访问主机虚拟机。在这种情况下，您可以使用该过程将虚拟机连接到 NSX-T Data Center 逻辑交换机。

该过程中显示的示例说明了如何将名为 app-vm 的虚拟机连接到名为 app-switch 的逻辑交换机。



基于安装的 vSphere Client 应用程序不支持将虚拟机连接到 NSX-T Data Center 逻辑交换机。如果您没有（基于 Web 的）vSphere Web Client，请参阅[将单独 ESXi 上托管的虚拟机连接到 NSX-T Data Center 逻辑交换机](#)。

前提条件

- 必须在已添加到 NSX-T Data Center 结构层的管理程序上托管虚拟机。
- 结构层节点必须具有 NSX-T Data Center 管理层面 (MPA) 和 NSX-T Data Center 控制层面 (LCP) 连接。
- 必须将结构层节点添加到传输区域中。
- 必须创建一个逻辑交换机。

步骤

- 1 在 vSphere Web Client 中，编辑虚拟机设置并将虚拟机连接到 NSX-T Data Center 逻辑交换机。

例如：



- 2 单击**确定**。

结果

在将虚拟机连接到逻辑交换机后，逻辑交换机端口将添加到逻辑交换机中。您可以在**高级网络和安全 > 网络 > 交换 > 端口**中查看逻辑交换机端口和 NSX Manager 上的 VIF 连接 ID。

使用 GET `https://<mgr-ip>/api/v1/logical-ports/` API 调用查看相应 VIF 连接 ID 的端口详细信息和管理状态。要查看运行状态，请使用具有相应逻辑端口 ID 的 `https://<mgr-ip>/api/v1/logical-ports/<logical-port-id>/status` API 调用。

如果两个虚拟机连接到同一逻辑交换机并在同一子网中配置了 IP 地址，则它们应该可以 ping 通对方。

后续步骤

添加逻辑路由器。

您可以监控逻辑交换机端口上的活动以解决问题。请参阅 NSX-T Data Center 管理指南中的“监控逻辑交换机端口活动”。

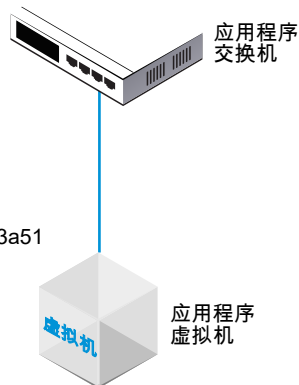
将单独 ESXi 上托管的虚拟机连接到 NSX-T Data Center 逻辑交换机

如果具有单独的 ESXi 主机，您无法通过基于 Web 的 vSphere Web Client 访问主机虚拟机。在这种情况下，您可以使用该过程将虚拟机连接到 NSX-T Data Center 逻辑交换机。

该过程中显示的示例说明了如何将名为 app-vm 的虚拟机连接到名为 app-switch 的逻辑交换机。

交换机的不透明网络 ID:
22b22448-38bc-419b-bea8-b51126bec7ad

虚拟机的外部 ID:
50066bae-0f8a-386b-e62e-b0b9c6013a51



前提条件

- 必须在已添加到 NSX-T Data Center 结构层的管理程序上托管虚拟机。
- 结构层节点必须具有 NSX-T Data Center 管理层面 (MPA) 和 NSX-T Data Center 控制层面 (LCP) 连接。
- 必须将结构层节点添加到传输区域中。
- 必须创建一个逻辑交换机。
- 您必须具有 NSX Manager API 的访问权限。
- 您必须具有虚拟机的 VMX 文件的写入访问权限。

步骤

- 1 通过使用（基于安装的）vSphere Client 应用程序或某种其他虚拟机管理工具，编辑虚拟机并添加一个 VMXNET 3 以太网适配器。

选择任何命名的网络。您将在后面的步骤中更改网络连接。



- 2 使用 NSX-T Data Center API 发出 GET `https://<nsx-mgr>/api/v1/fabric/virtual-machines/<VM-ID>` API 调用。

在结果中，找到虚拟机的 `externalId`。

例如：

```
GET https://<nsx-mgr>/api/v1/fabric/virtual-machines/60a5a5d5-ea2b-407e-a806-4fdc8468f735

{
  "resource_type": "VirtualMachine",
  "id": "60a5a5d5-ea2b-407e-a806-4fdc8468f735",
  "display_name": "app-vm",
  "compute_ids": [
    "instanceUuid:50066bae-0f8a-386b-e62e-b0b9c6013a51",
    "moIdOnHost:5",
    "externalId:50066bae-0f8a-386b-e62e-b0b9c6013a51",
    "hostLocalId:5",
    "locationId:564dc020-1565-e3f4-f591-ee3953eef3ff",
    "biosUuid:4206f47d-fef7-08c5-5bf7-ea26a4c6b18d"
  ],
  "external_id": "50066bae-0f8a-386b-e62e-b0b9c6013a51",
  "type": "REGULAR",
  "host_id": "cb82b0fa-a8f1-11e5-92a9-6b7d1f8661fa",
  "local_id_on_host": "5"
}
```

3 关闭虚拟机电源并从主机中取消注册虚拟机。

您可以使用虚拟机管理工具或 ESXi CLI（如下所示）。

```
[user@host:~] vim-cmd /vmsvc/getallvms
Vmid    Name      File           Guest OS      Version  Annotation
5       app-vm    [ds2] app-vm/app-vm.vmx  ubuntuGuest   vmx-08
8       web-vm    [ds2] web-vm/web-vm.vmx  ubuntu64Guest vmx-08

[user@host:~] vim-cmd /vmsvc/power.off 5
Powering off VM:

[user@host:~] vim-cmd /vmsvc/unregister 5
```

4 从 NSX Manager UI 中，获取逻辑交换机 ID。

例如：

app-switch

概览 监控 管理 相关

摘要 编辑

名称	app-switch
ID	b68e7ac3-877a-420e-af47-53e974c17915
位置	
描述	lswitch202 (created through automation)
管理状态	● 开启
复制模式	头复制
VLAN	不适用
VNI	71681
逻辑端口	1
流量类型	覆盖网络
传输区域	transportzone1
上行链路绑定策略名称	[Use Default]
N-VDS 模式	STANDARD
创建时间	9/10/2018, 12:20:46 PM, 创建者 admin
上次更新时间	9/26/2018, 2:01:14 PM, 创建者 admin

5 修改虚拟机的 VMX 文件。

删除 **ethernet1.networkName = "<name>"** 字段并添加以下字段：

- ethernet1.opaqueNetwork.id = "<logical switch's ID>"
- ethernet1.opaqueNetwork.type = "nsx.LogicalSwitch"
- ethernet1.externalId = "<VM's externalId>"
- ethernet1.connected = "TRUE"

- ethernet1.startConnected = "TRUE"

例如：

旧版本

```
ethernet1.pciSlotNumber = "224"
ethernet1.virtualDev = "vmxnet3"
ethernet1.networkName = "VM Network"
ethernet1.addressType = "vpx"
ethernet1.generatedAddress = "00:50:56:86:7b:d7"
ethernet1.uptCompatibility = "true"
ethernet1.present = "TRUE"
```

新版本

```
ethernet1.pciSlotNumber = "224"
ethernet1.virtualDev = "vmxnet3"
ethernet1.addressType = "vpx"
ethernet1.generatedAddress = "00:50:56:86:7b:d7"
ethernet1.uptCompatibility = "true"
ethernet1.present = "TRUE"
ethernet1.opaqueNetwork.id = "22b22448-38bc-419b-bea8-b51126bec7ad"
ethernet1.opaqueNetwork.type = "nsx.LogicalSwitch"
ethernet1.externalId = "50066bae-0f8a-386b-e62e-b0b9c6013a51"
ethernet1.connected = "TRUE"
ethernet1.startConnected = "TRUE"
```

- 6 在 NSX Manager UI 中，添加一个逻辑交换机端口，然后使用虚拟机的 externalId 进行 VIF 连接。
- 7 重新注册虚拟机，然后打开虚拟机电源。

您可以使用虚拟机管理工具或 ESXi CLI（如下所示）。

```
[user@host:~] vim-cmd /solo/register /path/to/file.vmx

For example:
[user@host:~] vim-cmd solo/registervm /vmfs/volumes/355f2049-6c704347/app-vm/app-vm.vmx
9

[user@host:~] vim-cmd /vmsvc/power.on 9
Powering on VM:
```

结果

在 NSX Manager UI 中的高级网络和安全 > 网络 > 交换 > 端口下面，找到与虚拟机的 externalId 匹配的 VIF 连接 ID，并确保管理和运行状态为“已连接/已连接”。

如果两个虚拟机连接到同一逻辑交换机并在同一子网中配置了 IP 地址，则它们应该可以 ping 通对方。

后续步骤

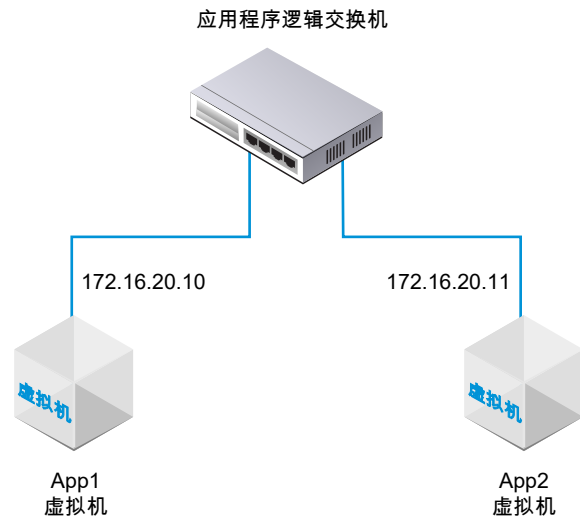
添加逻辑路由器。

您可以监控逻辑交换机端口上的活动以解决问题。请参阅 NSX-T Data Center 管理指南中的“监控逻辑交换机端口活动”。

将 KVM 上托管的虚拟机连接到 NSX-T Data Center 逻辑交换机

如果具有 KVM 主机，您可以使用该过程将虚拟机连接到 NSX-T Data Center 逻辑交换机。

该过程中显示的示例说明了如何将名为 app-vm 的虚拟机连接到名为 app-switch 的逻辑交换机。



前提条件

- 必须在已添加到 NSX-T Data Center 结构层的管理程序上托管虚拟机。
- 结构层节点必须具有 NSX-T Data Center 管理层面 (MPA) 和 NSX-T Data Center 控制层面 (LCP) 连接。
- 必须将结构层节点添加到传输区域中。
- 必须创建一个逻辑交换机。

步骤

- 1 从 KVM CLI 中，运行 `virsh dumpxml <your vm> | grep interfaceid` 命令。
- 2 在 NSX Manager UI 中，添加一个逻辑交换机端口，然后使用虚拟机的接口 ID 进行 VIF 连接。

结果

在 NSX Manager UI 中的 **高级网络和安全 > 网络 > 交换 > 端口** 下面，找到 VIF 连接 ID 并确保管理和运行状态为“已连接/已连接”。

如果两个虚拟机连接到同一逻辑交换机并在同一子网中配置了 IP 地址，则它们应该可以 ping 通对方。

后续步骤

添加逻辑路由器。

您可以监控逻辑交换机端口上的活动以解决问题。请参阅 NSX-T Data Center 管理指南中的“监控逻辑交换机端口活动”。

创建逻辑交换机端口

逻辑交换机具有多个交换机端口。逻辑交换机端口可将另一个网络组件、虚拟机或容器连接到逻辑交换机。

如果将虚拟机连接到由 vCenter Server 管理的 ESXi 主机上的逻辑交换机，则会自动创建一个逻辑交换机端口。有关将虚拟机连接到逻辑交换机的详细信息，请参见[将虚拟机连接到逻辑交换机](#)。

有关将容器连接到逻辑交换机的详细信息，请参阅《适用于 Kubernetes 的 NSX-T 容器插件安装和管理指南》。

注 绑定到容器的逻辑交换机端口的 IP 地址和 MAC 地址由 NSX Manager 分配。请勿手动更改地址绑定。

要监控逻辑交换机端口上的活动，请参见[监控逻辑交换机端口活动](#)。

前提条件

确认创建了一个逻辑交换机。请参见第 13 章 [逻辑交换机](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择 **高级网络和安全 > 网络 > 交换 > 端口 > 添加**。
- 3 在 **常规** 选项卡中，填写端口详细信息。

选项	说明
名称和说明	输入名称和可选的说明。
逻辑交换机	从下拉菜单中选择一个逻辑交换机。
管理状态	选择 已连接 或 未连接 。
连接类型	选择 无 或 VIF 。
连接 ID	如果连接类型为 VIF，请输入连接 ID。

通过使用 API，您可以将连接类型设置为其他值（LOGICALROUTER、BRIDGEENDPOINT、DHCP_SERVICE、METADATA_PROXY、L2VPN_SESSION）。如果连接类型为 DHCP 服务、元数据代理或 L2 VPN 会话，则端口的交换配置文件必须为默认配置文件。您不能使用任何用户定义的配置文件。

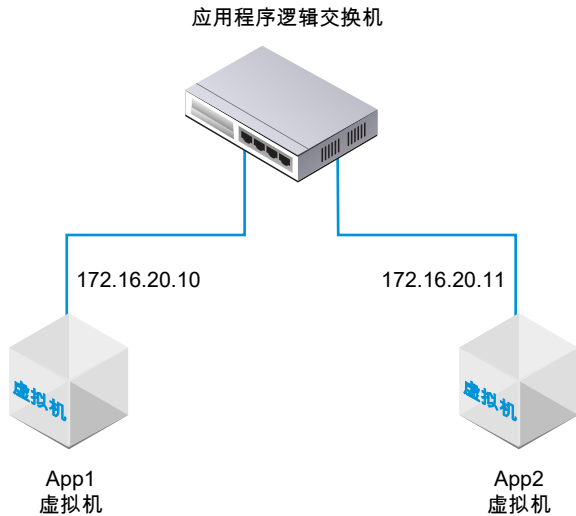
- 4 （可选）在 **交换配置文件** 选项卡中，选择交换配置文件。
- 5 单击 **保存**。

测试第 2 层连接

在成功设置逻辑交换机并将虚拟机连接到逻辑交换机后，您可以测试连接的虚拟机的网络连接。

如果根据拓扑正确配置了您的网络环境，App2 虚拟机可以 ping 通 App1 虚拟机。

图 13-2. 逻辑交换机拓扑



步骤

- 1 使用 SSH 或虚拟机控制台登录到逻辑交换机连接的一个虚拟机。
例如，App2 虚拟机 172.16.20.11。
- 2 对连接到逻辑交换机的第二个虚拟机执行 ping 操作以测试连接。

```
$ ping -c 2 172.16.20.10
PING 172.16.20.10 (172.16.20.10) 56(84) bytes of data.
64 bytes from 172.16.20.10: icmp_seq=1 ttl=63 time=0.982 ms
64 bytes from 172.16.20.10: icmp_seq=2 ttl=63 time=0.654 ms
64 bytes from 172.16.20.10: icmp_seq=3 ttl=63 time=0.791 ms

--- 172.16.20.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1990ms
rtt min/avg/max/mdev = 0.654/0.809/0.902/0.104 ms
```

- 3 (可选) 确定导致 ping 失败的问题。
 - a 验证虚拟机网络设置是否正确。
 - b 验证虚拟机网络适配器是否连接到正确的逻辑交换机。
 - c 验证逻辑交换机管理状态是否为“已连接”。
 - d 从 NSX Manager 中，选择高级网络和安全 > 网络 > 交换 > 交换机。

- e 单击逻辑交换机并记下 UUID 和 VNI 信息。
- f 运行以下命令以解决该问题。

命令	说明
get logical-switch <vni-or-uuid> arp-table	显示指定逻辑交换机的 ARP 表。 示例输出。
	<pre>nsx-manager1> get logical-switch 41866 arp-table VNI IP MAC Connection-ID 41866 172.16.20.11 00:50:56:b1:70:5e 295422</pre>
get logical-switch <vni-or-uuid> connection-table	显示指定逻辑交换机的连接。 示例输出。
	<pre>nsx-manager1> get logical-switch 41866 connection-table Host-IP Port ID 192.168.110.37 36923 295420 192.168.210.53 37883 295421 192.168.210.54 57278 295422</pre>
get logical-switch <vni-or-uuid> mac-table	显示指定逻辑交换机的 MAC 表。 示例输出。
	<pre>nsx-manager1> get logical-switch 41866 mac-table VNI MAC VTEP-IP Connection-ID 41866 00:50:56:86:f2:b2 192.168.250.102 295421 41866 00:50:56:b1:70:5e 192.168.250.101 295422</pre>
get logical-switch <vni-or-uuid> stats	显示有关指定逻辑交换机的统计信息。 示例输出。
	<pre>nsx-manager1> get logical-switch 41866 stats update.member 11 update.vtep 11 update.mac 4 update.mac.invalidate 0 update.arp 7 update.arp.duplicate 0 query.mac 2 query.mac.miss 0 query.arp 9 query.arp.miss 6</pre>
get logical-switch <vni-or-uuid> stats-sample	显示一段时间的所有逻辑交换机统计信息的摘要。 示例输出。
	<pre>nsx-manager1> get logical-switch 41866 stats-sample 21:00:00 21:10:00 21:20:00 21:30:00 21:40:00 update.member 0 0 0 0 0 update.vtep 0 0 0 0 0 update.mac 0 0 0 0 0 update.mac.invalidate 0 0 0 0 0 update.arp 0 0 0 0 0 update.arp.duplicate 0 0 0 0 0</pre>

命令	说明
	<pre>query.mac 0 0 0 0 0 query.mac.miss 0 0 0 0 0 query.arp 0 0 0 0 0 query.arp.miss 0 0 0 0 0</pre>
<pre>get logical-switch <vni-or-uuid> vtep</pre>	显示与指定逻辑交换机相关的所有虚拟隧道端点。 示例输出。 <pre>nsx-manager1> get logical-switch 41866 vtep VNI IP LABEL Segment MAC Connection-ID 41866 192.168.250.102 0x8801 192.168.250.0 00:50:56:65:f5:fc 295421 41866 192.168.250.100 0x1F801 192.168.250.0 02:50:56:00:00:00 295420 41866 192.168.250.101 0x16001 192.168.250.0 00:50:56:64:7c:28 295422</pre>

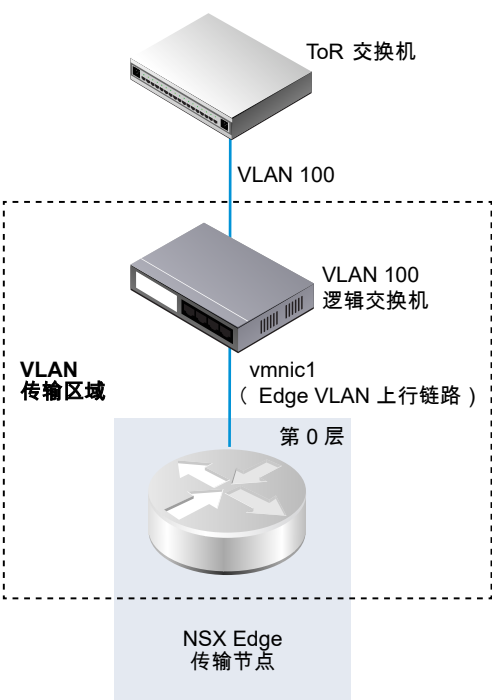
结果

连接到逻辑交换机的第一个虚拟机可以将数据包发送到第二个虚拟机。

为 NSX Edge 上行链路创建 VLAN 逻辑交换机

Edge 上行链路通过 VLAN 逻辑交换机连接到外部。

在创建 VLAN 逻辑交换机时，请务必记住要构建的特定拓扑。例如，以下简单拓扑显示 VLAN 传输区域中的单个 VLAN 逻辑交换机。该 VLAN 逻辑交换机具有 VLAN ID 100。这与用于 Edge 的 VLAN 上行链路的管理程序主机端口连接的 ToR 端口上的 VLAN ID 匹配。



前提条件

- 要创建 VLAN 逻辑交换机，必须先创建一个 VLAN 传输区域。
- 必须将一个 NSX-T Data Center vSwitch 添加到 NSX Edge 中。要在 Edge 上进行确认，请运行 `get host-switches` 命令。例如：

```
nsx-edge1> get host-switches

Host Switch      : c0a78378-1c20-432a-9e23-ddb34f1c80c9
Switch Name     : hs1
Transport Zone   : c46dcd72-808a-423d-b4cc-8752c33f6b2c
Transport Zone   : 73def985-d122-4b7b-ab6a-a58176dfc32d
Physical Port    : fp-eth0
Uplink Name      : uplink-1
Transport VLAN   : 4096
Default Gateway  : 192.168.150.1
Subnet Mask      : 255.255.255.0
Local VTEP Device : fp-eth0
Local VTEP IP    : 192.168.150.102
```

- 确认结构层节点已成功连接到 NSX-T Data Center 管理层面代理 (MPA) 和 NSX-T Data Center 本地控制层面 (LCP)。

在 GET `https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/state` API 调用中，state 必须为 success。请参见 NSX-T Data Center 安装指南。

步骤

- 1 从浏览器中，登录到 `https://<nsx-mgr>` 中的 NSX Manager。
- 2 选择 **高级网络和安全 > 网络 > 交换 > 交换机 > 添加**。
- 3 键入逻辑交换机的名称。
- 4 为逻辑交换机选择一个传输区域。
- 5 选择上行链路绑定策略。
- 6 对于管理状态，选择 **开启** 或 **关闭**。
- 7 键入 VLAN ID。

如果没有到物理 ToR 的上行链路的 VLAN ID，请在 VLAN 字段中输入 0。

- 8 (可选) 单击 **交换配置文件** 选项卡，然后选择交换配置文件。

结果

注 如果您有两个具有相同 VLAN ID 的 VLAN 逻辑交换机，则无法将它们连接到同一个 Edge N-VDS (以前称为主机交换机)。如果您有一个 VLAN 逻辑交换机和一个覆盖逻辑交换机，且 VLAN 逻辑交换机的 VLAN ID 与覆盖逻辑交换机的传输 VLAN ID 相同，则它们也不能连接到同一个 Edge N-VDS。

后续步骤

添加逻辑路由器。

逻辑交换机和逻辑端口的交换配置文件

交换配置文件包括逻辑交换机和逻辑端口的第 2 层网络配置详细信息。NSX Manager 支持几种类型的交换配置文件，并为每种配置文件类型保留一个或多个系统定义的默认交换配置文件。

可以使用以下类型的交换配置文件。

- QoS（服务质量）
- 端口镜像
- IP 发现
- SpoofGuard
- 交换机安全
- MAC 管理

注 您无法在 NSX Manager 中编辑或删除默认交换配置文件，但可以创建自定义交换配置文件。

在使用默认配置文件之前，请确保这些设置符合您的需求。创建自定义配置文件时，某些设置具有默认值。切勿假定在默认配置文件中，这些设置也将具有默认值。

每个默认或自定义交换配置文件具有唯一的保留标识符。您可以使用该标识符将交换配置文件与逻辑交换机或逻辑端口相关联。例如，默认 QoS 交换配置文件 ID 为 f313290b-eba8-4262-bd93-fab5026e9495。

可以将逻辑交换机或逻辑端口与每种类型的一个交换配置文件相关联。例如，您不能将两个不同的 QoS 交换配置文件与一个逻辑交换机或逻辑端口相关联。

如果在创建或更新逻辑交换机时未关联交换配置文件类型，则 NSX Manager 关联相应的默认系统定义交换配置文件。子逻辑端口从父逻辑交换机中继承默认系统定义的交换配置文件。

在创建或更新逻辑交换机或逻辑端口时，您可以选择关联默认或自定义交换配置文件。如果将交换配置文件与逻辑交换机关联或解除关联，将根据以下条件应用子逻辑端口的交换配置文件。

- 如果父逻辑交换机具有关联的配置文件，子逻辑端口将从父逻辑交换机中继承交换配置文件。
- 如果父逻辑交换机没有关联的交换配置文件，则为该逻辑交换机分配默认交换配置文件，并且该逻辑端口继承该默认交换配置文件。
- 如果明确将自定义配置文件与一个逻辑端口相关联，则该自定义配置文件覆盖现有的交换配置文件。

注 如果已将自定义交换配置文件与一个逻辑交换机相关联，但希望保留某个子逻辑端口的默认交换配置文件，您必须创建一个默认交换配置文件副本并将其与特定逻辑端口相关联。

如果将自定义交换配置文件与一个逻辑交换机或逻辑端口相关联，则无法删除该配置文件。您可以转到“摘要”视图的“分配给”部分并单击列出的逻辑交换机和逻辑端口，以确定任何逻辑交换机和逻辑端口是否与自定义交换配置文件相关联。

了解 QoS 交换配置文件

QoS 为需要高带宽的首选流量提供高质量和专用网络性能。QoS 机制确定分配足够带宽的优先顺序，控制延迟和抖动以及甚至在发生网络拥塞时减少首选数据包的数据丢失，从而实现该目的。该级别的网络服务是有效地使用现有的网络资源提供的。

对于该版本，支持调整和流量标记，即 CoS 和 DSCP。在由于拥塞而在逻辑交换机中缓冲流量时，第 2 层服务等级 (Class of Service, CoS) 允许您指定数据包的优先级。第 3 层差分服务代码点 (Differentiated Services Code Point, DSCP) 根据 DSCP 值检测数据包。CoS 始终应用于数据包，而不考虑受信任模式。

NSX-T Data Center 信任虚拟机应用的 DSCP 设置，或者在逻辑交换机级别修改和设置 DSCP 值。在每种情况下，DSCP 值将传播到 封装帧的外部 IP 标头。这样，外部物理网络就可以根据外部标头上的 DSCP 设置优先处理流量。在 DSCP 处于受信任模式时，将从内部标头中复制 DSCP 值。在处于不受信任模式时，不会保留内部标头的 DSCP 值。

注 DSCP 设置仅适用于隧道流量。这些设置不适用于同一 Hypervisor 中的流量。

您可以使用 QoS 交换配置文件配置平均输入和输出带宽值以设置传输限制速率。峰值带宽速率用于支持逻辑交换机允许的突发流量，以防止在北向网络链路上发生拥塞。这些设置并不能保证带宽，但有助于限制使用网络带宽。您将观察到的实际带宽取决于端口的链路速度或交换配置文件中的值（以较低者为准）。

QoS 交换配置文件设置将应用于逻辑交换机，并且子逻辑交换机端口继承这些设置。

配置自定义 QoS 交换配置文件

您可以定义 DSCP 值并配置输入和输出设置以创建自定义 QoS 交换配置文件。

前提条件

- 熟悉 QoS 交换配置文件概念。请参见[了解 QoS 交换配置文件](#)。
- 确定要优先处理的网络流量。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择 **高级网络和安全 > 网络 > 交换 > 交换配置文件 > 添加**

3 选择 QoS 并填写 QoS 交换配置文件详细信息。

选项	说明
名称和说明	指定自定义 QoS 交换配置文件的名称。 您可以选择描述在该配置文件中修改的设置。
模式	<p>从“模式”下拉菜单中选择受信任或不受信任选项。</p> <p>在选择“受信任”模式时，内部标头 DSCP 值将应用于 IP/IPv6 流量的外部 IP 标头。对于非 IP/IPv6 流量，外部 IP 标头使用默认值。在基于覆盖网络的逻辑端口上支持“受信任”模式。默认值为 0。</p> <p>在基于覆盖网络和基于 VLAN 的逻辑端口上支持“不受信任”模式。对于基于覆盖网络的逻辑端口，出站 IP 标头的 DSCP 值设置为配置的值，而不考虑逻辑端口的内部数据包类型。对于基于 VLAN 的逻辑端口，IP/IPv6 数据包的 DSCP 值设置为配置的值。“不受信任”模式的 DSCP 值范围是 0 到 63 之间。</p> <p>注 DSCP 设置仅适用于隧道流量。这些设置不适用于同一 Hypervisor 中的流量。</p>
优先级	<p>设置 DSCP 值。</p> <p>优先级值的范围为 0 到 63。</p>
服务类别	<p>设置 CoS 值。</p> <p>在基于 VLAN 的逻辑端口上支持 CoS。CoS 将网络中具有类似类型的流量划分到一起，并将每种类型的流量视为具有自己的服务优先级的等级。将减慢较低优先级的流量，或者在某些情况下，丢弃这些流量，以便为较高优先级的流量提供更好的吞吐量。也可以为具有零个数据包的 VLAN ID 配置 CoS。</p> <p>CoS 值范围是 0 到 7，其中 0 是最佳效果服务。</p>
输入	<p>为从虚拟机到逻辑网络的出站网络流量设置自定义值。</p> <p>您可以使用平均带宽以减少网络拥塞。峰值带宽速率用于支持突发流量，并且突发大小基于峰值带宽的持续时间。您可以在突发大小设置中设置突发持续时间。您不能保证带宽。不过，您可以使用“平均值”、“峰值”和“突发大小”设置以限制网络带宽。</p> <p>例如，如果平均带宽为 30 Mbps，峰值带宽为 60 Mbps，允许的持续时间为 0.1 秒，则突发大小为 $60 * 1000000 * 0.10/8 = 750000$ 字节。</p> <p>默认值 0 在输入流量上禁用速率限制。</p>
输入广播	<p>为从虚拟机到逻辑网络的基于广播的出站网络流量设置自定义值。</p> <p>为从虚拟机到逻辑网络的基于广播的出站网络流量设置自定义值。例如，如果将逻辑交换机的平均带宽设置为 3000 Kbps，峰值带宽为 6000 Kbps，允许的持续时间为 0.1 秒，则突发大小为 $6000 * 1000 * 0.10/8 = 75000$ 字节。</p> <p>默认值 0 在输入广播流量上禁用速率限制。</p>
输出	<p>为从逻辑网络到虚拟机的入站网络流量设置自定义值。</p> <p>默认值 0 在输出流量上禁用速率限制。</p>

如果未配置输入、输入广播和输出选项，则使用默认值。

4 单击保存。

结果

自定义 QoS 交换配置文件将显示为一个链接。

后续步骤

将该 QoS 自定义交换配置文件连接到一个逻辑交换机或逻辑端口，以便将该交换配置文件中修改的参数应用于网络流量。请参见[将自定义配置文件与逻辑交换机相关联](#)或[将自定义配置文件与逻辑端口相关联](#)。

了解端口镜像交换配置文件

通过使用逻辑端口镜像，您可以复制和重定向流入或流出连接到虚拟机 VIF 端口的逻辑交换机端口的所有流量。镜像的流量在常规路由封装 (Generic Routing Encapsulation, GRE) 隧道中以封装形式发送到一个收集器，以便在通过网络传输到远程目标时保留所有原始数据包信息。

我们建议您仅将端口镜像用于故障排除。

注 不建议使用端口镜像进行监控，因为长时间使用时，性能会受到影响。

与物理端口镜像相比，逻辑端口镜像确保捕获所有虚拟机网络流量。如果仅在物理网络中实现端口镜像，则无法镜像某些虚拟机网络流量。发生这种情况是因为，位于同一主机上的虚拟机之间的通信从不进入物理网络，因此，不会镜像这些通信。通过使用逻辑端口镜像，您可以继续镜像虚拟机流量，即使将该虚拟机迁移到其他主机。

对于 NSX-T Data Center 域中的虚拟机端口和物理应用程序的端口，端口镜像过程是类似的。您可以转发连接到逻辑网络的工作负载捕获的流量，并将该流量镜像到一个收集器。应该可以从托管虚拟机的客户机 IP 地址中访问该 IP 地址。此过程也适用于连接到网关节点的物理应用程序。

配置自定义端口镜像交换配置文件

您可以使用不同的目标和键值创建自定义端口镜像交换配置文件。

前提条件

- 熟悉端口镜像交换配置文件概念。请参见[了解端口镜像交换配置文件](#)。
- 确定要将网络流量重定向到的目标逻辑端口 ID 的 IP 地址。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择 **高级网络和安全 > 网络 > 交换 > 交换配置文件 > 添加**
- 3 选择**端口镜像**并填写端口镜像交换配置文件详细信息。

选项	说明
名称和说明	指定自定义端口镜像交换配置文件的名称。 您可以选择描述自定义该配置文件时修改的设置。
方向	从下拉菜单中选择一个选项以将该源用于 输入 、 输出 或 双向 流量。 “输入”是从虚拟机到逻辑网络的出站网络流量。 “输出”是从逻辑网络到虚拟机的入站网络流量。 “双向”是从虚拟机到逻辑网络以及从逻辑网络到虚拟机的双向流量。这是默认选项。
数据包截断	可选。范围是 60-65535。

选项	说明
键	<p>输入一个随机 32 位值以标识来自逻辑端口的镜像数据包。</p> <p>该键值将复制到每个镜像数据包的 GRE 标头中的键字段。如果该键值设置为 0，则将默认定义复制到 GRE 标头中的键字段。</p> <p>默认 32 位值由以下值组成。</p> <ul style="list-style-type: none"> ■ 前 24 位是一个 VNI 值。VNI 是封装的帧的 IP 标头的一部分。 ■ 第 25 位指示前 24 位是否为有效的 VNI 值。1 表示有效的值，0 表示无效的值。 ■ 第 26 位指示镜像流量的方向。1 表示输入方向，0 表示输出方向。 ■ 不使用剩余的 6 位。
目标	<p>输入镜像会话的收集器的目标 ID。</p> <p>目标 IP 地址 ID 只能是网络中的 IPv4 地址或 NSX-T Data Center 未管理的远程 IPv4 地址。您最多可以添加三个以逗号分隔的目标 IP 地址。</p>

4 单击保存。

结果

自定义端口镜像交换配置文件将显示为一个链接。

后续步骤

将该交换配置文件连接到一个逻辑交换机或逻辑端口。请参见[将自定义配置文件与逻辑交换机相关联](#)或[将自定义配置文件与逻辑端口相关联](#)。

验证自定义的端口镜像交换配置文件是否正常工作。请参见[验证自定义端口镜像交换配置文件](#)。

验证自定义端口镜像交换配置文件

在开始使用自定义端口镜像交换配置文件之前，请验证自定义是否正常工作。

前提条件

- 确认配置了自定义端口镜像交换配置文件。请参见[配置自定义端口镜像交换配置文件](#)。
- 确认自定义端口镜像交换配置文件与一个逻辑交换机相关联。请参见[将自定义配置文件与逻辑交换机相关联](#)。

步骤

- 1 找到两个具有到配置了端口镜像的逻辑端口的 VIF 连接的虚拟机。
例如，虚拟机 1 10.70.1.1 和虚拟机 2 10.70.1.2 具有 VIF 连接，并且它们位于相同的逻辑网络中。
- 2 为某个目标 IP 地址运行 tcpdump 命令。
sudo tcpdump -n -i eth0 dst host *destination_IP_address* and proto gre
例如，目标 IP 地址为 10.24.123.196。
- 3 登录到第一个虚拟机并对第二个虚拟机执行 ping 操作，以验证在目标地址中是否收到相应的 ECHO 请求和回复。

后续步骤

将该端口镜像自定义交换配置文件与一个逻辑交换机相关联，以便将交换配置文件中修改的参数应用于网络流量。请参见[将自定义配置文件与逻辑交换机相关联](#)。

了解 IP 发现交换配置文件

IP 发现使用 DHCP 和 DHCPv6 侦听、地址解析协议 (Address Resolution Protocol, ARP) 侦听、邻居发现 (Neighbor Discovery, ND) 侦听和 VM Tools 来发现 MAC 和 IP 地址。

发现的 MAC 地址和 IP 地址将用于实现 ARP/ND 抑制，从而最大限度减少连接到同一逻辑交换机的虚拟机之间的流量。这些地址也供 SpoofGuard 和分布式防火墙 (DFW) 组件使用。DFW 使用地址绑定来确定防火墙规则中的对象的 IP 地址。

DHCP/DHCPv6 侦听检查在 DHCP/DHCPv6 客户端和服务器之间交换的 DHCP/DHCPv6 数据包以发现 IP 和 MAC 地址。

ARP 侦听检查虚拟机的出站 ARP 和 GARP（免费 ARP）数据包以发现 IP 和 MAC 地址。

VM Tools 是一个在 ESXi 托管的虚拟机上运行的软件，可以提供该虚拟机的配置信息，包括 MAC 和 IP 或 IPv6 地址。该 IP 发现方法仅适用于在 ESXi 主机上运行的虚拟机。

ND 侦听相当于 IPv6 的 ARP 侦听。它会检查邻居请求 (NS) 和邻居通告 (NA) 消息，以发现 IP 和 MAC 地址。

重复地址检测会检查新发现的 IP 地址是否已存在于不同端口的已实现绑定列表中。对同一分段上的端口执行此检查。如果检测到重复地址，则会将新发现的地址添加到已发现列表，而是将其添加到已实现绑定列表中。所有重复 IP 都有关联的发现时间戳。如果通过将已实现绑定列表上的 IP 添加到忽略绑定列表或者禁用侦听移除该 IP，那么会将具有最早时间戳的重复 IP 移动到已实现绑定列表。通过 API 调用可获得重复地址信息。

默认情况下，发现方法 ARP 侦听和 ND 侦听在“首次使用时信任 (Trust on First Use, TOFU)”模式下运行。在 TOFU 模式下，当发现地址并将其添加到已实现绑定列表中时，该绑定将始终保留在已实现列表中。TOFU 应用于使用 ARP/ND 侦听发现的前“n”个唯一 <IP、MAC、VLAN> 绑定，其中“n”是您配置的绑定限制。对于 ARP/ND 侦听，您可以禁用 TOFU。然后，这些方法将在“每次使用时信任” (Trust On Every Use, TOEU) 模式下运行。在 TOEU 模式下，发现某个地址后，会将其添加到已实现绑定列表中，在该地址被删除或过期时，会从已实现的绑定列表中将其移除。DHCP 侦听和 VM Tools 始终在 TOEU 模式下运行。

对于每个端口，NSX Manager 都会维护一个忽略绑定列表，其中包含无法绑定到该端口的 IP 地址。通过导航到[高级网络和安全 > 交换 > 端口](#)并选择一个端口，您可以将发现的绑定添加到忽略绑定列表。您也可以通过将现有已发现或已实现绑定复制到[忽略绑定](#)来删除这些绑定。

注 TOFU 与 SpoofGuard 不同，它不会以与 SpoofGuard 相同的方式来阻止流量。有关详细信息，请参见[了解 SpoofGuard 分段配置文件](#)。

对于 Linux 虚拟机，ARP 不稳定问题可能会导致 ARP 侦听获取不正确的信息。可以使用 ARP 筛选器防止该问题。有关详细信息，请参见<http://linux-ip.net/html/ether-arp.html#ether-arp-flux>。

配置 IP 发现交换配置文件

NSX-T Data Center 有多个默认的 IP 发现交换配置文件。也可以创建更多的配置文件。

前提条件

熟悉 IP 发现交换配置文件概念。请参见[了解 IP 发现交换配置文件](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 选择 **高级网络和安全 > 网络 > 交换 > 交换配置文件 > 添加**。
- 3 选择 **IP 发现** 并指定 IP 发现交换配置文件详细信息。

选项	说明
名称和说明	输入名称和可选的说明。
ARP 侦听	适用于 IPv4 环境。虚拟机具有静态 IP 地址时适用。
ARP 绑定限制	可以绑定到一个端口的最大 IPv4 IP 地址数量。允许的最小值为 1（默认值），最大值为 256。
ARP ND 绑定限制超时	如果禁用 TOFU，ARP/ND 绑定表中 IP 地址的超时值（以分钟为单位）。如果某地址超时，新发现的地址将取代该地址。
DHCP 侦听	适用于 IPv4 环境。虚拟机具有 IPv4 地址时适用。
DHCP V6 侦听	适用于 IPv6 环境。虚拟机具有 IPv6 地址时适用。
VM Tools	仅适用于 ESXi 托管的虚拟机。
VM Tools (IPv6)	仅适用于 ESXi 托管的虚拟机。
邻居发现侦听	适用于 IPv6 环境。虚拟机具有静态 IP 地址时适用。
邻居发现绑定限制	可以绑定到一个端口的最大 IPv6 地址数量。
首次使用时信任	适用于 ARP 和 ND 侦听。
重复的 IP 检测	适用于所有侦听方法以及 IPv4 和 IPv6 环境。

- 4 单击**添加**。

后续步骤

将该 IP 发现自定义交换配置文件连接到一个逻辑交换机或逻辑端口，以便将该交换配置文件中修改的参数应用于网络流量。请参见[将自定义配置文件与逻辑交换机相关联](#)或[将自定义配置文件与逻辑端口相关联](#)。

了解 SpoofGuard

SpoofGuard 有助于防止一种称为“网络欺骗”或“网络钓鱼”的恶意攻击。SpoofGuard 策略阻止确定为欺骗的流量。

SpoofGuard 工具旨在防止您环境中的虚拟机更改其现有的 IP 地址。如果虚拟机的 IP 地址与 SpoofGuard 上的相应逻辑端口和交换机地址绑定中的 IP 地址不匹配，将完全禁止虚拟机的 vNIC 访问网络。可以在端口或交换机级别配置 SpoofGuard。在您的环境中使用 SpoofGuard 可能有以下几个原因：

- 防止恶意虚拟机使用现有虚拟机的 IP 地址。
- 确保无法在没有干预的情况下更改虚拟机的 IP 地址 - 在某些环境中，在没有正确的更改控制检查的情况下，最好禁止虚拟机更改其 IP 地址。SpoofGuard 确保虚拟机所有者无法直接更改 IP 地址并继续工作而不会受到妨碍，从而简化了该过程。
- 保证不会无意（或有意）绕过分布式防火墙 (Distributed Firewall, DFW) 规则 - 对于将 IP 集作为源或目标创建的 DFW 规则，始终存在虚拟机可能在数据包标头中伪造其 IP 地址的可能性，从而绕过相关的规则。

NSX-T Data Center SpoofGuard 配置包括以下内容：

- MAC SpoofGuard - 验证数据包的 MAC 地址。
- IP SpoofGuard - 验证数据包的 IP 地址。
- 动态地址解析协议 (Dynamic Address Resolution Protocol, ARP) 检查（即，ARP）以及无故地址解析协议 (Gratuitous Address Resolution Protocol, GARP) SpoofGuard 和邻居发现 (Neighbor Discovery, ND) SpoofGuard 验证针对的都是 ARP/GARP/ND 负载中的 MAC 源、IP 源和 IP-MAC 源映射。

在端口级别，允许的 MAC/VLAN/IP 允许列表是通过端口的地址绑定属性提供的。在虚拟机发送流量时，如果流量的 IP/MAC/VLAN 与端口的 IP/MAC/VLAN 属性不匹配，则会丢弃该流量。端口级别 SpoofGuard 处理流量验证，即，流量与 VIF 配置是否一致。

在交换机级别，允许的 MAC/VLAN/IP 允许列表是通过交换机的地址绑定属性提供的。这通常是交换机的允许的 IP 范围/子网，交换机级别 SpoofGuard 处理流量授权。

端口级别和交换机级别 SpoofGuard 必须允许流量，然后才允许流量进入交换机。可以使用 SpoofGuard 交换机配置文件来控制端口和交换机级别 SpoofGuard 的激活或停用。

配置端口地址绑定

地址绑定指定逻辑端口的 IP 和 MAC 地址，并用于指定 SpoofGuard 中的端口白名单。

通过使用端口地址绑定，您可以指定逻辑端口的 IP 和 MAC 地址以及 VLAN（如果适用）。如果启用 SpoofGuard，它确保在数据路径中强制实施指定的地址绑定。除了 SpoofGuard 以外，端口地址绑定还用于 DFW 规则转换。

步骤

- 1 在 NSX Manager 中，选择**高级网络和安全 > 网络 > 交换 > 端口**。

- 2 单击要将地址绑定应用到的逻辑端口。

将显示逻辑端口摘要。

- 3 在**概览**选项卡中，展开**地址绑定 > 手动绑定**。

- 4 单击**添加**。

将显示“添加地址绑定”对话框。

- 5 指定要将地址绑定应用到的逻辑端口的 IP 地址（IPv4 地址、IPv6 地址或 IPv6 子网）和 MAC 地址。例如，对于 IPv6，2001::/64 是 IPv6 子网，2001::1 是主机 IP，而 2001::1/64 则是无效输入。还可以指定 VLAN ID。

- 6 单击**添加**。

后续步骤

在配置 [SpoofGuard 交换配置文件](#) 时，请使用端口地址绑定。

配置 SpoofGuard 交换配置文件

在配置 SpoofGuard 时，如果某个虚拟机的 IP 地址发生变化，可能会阻止来自该虚拟机的流量，直到将配置的相应端口/交换机地址绑定更新为新 IP 地址。

为包含客户机的端口组启用 SpoofGuard。如果为每个网络适配器启用 SpoofGuard，它将检查数据包以查找指定的 MAC 及其相应的 IP 地址。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**高级网络和安全 > 网络 > 交换 > 交换配置文件 > 添加**。
- 3 选择 **SpoofGuard**。
- 4 输入名称和可选的说明。
- 5 要启用端口级别的 SpoofGuard，请将**端口绑定**设置为已启用。
- 6 单击**添加**。

结果

将使用 SpoofGuard 配置文件创建一个新的交换配置文件。

后续步骤

将 SpoofGuard 配置文件与一个逻辑交换机或逻辑端口相关联。请参见[将自定义配置文件与逻辑交换机相关联](#)或[将自定义配置文件与逻辑端口相关联](#)。

了解交换机安全交换配置文件

交换机安全通过以下方法提供无状态第 2 层和第 3 层安全性：检查逻辑交换机的输入流量，并将 IP 地址、MAC 地址和协议与一组允许的地址和协议进行匹配以丢弃从虚拟机发送的未授权的数据包。您可以使用交换机安全筛选掉来自网络中的虚拟机的恶意攻击以保护逻辑交换机完整性。

您可以配置网桥协议数据单元 (Bridge Protocol Data Unit, BPDU) 筛选器、DHCP 侦听、DHCP 服务器阻止以及速率限制选项以自定义逻辑交换机上的交换机安全交换配置文件。

配置自定义交换机安全交换配置文件

您可以使用允许的 BPDU 列表中的 MAC 目标地址创建自定义交换机安全交换配置文件并配置速率限制。

前提条件

熟悉交换机安全交换配置文件概念。请参见[了解交换机安全交换配置文件](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**高级网络和安全 > 网络 > 交换**。
- 3 单击**交换配置文件**选项卡。
- 4 单击**添加**，然后选择**交换机安全**。
- 5 填写交换机安全配置文件详细信息。

选项	说明
名称和说明	指定自定义交换机安全配置文件的名称。 您可以选择描述在该配置文件中修改的设置。
BPDU 筛选器	切换 BPDU 筛选器 按钮以启用 BPDU 筛选。默认情况下，将禁用该按钮。 如果启用了 BPDU 筛选器，将阻止到 BPDU 目标 MAC 地址的所有流量。如果启用，BPDU 筛选器还会在逻辑交换机端口上禁用 STP，因为这些端口应该不会加入 STP。
BPDU 筛选器允许列表	单击 BPDU 目标 MAC 地址列表中的目标 MAC 地址以允许将流量传输到允许的目标。您必须启用 BPDU 筛选器 才能从该列表中进行选择。
DHCP 筛选器	切换 服务器阻止 按钮和 客户端阻止 按钮以启用 DHCP 筛选。默认情况下，将禁用这两个按钮。 “DHCP 服务器阻止”阻止从 DHCP 服务器到 DHCP 客户端的流量。请注意，它不会阻止从 DHCP 服务器到 DHCP 中继代理的流量。 “DHCP 客户端阻止”阻止 DHCP 请求以禁止虚拟机获取 DHCP IP 地址。
DHCPv6 筛选器	切换 V6 服务器阻止 按钮和 V6 客户端阻止 按钮以启用 DHCP 筛选。默认情况下，将禁用这两个按钮。 “DHCPv6 服务器阻止”可阻止从 DHCPv6 服务器到 DHCPv6 客户端的流量。请注意，它不会阻止从 DHCP 服务器到 DHCP 中继代理的流量。筛选出 UDP 源端口号为 547 的数据包。 “DHCPv6 客户端阻止”会阻止 DHCP 请求以禁止虚拟机获取 DHCP IP 地址。筛选出 UDP 源端口号为 546 的数据包。

选项	说明
阻止非 IP 流量	<p>切换阻止非 IP 流量按钮以仅允许 IPv4、IPv6、ARP、GARP 和 BPDU 流量。</p> <p>将阻止其余非 IP 流量。允许的 IPv4、IPv6、ARP、GARP 和 BPDU 流量基于在地址绑定和 SpoofGuard 配置中设置的其他策略。</p> <p>默认情况下，将禁用该选项以允许将非 IP 流量作为常规流量进行处理。</p>
RA 防护	<p>切换RA 防护按钮以筛选出输入 IPv6 路由器通告。筛选出 ICMPv6 类型的 134 个数据包。默认情况下，将启用该选项。</p>
速率限制	<p>设置广播和多播流量的速率限制。默认情况下，将启用该选项。</p> <p>可以使用速率限制保护逻辑交换机或虚拟机，以免受到广播风暴等事件的影响。</p> <p>为了避免任何连接问题，最小速率限制值必须大于或等于 10 pps。</p>

6 单击添加。

结果

自定义交换机安全配置文件将显示为一个链接。

后续步骤

将该交换机安全自定义交换配置文件连接到一个逻辑交换机或逻辑端口，以便将该交换配置文件中修改的参数应用于网络流量。请参见[将自定义配置文件与逻辑交换机相关联](#)或[将自定义配置文件与逻辑端口相关联](#)。

了解 MAC 管理交换配置文件

MAC 管理交换配置文件支持两种功能：MAC 发现和 MAC 地址更改。

MAC 地址更改功能允许虚拟机更改其 MAC 地址。连接到端口的虚拟机可以运行管理命令以更改其 vNIC 的 MAC 地址，并仍然在该 vNIC 上发送和接收流量。仅在 ESXi 上支持该功能，而在 KVM 上不支持。默认情况下，将禁用该属性，但在使用 VMware Integrated OpenStack 部署客户机虚拟机时除外，此时，默认启用该属性。

MAC 发现提供到在一个 vNIC 后面配置多个 MAC 地址的部署的网络连接，例如，在嵌套管理程序部署中，ESXi 虚拟机在 ESXi 主机上运行，并且多个虚拟机在 ESXi 虚拟机中运行。如果未使用 MAC 发现，在 ESXi 虚拟机的 vNIC 连接到交换机端口时，其 MAC 地址是静态的。在 ESXi 虚拟机中运行的虚拟机没有网络连接，因为其数据包具有不同的源 MAC 地址。通过使用 MAC 发现，vSwitch 检查来自 vNIC 的每个数据包的源 MAC 地址，发现 MAC 地址并允许数据包通过。如果在特定时间段内未使用发现的 MAC 地址，则会将其移除。无法配置该到期属性。

MAC 学习还支持未知单播泛洪。通常，在端口收到的数据包具有未知目标 MAC 地址时，将丢弃该数据包。在启用未知单播泛洪的情况下，端口将未知单播流量泛洪到交换机上启用了 MAC 学习和未知单播泛洪的每个端口。默认情况下，将启用该属性，但只有在启用 MAC 发现时才启用。

可以配置可学习 MAC 地址的数量。最大值为 4096，这是默认值。您还可以设置达到限制设置时实施的策略。选项包括：

- **丢弃** - 来自未知源 MAC 地址的数据包被丢弃。此 MAC 地址的入站数据包将被视为未知单播。仅当端口启用了未知单播泛洪时，端口才会接收数据包。

- **允许** - 尽管不会学习该地址，但会转发来自未知源 MAC 地址的数据包。此 MAC 地址的入站数据包将被视为未知单播。仅当端口启用了未知单播泛洪时，端口才会接收数据包。

如果启用 MAC 发现或 MAC 地址更改以提高安全性，还要配置 SpoofGuard。

配置 MAC 管理交换配置文件

您可以创建 MAC 管理交换配置文件以管理 MAC 地址。

前提条件

熟悉 MAC 管理交换配置文件概念。请参见[了解 MAC 管理交换配置文件](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**高级网络和安全 > 网络 > 交换 > 交换配置文件 > 添加**。
- 3 选择 **MAC 管理**并填写 MAC 管理配置文件详细信息。

选项	说明
名称和说明	指定 MAC 管理配置文件的名称。 您可以选择描述在该配置文件中修改的设置。
MAC 更改	启用或禁用 MAC 地址更改功能。默认禁用该功能。
状态	启用或禁用 MAC 发现功能。默认禁用该功能。
未知的单播泛洪	启用或禁用未知的单播泛洪功能。默认启用该功能。此选项在启用 MAC 学习时可用
MAC 限制	设置 MAC 地址的最大数量。默认值为 4096。此选项在启用 MAC 学习时可用
MAC 限制策略	选择 允许 或 丢弃 。默认操作作为 允许 。此选项在启用 MAC 学习时可用

- 4 单击**添加**。

后续步骤

将该交换配置文件连接到一个逻辑交换机或逻辑端口。请参见[将自定义配置文件与逻辑交换机相关联](#)或[将自定义配置文件与逻辑端口相关联](#)。

将自定义配置文件与逻辑交换机相关联

您可以将自定义交换配置文件与逻辑交换机关联，以便配置文件应用于该交换机上的所有端口。

如果将自定义交换配置文件与一个逻辑交换机相关联，它们将覆盖现有的默认交换配置文件。子逻辑交换机端口将继承自定义交换配置文件。

注 如果已将自定义交换配置文件与一个逻辑交换机相关联，但希望保留某个子逻辑交换机端口的默认交换配置文件，您必须创建一个默认交换配置文件副本并将其与特定逻辑交换机端口相关联。

前提条件

- 确认配置了一个逻辑交换机。请参见[创建逻辑交换机](#)。

- 确认配置了一个自定义交换配置文件。请参见[逻辑交换机和逻辑端口的交换配置文件](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**高级网络和安全 > 网络 > 交换 > 交换机**。
- 3 单击该逻辑交换机以应用自定义交换配置文件。
- 4 单击**管理**选项卡。
- 5 从下拉菜单中选择自定义交换配置文件类型。
 - QoS
 - 端口镜像
 - IP 发现
 - SpoofGuard
 - 交换机安全
 - MAC 管理
- 6 单击**更改**。
- 7 从下拉菜单中选择以前创建的自定义交换配置文件。
- 8 单击**保存**。
逻辑交换机现在与自定义交换配置文件相关联。
- 9 验证是否在**管理**选项卡下面显示具有修改的配置的新自定义交换配置文件。
- 10 （可选）单击**相关**选项卡并从下拉菜单中选择**端口**，以验证是否将自定义交换配置文件应用于子逻辑端口。

后续步骤

如果不希望使用从逻辑交换机中继承的交换配置文件，您可以将自定义交换配置文件应用于子逻辑交换机端口。请参见[将自定义配置文件与逻辑端口相关联](#)。

将自定义配置文件与逻辑端口相关联

逻辑端口提供 VIF 的逻辑连接点、到路由器的修补连接或到外部网络的第 2 层网关连接。逻辑端口还公开交换配置文件、端口统计信息计数器以及逻辑链路状态。

您可以将子逻辑端口从逻辑交换机中继承的交换配置文件更改为不同的自定义交换配置文件。

前提条件

- 确认配置了一个逻辑端口。请参见[将虚拟机连接到逻辑交换机](#)。
- 确认配置了一个自定义交换配置文件。请参见[逻辑交换机和逻辑端口的交换配置文件](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**高级网络和安全 > 网络 > 交换 > 端口**。
- 3 单击该逻辑端口以应用自定义交换配置文件。
- 4 单击**管理**选项卡。
- 5 从下拉菜单中选择自定义交换配置文件类型。
 - QoS
 - 端口镜像
 - IP 发现
 - SpoofGuard
 - 交换机安全
 - MAC 管理
- 6 单击**更改**。
- 7 从下拉菜单中选择以前创建的自定义交换配置文件。
- 8 单击**保存**。

该逻辑端口现在与自定义交换配置文件相关联。

- 9 验证是否在**管理**选项卡下面显示具有修改的配置的新自定义交换配置文件。

后续步骤

您可以监控逻辑交换机端口上的活动以解决问题。请参阅 NSX-T Data Center 管理指南中的“监控逻辑交换机端口活动”。

增强型网络堆栈

增强型数据路径是一种网络堆栈模式，配置后可提供卓越的网络性能。它主要用于 NFV 工作负载，这些工作负载需要此模式提供的性能优势。

只能在 ESXi 主机上以增强型数据路径模式配置 N-VDS 交换机。ENS 还支持流经 Edge 虚拟机的流量。在增强型数据路径模式下，可以配置覆盖网络流量和 VLAN 流量。

自动分配 ENS 逻辑内核

自动将逻辑内核分配给 vNIC，以便由专用逻辑内核管理流入和流出 vNIC 的入站流量和出站流量。

在增强型数据路径模式下配置 N-VDS 交换机后，如果将单个逻辑内核与 vNIC 相关联，则该逻辑内核将负责处理流入或流出 vNIC 的双向流量。配置多个逻辑内核后，主机会自动确定必须由哪个逻辑内核处理 vNIC 的流量。

可根据以下任一参数为 vNIC 分配逻辑内核。

- **vNIC-count:** 主机假定某个 vNIC 方向上的入站流量或出站流量传输需要相同的 CPU 资源量。将根据可用的逻辑内核池为每个逻辑内核分配相同数量的 vNIC。这是默认模式。vNIC-count 模式很可靠，但对于非对称流量而言并不是最佳模式。
- **CPU-usage:** 主机通过使用内部统计信息预测在每个 vNIC 方向上传输入站或出站流量时的 CPU 使用情况。根据传输流量时的 CPU 使用情况，主机会更改逻辑内核分配，以平衡逻辑内核之间的负载。CPU-usage 模式优于 vNIC-count 模式，但在流量不稳定时不可靠。

在 CPU-usage 模式下，如果传输的流量频繁变化，则预测的所需 CPU 资源和 vNIC 分配也可能会频繁变化。过于频繁的分配变更可能会导致数据包丢失。

如果流量模式在各 vNIC 之间是对称的，则 vNIC-count 选项会提供不太会发生频繁变化的可靠行为。但是，如果流量模式是非对称的，vNIC-count 选项可能会导致数据包丢失，因为它不会区分各 vNIC 之间的流量差异。

在 vNIC-count 模式下，建议配置适当数量的逻辑内核，以便将每个逻辑内核分配给相同数量的 vNIC。如果与每个逻辑内核关联的 vNIC 的数量各不相同，则说明 CPU 分配不合理，因而性能不具有确定性。

当已连接或断开连接某个 vNIC，或者添加或移除某个逻辑内核后，主机会自动检测所发生的更改，并重新进行平衡。

步骤

- ◆ 要从一种模式切换到另一种模式，请运行以下命令。

```
set ens lcore-assignment-mode <host-switch-name> <ens-lc-mode>
```

其中，可以将 *<ens-lc-mode>* 设为 **vNIC-count** 或 **cpu-usage**。

vNIC-count 是基于 vNIC/方向计数的逻辑内核分配。

cpu-usage 是基于 CPU 使用情况的逻辑内核分配。

配置客户机 VLAN 间路由

在覆盖网络上，NSX-T 支持路由 L3 域上的 VLAN 间流量。在路由过程中，虚拟分布式路由器 (Virtual Distributed Router, VDR) 使用 VLAN ID 在 VLAN 子网之间路由数据包。

VLAN 间路由消除了每个虚拟机只能使用 10 个 vNIC 的限制。支持 VLAN 间路由的 NSX-T 可确保能够在 vNIC 上创建多个 VLAN 子接口并将其用于不同的网络连接服务。例如，虚拟机的一个 vNIC 可以分为多个子接口。每个子接口都属于一个子网，可以托管一个网络连接服务，如 SNMP 或 DHCP。例如，使用 VLAN 间路由时，VLAN-10 上的子接口可以访问 VLAN-10 或任何其他 VLAN 上的子接口。

虚拟机上的每个 vNIC 均通过父逻辑端口连接到 N-VDS，从而管理未标记的数据包。

要创建子接口，请在增强型 N-VDS 交换机上，使用此过程中所述的 API 调用，创建一个使用具有关联 VIF 的 API 的子端口。使用 VLAN ID 标记的子接口将关联到新的逻辑交换机，例如，VLAN10 将连接到逻辑交换机 LS-VLAN-10。必须将 VLAN10 的所有子接口连接到 LS-VLAN-10。子接口的 VLAN ID 与其关联的逻辑交换机之间的这种一对一映射是一项重要的必备条件。例如，如果将具有 VLAN20 的子端口添加到映射到 VLAN-10 的逻辑交换机 LS-VLAN-10，则会导致 VLAN 之间的数据包路由无法正常工作。此类配置错误会导致 VLAN 间路由无法正常工作。

前提条件

- 在将 VLAN 子接口关联到逻辑交换机之前，请确保逻辑交换机未与其他 VLAN 子接口相关联。如果存在不匹配的情况，VLAN 间路由可能无法在覆盖网络上正常运行。
- 确保主机运行 ESXi v 6.7 U2 或更高版本。

步骤

- 1 要为 vNIC 创建子接口，请确保将该 vNIC 更新为父端口。进行以下 REST API 调用。

```
PUT https://<nsx-mgr-ip>/api/v1/logical-ports/<Logical-Port UUID-of-the-vNIC>
{
  "resource_type" : "LogicalPort",
  "display_name" : "parentport",
  "attachment" : {
    "attachment_type" : "VIF",
    "context" : {
      "resource_type" : "VifAttachmentContext",
      "vif_type": "PARENT"
    },
    "id" : "<Attachment UUID of the vNIC>"
  },
  "admin_state" : "UP",
  "logical_switch_id" : "UUID of Logical Switch to which the vNIC is connected",
  "_revision" : 0
}
```

- 2 要与虚拟机上的子接口关联的 N-VDS 上的父 vNIC 端口创建子端口，请进行 API 调用。在进行 API 调用之前，请确认存在逻辑交换机，以便将子端口连接到虚拟机上的子接口。

```
POST https://<nsx-mgr-ip>/api/v1/logical-ports/
{
  "resource_type" : "LogicalPort",
  "display_name" : "<Name of the Child PORT>",
  "attachment" : {
    "attachment_type" : "VIF",
    "context" : {
      "resource_type" : "VifAttachmentContext",
      "parent_vif_id" : "<UUID of the PARENT port from Step 1>",
      "traffic_tag" : <VLAN ID>,
      "app_id" : "<ID of the attachment>", ==> display id(can give any string). Must be unique.
    },
    "vif_type" : "CHILD"
  },
  "id" : "<ID of the CHILD port>"
}
```

```

    },
    "logical_switch_id" : "<UUID of the Logical switch(not the PARENT PORT's logical switch)
to which Child port would be connected to>",
    "address_bindings" : [ { "mac_address" : "<vNIC MAC address>", "ip_address" : "<IP
address to the corresponding VLAN>", "vlan" : <VLAN ID> } ],
    "admin_state" : "UP"
}

```

结果

NSX-T Data Center 将在虚拟机上创建子接口。

第 2 层桥接

如果 NSX-T Data Center 逻辑交换机需要建立到支持 VLAN 的端口组的第 2 层连接，或者需要访问位于 NSX-T Data Center 部署外部的其他设备（如网关），您可以使用 NSX-T Data Center 第 2 层网桥。第 2 层网桥在迁移时特别有用，此时，您需要在物理和虚拟工作负载之间拆分子网。

第 2 层网桥中涉及的 NSX-T Data Center 概念包括 Edge 群集和 Edge 网桥文件。您可以使用 NSX Edge 传输节点配置第 2 层桥接。要使用 NSX Edge 传输节点进行桥接，您需要创建一个 Edge 网桥配置文件。Edge 网桥配置文件指定要用于桥接的 Edge 群集，以及充当主网桥和备份网桥的 Edge 传输节点。

Edge 网桥配置文件会连接到逻辑交换机，该映射会指定用于桥接的 Edge 上的物理上行链路以及要与逻辑交换机关联的 VLAN ID。逻辑交换机可连接到多个网桥配置文件。

创建 Edge 网桥配置文件

Edge 网桥配置文件使 NSX Edge 集群能够提供到逻辑交换机的第 2 层桥接。

创建 Edge 网桥配置文件时，如果将故障切换模式设置为主动，并进行故障切换，则备用节点将成为活动节点。故障节点恢复后，它将再次成为活动节点。如果将故障切换模式设置为非主动，并进行故障切换，则备用节点将成为活动节点。故障节点恢复后，它将成为备用节点。通过在备用 Edge 节点上运行 CLI 命令 `set l2bridge-port <uuid> state active`，可以手动将备用 Edge 节点设置为活动节点。该命令只能在非主动模式下应用。否则，将出现错误。在非主动模式下，当在备用节点上应用此命令时，它将触发 HA 故障切换，当在活动节点上应用时，它将被忽略。有关详细信息，请参见《NSX-T Data Center 命令行界面参考》。

前提条件

- 验证您的 NSX Edge 集群是否具有两个 NSX Edge 传输节点。

步骤

- 1 选择 **系统 > 结构层 > 配置文件 > Edge 网桥配置文件 > 添加**。
- 2 输入 Edge 网桥配置文件的名称和可选的描述。
- 3 选择一个 NSX Edge 集群。
- 4 选择一个主节点。

- 5 选择一个备份节点。
- 6 选择一种故障切换模式。
选项为**主动**和**非主动**。
- 7 单击**添加**按钮。

后续步骤

现在，您可以将逻辑交换机与网桥配置文件相关联。

配置基于 Edge 的桥接

当配置基于 Edge 的桥接时，在为 Edge 集群创建 Edge 网桥配置文件后，需要执行一些额外的配置。

请注意，不支持在同一 Edge 节点上两次桥接一个逻辑交换机。但是，可以将两个 VLAN 桥接到两个不同 Edge 节点上的同一逻辑交换机。

共有三个配置选项。

选项 1：配置混杂模式

- 在端口组上设置混杂模式。
- 在端口组上允许伪信号。
- 运行以下命令，在运行 Edge 虚拟机的 ESXi 主机上启用反向筛选器：

```
esxcli system settings advanced set -o /Net/ReversePathFwdCheckPromisc -i 1
```

然后，按照以下步骤在端口组上禁用和启用混杂模式：

- 编辑端口组的设置。
 - 禁用混杂模式并保存设置。
 - 再次编辑端口组的设置。
 - 启用混杂模式并保存设置。
- 共享同一组 VLAN 的同一个主机上没有任何其他端口组处于混杂模式。
 - 活动和备用 Edge 虚拟机应位于不同的主机上。如果它们位于同一个主机上，吞吐量可能会下降，因为 VLAN 流量需要同时转发至处于混杂模式的两个虚拟机。

选项 2：配置 MAC 学习

如果 Edge 部署在安装了 NSX-T 的主机上，则它可以连接到 VLAN 逻辑交换机或分段。逻辑交换机必须具有启用了 MAC 学习的 MAC 管理配置文件。同样，分段必须具有启用了 MAC 学习的 MAC 发现配置文件。

选项 3：配置池端口

- 1 检索要配置为池端口的中继虚拟网卡的端口号。
 - a 登录到 vSphere Web Client，然后导航到**主页 > 网络**。

- b 单击 NSX Edge 中继接口所连接到的分布式端口组，然后单击**端口**以查看端口和连接的虚拟机。请记住与中继接口关联的端口号。在获取和更新含糊数据时将使用此端口号。

2 检索 vSphere Distributed Switch 的 dvsUuid 值。

- a 登录到 vCenter MOB UI: <https://<vc-ip>/mob>。
- b 单击**内容**。
- c 单击与 **rootFolder** 关联的链接（例如: *group-d1 (Datacenters)*）。
- d 单击与 **childEntity** 关联的链接（例如: *datacenter-1*）。
- e 单击与 **networkFolder** 关联的链接（例如: *group-n6*）。
- f 单击与 NSX Edge 关联的 vSphere Distributed Switch 的 DVS 名称链接（例如: *dvs-1 (Mgmt_VDS)*）。
- g 复制 **uuid** 字符串的值。在获取和更新含糊数据时将对 **dvsUuid** 使用此值。

3 验证指定的端口是否存在含糊数据。

- a 转到 <https://<vc-ip>/mob/?moid=DVSManager&vmodl=1>。
- b 单击 **fetchOpaqueDataEx**。
- c 在 **selectionSet** 值框中，粘贴以下 XML 输入：

```
<selectionSet xsi:type="DVPortSelection">
  <dvsUuid>c2 1d 11 50 6a 7c 77 68-e6 ba ce 6a 1d 96 2a 15</dvsUuid> <!-- example
dvsUuid -->
  <portKey>393</portKey> <!-- example port number -->
</selectionSet>
```

使用您为 NSX Edge 中继接口检索到的端口号和 **dvsUuid** 值。

- d 将 **isRuntime** 设置为 **false**。
- e 单击**调用方法**。如果结果显示 **vim.dvs.OpaqueData.ConfigInfo** 的值，则表明已存在含糊数据集，请在设置池端口时使用 **edit** 操作。如果 **vim.dvs.OpaqueData.ConfigInfo** 的值为空，请在设置池端口时使用 **add** 操作。

4 在 vCenter Managed Object Browser (MOB) 中配置池端口。

- a 转到 <https://<vc-ip>/mob/?moid=DVSManager&vmodl=1>。
- b 单击 **updateOpaqueDataEx**。
- c 在 **selectionSet** 框中，粘贴以下 XML 内容。例如，

```
<selectionSet xsi:type="DVPortSelection">
  <dvsUuid>c2 1d 11 50 6a 7c 77 68-e6 ba ce 6a 1d 96 2a 15</dvsUuid> <!-- example
dvsUuid -->
  <portKey>393</portKey> <!-- example port number -->
</selectionSet>
```

使用从 vCenter MOB 检索到的 **dvsUuid** 值。

- d 在 opaqueDataSpec 框中，粘贴以下 XML 内容之一。

如果未设置含糊数据，使用此输入启用池端口（operation 设置为 add）：

```
<opaqueDataSpec>
  <operation>add</operation>
  <opaqueData>
    <key>com.vmware.etherswitch.port.extraEthFRP</key>
    <opaqueData
xsi:type="vmobl.Binary">AAABAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    </opaqueData>
  </opaqueDataSpec>
```

如果已设置含糊数据，使用此输入启用池端口（operation 设置为 edit）：

```
<opaqueDataSpec>
  <operation>edit</operation>
  <opaqueData>
    <key>com.vmware.etherswitch.port.extraEthFRP</key>
    <opaqueData
xsi:type="vmobl.Binary">AAABAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    </opaqueData>
  </opaqueDataSpec>
```

使用此输入禁用池端口：

```
<opaqueDataSpec>
  <operation>edit</operation>
  <opaqueData>
    <key>com.vmware.etherswitch.port.extraEthFRP</key>
    <opaqueData
xsi:type="vmobl.Binary">AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=</opaqueData>
  </opaqueData>
</opaqueDataSpec>
```

- e 将 isRuntime 设置为 false。
- f 单击调用方法。

创建支持网桥的第 2 层逻辑交换机

如果您的虚拟机连接到 NSX-T Data Center 覆盖网络，则可以配置网桥支持的逻辑交换机，以提供与 NSX-T Data Center 部署外部的其他设备或虚拟机的第 2 层连接。

前提条件

- 确认您拥有 Edge 网桥配置文件。
- 至少将一个 ESXi 或 KVM 主机用作常规传输节点。该节点托管的虚拟机需要与 NSX-T Data Center 部署外部的设备进行连接。
- 在 NSX-T Data Center 部署外部具有一个虚拟机或其他终端设备。该终端设备必须连接到与支持网桥的逻辑交换机的 VLAN ID 匹配的 VLAN 端口。
- 将覆盖网络传输区域中的一个逻辑交换机用作支持网桥的逻辑交换机。

步骤

- 1 从浏览器中，登录到 `https://<nsx-mgr>` 中的 NSX Manager。
- 2 选择**高级网络和安全 > 网络 > 交换**。
- 3 单击覆盖网络交换机的名称（流量类型：覆盖网络）。
- 4 单击与**相关 > Edge 网桥配置文件**。
- 5 单击**连接**。
- 6 要连接到 Edge 网桥配置文件，请执行以下操作：
 - a 选择一个 Edge 网桥配置文件
 - b 选择一个传输区域。
 - c 输入 VLAN ID。
 - d 单击**保存**。

- 7 如果尚未将虚拟机连接到逻辑交换机，请连接虚拟机。

这些虚拟机必须位于 Edge 网桥配置文件所在的传输区域中的传输节点上。

结果

您可以将 ping 命令从 NSX-T Data Center 内部虚拟机发送到 NSX-T Data Center 外部的节点以测试网桥是否正常工作。

可以通过单击**监控**选项卡来监控网桥交换机上的流量。

还可以使用 GET `https://192.168.110.31/api/v1/bridge-endpoints/<endpoint-id>/statistics` API 调用来查看网桥流量：

```
{
  "tx_packets": {
    "total": 134416,
```

```
    "dropped": 0,  
    "multicast_broadcast": 0  
  },  
  "rx_bytes": {  
    "total": 22164,  
    "multicast_broadcast": 0  
  },  
  "tx_bytes": {  
    "total": 8610134,  
    "multicast_broadcast": 0  
  },  
  "rx_packets": {  
    "total": 230,  
    "dropped": 0,  
    "multicast_broadcast": 0  
  },  
  "last_update_timestamp": 1454979822860,  
  "endpoint_id": "ba5ba59d-22f1-4a02-b6a0-18ef0e37ef31"  
}
```

NSX-T Data Center 支持 2 层路由模型。

Tier-0 逻辑路由器位于顶层。在北向，Tier-0 逻辑路由器连接到一个或多个物理路由器或第 3 层交换机，并作为物理基础架构的网关。在南向，Tier-0 逻辑路由器连接到一个或多个 Tier-1 逻辑路由器，或直接连接到一个或多个逻辑交换机。

Tier-1 逻辑路由器位于底层。在北向，Tier-1 逻辑路由器连接到 Tier-0 逻辑路由器。在南向，它连接到一个或多个逻辑交换机。

注 如果使用**高级网络和安全**用户界面来修改策略“略界”面中创建的对象，则某些设置可能无法配置。这些只读设置的旁边有此图标：⊖。有关详细信息，请参见第 1 章 [NSX Manager 概览](#)。

本章讨论了以下主题：

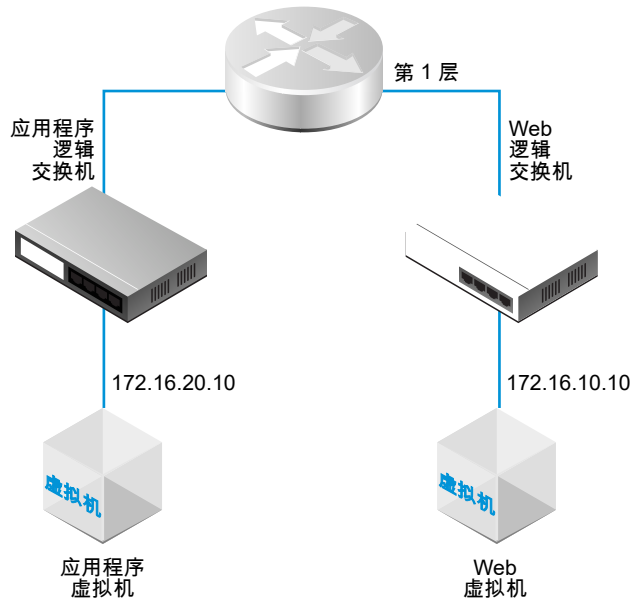
- [Tier-1 逻辑路由器](#)
- [Tier-0 逻辑路由器](#)

Tier-1 逻辑路由器

Tier-1 逻辑路由器具有下行链路端口以连接到逻辑交换机，并具有上行链路端口以连接到 Tier-0 逻辑路由器。

在添加逻辑路由器时，请务必规划要构建的网络拓扑。

图 14-1. Tier-1 逻辑路由器拓扑



例如，该简单拓扑显示两个连接到 Tier-1 逻辑路由器的逻辑交换机。每个逻辑交换机连接了单个虚拟机。两个虚拟机可以位于不同主机集群或同一主机集群中的不同主机或同一主机上。如果逻辑路由器未隔离这些虚拟机，在这些虚拟机上配置的基础 IP 地址必须位于同一子网中。如果逻辑路由器隔离这些虚拟机，这些虚拟机上的 IP 地址必须位于不同的子网中。

在某些场景中，外部客户端发送 ARP 查询以发现绑定到 LB VIP 端口的 MAC 地址。但是，LB VIP 端口没有 MAC 地址，无法处理此类查询。在 Tier-1 逻辑路由器的集中式服务端口上实施代理 ARP 以代表 LB VIP 端口处理 ARP 查询。

在为 Tier-1 逻辑路由器配置 DNAT、Edge 防火墙和负载均衡器时，将按以下顺序处理与另一个 Tier-1 逻辑路由器之间的流量：DNAT、Edge 防火墙和负载均衡器。先通过 DNAT 处理 Tier-1 逻辑路由器中的流量，然后进行负载均衡器处理。将跳过 Edge 防火墙处理。

在 Tier-0 或 Tier-1 逻辑路由器上，您可以配置不同类型的端口。一种类型称为集中式服务端口 (Centralized Service Port, CSP)。您必须在 Tier-1 逻辑路由器或处于活动-备用模式的 Tier-0 逻辑路由器上配置 CSP 以连接到 VLAN 支持的逻辑交换机，或者创建单独的 Tier-1 逻辑路由器。CSP 在 Tier-1 逻辑路由器或处于活动-备用模式的 Tier-0 逻辑路由器上支持以下服务：

- NAT
- 负载均衡
- 有状态防火墙
- VPN (IPsec 和 L2VPN)

创建 Tier-1 逻辑路由器

必须将 Tier-1 逻辑路由器连接到 Tier-0 逻辑路由器以进行北向物理路由器访问。

前提条件

- 确认配置了逻辑交换机。请参见[创建逻辑交换机](#)。
- 确认部署了一个 NSX Edge 群集以执行网络地址转换 (NAT) 配置。请参见 [NSX-T Data Center 安装指南](#)。
- 熟悉 Tier-1 逻辑路由器拓扑。请参见 [Tier-1 逻辑路由器](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择 **高级网络和安全 > 路由器 > 路由器 > 添加**。
- 3 选择 **Tier-1 路由器**并输入逻辑路由器的名称和可选描述。
- 4 （可选）选择一个 Tier-0 逻辑路由器以连接到该 Tier-1 逻辑路由器。

如果尚未配置任何 Tier-0 逻辑路由器，您可以将该字段暂时保留空白，以后再编辑路由器配置。

- 5 （可选）选择一个 NSX Edge 群集。

要取消选择选定的群集，请单击 **x** 图标。如果将 Tier-1 逻辑路由器用于 NAT 配置，则必须将其连接到一个 NSX Edge 群集。如果尚未配置任何 NSX Edge 群集，则可以将该字段暂时留空，以后再编辑路由器配置。

- 6 （可选）单击**备用重新放置**开关以启用或禁用备用重新放置。

备用重新放置意味着，如果运行活动或备用逻辑路由器的 Edge 节点发生故障，则会在另一个 Edge 节点上创建新的备用逻辑路由器以保持高可用性。如果发生故障的 Edge 节点正在运行活动逻辑路由器，原始备用逻辑路由器将变为活动逻辑路由器，并创建新的备用逻辑路由器。如果发生故障的 Edge 节点正在运行备用逻辑路由器，新的备用逻辑路由器将替换该路由器。

- 7 （可选）如果选择了 NSX Edge 群集，则选择故障切换模式。

选项	说明
主动	如果首选节点发生故障并恢复，它将取代对等节点并变为活动节点。对等节点将其状态更改为备用。这是默认选项。
非主动	如果首选节点发生故障并恢复，它将检查对等节点是否为活动节点。如果是，首选节点不会取代对等节点并作为备用节点。

- 8 （可选）单击**高级选项卡**，然后输入 **Tier-1 内转换子网**的值。

- 9 单击**添加**。

结果

在创建逻辑路由器后，如果要从路由器的配置中移除 Edge 群集，请执行以下步骤：

- 单击路由器的名称以查看配置详细信息。

- 选择**服务 > Edge 防火墙**。
- 单击**禁用防火墙**。
- 单击**概览**选项卡，然后单击**编辑**。
- 在 **Edge 群集** 字段中，单击 **x** 图标。
- 单击**保存**。

如果该逻辑路由器支持的虚拟机超过 5000 个，则必须在 NSX Edge 群集的每个节点上运行以下命令以增加 ARP 表的大小。

```
set debug-mode
set dataplane neighbor max-arp-logical-router 10000
```

您必须在数据层面重新启动或节点重新引导后重新运行这些命令，因为更改不是永久性的。

后续步骤

为 Tier-1 逻辑路由器创建下行链路端口。请参见在 [Tier-1 逻辑路由器上添加下行链路端口](#)。

在 Tier-1 逻辑路由器上添加下行链路端口

在 Tier-1 逻辑路由器上创建下行链路端口时，该端口将作为同一子网中的虚拟机的默认网关。

前提条件

确认配置了一个 Tier-1 逻辑路由器。请参见[创建 Tier-1 逻辑路由器](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**高级网络和安全 > 网络 > 路由器**。
- 3 单击路由器的名称。
- 4 单击**配置**选项卡，然后选择**路由器端口**。
- 5 单击**添加**。
- 6 输入路由器端口的名称和可选描述。
- 7 在**类型**字段中，选择**下行链路**。
- 8 对于 **URPF 模式**，选择**严格**或**无**。
URPF（单播反向路径转发）是一项安全功能。
- 9 （可选）选择逻辑交换机。
- 10 选择该连接是创建交换机端口还是更新现有的交换机端口。
如果该连接用于现有的交换机端口，请从下拉菜单中选择该端口。
- 11 以 CIDR 表示法输入路由器端口 IP 地址。
例如，IP 地址可以是 172.16.10.1/24。

12 （可选）选择 DHCP 中继服务。

13 单击**添加**。

后续步骤

启用路由通告以在虚拟机和外部物理网络之间或连接到同一 Tier-0 逻辑路由器的不同 Tier-1 逻辑路由器之间提供南北向连接。请参见在 [Tier-1 逻辑路由器上配置路由通告](#)。

在 Tier-0 或 Tier-1 逻辑路由器上添加 VLAN 端口

如果只有 VLAN 支持的逻辑交换机，则可以将这些交换机连接到 Tier-0 或 Tier-1 路由器上的 VLAN 端口，以便 NSX-T Data Center 可以提供第 3 层服务。

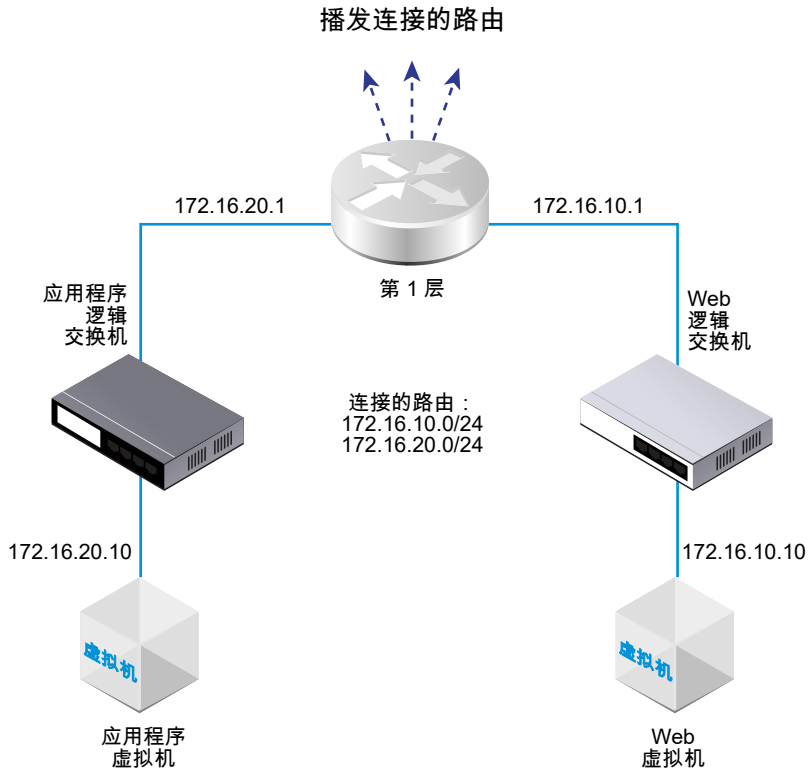
步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**高级网络和安全 > 网络 > 路由器**。
- 3 单击路由器的名称。
- 4 单击**配置**选项卡，然后选择**路由器端口**。
- 5 单击**添加**。
- 6 输入路由器端口的名称和可选描述。
- 7 在**类型**字段中，选择**集中式**。
- 8 对于 **URPF 模式**，选择**严格**或**无**。
URPF（单播反向路径转发）是一项安全功能。
- 9 （必选）选择逻辑交换机。
- 10 选择该连接是创建交换机端口还是更新现有的交换机端口。
如果该连接用于现有的交换机端口，请从下拉菜单中选择该端口。
- 11 以 CIDR 表示法输入路由器端口 IP 地址。
- 12 单击**添加**。

在 Tier-1 逻辑路由器上配置路由通告

要在连接到不同的 Tier-1 逻辑路由器的逻辑交换机连接的虚拟机之间提供第 3 层连接，必须允许将 Tier-1 路由通告到 Tier-0。您不需要在 Tier-1 和 Tier-0 逻辑路由器之间配置路由协议或静态路由。在启用路由通告时，NSX-T Data Center 自动创建 NSX-T Data Center 静态路由。

例如，要通过其他对等路由器提供与虚拟机之间的连接，Tier-1 逻辑路由器必须为连接的路由配置路由通告。如果不希望通告所有直连路由，您可以指定要通告的路由。



前提条件

- 确认虚拟机已连接到逻辑交换机。请参见第 13 章 逻辑交换机。
- 确认配置了 Tier-1 逻辑路由器的下行链路端口。请参见在 Tier-1 逻辑路由器上添加下行链路端口。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择高级网络和安全 > 网络 > 路由器。
- 3 单击 Tier-1 路由器的名称。
- 4 从路由下拉菜单中选择路由通告。
- 5 单击编辑以编辑路由通告配置。

可以切换以下开关：

- 状态
- 通告所有 NSX 连接的路由
- 通告所有 NAT 路由
- 通告所有静态路由
- 通告所有 LB VIP 路由
- 通告所有 LB SNAT IP 路由

- 通告所有 DNS 转发器路由

- a 单击**保存**。

6 单击**添加**以通告路由。

- a 输入名称和可选的说明。

- b 以 CIDR 格式输入路由前缀。

- c 单击**应用筛选器**以设置以下选项：

操作	指定 允许 或 拒绝 。
匹配路由类型	选择一个或多个以下选项： <ul style="list-style-type: none"> ■ 任意 ■ NSX 已连接 ■ Tier-1 LB VIP ■ 静态 ■ Tier-1 NAT ■ Tier-1 LB SNAT
前缀运算符	选择 GE 或 EQ 。

- d 单击**添加**。

后续步骤

熟悉 Tier-0 逻辑路由器拓扑并创建 Tier-0 逻辑路由器。请参见 [Tier-0 逻辑路由器](#)。

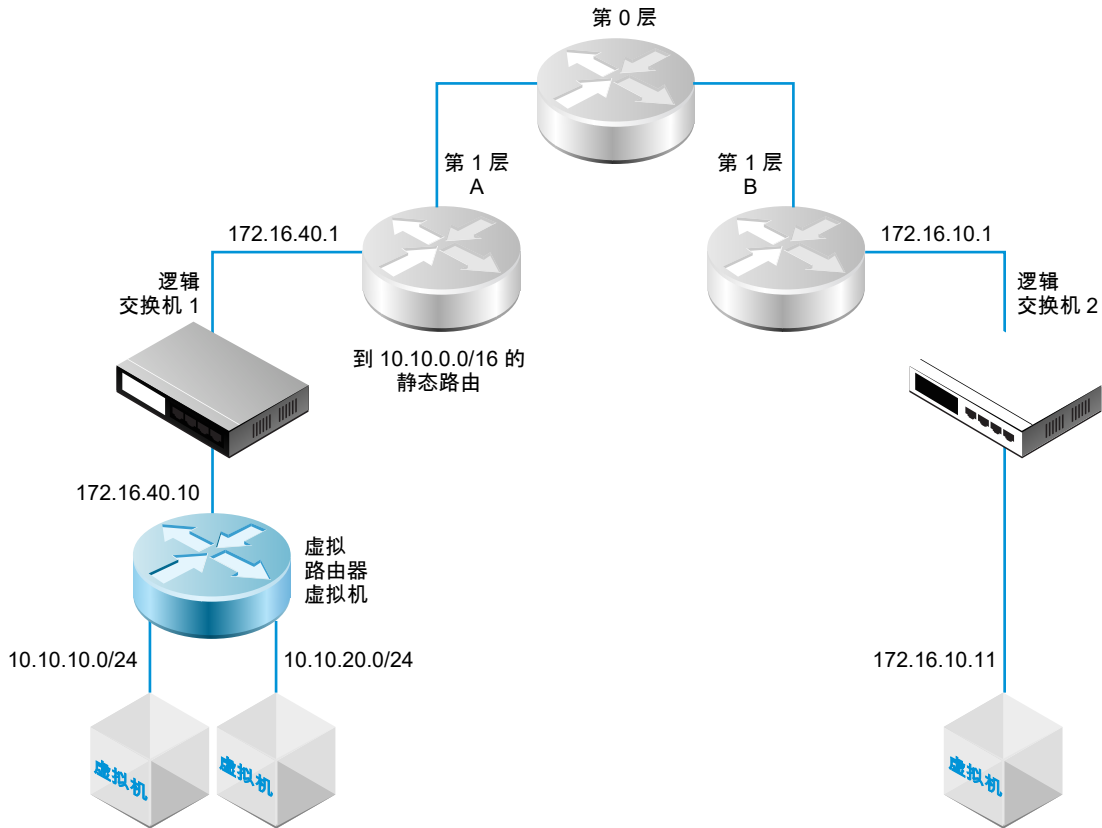
如果已将一个 Tier-0 逻辑路由器连接到 Tier-1 逻辑路由器，您可以验证该 Tier-0 路由器是否发现 Tier-1 路由器连接的路由。请参见[验证 Tier-0 路由器是否学习来自 Tier-1 路由器的路由](#)。

配置 Tier-1 逻辑路由器静态路由

您可以在 Tier-1 逻辑路由器上配置静态路由，以提供从 NSX-T Data Center 到一组可通过虚拟路由器访问的网络的连接。

例如，在下图中，Tier-1 A 逻辑路由器具有到 NSX-T Data Center 逻辑交换机的下行链路端口。该下行链路端口 (172.16.40.1) 为虚拟路由器虚拟机提供默认网关。虚拟路由器虚拟机和 Tier-1 A 通过相同 NSX-T Data Center 逻辑交换机连接在一起。Tier-1 逻辑路由器具有静态路由 10.10.0.0/16，它汇总了通过虚拟路由器访问的网络。Tier-1 A 配置了路由通告以将静态路由通告到 Tier-1 B。

图 14-2. Tier-1 逻辑路由器静态路由拓扑



支持递归静态路由。

前提条件

确认配置了一个下行链路端口。请参见在 [Tier-1 逻辑路由器上添加下行链路端口](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择高级网络和安全 > 网络 > 路由器。
- 3 单击 Tier-1 路由器的名称。
- 4 单击路由选项卡，然后从下拉菜单中选择静态路由。
- 5 单击添加。
- 6 以 CIDR 格式输入一个网络地址。

支持基于 IPv6 的静态路由。IPv6 前缀只能有 IPv6 下一跃点。

例如，10.10.10.0/16 或 IPv6 地址。

- 7 单击添加以添加一个下一跃点 IP 地址。

例如，172.16.40.10。也可以单击铅笔图标，然后从下拉菜单中选择空以指定空路由。要添加另一个下一跃点地址，请再次单击添加。

8 单击对话框底部的**添加**。

将在该行中显示新创建的静态路由网络地址。

9 从 Tier-1 逻辑路由器中，选择**路由 > 路由通告**。**10** 单击**编辑**，然后选择**通告所有静态路由**。**11** 单击**保存**。

将在 NSX-T Data Center 覆盖网络中传播静态路由。

创建独立 Tier-1 逻辑路由器

独立 Tier-1 逻辑路由器无下行链路，也不连接到 Tier-0 路由器。它具有服务路由器，但没有分布式路由器。可以将服务路由器部署在一个 NSX Edge 节点上，也可以在主动-备用模式下部署在两个 NSX Edge 节点上。

独立 Tier-1 逻辑路由器：

- 不能连接到 Tier-0 逻辑路由器。
- 不能有以下行链路。
- （如果用于连接负载均衡器 (LB) 服务）只能有一个集中式服务端口 (CSP)。
- 可以连接到覆盖网络逻辑交换机或 VLAN 逻辑交换机。
- 支持 IPSec、DNAT、防火墙、负载均衡器和服务插入的任意组合。对于输入，处理顺序为：IPSec - DNAT - 防火墙 - 负载均衡器 - 服务插入。对于输出，处理顺序为：服务插入 - 负载均衡器 - 防火墙 - DNAT - IPSec。

通常，独立 Tier-1 逻辑路由器连接到常规 Tier-1 逻辑路由器所连接到的逻辑交换机。配置静态路由和路由通告后，独立 Tier-1 逻辑路由器可以通过常规 Tier-1 逻辑路由器与其他设备通信。

使用独立 Tier-1 逻辑路由器之前，请注意以下事项：

- 要为独立 Tier-1 逻辑路由器指定默认网关，必须添加静态路由。子网应为 0.0.0.0/0 且下一跃点为连接到同一交换机的常规 Tier-1 路由器的 IP 地址。
- 支持独立路由器上的 ARP 代理。您可以在 CSP 的子网中配置 LB 虚拟服务器 IP 或 LB SNAT IP。例如，如果 CSP IP 为 1.1.1.1/24，则虚拟 IP 可能为 1.1.1.2。如果已正确配置路由，虚拟 IP 也可能为另一个子网中的 IP（如 2.2.2.2），以便 2.2.2.2 的流量可以到达独立路由器。
- 对于 NSX Edge 虚拟机，不能有多个 CSP 连接到同一个 VLAN 支持的逻辑交换机或具有相同 VLAN ID 的 VLAN 支持的不同逻辑交换机。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**高级网络和安全 > 路由器 > 路由器 > 添加**。
- 3 选择 **Tier-1 路由器**并输入逻辑路由器的名称和可选描述。
- 4 （必选） 选择一个 NSX Edge 群集以连接到该 Tier-1 逻辑路由器。

5 （必选）选择故障切换模式和群集成员。

选项	说明
主动	如果首选节点发生故障并恢复，它将取代对等节点并变为活动节点。对等节点将其状态更改为备用。这是默认选项。
非主动	如果首选节点发生故障并恢复，它将检查对等节点是否为活动节点。如果是，首选节点不会取代对等节点并作为备用节点。

6 单击**添加**。

7 单击刚创建的路由器的名称。

8 单击**配置**选项卡，然后选择**路由器端口**。

9 单击**添加**。

10 输入路由器端口的名称和可选描述。

11 在**类型**字段中，选择**集中式**。

12 对于 **URPF 模式**，选择**严格**或**无**。

URPF（单播反向路径转发）是一项安全功能。

13 （必选）选择逻辑交换机。

14 选择该连接是创建交换机端口还是更新现有的交换机端口。

15 以 CIDR 表示法输入路由器端口 IP 地址。

16 单击**添加**。

Tier-0 逻辑路由器

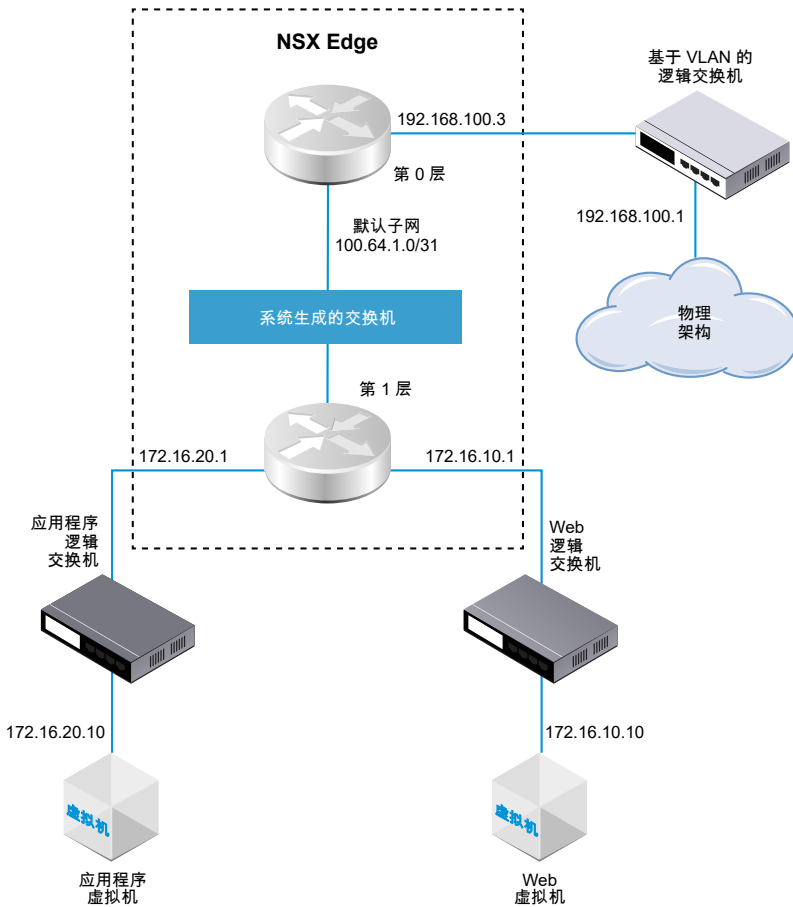
Tier-0 逻辑路由器在逻辑和物理网络之间提供网关服务。

NSX Cloud 说明 如果使用 NSX Cloud，请参见 [NSX Cloud 支持的 NSX-T Data Center 功能](#) 以查看自动生成的逻辑实体、支持的功能以及 NSX Cloud 所需的配置的列表。

Edge 节点只能支持一个 Tier-0 网关或逻辑路由器。在创建 Tier-0 网关或逻辑路由器时，请确保您创建的 Tier-0 网关或逻辑路由器没有超过 NSX Edge 集群中的 Edge 节点数。

在添加 Tier-0 逻辑路由器时，请务必规划要构建的网络拓扑。

图 14-3. Tier-0 逻辑路由器拓扑



为了简单起见，示例拓扑显示单个 Tier-1 逻辑路由器，它连接到在单个 NSX Edge 节点上托管的单个 Tier-0 逻辑路由器。请记住，这不是建议的拓扑。理想情况下，您应该使用至少两个 NSX Edge 节点以充分利用逻辑路由器设计。

Tier-1 逻辑路由器具有一个 Web 逻辑交换机和一个应用程序逻辑交换机，并且它们连接了相应的虚拟机。在将 Tier-1 路由器连接到 Tier-0 路由器时，将在 Tier-1 路由器和 Tier-0 路由器之间自动创建路由器-链路交换机。因此，该交换机标记为系统生成的交换机。

在某些情况下，外部客户端发送绑定到环回或 IKE IP 端口的 MAC 地址的 ARP 查询。但是，环回和 IKE IP 端口没有 MAC 地址，无法处理此类查询。在 Tier-0 逻辑路由器的上行链路和集中式服务端口上实施代理 ARP，以便代表环回和 IKE IP 端口处理 ARP 查询。

在为 Tier-0 逻辑路由器配置 DNAT、IPsec 和 Edge 防火墙时，将按以下顺序处理流量：IPsec、DNAT 和 Edge 防火墙。

在 Tier-0 或 Tier-1 逻辑路由器上，您可以配置不同类型的端口。一种类型称为集中式服务端口 (Centralized Service Port, CSP)。您必须在 Tier-1 逻辑路由器或处于活动-备用模式的 Tier-0 逻辑路由器上配置 CSP 以连接到 VLAN 支持的逻辑交换机，或者创建单独的 Tier-1 逻辑路由器。CSP 在 Tier-1 逻辑路由器或处于活动-备用模式的 Tier-0 逻辑路由器上支持以下服务：

- NAT

- 负载均衡
- 有状态防火墙
- VPN (IPsec 和 L2VPN)

创建 Tier-0 逻辑路由器

Tier-0 逻辑路由器具有下行链路端口以连接到 NSX-T Data Center Tier-1 逻辑路由器，并具有上行链路端口以连接到外部网络。

前提条件

- 确认安装了至少一个 NSX Edge。请参阅《NSX-T Data Center 安装指南》。
- 确认配置了一个 NSX Edge 群集。请参见 NSX-T Data Center 安装指南。
- 熟悉 Tier-0 逻辑路由器的网络拓扑。请参见 [Tier-0 逻辑路由器](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 选择**高级网络和安全** > **路由器** > **路由器** > **添加**。
- 3 从下拉菜单中选择 **Tier-0 路由器**。
- 4 指定 Tier-0 逻辑路由器的名称。
- 5 从下拉菜单中选择一个现有的 NSX Edge 群集以支持该 Tier-0 逻辑路由器。
- 6 （可选）选择一种高可用性模式。

默认情况下，将使用活动-活动模式。在活动-活动模式下，将在所有成员之间进行流量负载平衡。在活动-备用模式下，将由选举的活动成员处理所有流量。如果活动成员发生故障，将选举新的成员以作为活动成员。

- 7 （可选）单击**高级**选项卡以输入一个子网以作为 Tier-0 内中转子网。

这是将 Tier-0 服务路由器连接到其分布式路由器的子网。如果将该字段保留空白，则使用默认 169.0.0.0/28 子网。

- 8 （可选）单击**高级**选项卡以输入一个子网以作为 Tier-0 到 Tier-1 的中转子网。

这是将 Tier-0 路由器连接到该 Tier-0 路由器连接的任何 Tier-1 路由器的子网。如果将该字段保留空白，则为这些 Tier-0 到 Tier-1 的连接分配的默认地址空间为 100.64.0.0/16。将在 100.64.0.0/16 地址空间中为每个 Tier-0 到 Tier-1 的对等连接提供一个 /31 子网。

- 9 单击**保存**。

新的 Tier-0 逻辑路由器将显示为一个链接。

- 10 （可选）单击 Tier-0 逻辑路由器链接以查看摘要。

后续步骤

将 Tier-1 逻辑路由器连接到该 Tier-0 逻辑路由器。

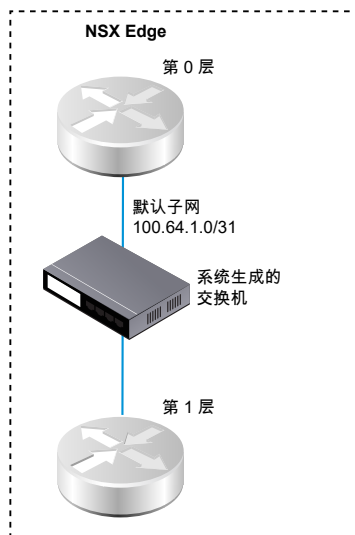
配置 Tier-0 逻辑路由器以将其连接到 VLAN 逻辑交换机，以便创建到外部网络的上行链路。请参见[将 Tier-0 逻辑路由器连接到 NSX Edge 上行链路的 VLAN 逻辑交换机](#)。

连接 Tier-0 和 Tier-1

您可以将 Tier-0 逻辑路由器连接到 Tier-1 逻辑路由器，以便 Tier-1 逻辑路由器具有北向和东西向网络连接。

在将 Tier-1 逻辑路由器连接到 Tier-0 逻辑路由器时，将在两个路由器之间创建路由器-链路交换机。该交换机在拓扑中标记为系统生成的交换机。为这些 Tier-0 到 Tier-1 的连接分配的默认地址空间为 100.64.0.0/16。将在 100.64.0.0/16 地址空间中为每个 Tier-0 到 Tier-1 的对等连接提供一个 /31 子网。您可以选择在 Tier-0 **摘要 > 高级配置** 中配置地址空间。

下图显示了一个示例拓扑。



步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**高级网络和安全 > 网络 > 路由器**。
- 3 选择 Tier-1 逻辑路由器。
- 4 从**摘要**选项卡中，单击**编辑**。
- 5 从下拉菜单中选择 Tier-0 逻辑路由器。
- 6 （可选）从下拉菜单中选择一个 NSX Edge 群集。

如果要将 Tier-1 路由器用于服务（如 NAT），则需要使用 Edge 设备支持该路由器。如果未选择 NSX Edge 群集，则 Tier-1 路由器无法执行 NAT。

- 7 指定成员和首选成员。

如果选择一个 NSX Edge 群集并将成员和首选成员字段留空，NSX-T Data Center 将从指定的群集中设置支持 Edge 设备。

- 8 单击**保存**。

- 9 单击 Tier-1 路由器的**配置**选项卡，以验证是否创建了新的点对点链接端口 IP 地址。

例如，链接端口的 IP 地址可能是 100.64.1.1/31。

- 10 从导航面板中选择 Tier-O 逻辑路由器。

- 11 单击 Tier-O 路由器的**配置**选项卡，以验证是否创建了新的点对点链接端口 IP 地址。

例如，链接端口的 IP 地址可能是 100.64.1.1/31。

后续步骤

验证 Tier-O 路由器是否发现 Tier-1 路由器通告的路由。

验证 Tier-O 路由器是否学习来自 Tier-1 路由器的路由

在 Tier-1 逻辑路由器将路由通告到 Tier-O 逻辑路由器时，这些路由将在 Tier-O 路由器的路由表中列出为 NSX-T Data Center 静态路由。

步骤

- 1 在 NSX Edge 上，运行 `get logical-routers` 命令以查找 Tier-O 服务路由器的 VRF 编号。

```
nsx-edge-1> get logical-routers
Logical Router
UUID          : 736a80e3-23f6-5a2d-81d6-bbefb2786666
vrf           : 0
type          : TUNNEL

Logical Router
UUID          : 421a2d0d-f423-46f1-93a1-2f9e366176c8
vrf           : 5
type          : SERVICE_ROUTER_TIER0

Logical Router
UUID          : f3ce9d7d-7123-47d6-aba6-45cf1388ca7b
vrf           : 6
type          : DISTRIBUTED_ROUTER

Logical Router
UUID          : c8e64eff-02b2-4462-94ff-89f3788f1a61
vrf           : 7
type          : SERVICE_ROUTER_TIER1

Logical Router
UUID          : fb6c3f1f-599f-4421-af8a-99692dff3dd4
vrf           : 8
type          : DISTRIBUTED_ROUTER
```

- 2 运行 `vrf <number>` 命令以进入 Tier-0 服务路由器上下文。

```
nsx-edge-1> vrf 5
nsx-edge1(tier0_sr)>
```

- 3 在 Tier-0 服务路由器上，运行 `get route` 命令并确保在路由表中显示预期的路由。

请注意，NSX-T Data Center 静态路由 (ns) 是 Tier-0 路由器学习的，因为 Tier-1 路由器正在通告路由。

```
nsx-edge1(tier0_sr)> get route

Flags: c - connected, s - static, b - BGP, ns - nsx_static
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT

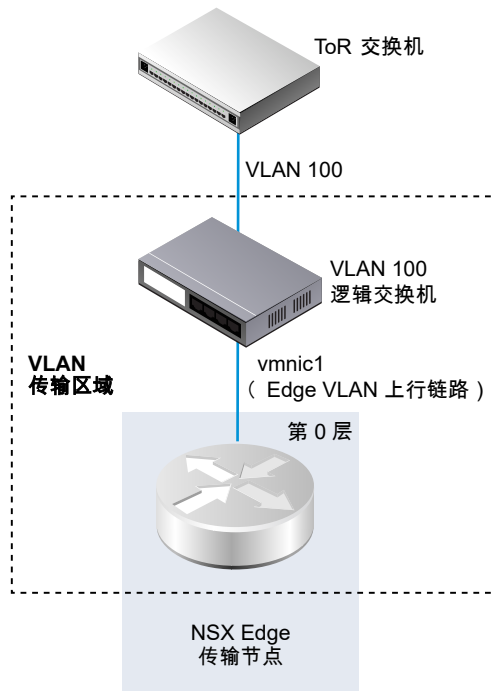
Total number of routes: 7

b    10.10.10.0/24      [20/0]      via 192.168.100.254
rl   100.91.176.0/31   [0/0]      via 169.254.0.1
c    169.254.0.0/28    [0/0]      via 169.254.0.2
ns   172.16.10.0/24    [3/3]      via 169.254.0.1
ns   172.16.20.0/24    [3/3]      via 169.254.0.1
c    192.168.100.0/24  [0/0]      via 192.168.100.2
```

将 Tier-0 逻辑路由器连接到 NSX Edge 上行链路的 VLAN 逻辑交换机

要创建 NSX Edge 上行链路，请将 Tier-0 路由器连接到 VLAN 交换机。

以下简单拓扑显示 VLAN 传输区域中的 VLAN 逻辑交换机。VLAN 逻辑交换机具有一个 VLAN ID，它与 Edge 的 VLAN 上行链路的 ToR 端口上的 VLAN ID 相匹配。



前提条件

创建一个 VLAN 逻辑交换机。请参见为 [NSX Edge 上行链路创建 VLAN 逻辑交换机](#)。

创建一个 Tier-0 路由器。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择高级网络和安全 > 网络 > 路由器。
- 3 选择 Tier-0 逻辑路由器。
- 4 从配置选项卡中，添加一个新的逻辑路由器端口。
- 5 键入该端口的名称，例如，uplink。
- 6 选择上行链路类型。
- 7 选择一个 Edge 传输节点。
- 8 选择一个 VLAN 逻辑交换机。
- 9 以 CIDR 格式键入与 ToR 交换机上连接的端口位于同一子网中的 IP 地址。

结果

将为 Tier-0 路由器添加一个新的上行链路端口。

后续步骤

配置 BGP 或静态路由。

验证 Tier-0 逻辑路由器和 TOR 连接

要使路由在 Tier-0 路由器的上行链路上正常工作，必须建立到架顶式设备的连接。

前提条件

- 确认 Tier-0 逻辑路由器连接到 VLAN 逻辑交换机。请参见将 [Tier-0 逻辑路由器连接到 NSX Edge 上行链路的 VLAN 逻辑交换机](#)。

步骤

- 1 登录到 NSX Manager CLI。
- 2 在 NSX Edge 上，运行 `get logical-routers` 命令以查找 Tier-0 服务路由器的 VRF 编号。

```
nsx-edge-1> get logical-routers
Logical Router
UUID          : 736a80e3-23f6-5a2d-81d6-bbfeb2786666
vrf           : 0
type          : TUNNEL

Logical Router
UUID          : 421a2d0d-f423-46f1-93a1-2f9e366176c8
vrf : 5
type          : SERVICE_ROUTER_TIER0

Logical Router
UUID          : f3ce9d7d-7123-47d6-aba6-45cf1388ca7b
vrf           : 6
type          : DISTRIBUTED_ROUTER

Logical Router
UUID          : c8e64eff-02b2-4462-94ff-89f3788f1a61
vrf           : 7
type          : SERVICE_ROUTER_TIER1

Logical Router
UUID          : fb6c3f1f-599f-4421-af8a-99692dff3dd4
vrf           : 8
type          : DISTRIBUTED_ROUTER
```

- 3 运行 `vrf <number>` 命令以进入 Tier-0 服务路由器上下文。

```
nsx-edge-1> vrf 5
nsx-edge1(tier0_sr)>
```

4 在 Tier-0 服务路由器上，运行 `get route` 命令并确保在路由表中显示预期的路由。

请注意，到 TOR 的路由显示为 **connected (c)**。

```
nsx-edge1(tier0_sr)> get route

Flags: c - connected, s - static, b - BGP, ns - nsx_static
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT

Total number of routes: 7

b    10.10.10.0/24      [20/0]      via 192.168.100.254
rl   100.91.176.0/31   [0/0]      via 169.254.0.1
c    169.254.0.0/28    [0/0]      via 169.254.0.2
ns   172.16.10.0/24    [3/3]      via 169.254.0.1
ns   172.16.20.0/24    [3/3]      via 169.254.0.1
c    192.168.100.0/24  [0/0]      via 192.168.100.2
```

5 对 TOR 执行 ping 操作。

```
nsx-edge1(tier0_sr)> ping 192.168.100.254
PING 192.168.100.254 (192.168.100.254): 56 data bytes
64 bytes from 192.168.100.254: icmp_seq=0 ttl=64 time=2.822 ms
64 bytes from 192.168.100.254: icmp_seq=1 ttl=64 time=1.393 ms
^C
nsx-edge1>
--- 192.168.100.254 ping statistics ---
3 packets transmitted, 2 packets received, 33.3% packet loss
round-trip min/avg/max/stddev = 1.393/2.107/2.822/0.715 ms
```

结果

将在 Tier-0 逻辑路由器和物理路由器之间发送数据包以验证连接。

后续步骤

根据您的网络要求，您可以配置静态路由或 BGP。请参见[配置静态路由](#)或在 [Tier-0 逻辑路由器上配置 BGP](#)。

添加环回路由器端口

您可以将环回端口添加到 Tier-0 逻辑路由器中。

环回端口可用于以下用途：

- 路由协议的路由器 ID
- NAT
- BFD

■ 路由协议的源地址

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**高级网络和安全 > 网络 > 路由器**。
- 3 选择 Tier-0 逻辑路由器。
- 4 选择**配置 > 路由器端口**。
- 5 单击**添加**。
- 6 输入名称和可选的说明。
- 7 选择**环回类型**。
- 8 选择一个 Edge 传输节点。
- 9 使用 CIDR 格式输入一个 IP 地址。

结果

将为 Tier-0 路由器添加一个新端口。

在 Tier-0 或 Tier-1 逻辑路由器上添加 VLAN 端口

如果只有 VLAN 支持的逻辑交换机，则可以将这些交换机连接到 Tier-0 或 Tier-1 路由器上的 VLAN 端口，以便 NSX-T Data Center 可以提供第 3 层服务。

步骤

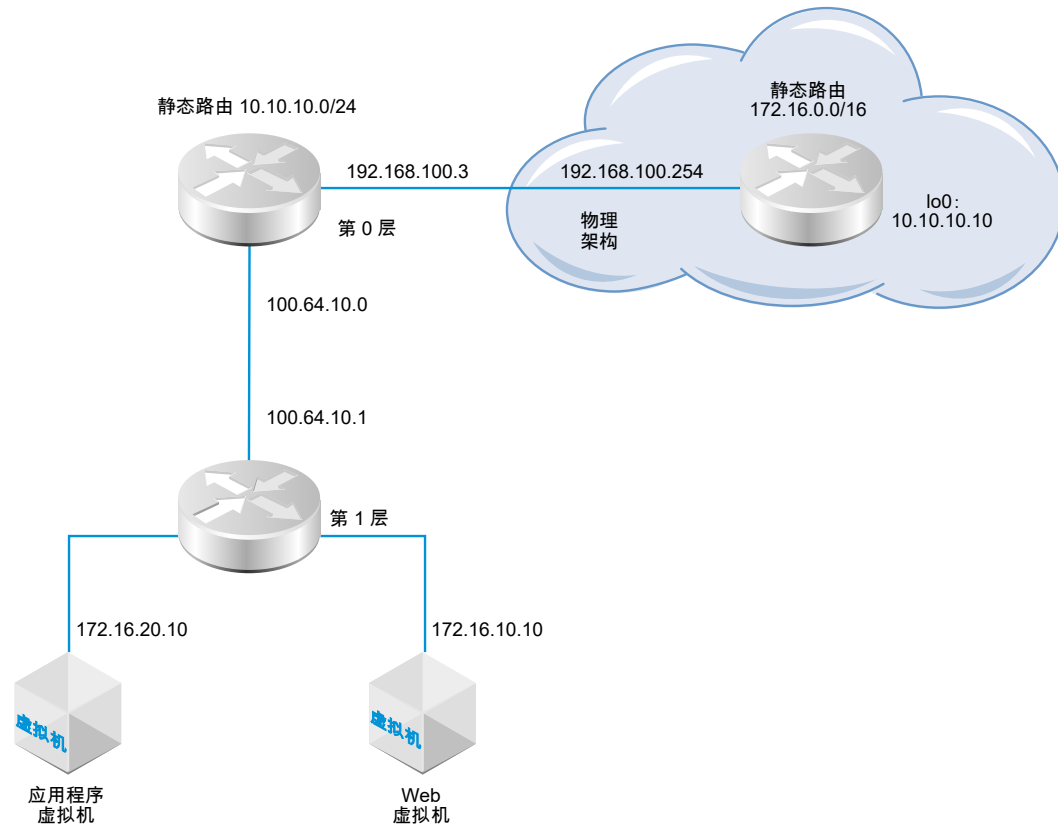
- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**高级网络和安全 > 网络 > 路由器**。
- 3 单击路由器的名称。
- 4 单击**配置**选项卡，然后选择**路由器端口**。
- 5 单击**添加**。
- 6 输入路由器端口的名称和可选描述。
- 7 在**类型**字段中，选择**集中式**。
- 8 对于 **URPF 模式**，选择**严格**或**无**。
URPF（单播反向路径转发）是一项安全功能。
- 9 （必选）选择逻辑交换机。
- 10 选择该连接是创建交换机端口还是更新现有的交换机端口。
如果该连接用于现有的交换机端口，请从下拉菜单中选择该端口。
- 11 以 CIDR 表示法输入路由器端口 IP 地址。
- 12 单击**添加**。

配置静态路由

您可以在 Tier-0 路由器上配置到外部网络的静态路由。在配置静态路由后，不需要将该路由从 Tier-0 通告到 Tier-1，因为 Tier-1 路由器自动具有到它连接的 Tier-0 路由器的静态默认路由。

静态路由拓扑显示一个 Tier-0 逻辑路由器，它具有到物理架构中的 10.10.10.0/24 前缀的静态路由。出于测试目的，在外部路由器环回接口上配置了 10.10.10.10/32 地址。外部路由器具有到 172.16.0.0/16 前缀的静态路由以到达应用程序程序和 Web 虚拟机。

图 14-4. 静态路由拓扑



支持递归静态路由。

前提条件

- 确认连接了物理路由器和 Tier-0 逻辑路由器。请参见验证 [Tier-0 逻辑路由器和 TOR 连接](#)。
- 确认配置了 Tier-1 路由器以通告连接的路由。请参见创建 [Tier-1 逻辑路由器](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择高级网络和安全 > 网络 > 路由器。
- 3 选择 Tier-0 逻辑路由器。
- 4 单击路由选项卡，然后从下拉菜单中选择静态路由。

5 选择**添加**。

6 以 CIDR 格式输入一个网络地址。

例如，10.10.10.0/24。

7 单击**添加 (+)** 以添加下一跃点 IP 地址。

例如，192.168.100.254。也可以单击铅笔图标，然后从下拉菜单中选择**空**以指定空路由。

8 指定管理距离。

9 从下拉列表中选择逻辑路由器端口。

该列表包括 IPSec 虚拟隧道接口 (VTI) 端口。

10 单击**添加**按钮。

后续步骤

检查是否正确配置了静态路由。请参见[验证静态路由](#)。

验证静态路由

可以使用 CLI 验证是否连接了静态路由。您还必须验证外部路由器是否可以 ping 通内部虚拟机，以及内部虚拟机是否可以 ping 通外部路由器。

前提条件

确认配置了一个静态路由。请参见[配置静态路由](#)。

步骤

1 登录到 NSX Manager CLI。

2 确认该静态路由。

a 获取服务路由器 UUID 信息。

```
get logical-routers
```

```
nsx-edge1> get logical-routers
Logical Router
UUID          : 736a80e3-23f6-5a2d-81d6-bbefb2786666
vrf           : 2
type          : TUNNEL

Logical Router
UUID          : d40bbfa4-3e3d-4178-8615-6f42ea335037
vrf           : 4
type          : SERVICE_ROUTER_TIER0

Logical Router
UUID          : d0289ba4-250e-41b4-8ffc-7cab4a46c3e4
vrf           : 5
type          : DISTRIBUTED_ROUTER

Logical Router
UUID          : a6ee6316-2212-4171-99cc-930c98bcad7f
vrf           : 6
type          : DISTRIBUTED_ROUTER
```

b 从输出中找到 UUID 信息。

```
Logical Router
UUID          : d40bbfa4-3e3d-4178-8615-6f42ea335037
vrf           : 4
type          : SERVICE_ROUTER_TIER0
```

c 验证静态路由是否正常工作。

```
get logical-router d40bbfa4-3e3d-4178-8615-6f42ea335037 route static
```

```
Flags: c - connected, s - static, b - BGP, ns - nsx_static
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT

s    10.10.10.0/24      [1/1]      via 192.168.100.254
rl   100.64.1.0/31     [0/0]      via 169.0.0.1
ns   172.16.10.0/24    [3/3]      via 169.0.0.1
ns   172.16.20.0/24    [3/3]      via 169.0.0.1
```

- 3 从外部路由器中，对内部虚拟机执行 ping 操作以确认可通过 NSX-T Data Center 覆盖网络访问这些虚拟机。

- a 连接到外部路由器。

```
ping 172.16.10.10
```

```
PING 172.16.10.10 (172.16.10.10) 56(84) bytes of data.
64 bytes from 172.16.10.10: icmp_req=1 ttl=62 time=127 ms
64 bytes from 172.16.10.10: icmp_req=2 ttl=62 time=1.96 ms
^C
--- 172.16.10.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.966/64.793/127.620/62.827 ms
```

- b 测试网络连接。

```
tracert 172.16.10.10
```

```
tracert to 172.16.10.10 (172.16.10.10), 30 hops max, 60 byte packets
 1  192.168.100.3 (192.168.100.3)  0.640 ms  0.575 ms  0.696 ms
 2  100.64.1.1 (100.64.1.1)  0.656 ms  0.604 ms  0.578 ms
 3  172.16.10.10 (172.16.10.10)  3.397 ms  3.703 ms  3.790 ms
```

- 4 从这些虚拟机中，对外部 IP 地址执行 ping 操作。

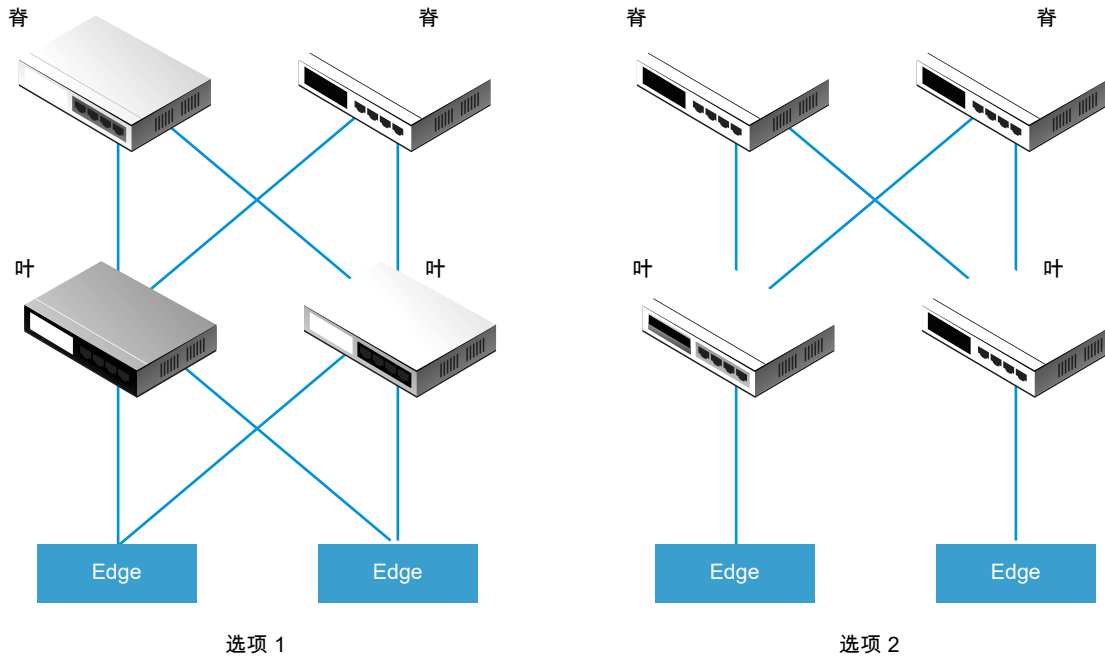
```
ping 10.10.10.10
```

```
PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data.
64 bytes from 10.10.10.10: icmp_req=1 ttl=62 time=119 ms
64 bytes from 10.10.10.10: icmp_req=2 ttl=62 time=1.93 ms
^C
--- 10.10.10.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.936/60.865/119.795/58.930 ms
```

BGP 配置选项

要充分利用 Tier-0 逻辑路由器，必须在 Tier-0 路由器和外部架顶式对等项之间使用 BGP 为拓扑配置冗余和对称性。这种设计有助于确保在链路和节点发生故障时保持连接。

共有两种配置模式：活动-活动和活动-备用。下图显示了对称配置选项。在每个拓扑中显示了两个 NSX Edge 节点。对于活动-活动配置，在创建 Tier-0 上行链路端口时，您可以将每个上行链路端口与最多 8 个 NSX Edge 传输节点相关联。每个 NSX Edge 节点可以具有两个上行链路。



对于选项 1，在配置物理叶节点路由器时，它们应该与 NSX Edge 之间具有 BGP 邻居关系。路由重新分发应包括相同的网络前缀并具有到所有 BGP 邻居的相等 BGP 衡量指标。在 Tier-0 逻辑路由器配置中，所有叶节点路由器应配置为 BGP 邻居。

在配置 Tier-0 路由器的 BGP 邻居时，如果未指定本地地址（源 IP 地址），则将 BGP 邻居配置发送到与 Tier-0 逻辑路由器上行链路关联的所有 NSX Edge 节点。如果配置了本地地址，则将配置发送到上行链路具有该 IP 地址的 NSX Edge 节点。

对于选项 1，如果上行链路位于 NSX Edge 节点上的同一子网中，则可以忽略本地地址。如果 NSX Edge 节点上的上行链路位于不同的子网中，则应该在 Tier-0 路由器的 BGP 邻居配置中指定本地地址以防止将配置发送到所有关联的 NSX Edge 节点。

对于选项 2，请确保 Tier-0 逻辑路由器配置包括 Tier-0 服务路由器的本地 IP 地址。叶节点路由器仅配置了它们作为 BGP 邻居直接连接到的 NSX Edge。

在 Tier-0 逻辑路由器上配置 BGP

为了使虚拟机与外界之间能够相互访问，您可以在 Tier-0 逻辑路由器与物理基础架构中的路由器之间配置外部或内部 BGP (eBGP/iBGP) 连接。

iBGP 功能具有以下功能和限制：

- 支持重新分发、前缀列表和路由映射。
- 不支持路由反射器。
- 不支持 BGP 联盟。

在配置 BGP 时，您必须为 Tier-0 逻辑路由器配置本地自治系统 (Autonomous System, AS) 编号。例如，以下拓扑显示本地 AS 编号为 64510。您还必须配置远程 AS 编号。EBGP 邻居必须直接连接并与 Tier-0 上行链路位于同一子网中。如果它们不在同一子网中，那么应使用 BGP 多点跳跃。

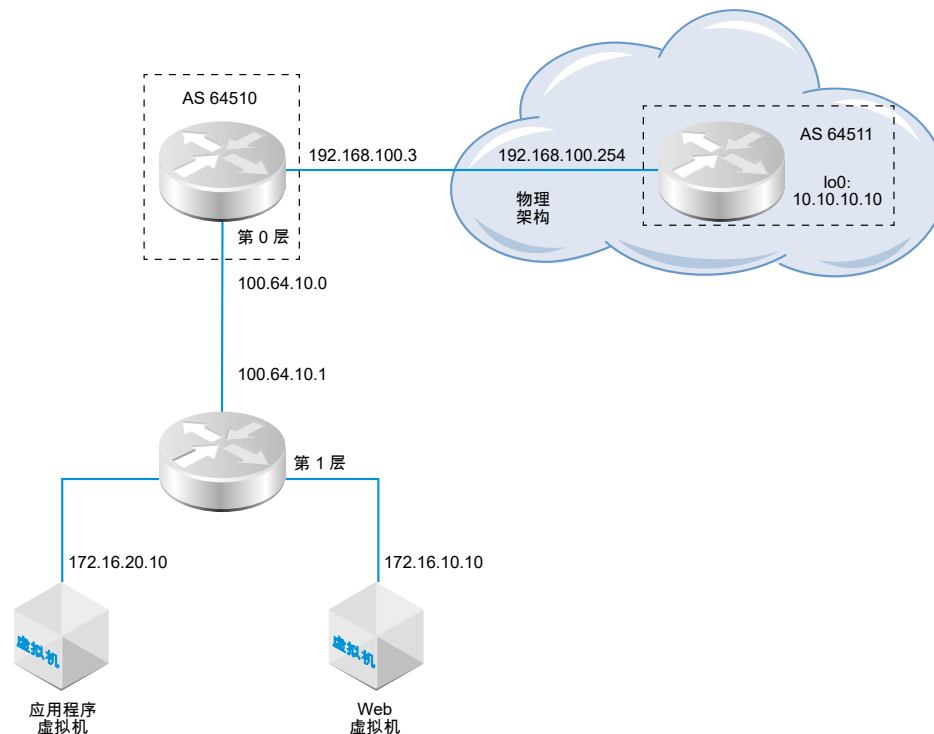
在主动-主动模式下，Tier-0 逻辑路由器支持 SR（服务路由器）间路由。如果路由器 #1 无法与北向物理路由器通信，流量将重新路由到主动-主动群集中的路由器 #2。如果路由器 #2 能够与物理路由器通信，则路由器 #1 与物理路由器之间的流量不会受到影响。

在将处于主动-主动模式的 Tier-0 逻辑路由器连接到处于活动-备用模式的 Tier-1 逻辑路由器的拓扑中，您必须启用“SR 间路由”来处理非对称路由。如果在其中一个 SR 上配置静态路由，或者一个 SR 需要访问另一个 SR 的上行链路，则存在非对称路由。此外，还要注意以下情况：

- 如果在一个 SR 上配置静态路由（例如，Edge 节点 #1 上的 SR #1），而另一个 SR（例如，Edge 节点 #2 上的 SR #2）可能会从 eBGP 对等项中发现相同的路由，并优先使用所发现的路由，而不是使用 SR #1 上的静态路由（可能更高效一些）。要确保 SR #2 使用在 SR #1 上配置的静态路由，请将 Tier-1 逻辑路由器配置为抢占模式，并将 Edge 节点 #1 配置为首选节点。
- 如果 Tier-0 逻辑路由器在 Edge 节点 #1 上使用一个上行链路端口，而在 Edge 节点 #2 上使用另一个上行链路端口，并且这两个上行链路位于不同的子网中，则从租户虚拟机到上行链路的 ping 流量可以正常工作。如果这两个上行链路位于同一子网中，则 ping 流量将失败。

注 将自动从 Tier-0 逻辑路由器的上行链路上配置的 IP 地址中选择用于在 Edge 节点上建立 BGP 会话的路由器 ID。当路由器 ID 变化时，Edge 节点上的 BGP 会话可能会抖动。当删除为路由器 ID 自动选择的 IP 地址时，或者删除分配有此 IP 的逻辑路由器端口时，可能会发生这种情况。

图 14-5. BGP 连接拓扑



当出现涉及 BGP 或 BFD 的连接故障时，请注意以下场景：

- 在仅配置了 BGP 的情况下，如果所有 BGP 邻居均关闭，则服务路由器将处于“关闭”状态。
- 在仅配置了 BFD 的情况下，如果所有 BFD 邻居均关闭，则服务路由器将处于“关闭”状态。

- 在配置了 BGP 和 BFD 的情况下，如果所有 BGP 和 BFD 邻居均关闭，则服务路由器将处于“关闭”状态。
- 在配置了 BGP 和静态路由的情况下，如果所有 BGP 邻居均关闭，则服务路由器将处于“关闭”状态。
- 在仅配置了静态路由的情况下，服务路由器始终处于“打开”状态，除非节点出现故障或处于维护模式。

前提条件

- 确认配置了 Tier-1 路由器以通告连接的路由。请参见在 [Tier-1 逻辑路由器上配置路由通告](#)。严格来说，这并不是 BGP 配置的必备条件，但如果您具有双层拓扑并打算将 Tier-1 网络重新分发到 BGP，则需要执行该步骤。
- 确认配置了一个 Tier-0 路由器。请参见 [创建 Tier-0 逻辑路由器](#)。
- 确保 Tier-0 逻辑路由器已从 Tier-1 逻辑路由器中发现路由。请参见 [验证 Tier-0 路由器是否学习来自 Tier-1 路由器的路由](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择 **高级网络和安全 > 网络 > 路由器**。
- 3 选择 Tier-0 逻辑路由器。
- 4 单击 **路由** 选项卡，然后从下拉菜单中选择 **BGP**。
- 5 单击 **编辑**。
 - a 输入本地 AS 编号。
例如，64.510。
 - b 单击 **状态** 开关以启用或禁用 BGP。
 - c 单击 **ECMP** 开关以启用或禁用 ECMP。
 - d 单击 **平滑重启** 开关以启用或禁用平滑重启。
仅当与 Tier-0 路由器关联的 NSX Edge 群集只有一个 Edge 节点时，才支持平滑重启。
 - e 如果此逻辑路由器未处于主动-主动模式，请单击 **服务路由器间路由** 开关以启用或禁用“服务路由器间路由”。
 - f 配置路由聚合。
 - g 单击 **保存**。
- 6 单击 **添加** 以添加一个 BGP 邻居。
- 7 输入邻居 IP 地址。
例如，192.168.100.254。

- 8 指定最大跃点限制。
默认值为 1。
- 9 输入远程 AS 编号。
例如，64511（eBGP 邻居）或 64510（iBGP 邻居）。
- 10 配置定时器（保持活动状态时间和抑制时间）和密码。
- 11 单击 **本地地址** 选项卡以选择一个本地地址。
a （可选）取消选中 **所有上行链路** 以查看环回端口以及上行链路端口。
- 12 单击 **地址系列** 选项卡以添加一个地址系列。
- 13 单击 **BFD 配置** 选项卡以启用 BFD。
- 14 单击 **保存**。

后续步骤

测试 BGP 是否正常工作。请参见从 [Tier-0 服务路由器中验证 BGP 连接](#)。

从 Tier-0 服务路由器中验证 BGP 连接

可以使用 CLI 从 Tier-0 服务路由器中验证是否建立了到邻居的 BGP 连接。

前提条件

确认配置了 BGP。请参见在 [Tier-0 逻辑路由器上配置 BGP](#)。

步骤

- 1 登录到 NSX Manager CLI。
- 2 在 NSX Edge 上，运行 `get logical-routers` 命令以查找 Tier-0 服务路由器的 VRF 编号。

```
nsx-edge-1> get logical-routers
Logical Router
UUID          : 736a80e3-23f6-5a2d-81d6-bbefb2786666
vrf           : 0
type          : TUNNEL

Logical Router
UUID          : 421a2d0d-f423-46f1-93a1-2f9e366176c8
vrf           : 5
type          : SERVICE_ROUTER_TIER0

Logical Router
UUID          : f3ce9d7d-7123-47d6-aba6-45cf1388ca7b
vrf           : 6
type          : DISTRIBUTED_ROUTER

Logical Router
UUID          : c8e64eff-02b2-4462-94ff-89f3788f1a61
vrf           : 7
```

```

type          : SERVICE_ROUTER_TIER1

Logical Router
UUID          : fb6c3f1f-599f-4421-af8a-99692dff3dd4
vrf           : 8
type          : DISTRIBUTED_ROUTER

```

- 3 运行 `vrf <number>` 命令以进入 Tier-0 服务路由器上下文。

```

nsx-edge-1> vrf 5
nsx-edge1(tier0_sr)>

```

- 4 验证 BGP 状态是否为 Established, up。

```
get bgp neighbor
```

```

BGP neighbor: 192.168.100.254   Remote AS: 64511
BGP state: Established, up
Hold Time: 180s   Keepalive Interval: 60s
Capabilities:
    Route Refresh: advertised and received
    Address Family: IPv4 Unicast:advertised and received
    Graceful Restart: none
    Restart Remaining Time: 0
Messages: 28 received, 31 sent
Minimum time between advertisements: 30s (default)
For Address Family IPv4 Unicast:advertised and received
    Route Refresh: 0 received, 0 sent
    Prefixes: 2 received, 2 sent, 2 advertised
1 Connections established, 2 dropped
Local host: 192.168.100.3, Local port: 179
Remote host: 192.168.100.254, Remote port: 33044

```

后续步骤

从外部路由器中检查 BGP 连接。请参见[验证南北向连接和路由重新分发](#)。

在 Tier-0 逻辑路由器上配置 BFD

BFD（双向转发检测）是一种可以检测转发路径故障的协议。

注 在此版本中，不支持通过虚拟隧道接口 (VTI) 端口执行 BFD。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 选择 **高级网络和安全 > 网络 > 路由器**。
- 3 选择 Tier-0 逻辑路由器。

- 4 单击**路由**选项卡，然后从下拉菜单中选择 **BFD**。
- 5 单击**编辑**以配置 BFD。
- 6 单击**状态**切换按钮以启用 BFD。

您可以选择更改全局 BFD 属性**接收间隔**、**发送间隔**和**声明失效间隔**。

- 7 （可选）在“静态路由下一跃点的 BFD 对等项”下面，单击**添加**以添加一个 BFD 对等项。

指定对等项 IP 地址并将管理状态设置为**已启用**。您可以选择覆盖全局 BFD 属性**接收间隔**、**发送间隔**和**声明失效间隔**。

在 Tier-0 逻辑路由器上启用路由重新分发

在启用路由重新分发时，Tier-0 逻辑路由器开始与其北向路由器共享指定的路由。

前提条件

- 确认连接了 Tier-0 和 Tier-1 逻辑路由器，以便通告 Tier-1 逻辑路由器网络以在 Tier-0 逻辑路由器上重新分发这些网络。请参见[连接 Tier-0 和 Tier-1](#)。
- 如果要从路由重新分发中筛选特定的 IP 地址，请确认配置了路由映射。请参见[创建路由映射](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**高级网络和安全 > 网络 > 路由器**。
- 3 选择 Tier-0 逻辑路由器。
- 4 单击**路由**选项卡，然后从下拉菜单中选择**路由重新分发**。
- 5 单击**编辑**以启用或禁用路由重新分发。

6 单击添加以添加一组路由重新分发条件。

选项	说明
名称和说明	为路由重新分发指定一个名称。您可以选择提供相应的说明。 例如，名称为 advertise-to-bgp-neighbor。
源	选择一个或多个以下源： <ul style="list-style-type: none"> ■ TO 直连 ■ TO 上行链路 ■ TO 下行链路 ■ TO CSP ■ TO 环回 ■ TO 静态 ■ TO NAT ■ TO DNS 转发器 IP ■ TO IPsec 本地 IP ■ T1 直连 ■ T1 CSP ■ T1 下行链路 ■ T1 静态 ■ T1 LB SNAT ■ T1 NAT ■ T1 LB VIP ■ T1 DNS 转发器 IP
路由映射	(可选) 分配路由映射以从路由重新分发中筛选一组 IP 地址。

验证南北向连接和路由重新分发

可以使用 CLI 验证是否发现 BGP 路由。也可以从外部路由器中检查是否可以访问 NSX-T Data Center 连接的虚拟机。

前提条件

- 确认配置了 BGP。请参见在 [Tier-0 逻辑路由器上配置 BGP](#)。
- 确认将 NSX-T Data Center 静态路由设置为要进行重新分发。请参见在 [Tier-0 逻辑路由器上启用路由重新分发](#)。

步骤

- 1 登录到 NSX Manager CLI。
- 2 查看从外部 BGP 邻居中发现的路由。

```
nsx-edge1(tier0_sr)> get route bgp

Flags: c - connected, s - static, b - BGP, ns - nsx_static
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT
```

```
b    10.10.10.0/24          [20/0]          via 192.168.100.254
```

- 3 从外部路由器中，检查是否发现了 BGP 路由，以及是否可以通过 NSX-T Data Center 覆盖网络访问虚拟机。

- a 列出 BGP 路由。

```
user@router# run show ip route bgp
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

B>* 172.16.10.0/24 [20/0] via 192.168.100.2, eth2, 00:00:48
B>* 172.16.20.0/24 [20/0] via 192.168.100.2, eth2, 00:00:48
B>* 172.16.30.0/24 [20/0] via 192.168.100.2, eth2, 00:00:48
```

- b 从外部路由器中，对 NSX-T Data Center 连接的虚拟机执行 ping 操作。

```
ping 172.16.10.10
```

```
PING 172.16.10.10 (172.16.10.10) 56(84) bytes of data.
64 bytes from 172.16.10.10: icmp_req=1 ttl=62 time=127 ms
64 bytes from 172.16.10.10: icmp_req=2 ttl=62 time=1.96 ms
^C
--- 172.16.10.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.966/64.793/127.620/62.827 ms
```

- c 检查通过 NSX-T Data Center 覆盖网络的路径。

```
traceroute 172.16.10.10
```

```
traceroute to 172.16.10.10 (172.16.10.10), 30 hops max, 60 byte packets
 1  192.168.100.3 (192.168.100.3)  0.640 ms  0.575 ms  0.696 ms
 2  100.91.176.1 (100.91.176.1)  0.656 ms  0.604 ms  0.578 ms
 3  172.16.10.10 (172.16.10.10)  3.397 ms  3.703 ms  3.790 ms
```

- 4 从内部虚拟机中，对外部 IP 地址执行 ping 操作。

```
ping 10.10.10.10
```

```
PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data.
64 bytes from 10.10.10.10: icmp_req=1 ttl=62 time=119 ms
64 bytes from 10.10.10.10: icmp_req=2 ttl=62 time=1.93 ms
^C
--- 10.10.10.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.936/60.865/119.795/58.930 ms
```

后续步骤

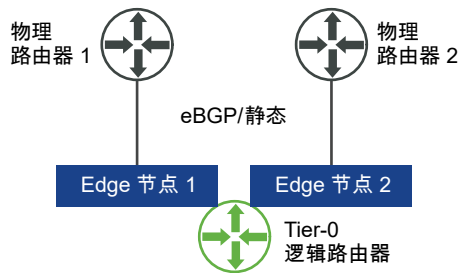
配置额外的路由功能，例如，ECMP。

了解 ECMP 路由

等价多路径 (Equal cost multi-path, ECMP) 路由协议将上行链路添加到 Tier-0 逻辑路由器，并为 NSX Edge 集群中的每个 Edge 节点配置该上行链路以增加南北向通信带宽。ECMP 路由路径用于流量负载均衡并为发生故障的路径提供容错。

Tier-0 逻辑路由器必须处于活动-活动模式才能使用 ECMP。最多支持 8 个 ECMP 路径。NSX Edge 上的 ECMP 实现基于协议号、源和目标地址以及源和目标端口的五元组。用于在 ECMP 路径之间分发数据的算法不是循环的。因此，某些路径可能会比其他路径传输更多流量。请注意，如果协议为 IPv6，并且 IPv6 标头具有多个扩展标头，则 ECMP 将仅基于源和目标地址。

图 14-6. ECMP 路由拓扑



例如，上面的拓扑显示单个处于活动-活动模式的 Tier-0 逻辑路由器在双节点 NSX Edge 集群上运行。配置了两个上行链路端口，在每个 Edge 节点上具有一个端口。

为第二个 Edge 节点添加上行链路端口

在启用 ECMP 之前，您必须配置一个上行链路以将 Tier-0 逻辑路由器连接到 VLAN 逻辑交换机。

前提条件

- 确认配置了一个传输区域和两个传输节点。请参见 [NSX-T Data Center 安装指南](#)。
- 确认配置了两个 Edge 节点和一个 Edge 群集。请参见 [NSX-T Data Center 安装指南](#)。
- 确认具有上行链路的 VLAN 逻辑交换机。请参见 [NSX Edge 上行链路创建 VLAN 逻辑交换机](#)。
- 确认配置了一个 Tier-0 逻辑路由器。请参见 [创建 Tier-0 逻辑路由器](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择 **高级网络和安全 > 网络 > 路由器**。
- 3 选择 Tier-0 逻辑路由器。
- 4 单击 **配置** 选项卡以添加一个路由器端口。
- 5 单击 **添加**。

6 填写路由器端口详细信息。

选项	说明
名称	指定路由器端口的名称。
说明	提供额外的说明以指出该端口用于 ECMP 配置。
类型	接受默认类型上行链路。
MTU	如果将该字段保留空白，则使用默认值 1500。
传输节点	从下拉菜单中分配 Edge 传输节点。
URPF 模式	单播反向路径转发是一项安全功能。如果在 ECMP 模式下具有多个活动-活动 Edge 节点，建议将其设置为无。默认值为严格。
逻辑交换机	从下拉菜单中分配 VLAN 逻辑交换机。
逻辑交换机端口	指定新交换机端口的名称。 也可以使用现有的交换机端口。
IP 地址/掩码	输入与 ToR 交换机上连接的端口位于同一子网中的 IP 地址。

7 单击保存。

结果

将在 Tier-0 路由器和 VLAN 逻辑交换机中添加新的上行链路端口，并在两个 Edge 节点上配置 Tier-0 逻辑路由器。

后续步骤

为第二个邻居创建 BGP 连接并启用 ECMP 路由。请参见[添加第二个 BGP 邻居并启用 ECMP 路由](#)。

添加第二个 BGP 邻居并启用 ECMP 路由

在启用 ECMP 路由之前，您必须添加一个 BGP 邻居并使用新添加的上行链路信息配置该邻居。

前提条件

确认第二个 Edge 节点配置了上行链路端口。请参见[为第二个 Edge 节点添加上行链路端口](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择高级网络和安全 > 网络 > 路由器。
- 3 选择 Tier-0 逻辑路由器。
- 4 单击路由选项卡，然后从下拉菜单中选择 BGP。
- 5 在“邻居”部分下面，单击添加以添加一个 BGP 邻居。
- 6 输入邻居 IP 地址。

例如，192.168.200.254。

- 7 （可选）指定最大跃点限制。

默认值为 1。

- 8 输入远程 AS 编号。

例如，64.511。

- 9 （可选）单击 **本地地址** 选项卡以选择一个本地地址。

- a （可选）取消选中 **所有上行链路** 以查看环回端口以及上行链路端口。

- 10 （可选）单击 **地址系列** 选项卡以添加一个地址系列。

- 11 （可选）单击 **BFD 配置** 选项卡以启用 BFD。

- 12 单击 **保存**。

将显示新添加的 BGP 邻居。

- 13 单击“BGP 配置”部分旁边的 **编辑**。

- 14 单击 **ECMP** 切换按钮以启用 ECMP。

“状态”按钮必须显示为“已启用”。

- 15 单击 **保存**。

结果

多个 ECMP 路由路径将连接到逻辑交换机的虚拟机与 Edge 群集中的两个 Edge 节点相连。

后续步骤

测试 ECMP 路由连接是否正常工作。请参见[验证 ECMP 路由连接](#)。

验证 ECMP 路由连接

可以使用 CLI 验证是否建立了到邻居的 ECMP 路由连接。

前提条件

确认配置了 ECMP 路由。请参见[为第二个 Edge 节点添加上行链路端口](#)和[添加第二个 BGP 邻居并启用 ECMP 路由](#)。

步骤

- 1 登录到 NSX Manager CLI。
- 2 获取分布式路由器 UUID 信息。

```
get logical-routers
```

```
Logical Router
UUID          : 736a80e3-23f6-5a2d-81d6-bbefb2786666
vrf           : 2
type          : TUNNEL
```

```

Logical Router
UUID          : d40bbfa4-3e3d-4178-8615-6f42ea335037
vrf           : 4
type          : SERVICE_ROUTER_TIER0

Logical Router
UUID          : d0289ba4-250e-41b4-8ffc-7cab4a46c3e4
vrf           : 5
type          : DISTRIBUTED_ROUTER

Logical Router
UUID          : a6ee6316-2212-4171-99cc-930c98bcad7f
vrf           : 6
type          : DISTRIBUTED_ROUTER

```

- 3 从输出中找到 UUID 信息。

```

Logical Router
UUID          : d0289ba4-250e-41b4-8ffc-7cab4a46c3e4
vrf           : 5
type          : DISTRIBUTED_ROUTER

```

- 4 键入 Tier-0 分布式路由器的 VRF。

```
vrf 5
```

- 5 验证 Tier-0 分布式路由器是否连接到 Edge 节点。

```
get forwarding
```

例如, edge-node-1 和 edge-node-2。

- 6 输入 **exit** 以退出 vrf 上下文。

- 7 确认已连接 Tier-0 分布式路由器。

```
get logical-router <UUID> route
```

UUID 的路由类型应显示为 NSX_CONNECTED。

- 8 在两个 Edge 节点上启动 SSH 会话。

- 9 启动一个会话以捕获数据包。

```
set capture session 0 interface fp-eth1 dir tx
```

```
set capture session 0 expression src net <IP_Address>
```

- 10 使用可生成从连接到 Tier-0 路由器的源虚拟机到目标虚拟机的流量的任何工具。

- 11 观察两个 Edge 节点上的流量。

创建 IP 前缀列表

IP 前缀列表包含一个或多个分配了访问权限以进行路由通告的 IP 地址。该列表中的 IP 地址是按顺序进行处理的。IP 前缀列表是通过输入或输出方向的 BGP 邻居筛选器或路由映射引用的。

例如，您可以将 IP 地址 192.168.100.3/27 添加到 IP 前缀列表中，并拒绝将路由重新分发到北向路由器。也可以在 IP 地址后面附加小于或等于 (le) 或大于或等于 (ge) 修饰符以允许或限制路由重新分发。例如，192.168.100.3/27 ge 24 le 30 修饰符与长度大于或等于 24 位且小于或等于 30 位的子网掩码相匹配。

注 路由的默认操作为**拒绝**。在创建一个前缀列表以拒绝或允许特定路由时，如果要允许所有其他路由，请务必创建一个无特定网络地址（从下拉列表中选择**任意**）且操作为**允许**的 IP 前缀。

前提条件

确认配置了一个 Tier-0 逻辑路由器。请参见[创建 Tier-0 逻辑路由器](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**高级网络和安全 > 网络 > 路由器**。
- 3 选择 Tier-0 逻辑路由器。
- 4 单击**路由**选项卡，然后从下拉菜单中选择 **IP 前缀列表**。
- 5 单击**添加**。
- 6 输入 IP 前缀列表的名称。
- 7 单击**添加**以指定前缀。
 - a 使用 CIDR 格式输入一个 IP 地址。
例如，192.168.100.3/27。
 - b 从下拉菜单中选择**拒绝**或**允许**。
 - c （可选）在 **le** 或 **ge** 修饰符中设置一定范围的 IP 地址位数。
例如，将 **le** 设置为 30 并将 **ge** 设置为 24。
- 8 重复上述步骤以指定其他前缀。
- 9 单击窗口底部的**添加**。

创建社区属性列表

您可以创建 BGP 社区属性列表，以便基于社区属性列表配置路由映射。

前提条件

确认配置了一个 Tier-0 逻辑路由器。请参见[创建 Tier-0 逻辑路由器](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。

- 2 选择**高级网络和安全 > 网络 > 路由器**。
- 3 选择 Tier-0 逻辑路由器。
- 4 单击**路由**选项卡，然后从下拉菜单中选择**社区属性列表**。
- 5 单击**添加**。
- 6 输入社区属性列表的名称。
- 7 使用 aa:nn 格式指定社区属性（例如 300:500），然后按 Enter 键。重复以上步骤以添加其他社区属性。

此外，您还可以单击下拉箭头并选择以下一个或多个选项：

- NO_EXPORT_SUBCONFED - 不通告到 EBGp 对等项。
- NO_ADVERTISE - 不通告到任何对等项。
- NO_EXPORT - 不通告到外部 BGP 联合。

- 8 单击**添加**。

创建路由映射

路由映射由一系列 IP 前缀列表、BGP 路径属性和关联的操作组成。路由器扫描该序列以查找匹配的 IP 地址。如果找到一个匹配的地址，路由器将执行操作，而不再扫描其他地址。

可以在 BGP 邻居级别和路由重新分发中引用路由映射。如果在路由映射中引用 IP 前缀列表并应用了路由映射允许或拒绝操作，在路由映射序列中指定的操作将覆盖 IP 前缀列表中指定的操作。

前提条件

确认配置了一个 IP 前缀列表。请参见[创建 IP 前缀列表](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**高级网络和安全 > 网络 > 路由器**。
- 3 选择 Tier-0 逻辑路由器。
- 4 选择**路由 > 路由映射**。
- 5 单击**添加**。
- 6 输入路由映射的名称和可选说明。
- 7 单击**添加**以在路由映射中添加一个条目。
- 8 编辑列**匹配 IP 前缀列表/社区属性列表**以选择 IP 前缀列表或社区属性列表，但不能同时选择两者。

9 （可选）设置 BGP 属性。

BGP 属性	说明
AS 路径前置	在路径前面放置一个或多个 AS（自主系统）编号以使路径更长，因此，通常不是首选的路径。
MED	多出口区分符向外部对等项指示 AS 的首选路径。
权重	设置权重以影响路径选择。范围是 0-65535。
社区属性	使用 aa:nn 格式指定社区属性，例如 300:500。或者，使用下拉菜单选择以下选项之一： <ul style="list-style-type: none"> ■ NO_EXPORT_SUBCONFED - 不通告到 EBGp 对等项。 ■ NO_ADVERTISE - 不通告到任何对等项。 ■ NO_EXPORT - 不通告到外部 BGP 联合。

10 在“操作”列中，选择允许或拒绝。

您可以允许或禁止 IP 前缀列表中的 IP 地址通告其地址。

11 单击保存。

配置转发启动定时器

您可以为 Tier-0 逻辑路由器配置转发启动定时器。

转发启动定时器定义在建立第一个 BGP 会话后路由器发送启动通知之前必须等待的时间（秒）。在 NSX Edge 上使用动态路由 (BGP) 的逻辑路由器的活动-活动或活动-备用配置进行故障切换时，该定时器（以前称为转发延迟）可以最大限度减少停机时间。应将其设置为在建立第一个 BGP/BFD 会话后外部路由器 (TOR) 将所有路由通告到该路由器所需的秒数。定时器值应与路由器必须发现的北向动态路由数成正比。在单个 Edge 节点设置上，该定时器应设置为 0。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择高级网络和安全 > 网络 > 路由器。
- 3 选择 Tier-0 逻辑路由器。
- 4 选择路由 > 全局配置。
- 5 单击编辑。
- 6 为转发启动定时器输入一个值。
- 7 单击保存。

您可以通过**高级网络和安全**选项卡配置 NAT。

注 如果使用**高级网络和安全**用户界面来修改策略“略界”面中创建的对象，则某些设置可能无法配置。这些只读设置的旁边有此图标：⊖。有关详细信息，请参见第 1 章 **NSX Manager 概览**。

本章讨论了以下主题：

- **网络地址转换**

网络地址转换

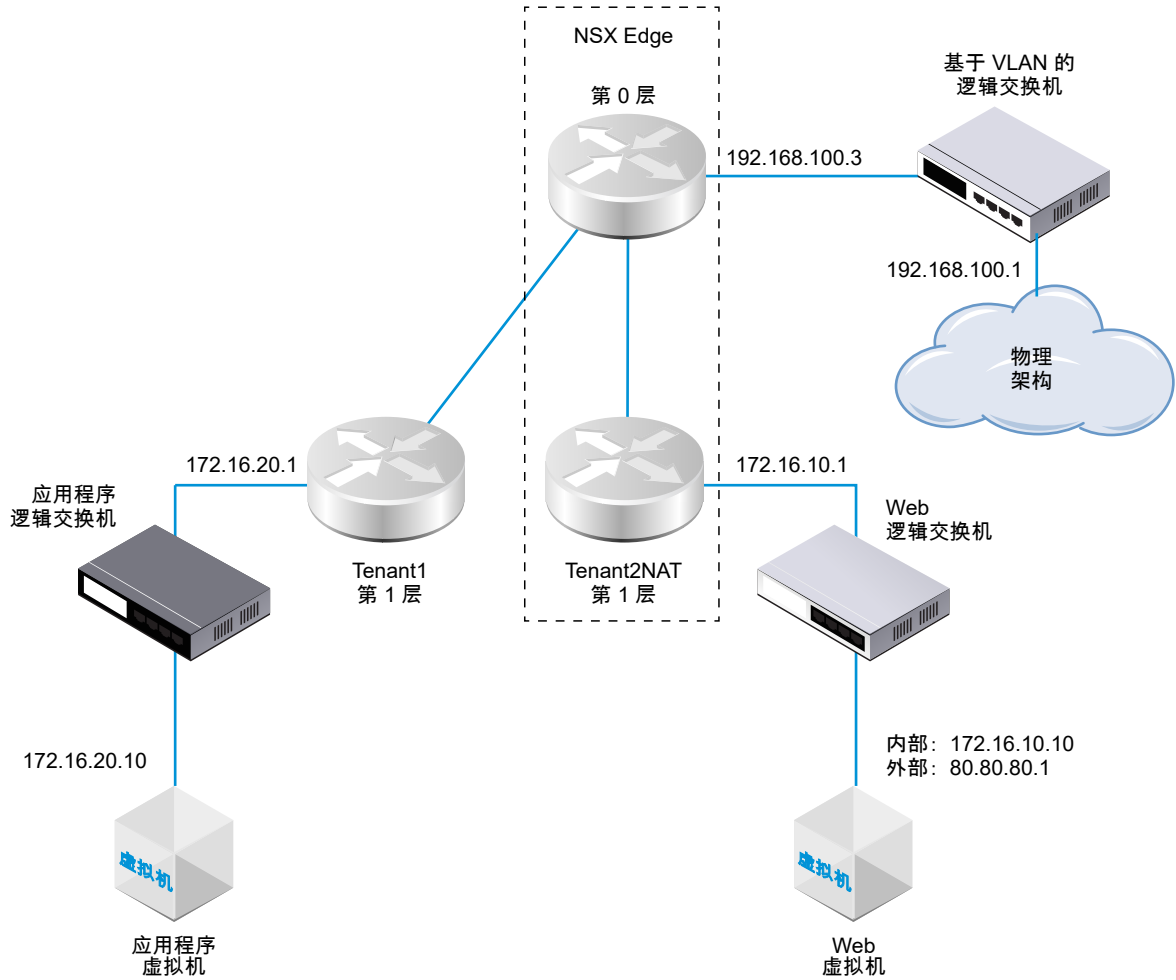
可以在 Tier-0 和 Tier-1 逻辑路由器上配置 NSX-T Data Center 中的网络地址转换 (NAT)。

例如，下图显示了两个在 Tenant2NAT 上配置了 NAT 的 Tier-1 逻辑路由器。Web 虚拟机简单配置为将 172.16.10.10 作为其 IP 地址，并将 172.16.10.1 作为其默认网关。

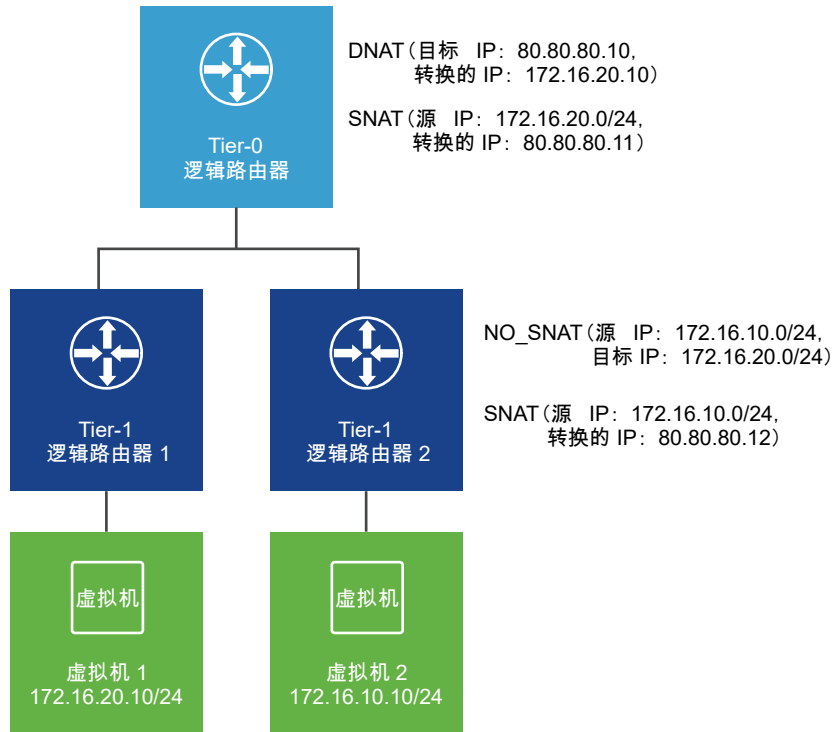
在 Tenant2NAT 逻辑路由器到 Tier-0 逻辑路由器的上行链路连接上强制实施了 NAT。

要启用 NAT 配置，Tenant2NAT 必须在 NSX Edge 集群上具有一个服务组件。因此，Tenant2NAT 显示在 NSX Edge 中。为了进行比较，可以将 Tenant1 放在 NSX Edge 外部，因为它不使用任何 Edge 服务。

图 15-1. NAT 拓扑



注意：在以下场景中，不支持 NAT 发夹处理。Tier-0 逻辑路由器配置了 DNAT 和 SNAT。Tier-1 逻辑路由器 2 配置了 NO_SNAT 和 SNAT。虚拟机 2 将不能使用虚拟机 1 的外部地址 80.80.80.10 访问虚拟机 1。



以下几节介绍了如何使用管理器 UI 创建 NAT 规则。您也可以进行 API 调用 (POST /api/v1/logical-routers/<logical-router-id>/nat/rules?action=create_multiple) 以同时创建多个 NAT 规则。有关详细信息，请参阅《NSX-T Data Center API 指南》。

Tier-1 NAT

Tier-1 逻辑路由器支持源 NAT (SNAT)、目标 NAT (DNAT) 和反射 NAT。

在 Tier-1 路由器上配置源 NAT

源 NAT (Source NAT, SNAT) 更改数据包 IP 标头中的源地址。它还可能更改 TCP/UDP 标头中的源端口。典型的用途是将专用 (RFC1918) 地址/端口更改为离开您的网络的数据包的公共地址/端口。

您可以创建一个规则，以启用或禁用源 NAT。

在该示例中，从 Web 虚拟机中收到数据包时，Tenant2NAT Tier-1 路由器将数据包的源 IP 地址从 172.16.10.10 更改为 80.80.80.1。通过使用公共源地址，专用网络外部的目标可以路由回原始源。

前提条件

- Tier-0 路由器必须将一个上行链路连接到基于 VLAN 的逻辑交换机。请参见[将 Tier-0 逻辑路由器连接到 NSX Edge 上行链路的 VLAN 逻辑交换机](#)。
- Tier-0 路由器必须在到物理架构的上行链路上配置路由（静态或 BGP）和路由重新分发。请参阅[配置静态路由](#)、[在 Tier-0 逻辑路由器上配置 BGP](#)和[在 Tier-0 逻辑路由器上启用路由重新分发](#)。
- Tier-1 路由器必须分别配置一个到 Tier-0 路由器的上行链路。Tenant2NAT 必须由一个 NSX Edge 群集提供支持。请参见[连接 Tier-0 和 Tier-1](#)。

- Tier-1 路由器必须配置了下行链路端口和路由通告。请参见在 [Tier-1 逻辑路由器上添加下行链路端口](#) 和在 [Tier-1 逻辑路由器上配置路由通告](#)。
- 虚拟机必须连接到正确的逻辑交换机。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 选择 **高级网络和安全 > 网络 > 路由器**。
- 3 单击一个要在其中配置 NAT 的 Tier-1 逻辑路由器。
- 4 选择 **服务 > NAT**。
- 5 单击 **添加**。
- 6 指定优先级值。
值越小，规则的优先级越高。
- 7 对于 **操作**，选择 **SNAT** 以启用源 NAT，或者选择 **NO_SNAT** 以禁用源 NAT。
- 8 选择协议类型。
默认情况下，将选择 **任何协议**。
- 9 （可选）对于 **源 IP**，以 CIDR 格式指定一个 IP 地址或 IP 地址范围。
如果将此字段留空，将转换路由器下行链路端口上的所有源。在此示例中，源 IP 地址为 172.16.10.10。
- 10 （可选）对于 **目标 IP**，以 CIDR 格式指定一个 IP 地址或 IP 地址范围。
如果将此字段留空，NAT 将应用于本地子网外部的所有目标。
- 11 如果 **操作** 为 **SNAT**，对于 **转换的 IP**，以 CIDR 格式指定一个 IP 地址或 IP 地址范围。
在该示例中，转换的 IP 地址为 80.80.80.1。
- 12 （可选）对于 **应用对象**，选择一个路由器端口。
- 13 （可选）设置规则的状态。
默认情况下启用规则。
- 14 （可选）更改日志记录状态。
默认情况下禁用日志记录。
- 15 （可选）更改防火墙绕过设置。
默认情况下启用该设置。

结果

将在“NAT”下面列出新规则。例如：

Tenant2NAT

概览配置路由服务

NAT刷新

未收集任何统计信息

+添加编辑删除

ID	操作	匹配					已转换		应用对象	统计信息
		协议	源 IP	源端口	目标 IP	目标端口	IP	端口		
优先级: 1024										
1028	SNAT	任意	172.16.10.10	任意	任意	任意	80.80.80.1	任意		

后续步骤

配置 Tier-1 路由器以通告 NAT 路由。

要将 Tier-0 路由器上游的 NAT 路由通告到物理架构，请配置 Tier-0 路由器以通告 Tier-1 NAT 路由。

在 Tier-1 路由器上配置目标 NAT

目标 NAT 更改数据包 IP 标头中的目标地址。它还可能会更改 TCP/UDP 标头中的目标端口。它的典型用途是，将具有公共地址/端口目标的入站数据包重定向到您的网络中的专用 IP 地址/端口。

您可以创建一个规则，以启用或禁用目标 NAT。

在该示例中，从应用程序虚拟机中收到数据包时，Tenant2NAT Tier-1 路由器将数据包的目标 IP 地址从 172.16.10.10 更改为 80.80.80.1。通过使用公共目标地址，可以从专用网络外部连接到专用网络中的目标。

前提条件

- Tier-0 路由器必须将一个上行链路连接到基于 VLAN 的逻辑交换机。请参见[将 Tier-0 逻辑路由器连接到 NSX Edge 上行链路的 VLAN 逻辑交换机](#)。
- Tier-0 路由器必须在到物理架构的上行链路上配置路由（静态或 BGP）和路由重新分发。请参阅[配置静态路由](#)、[在 Tier-0 逻辑路由器上配置 BGP](#)和[在 Tier-0 逻辑路由器上启用路由重新分发](#)。
- Tier-1 路由器必须分别配置一个到 Tier-0 路由器的上行链路。Tenant2NAT 必须由一个 NSX Edge 群集提供支持。请参见[连接 Tier-0 和 Tier-1](#)。
- Tier-1 路由器必须配置了下行链路端口和路由通告。请参见[在 Tier-1 逻辑路由器上添加下行链路端口](#)和[在 Tier-1 逻辑路由器上配置路由通告](#)。
- 虚拟机必须连接到正确的逻辑交换机。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择[高级网络和安全](#) > [网络](#) > [路由器](#)。
- 3 单击一个要在其中配置 NAT 的 Tier-1 逻辑路由器。
- 4 选择[服务](#) > [NAT](#)。
- 5 单击[添加](#)。

6 指定优先级值。

值越小，规则的优先级越高。

7 对于**操作**，选择 **DNAT** 以启用目标 NAT，或者选择 **NO_DNAT** 以禁用目标 NAT。**8** 选择协议类型。

默认情况下，将选择**任何协议**。

9 （可选）对于**源 IP**，以 CIDR 格式指定一个 IP 地址或 IP 地址范围。

如果将“源 IP”保留空白，NAT 将应用于本地子网外部的所有源。

10 对于**目标 IP**，以 CIDR 格式指定一个 IP 地址或 IP 地址范围。

在此示例中，目标 IP 地址为 80.80.80.1。

11 如果**操作**为 **DNAT**，对于**转换的 IP**，以 CIDR 格式指定一个 IP 地址或 IP 地址范围。

在该示例中，内部/转换的 IP 地址为 172.16.10.10。

12 （可选）如果**操作**为 **DNAT**，对于**转换的端口**，指定转换端口。**13** （可选）对于**应用对象**，选择一个路由器端口。**14** （可选）设置规则的状态。

默认情况下启用规则。

15 （可选）更改日志记录状态。

默认情况下禁用日志记录。

16 （可选）更改防火墙绕过设置。

默认情况下启用该设置。

结果

将在“NAT”下面列出新规则。例如：

Tenant2NAT

概览

配置

路由

服务

NAT

刷新

未收集任何统计信息

+ 添加

编辑

删除

ID	操作	匹配					已转换		应用对象	统计信息
		协议	源 IP	源端口	目标 IP	目标端口	IP	端口		
优先级: 1024										
1029	DNAT	任意	任意	任意	80.80.80.1	任意	172.16.10.10	任意		

后续步骤

配置 Tier-1 路由器以通告 NAT 路由。

要将 Tier-0 路由器上游的 NAT 路由通告到物理架构，请配置 Tier-0 路由器以通告 Tier-1 NAT 路由。

将 Tier-1 NAT 路由通告到上游 Tier-0 路由器

通过通告 Tier-1 NAT 路由，可以使上游 Tier-0 路由器发现这些路由。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**高级网络和安全 > 网络 > 路由器**。
- 3 单击一个已在其中配置 NAT 的 Tier-1 逻辑路由器。
- 4 从该 Tier-1 路由器中，选择**路由 > 路由通告**。
- 5 单击**编辑**以编辑路由通告配置。

可以切换以下开关：

- 状态
- 通告所有 NSX 连接的路由
- 通告所有 NAT 路由
- 通告所有静态路由
- 通告所有 LB VIP 路由
- 通告所有 LB SNAT IP 路由
- 通告所有 DNS 转发器路由

- 6 单击**保存**。

后续步骤

将 Tier-1 NAT 路由从 Tier-0 路由器通告到上游物理架构。

将 Tier-1 NAT 路由通告到物理架构

通过从 Tier-0 路由器中通告 Tier-1 NAT 路由，可以使上游物理架构发现这些路由。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**路由**。
- 3 单击一个连接到已在其中配置 NAT 的 Tier-1 路由器的 Tier-0 逻辑路由器。
- 4 从该 Tier-0 路由器中，选择**路由 > 路由重新分发**。
- 5 单击**编辑**以启用或禁用路由重新分发。

6 单击**添加**以添加一组路由重新分发条件。

选项	说明
名称和说明	为路由重新分发指定一个名称。您可以选择提供相应的说明。 例如，名称为 advertise-to-bgp-neighbor。
源	选择一个或多个以下源： <ul style="list-style-type: none"> ■ TO 直连 ■ TO 上行链路 ■ TO 下行链路 ■ TO CSP ■ TO 环回 ■ TO 静态 ■ TO NAT ■ TO DNS 转发器 IP ■ TO IPsec 本地 IP ■ T1 直连 ■ T1 CSP ■ T1 下行链路 ■ T1 静态 ■ T1 LB SNAT ■ T1 NAT ■ T1 LB VIP ■ T1 DNS 转发器 IP
路由映射	(可选) 分配路由映射以从路由重新分发中筛选一组 IP 地址。

验证 Tier-1 NAT

验证 SNAT 和 DNAT 规则是否正常工作。

步骤

- 1 登录到 NSX Edge。
- 2 运行 `get logical-routers` 以确定 Tier-0 服务路由器的 VRF 编号。
- 3 运行 `vrf <number>` 命令以进入 Tier-0 服务路由器上下文。
- 4 运行 `get route` 命令并确保显示 Tier-1 NAT 地址。

```

nsx-edge(tier0_sr)> get route

Flags: c - connected, s - static, b - BGP, ns - nsx_static
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT

Total number of routes: 8

t1n  80.80.80.1/32      [3/3]      via 169.0.0.1
...
```

- 5 如果 Web 虚拟机设置为提供网页，请确保您可以打开 <http://80.80.80.1> 中的网页。
- 6 确保物理架构中的 Tier-0 路由器的上游邻居可以 ping 通 80.80.80.1。
- 7 在 ping 仍在运行时，检查 DNAT 规则的“统计信息”列。
应该具有一个活动会话。

Tier-0 NAT

活动-备用模式下的 Tier-0 逻辑路由器支持源 NAT (SNAT)、目标 NAT (DNAT) 和反射 NAT。活动-活动模式下的 Tier-0 逻辑路由器仅支持反射 NAT。

在 Tier-0 逻辑路由器上配置源和目标 NAT

可以在主动-备用模式下运行的 Tier-0 逻辑路由器上配置源和目标 NAT。

还可以为 IP 地址或地址范围禁用 SNAT 或 DNAT。如果多个 NAT 规则应用于一个地址，将应用具有最高优先级的规则。

在 Tier-0 逻辑路由器的上行链路上配置的 SNAT 将处理来自 Tier-1 逻辑路由器以及来自 Tier-0 逻辑路由器上的另一个上行链路的流量。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**高级网络和安全 > 网络 > 路由器**。
- 3 单击 Tier-0 逻辑路由器。
- 4 选择**服务 > NAT**。
- 5 单击**添加**以添加 NAT 规则。
- 6 指定优先级值。
较低的值意味着更高的优先级。
- 7 对于**操作**，选择 **SNAT**、**DNAT**、**反射**、**NO_SNAT** 或 **NO_DNAT**。
- 8 选择协议类型。
默认情况下，将选择**任何协议**。
- 9 （必选）对于**源 IP**，以 CIDR 格式指定一个 IP 地址或 IP 地址范围。
如果将此字段留空，此 NAT 规则将应用于本地子网外部的所有源。
- 10 对于**目标 IP**，以 CIDR 格式指定一个 IP 地址或 IP 地址范围。
- 11 对于**转换的 IP**，以 CIDR 格式指定一个 IP 地址或 IP 地址范围。
- 12 （可选）如果**操作**为 **DNAT**，对于**转换的端口**，指定转换端口。
- 13 （可选）对于**应用对象**，选择一个路由器端口。

14 （可选）设置规则的状态。

默认情况下启用规则。

15 （可选）更改日志记录状态。

默认情况下禁用日志记录。

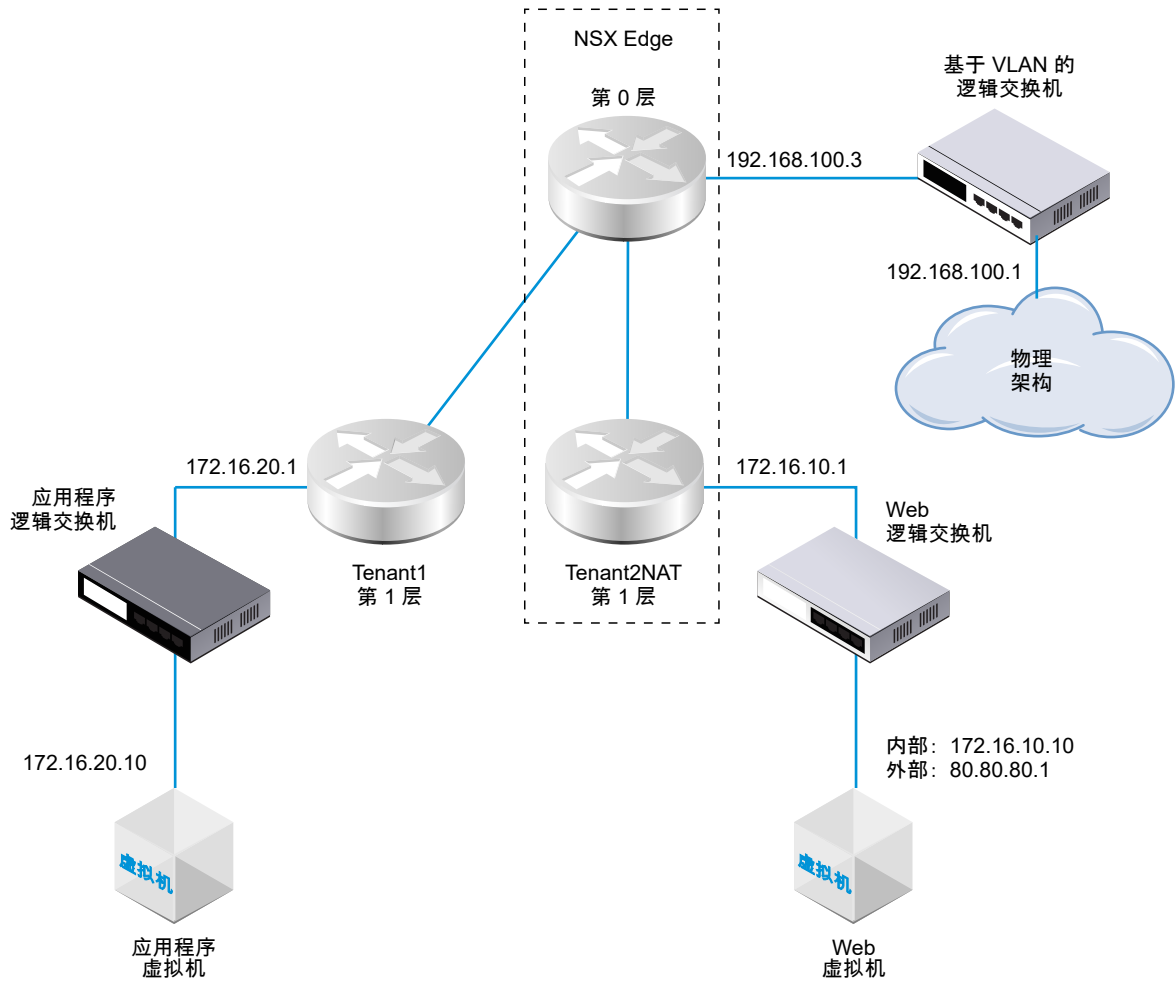
16 （可选）更改防火墙绕过设置。

默认情况下启用该设置。

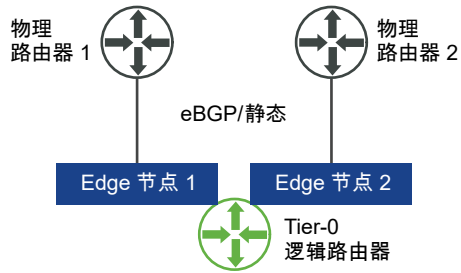
反射 NAT

如果 Tier-0 逻辑路由器在活动-活动模式下运行，您无法配置有状态 NAT，在该模式下，不对称的路径可能会导致出现问题。对于活动-活动路由器，您可以配置反射 NAT（有时称为无状态 NAT）。

在该示例中，从 Web 虚拟机中收到数据包时，Tenant2NAT Tier-1 路由器将数据包的源 IP 地址从 172.16.10.10 更改为 80.80.80.1。通过使用公共源地址，专用网络外部的目标可以路由回原始源。



在涉及两个活动-活动 Tier-0 路由器时（如下所示），必须配置反射 NAT。



在 Tier-0 或 Tier-1 逻辑路由器上配置反射 NAT

如果 Tier-0 或 Tier-1 逻辑路由器在主动-主动模式下运行，则无法配置有状态 NAT，在此情况下，不对称的路径可能会导致出现问题。对于主动-主动路由器，可以使用反射 NAT（有时称为无状态 NAT）。

对于反射 NAT，可以配置要转换的单个源地址，也可以配置一个地址范围。如果配置源地址范围，您还必须配置一个转换地址范围。两个范围的大小必须相同。地址转换将是确定性的，这意味着源地址范围中的第一个地址将转换为转换地址范围中的第一个地址，源范围中的第二个地址将转换为转换范围中的第二个地址，依此类推。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**高级网络和安全 > 网络 > 路由器**。
- 3 单击一个要在其中配置反射 NAT 的 Tier-0 或 Tier-1 逻辑路由器。
- 4 选择**服务 > NAT**。
- 5 单击**添加**。
- 6 指定优先级值。
值越小，规则的优先级越高。
- 7 对于**操作**，选择**反射**。
- 8 对于**源 IP**，以 CIDR 格式指定一个 IP 地址或 IP 地址范围。
- 9 对于**转换的 IP**，以 CIDR 格式指定一个 IP 地址或 IP 地址范围。
- 10 （可选）设置规则的状态。
默认情况下启用规则。
- 11 （可选）更改日志记录状态。
默认情况下禁用日志记录。
- 12 （可选）更改防火墙绕过设置。
默认情况下启用该设置。

结果

将在“NAT”下面列出新规则。例如：

Tier0-LR-1

概览 配置 路由 服务

NAT | 刷新

规则统计信息总计 | 上次更新时间: 2019年3月6日 18:07:59

活动会话

数据包计数

字节 数据

+ 添加

编辑

删除

ID	操作	匹配					已转换		应用对象	统计信息
		协议	源 IP	源端口	目标 IP	目标端口	IP	端口		
优先级: 1024										
2048	反射	任意	80.80.80.1	任意	任意	任意	172.16.10.10	任意		

您可以创建 IP 集、IP 池、MAC 集、NS 组和 NS 服务。您还可以管理虚拟机的标记。

注 如果使用**高级网络和安全**用户界面来修改策略“略界”面中创建的对象，则某些设置可能无法配置。这些只读设置的旁边有此图标：⊖。有关详细信息，请参见第 1 章 **NSX Manager 概览**。

本章讨论了以下主题：

- 创建 IP 集
- 创建 IP 池
- 创建 MAC 集
- 创建 NS 组
- 配置服务和服务组
- 管理虚拟机的标记

创建 IP 集

IP 集是一组 IP 地址，可以用作防火墙规则中的源和目标。

IP 集可以包含各个 IP 地址、IP 范围和子网的组合。您可以指定 IPv4 和/或 IPv6 地址。IP 集可以是 NS 组的成员。按照此方法创建的任何 IP 集在策略模式下将不可见。在策略模式下，可以创建组并添加 IP 地址、范围、网络地址或 MAC 地址作为成员，方法是导航到**清单 > 组 > 设置成员**并指定 IP 或 MAC 地址。

注 防火墙规则的源或目标范围支持 IPv4 地址和 IPv6 地址。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 选择**高级网络和安全 > 清单 > 组 > IP 集 > 添加**。
- 3 输入名称。
- 4 （可选）输入说明。
- 5 在**成员**中，以逗号分隔列表形式输入单个 IP 地址、IP 范围和子网。
- 6 单击**保存**。

创建 IP 池

在创建 L3 子网时，您可以使用 IP 池分配 IP 地址或子网。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**高级网络和安全 > 清单 > 组 > IP 池 > 添加**。
- 3 输入新 IP 池的名称。
- 4 （可选）输入说明。
- 5 单击**添加**。
- 6 单击 IP 范围单元格，然后输入 IP 范围。
将鼠标悬停在任何单元格的右上角，然后单击铅笔图标以编辑该单元格。
- 7 （可选）输入网关。
- 8 输入具有后缀的 CIDR IP 地址。
- 9 （可选）输入 DNS 服务器。
- 10 （可选）输入 DNS 后缀。
- 11 单击**保存**。

创建 MAC 集

MAC 集是一组 MAC 地址，可以用作第 2 层防火墙规则中的源和目标以及 NS 组的成员。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**高级网络和安全 > 清单 > 组 > MAC 集 > 添加**。
- 3 输入名称。
- 4 （可选）输入说明。
- 5 以逗号分隔列表的形式输入 MAC 地址。
- 6 单击**添加**。

创建 NS 组

可以将 NS 组配置为包含 IP 集、MAC 集、逻辑端口、逻辑交换机和其他 NS 组的组合。可以将具有逻辑交换机、逻辑端口和虚拟机的 NS 组指定为源和目标，以及在防火墙规则的 Applied To 字段中指定。具有 IP 集和 MAC 集的 NS 组在分布式防火墙 Applied To 字段中将被忽略。

NSX Cloud 说明 如果使用 NSX Cloud，请参见 [NSX Cloud 支持的 NSX-T Data Center 功能](#) 以查看自动生成的逻辑实体、支持的功能以及 NSX Cloud 所需的配置的列表。

NS 组具有以下特性：

- NS 组具有直接成员和有效成员。有效成员包括使用成员资格条件指定的成员，以及属于该 NS 组的成员的所有直接和有效成员。例如，假设 NSGroup-1 具有直接成员 LogicalSwitch-1。您添加 NSGroup-2 并将 NSGroup-1 和 LogicalSwitch-2 指定为成员。现在，NSGroup-2 具有直接成员 NSGroup-1 和 LogicalSwitch-2 以及有效成员 LogicalSwitch-1。接下来，添加 NSGroup-3 并将 NSGroup-2 指定为成员。NSGroup-3 现在具有直接成员 NSGroup-2 以及有效成员 LogicalSwitch-1 和 LogicalSwitch-2。从主组表中，单击一个组并选择 **相关 > NS 组** 将显示 NSGroup-1、NSGroup-2 和 NSGroup-3，因为这三者直接或间接将 LogicalSwitch-1 作为成员。
- NS 组最多可以具有 500 个直接成员。
- NS 组中的建议有效成员数限制为 5000 个。NSX Manager 每天检查两次 NS 组是否超过该限制，分别在早晨 7 点和晚上 7 点。超过该限制不会影响任何功能，但可能会对性能造成不利影响。
 - 当 NS 组的有效成员数超过 5000 的 80% 时，警告消息 NSGroup xyz is about to exceed the maximum member limit.Total number in NSGroup is ... 将出现在日志文件中。数值超过 5000 时，将出现警告消息 NSGroup xyz has reached the maximum numbers limit.Total number in NSGroup = ...
 - 当 NS 组中的转换的 VIF/IP/MAC 数超过 5000 时，警告消息 Container xyz has reached the maximum IP/MAC/VIF translations limit.Current translations count in Container - IPs:..., MACs:..., VIFs:...
- 支持的最大虚拟机数为 10,000 个。
- 您最多可以创建 10,000 个 NS 组。

对于可作为成员添加到 NS 组的所有对象，可以导航到任何对象的屏幕，选择 **相关 > NS 组**。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择 **高级网络和安全 > 清单 > 组 > 添加**。
- 3 输入 NS 组的名称。
- 4 （可选）输入说明。

5 （可选）单击**成员资格条件**。

对于每个条件，最多可以指定五个规则，且这些规则可与逻辑 AND 运算符结合使用。可用成员条件可应用于以下各项：

- **逻辑端口** - 可指定标记和可选范围。
- **逻辑交换机** - 可指定标记和可选范围。
- **虚拟机** - 可指定名称、标记、计算机操作系统名称或计算机名称（等于、包含、开头为、结尾为或不同于特定字符串）。
- **传输节点** - 可指定等于 Edge 节点或主机节点的节点类型。
- **IP 集** - 可指定标记和可选范围。

6 （可选）单击**成员**以选择成员。

可用成员类型包括：

- **AD 组** - 具有 AD 组的 NS 组只能在分布式防火墙规则的 `extended_source` 字段中使用，且必须是组中唯一的成员。例如，不能将同时具有 AD 组和 IP 集的 NS 组作为成员。
- **IP 集** - 可以同时包括 IPv4 和 IPv6 地址。
- **逻辑端口** - 可以同时包括 IPv4 和 IPv6 地址。
- **逻辑交换机** - 可以同时包括 IPv4 和 IPv6 地址。
- **MAC 集**
- **NS 组**
- **传输节点**
- **VIF**
- **虚拟机**

7 单击**添加**。

该组将添加到组表。单击组名可显示概览以及编辑组信息，包括成员资格条件、成员、应用程序和相关组。滚动到**概览**选项卡底部可添加和删除标记。有关详细信息，请参见[将标记添加到对象](#)。选择**相关> NS 组**可显示将选定 NS 组作为成员的所有 NS 组。

配置服务和服组

您可以配置 NS 服务并指定用于匹配网络流量的参数，例如，端口和协议对。也可以使用 NS 服务在防火墙规则中允许或阻止某些类型的流量。

NS 服务可以具有以下类型：

- 以太网
- IP
- IGMP

- ICMP
- ALG
- L4 端口集

L4 端口集支持标识源端口和目标端口。您可以指定单个端口或一定范围的端口，最多为 15 个端口。

NS 服务也可以是一组其他 NS 服务。采用组形式的 NS 服务可以具有以下类型：

- 第 2 层
- 第 3 层和更高的层

在创建 NS 服务后，您无法更改类型。某些 NS 服务是预定义的。您无法修改或删除这些服务。

创建 NS 服务

您可以创建 NS 服务以指定网络匹配使用的特性，或者定义在防火墙规则中阻止或允许的流量类型。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**高级网络和安全 > 清单 > 服务 > 添加**。
- 3 输入名称。
- 4 （可选）输入说明。
- 5 选择**指定协议**以配置单个服务，或者选择**将现有服务分组**以配置一组 NS 服务。
- 6 对于单个服务，请选择服务类型和协议。
可用的类型是**以太网、IP、IGMP、ICMP、ALG 和 L4 端口集**。
- 7 对于服务组，请为该组选择类型和成员。
可用的类型是**第 2 层和第 3 层和更高的层**。
- 8 单击**添加**。

管理虚拟机的标记

您可以在清单中查看虚拟机列表。您还可以为虚拟机添加标记以简化搜索过程。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 从导航面板中选择**高级网络和安全 > 清单 > 虚拟机**。

虚拟机列表显示为 4 列：虚拟机、外部 ID、源和标记。单击前三列标题中的筛选器图标来筛选列表。输入一串字符可进行部分匹配。如果列中的字符串包含您输入的字符串，则会显示该条目。输入用双引号括起来的一串字符可进行精确匹配。如果列中的字符串与您输入的字符串完全匹配，则会显示该条目。

- 3 从导航面板中选择**清单 > 虚拟机**。
- 4 选择一个虚拟机。
- 5 单击**管理标记**。
- 6 添加或删除标记。

选项	操作
添加标记	单击 添加 以指定一个标记和可选的范围。
删除标记	选择一个现有的标记，然后单击 删除 。

可以从 NSX Manager 分配给虚拟机的最大标记数为 25。所有其他受管对象（如逻辑交换机或端口）的最大标记数为 30。

- 7 单击**保存**。

您可以通过**高级网络和安全**选项卡配置 DHCP。

注 如果使用**高级网络和安全**用户界面来修改策略“略界”面中创建的对象，则某些设置可能无法配置。这些只读设置的旁边有此图标：⊖。有关详细信息，请参见第 1 章 **NSX Manager 概览**。

本章讨论了以下主题：

- DHCP
- 元数据代理

DHCP

通过使用 DHCP（动态主机配置协议），客户端可以从 DHCP 服务器中自动获取网络配置，例如，IP 地址、子网掩码、默认网关和 DNS 配置。

您可以创建 DHCP 服务器以处理 DHCP 请求，并创建 DHCP 中继服务以将 DHCP 流量中继到外部 DHCP 服务器。但是，您不应该在逻辑交换机上配置一个 DHCP 服务器，同时还在该同一个逻辑交换机连接的路由器端口上配置 DHCP 中继服务。在这种场景下，DHCP 请求将仅转到 DHCP 中继服务。

如果配置 DHCP 服务器，要提高安全性，请配置一个 DFW 规则以仅允许 UDP 端口 67 和 68 上来自有效 DHCP 服务器 IP 地址的流量通过。

注 将 Logical Switch/Logical Port/NSGroup 作为源、将 Any 作为目标并配置为丢弃端口 67 和 68 的 DHCP 数据包的 DFW 规则无法阻止 DHCP 流量。要阻止 DHCP 流量，请将 Any 配置为源和目标。

在该版本中，DHCP 服务器不支持客户机 VLAN 标记。

创建 DHCP 服务器配置文件

DHCP 服务器配置文件指定 NSX Edge 群集或 NSX Edge 群集成员。具有该配置文件的 DHCP 服务器处理来自连接到该配置文件中指定的 NSX Edge 节点的逻辑交换机上的虚拟机的 DHCP 请求。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 选择**高级网络和安全** > **网络** > **DHCP** > **服务器配置文件** > **添加**。
- 3 输入名称和可选的说明。

- 4 从下拉菜单中选择一个 NSX Edge 群集。
- 5 （可选）选择该 NSX Edge 群集的成员。
您最多可以指定 2 个成员。

后续步骤

创建 DHCP 服务器。请参见[创建 DHCP 服务器](#)。

创建 DHCP 服务器

您可以创建 DHCP 服务器以处理来自连接到逻辑交换机的虚拟机的 DHCP 请求。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 选择**高级网络和安全 > 网络 > DHCP > 服务器 > 添加**。
- 3 输入名称和可选的说明。
- 4 以 CIDR 格式输入 DHCP 服务器的 IP 地址及其子网掩码。
例如，输入 `192.168.1.2/24`。
- 5 （必选）从下拉菜单中选择一个 DHCP 配置文件。
- 6 （可选）输入常用的选项，例如，域名、默认网关、DNS 服务器和子网掩码。
- 7 （可选）输入无类静态路由选项。
- 8 （可选）输入其他选项。
- 9 单击**保存**。
- 10 选择新创建的 DHCP 服务器。
- 11 展开“IP 池”部分。
- 12 单击**添加**以添加 IP 范围、默认网关、租约期限、警告阈值、错误阈值、无类静态路由选项以及其他选项。
- 13 展开“静态绑定”部分。
- 14 单击**添加**以添加 MAC 地址和 IP 地址之间的静态绑定、默认网关、主机名、租约期限、无类静态路由选项以及其他选项。

后续步骤

将 DHCP 服务器连接到逻辑交换机。请参见[将 DHCP 服务器连接到逻辑交换机](#)。

将 DHCP 服务器连接到逻辑交换机

您必须将 DHCP 服务器连接到一个逻辑交换机，然后 DHCP 服务器才能处理连接到该交换机的虚拟机的 DHCP 请求。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 选择**高级网络和安全 > 网络 > 交换**。
 - a 单击某个逻辑交换机的复选框。
 - b 单击**操作 > 连接 DHCP 服务器**。
- 3 或者，选择**高级网络和安全 > DHCP**。
 - a 单击**服务器**选项卡。
 - b 单击某个 DHCP 服务器的复选框。
 - c 单击**操作 > 连接到逻辑交换机**。

将 DHCP 服务器与逻辑交换机断开连接

您可以将 DHCP 服务器与逻辑交换机断开连接以重新配置您的环境。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 选择**高级网络和安全 > 网络 > 交换**。
- 3 单击要与 DHCP 服务器断开连接的逻辑交换机。
- 4 单击**操作 > 断开连接 DHCP 服务器**。

创建 DHCP 中继配置文件

DHCP 中继配置文件指定一个或多个外部 DHCP 或 DHCPv6 服务器。创建 DHCP/DHCPv6 中继服务时，必须指定一个 DHCP 中继配置文件。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 选择**高级网络和安全 > 网络 > DHCP > 中继配置文件 > 添加**。
- 3 输入名称和可选的说明。
- 4 输入一个或多个外部 DHCP/DHCPv6 服务器地址。

后续步骤

创建 DHCP/DHCPv6 中继服务。请参见[创建 DHCP 中继服务](#)。

创建 DHCP 中继服务

您可以创建 DHCP 中继服务以中继未在 NSX-T Data Center 中创建的 DHCP 客户端和 DHCP 服务器之间的流量。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 选择**高级网络和安全 > 网络 > DHCP > 中继服务 > 添加**。
- 3 输入名称和可选的说明。
- 4 从下拉菜单中选择一个 DHCP 中继配置文件。

后续步骤

将 DHCP 服务添加到逻辑路由器端口。请参见[将 DHCP 中继服务添加到逻辑路由器端口](#)。

将 DHCP 中继服务添加到逻辑路由器端口

您可以将 DHCP 中继服务添加到逻辑路由器端口。连接到该端口的逻辑交换机上的虚拟机，可以与该中继服务中配置的 DHCP 服务器进行通信。

前提条件

- 确认您具有配置的 DHCP 中继服务。请参见[创建 DHCP 中继服务](#)。
- 确认路由器端口的类型为**下行链路**。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 选择**高级网络和安全 > 网络 > 路由器**。
- 3 选择相应的路由器以显示更多的信息和配置选项。
- 4 选择**配置 > 路由器端口**。
- 5 选择连接到所需逻辑交换机的路由器端口，然后单击**编辑**。
- 6 从**中继服务**下拉列表中选择一个 DHCP 中继服务，然后单击**保存**。

也可以在添加新的逻辑路由器端口时选择 DHCP 中继服务。

删除 DHCP 租约

在某些情况下，您可能希望删除 DHCP 租约。例如，您希望 DHCP 客户端获取不同的 IP 地址，或者客户端关闭而未释放 IP 地址，并且您希望将该地址用于其他客户端。

您可以使用以下 API 删除 DHCP 租约：

```
DELETE /api/v1/dhcp/servers/<server-id>/leases?ip=<ip>&mac=<mac>
```

要确保删除正确的租约，请在 DELETE API 之前和之后调用以下 API：

```
GET /api/v1/dhcp/servers/<server-id>/leases
```

在调用 DELETE API 后，请确保 GET API 输出不显示删除的租约。

有关详细信息，请参见《NSX-T Data Center API 参考》。

元数据代理

通过使用元数据代理服务器，虚拟机实例可以从 OpenStack Nova API 服务器中检索实例特定的元数据。

以下步骤说明了元数据代理的工作方式：

- 1 虚拟机将 HTTP GET 发送到 `http://169.254.169.254:80` 以请求某些元数据。
- 2 连接到与虚拟机相同的逻辑交换机的元数据代理服务器读取请求，对标头进行相应的更改，然后将请求转发到 Nova API 服务器。
- 3 Nova API 服务器从 Neutron 服务器中请求和接收有关虚拟机的信息。
- 4 Nova API 服务器查找元数据并将其发送到元数据代理服务器。
- 5 元数据代理服务器将元数据转发到虚拟机。

元数据代理服务器在一个 NSX Edge 节点上运行。为实现高可用性，您可以将元数据代理配置为在 NSX Edge 集群中的两个或更多 NSX Edge 节点上运行。

添加元数据代理服务器

通过使用元数据代理服务器，虚拟机可以从 OpenStack Nova API 服务器中检索元数据。

前提条件

确认您创建了一个 NSX Edge 群集。有关详细信息，请参见 NSX-T Data Center 安装指南。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 选择 **高级网络和安全 > 网络 > DHCP > 元数据代理 > 添加**。
- 3 输入元数据代理服务器的名称。
- 4 （可选）输入说明。
- 5 输入 Nova 服务器的 URL 和端口。
有效端口值为 3000 - 9000。
- 6 输入 **密钥** 的值。
- 7 从下拉列表中选择 一个 NSX Edge 群集。
- 8 （可选）选择该 NSX Edge 群集的成员。

后续步骤

将元数据代理服务器连接到逻辑交换机。

将元数据代理服务器连接到逻辑交换机

要向连接到逻辑交换机的虚拟机提供元数据代理服务，您必须将一个元数据代理服务器连接到该交换机。

前提条件

确认您创建了一个逻辑交换机。有关详细信息，请参见 [创建逻辑交换机](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 选择 **高级网络和安全 > 网络 > DHCP > 元数据代理**。
- 3 选择一个元数据代理服务器。
- 4 选择 **操作 > 连接到逻辑交换机** 菜单选项。
- 5 从下拉列表选择一个逻辑交换机。

结果

也可以通过以下方法将元数据代理服务器连接到逻辑交换机：导航到 **交换 > 交换机**，选择一个交换机，然后选择 **操作 > 连接元数据代理** 菜单选项。

将元数据代理服务器与逻辑交换机断开连接

要停止为连接到逻辑交换机的虚拟机提供元数据代理服务或使用不同的元数据代理服务器，您可以将元数据代理服务器与逻辑交换机断开连接。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 选择 **高级网络和安全 > 网络 > DHCP > 元数据代理**。
- 3 选择一个元数据代理服务器。
- 4 选择 **操作 > 与逻辑交换机断开连接** 菜单选项。
- 5 从下拉列表选择一个逻辑交换机。

结果

也可以通过以下方法将元数据代理服务器与逻辑交换机断开连接：导航到 **交换 > 交换机**，选择一个交换机，然后选择 **操作 > 断开连接元数据代理** 菜单选项。

通过使用 IP 地址管理 (IP Address Management, IPAM)，您可以创建 IP 块以支持 NSX Container Plug-in (NCP)。有关 NCP 的详细信息，请参阅《适用于 Kubernetes 的 NSX-T 容器插件安装和管理指南》。

注 如果使用**高级网络和安全**用户界面来修改策略“略界”面中创建的对象，则某些设置可能无法配置。这些只读设置的旁边有此图标：⊖。有关详细信息，请参见第 1 章 **NSX Manager 概览**。

本章讨论了以下主题：

- 管理 IP 块
- 管理 IP 块的子网

管理 IP 块

设置 NSX Container Plug-in 要求您为这些容器创建 IP 块。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 选择**高级网络和安全** > **网络** > **IPAM**。
- 3 要添加 IP 块，请单击**添加**。
 - a 输入名称和可选的说明。
 - b 使用 CIDR 格式输入一个 IP 块。例如，10.10.10.0/24。
- 4 要编辑 IP 块，请单击 IP 块的名称。
 - a 在**概览**选项卡中，单击**编辑**。
您可以更改名称、说明或 IP 块值。
- 5 要管理 IP 块的标记，请单击 IP 块的名称。
 - a 在**概览**选项卡中，单击**管理**。
您可以添加或删除标记。

6 要删除一个或多个 IP 块，请选择这些块。

a 单击**删除**。

您无法删除已分配子网的 IP 块。

管理 IP 块的子网

您可以添加或删除 IP 块的子网。

步骤

1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。

2 选择**高级网络和安全 > 网络 > IPAM**。

3 单击 IP 块的名称。

4 单击**子网**选项卡。

5 要添加一个子网，请单击**添加**。

a 输入名称和可选的说明。

b 输入该子网的大小。

6 要删除一个或多个子网，请选择这些子网。

a 单击**删除**。

高级负载均衡

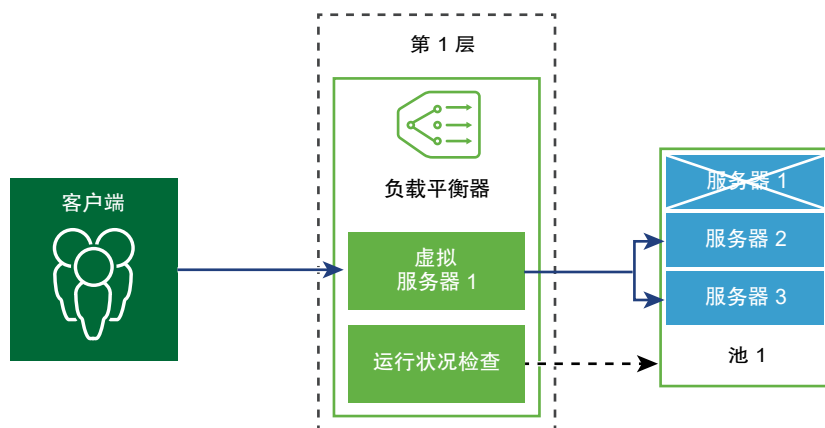
19

此信息介绍位于**高级网络和安全**选项卡下的 NSX-T Data Center 负载均衡配置。

有关 NSX 高级负载均衡器（Avi 网络）的信息，请访问 <https://www.vmware.com/products/nsx-advanced-load-balancer.html>。

注 如果使用**高级网络和安全**用户界面来修改策略“略界”面中创建的对象，则某些设置可能无法配置。这些只读设置的旁边有此图标：⊖。有关详细信息，请参见第 1 章 **NSX Manager 概览**。

NSX-T Data Center 逻辑负载均衡器为应用程序提供高可用性服务并将网络流量负载分布在多个服务器之间。



负载均衡器将入站服务请求均匀分布在多个服务器中，从方式上确保负载分配对用户透明。负载均衡有助于实现最佳的资源利用率，最大程度地提高吞吐量和减少响应时间，并避免过载。

您可以将虚拟 IP 地址映射到一组池服务器进行负载均衡。负载均衡器可接受虚拟 IP 地址上的 TCP、UDP、HTTP 或 HTTPS 请求，并确定要使用的池服务器。

根据环境要求，您可以增加现有的虚拟服务器和池成员来处理繁重的网络流量负载，从而提高负载均衡器性能。

注 仅在 Tier-1 逻辑路由器上支持逻辑负载均衡器。只能将一个负载均衡器连接到 Tier-1 逻辑路由器。

本章讨论了以下主题：

■ 负载均衡器重要概念

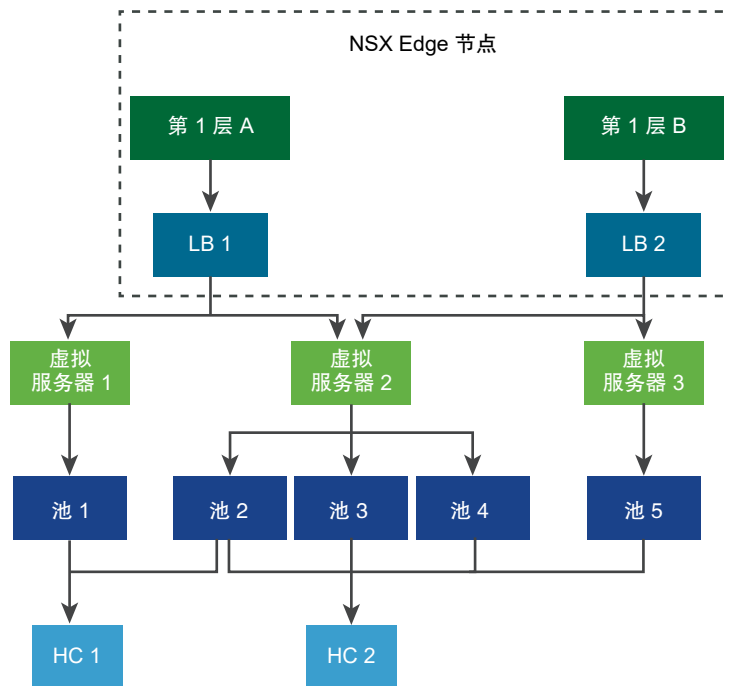
■ 配置负载均衡器组件

负载均衡器重要概念

负载均衡器包括虚拟服务器、服务器池和运行状况检查监控器。

负载均衡器连接到 Tier-1 逻辑路由器。负载均衡器托管一个或多个虚拟服务器。虚拟服务器是应用程序服务的一种抽象，由 IP、端口和协议的唯一组合表示。虚拟服务器与单个到多个服务器池相关联。服务器池包含一组服务器。服务器池包括各个服务器池成员。

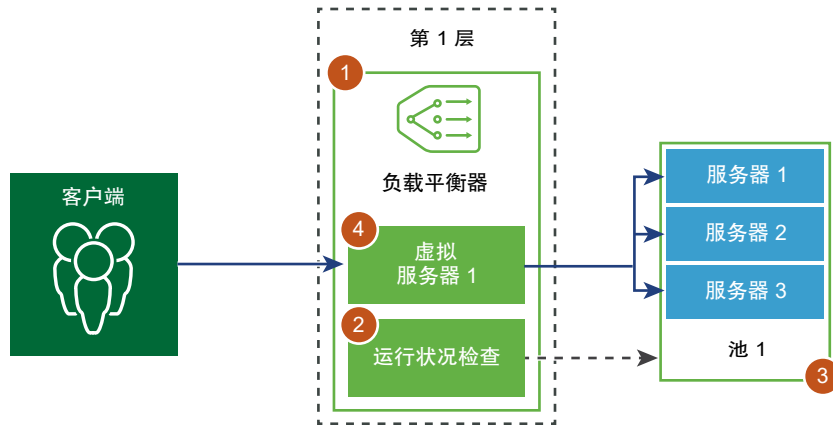
要测试每个服务器是否在正常运行应用程序，您可以添加运行状况检查监控器来检查服务器的运行状况。



配置负载均衡器组件

要使用逻辑负载均衡器，您必须首先配置负载均衡器并将其连接到 Tier-1 逻辑路由器。

接下来，可以设置服务器的运行状况检查监控。然后，必须为负载均衡器配置服务器池。最后，必须为负载均衡器创建第 4 层或第 7 层虚拟服务器。

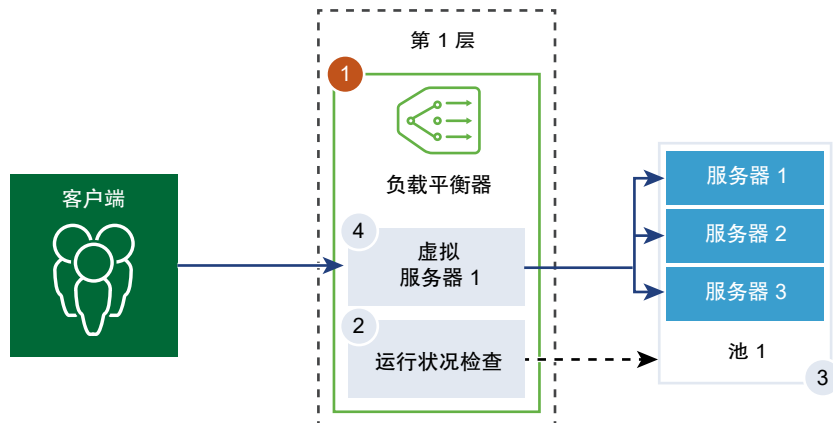


创建负载均衡器

创建负载均衡器并将其连接到 Tier-1 逻辑路由器。

您可以配置希望负载均衡器添加到错误日志的错误消息级别。

注 避免在因打印到该日志的消息数量（影响性能）而生成巨大流量的负载均衡器上将日志级别设置为 DEBUG。



前提条件

确认配置了一个 Tier-1 逻辑路由器。请参见[创建 Tier-1 逻辑路由器](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择高级网络和安全 > 网络 > 负载均衡器 > 添加。
- 3 输入负载均衡器的名称和描述。
- 4 根据可用资源选择负载均衡器的虚拟服务器大小和池成员数量。
- 5 在下拉菜单中定义错误日志的严重性级别。

负载均衡器将遇到的不同严重性级别的问题的相关问题收集到错误日志。

- 6 单击**确定**。
- 7 将新创建的负载平衡器与虚拟服务器相关联。
 - a 选择该负载平衡器，然后单击**操作 > 连接到虚拟服务器**。
 - b 从下拉菜单中选择现有虚拟服务器。
 - c 单击**确定**。
- 8 将新创建的负载平衡器连接到 Tier-1 逻辑路由器。
 - a 选择该负载平衡器，然后单击**操作 > 连接到逻辑路由器**。
 - b 从下拉菜单中选择现有的 Tier-1 逻辑路由器。

Tier-1 路由器必须处于活动-备用模式。
 - c 单击**确定**。
- 9 （可选）删除负载平衡器。

如果您不想再使用此负载平衡器，则必须首先将其从虚拟服务器和 Tier-1 逻辑路由器中分离。

配置主动运行状况监控器

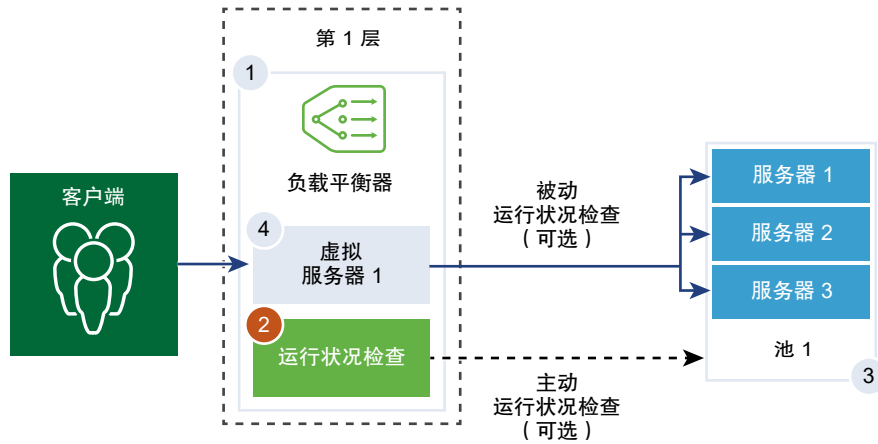
主动运行状况监控器用于检测服务器是否可用。主动运行状况监控器使用几种类型的测试，例如，向服务器发送基本 ping 操作，或发送高级 HTTP 请求以监控应用程序运行状况。

无法在特定时段内做出响应或响应错误的服务器将从未来的连接处理中排除，直到后续的定期运行状况检查认为这些服务器处于正常状态为止。

在将服务器池成员连接到一个虚拟服务器并且该虚拟服务器连接到一个 Tier-1 网关（以前称为 Tier-1 逻辑路由器）后，将对池成员执行主动运行状况检查。

如果该 Tier-1 网关连接到一个 Tier-0 网关，则会创建一个路由器链路端口，并使用其 IP 地址（通常采用 100.64.x.x 格式）为负载平衡器服务执行运行状况检查。如果 Tier-1 网关是单独的（仅具有一个集中式服务端口并且未连接到 Tier-0 网关），则使用集中式服务端口 IP 地址为负载平衡器服务执行运行状况检查。有关单独的 Tier-1 网关的信息，请参见[创建独立 Tier-1 逻辑路由器](#)。

注 可以为每个服务器池配置一个主动运行状况监控器。



步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择高级网络和安全 > 网络 > 负载均衡器 > 监控器 > 主动运行状况监控器 > 添加。
- 3 输入主动运行状况监控器的名称和描述。
- 4 从下拉菜单中选择监控器运行状况检查协议。

您也可以在 NSX Manager、http-monitor、https-monitor、Icmp-monitor、Tcp-monitor 和 Udp-monitor 中使用预定义的协议。

- 5 设置监控端口的值。
- 6 配置用于监控服务池的值。

您也可以接受主动运行状况监控器的默认值。

选项	说明
监控间隔	设置监控器向服务器发送另一个连接请求的时间（秒）。
失败检查计数	设置一个值，当连续失败的次数达到此值时，服务器被视为暂时不可用。
成功检查计数	设置一个数字，在此超时期限过后，服务器会再次尝试建立新连接，以查看其是否可用。
超时期限	设置在将服务器视为 DOWN 之前测试的次数。

例如，如果监控间隔设置为 5 秒且超时设置为 15 秒，则负载均衡器会每 5 秒向服务器发送一次请求。在每次探测中，如果在 15 秒内收到来自服务器的预期响应，则运行状况检查结果为 OK。如果没有收到响应，则结果为 CRITICAL。如果最近三次的运行状况检查结果均为 UP，则服务器将被视为 UP。

- 7 如果您选择 HTTP 作为运行状况检查协议，请填写以下详细信息。

选项	说明
HTTP 方法	从下拉菜单中选择检测服务器状态的方法：GET、OPTIONS、POST、HEAD 和 PUT。
HTTP 请求 URL	输入方法的请求 URI。

选项	说明
HTTP 请求版本	从下拉菜单中选择支持的请求版本。 您也可以接受默认版本 HTTP_VERSION_1_1。
HTTP 请求正文	输入请求正文。 对 POST 和 PUT 方法有效。
HTTP 响应代码	输入监控器要求与 HTTP 响应正文状态行匹配的字符串。 响应代码是以逗号分隔的列表。 例如, 200,301,302,401。
HTTP 响应正文	如果 HTTP 响应正文字符串与 HTTP 运行状况检查响应正文匹配, 则将服务器视为正常。

8 如果您选择 HTTP 作为运行状况检查协议, 请填写以下详细信息。

a 选择 SSL 协议列表。

TLS 版本 TLS1.1 和 TLS1.2 受支持, 默认情况下处于启用状态。TLS1.0 受支持, 但默认情况下处于禁用状态。

b 单击箭头并将协议移至选定部分。

c 分配默认 SSL 密码或创建自定义 SSL 密码。

d 完成以下详细信息, 以将 HTTP 用作运行状况检查协议。

选项	说明
HTTP 方法	从下拉菜单中选择检测服务器状态的方法: GET、OPTIONS、POST、HEAD 和 PUT。
HTTP 请求 URL	输入方法的请求 URI。
HTTP 请求版本	从下拉菜单中选择支持的请求版本。 您也可以接受默认版本 HTTP_VERSION_1_1。
HTTP 请求正文	输入请求正文。 对 POST 和 PUT 方法有效。
HTTP 响应代码	输入监控器要求与 HTTP 响应正文状态行匹配的字符串。 响应代码是以逗号分隔的列表。 例如, 200,301,302,401。
HTTP 响应正文	如果 HTTP 响应正文字符串与 HTTP 运行状况检查响应正文匹配, 则将服务器视为正常。

9 如果您选择 ICMP 作为运行状况检查协议, 请分配 ICMP 运行状况检查数据包的数据大小 (字节)。

10 如果您选择 TCP 作为运行状况检查协议, 则可以将参数留空。

如果未列出发送的数据和预期数据, 则会建立三向握手 TCP 连接以验证服务器运行状况。不会发送数据。预期数据 (如果列出) 必须是字符串, 并且可以位于响应中的任意位置。不支持正则表达式。

11 如果您选择 UDP 作为运行状况检查协议，请填写以下所需的详细信息。

必需选项	说明
发送的 UDP 数据	输入要在建立连接后发送到服务器的字符串。
预期 UDP 数据	输入要从服务器接收的字符串。 只有在收到的字符串与该定义匹配时，才会将服务器视为 UP。

12 单击完成。

后续步骤

将主动运行状况监控器与服务器池相关联。请参见[添加服务器池用于负载平衡](#)。

配置被动运行状况监控器

负载均衡器执行被动运行状况检查以在客户端连接期间监控故障，并将导致一致故障的服务器标记为 DOWN。

被动运行状况检查可监控通过负载均衡器的客户端流量是否出现故障。例如，如果池成员发送 TCP 重置 (RST) 以响应客户端连接，则负载均衡器会检测到该故障。如果连续发生多次故障，则负载均衡器会将服务器池成员视为暂时不可用，并在一段时间内停止向该池成员发送连接请求。一段时间后，负载均衡器会发送连接请求以检查池成员是否已恢复。如果该连接成功，则将池成员视为正常。否则，负载均衡器会等待一段时间，然后重试。

被动运行状况检查将以下情况视为客户端流量故障。

- 对于与第 7 层虚拟服务器关联的服务器池，如果与池成员的连接失败。例如，如果池成员在负载均衡器尝试在负载均衡器与池成员之间连接或执行 SSL 握手失败时发送 TCP RST。
- 对于与第 4 层 TCP 虚拟服务器关联的服务器池，如果池成员发送 TCP RST 以响应客户端 TCP SYN 或完全不响应。
- 对于与第 4 层 UDP 虚拟服务器关联的服务器池，如果收到 ICMP 错误消息（端口或目标无法访问）以响应客户端 UDP 数据包。

对于与第 7 层虚拟服务器关联的服务器池，发生任何 TCP 连接错误（例如，TCP RST 发送数据失败或 SSL 握手失败）时，失败的连接计数将递增。

对于与第 4 层虚拟服务器关联的服务器池，如果未收到对发送给服务器池成员的 TCP SYN 的响应或收到 TCP RST 以响应 TCP SYN，则将服务器池成员视为 DOWN。失败计数将递增。

对于第 4 层 UDP 虚拟服务器，如果收到 ICMP 错误消息（例如，端口或目标无法访问）以响应客户端通信，则将其视为 DOWN。

注 可以为每个服务器池配置一个被动运行状况监控器。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择 **高级网络和安全 > 网络 > 负载均衡器 > 监控器 > 被动运行状况监控器 > 添加**。

3 输入被动运行状况监控器的名称和描述。

4 配置用于监控服务池的值。

您也可以接受主动运行状况监控器的默认值。

选项	说明
失败检查计数	设置一个值，当连续失败的次数达到此值时，服务器被视为暂时不可用。
超时期限	设置在将服务器视为 DOWN 之前测试的次数。

例如，当连续故障次数达到配置值 5 时，则将该成员视为在 5 秒内暂时不可用。在此期限过后，该成员会再次尝试建立新连接，以查看其是否可用。如果该连接成功，则将该成员视为可用，失败计数将设置为零。但是，如果该连接失败，则它不用于另一个 5 秒超时间隔。

5 单击**确定**。

后续步骤

将被动运行状况监控器与服务器池相关联。请参见[添加服务器池用于负载平衡](#)。

添加服务器池用于负载平衡

服务器池包含一个或多个已配置并运行相同应用程序的服务器。可以将单个池与第 4 层和第 7 层虚拟服务器相关联。

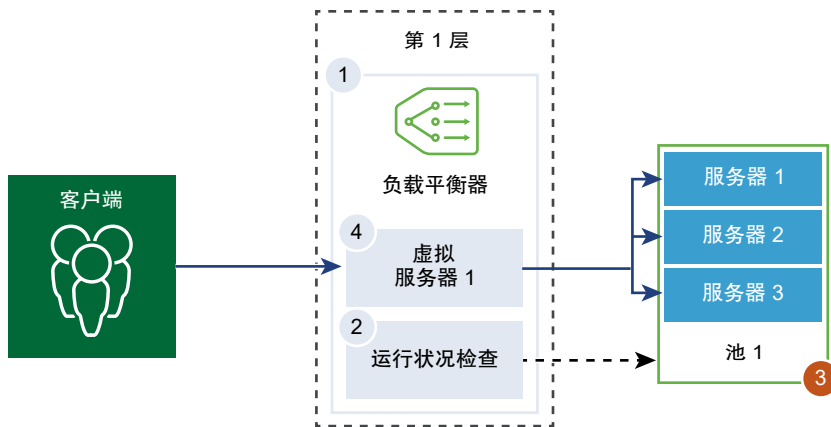
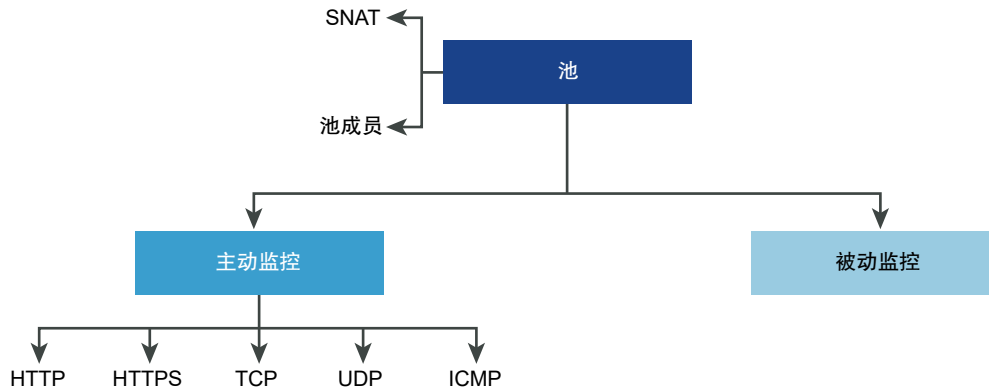


图 19-1. 服务器池参数配置



前提条件

- 如果使用动态池成员，则必须配置 NS 组。请参见[创建 NS 组](#)。
- 根据使用的监控功能，确认已配置主动或被动运行状况监控器。请参见[配置主动运行状况监控器](#)或[配置被动运行状况监控器](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择[高级网络和安全](#) > [网络](#) > [负载均衡器](#) > [服务器池](#) > [添加](#)。
- 3 输入负载均衡器池的名称和描述。
您可以选择描述由服务器池管理的连接。
- 4 选择服务器池的算法平衡方法。

负载均衡算法控制如何在成员之间分发入站连接。可以直接在服务器池或服务器上使用该算法。

所有负载均衡算法均跳过满足以下任何条件的服务器：

- 管理状态设置为 DISABLED。
- 管理状态设置为 GRACEFUL_DISABLED，并且没有匹配的持久性条目。
- 主动或被动运行状况检查状态为 DOWN。
- 达到服务器池最大并发连接数的连接限制。

选项	说明
ROUND_ROBIN	在能够处理入站客户端请求的可用服务器列表中循环遍历请求。 忽略服务器池成员权重（即使已配置）。
WEIGHTED_ROUND_ROBIN	每个服务器都会分配到一个权重值，表示该服务器相对于池中其他服务器的性能。 该值决定了发送到某个服务器的客户端请求数量（与池中的其他服务器相比）。 此负载均衡算法侧重于在可用服务器资源之间公平地分发负载。
LEAST_CONNECTION	根据服务器上已存在的连接数将客户端请求分发到多个服务器。 新连接会被发送到连接数最少的服务器。忽略服务器池成员权重（即使已配置）。

选项	说明
WEIGHTED_LEAST_CONNECTION	每个服务器都会分配到一个权重值，表示该服务器相对于池中其他服务器的性能。该值决定了发送到某个服务器的客户端请求数量（与池中的其他服务器相比）。该负载均衡算法侧重于使用权重值在可用服务器资源之间平均分配负载。默认情况下，如果未配置权重值且已启用启动缓慢，则权重值为 1。
IP-HASH	根据源 IP 地址的哈希值以及所有运行的服务器的总权重选择服务器。

5 切换“TCP 多路复用”按钮以启用此菜单项。

通过 TCP 多路复用，可以在负载均衡器和服务器之间使用相同的 TCP 连接，从而发送来自不同客户端 TCP 连接的多个客户端请求。

6 设置每个池为发送将来的客户端请求而保持活动状态的最大 TCP 多路复用连接数。

7 选择“源 NAT (SNAT)”模式。

根据拓扑，可能需要 SNAT，以便负载均衡器接收从服务器发送到客户端的流量。可以针对每个服务器池启用 SNAT。

模式	说明
透明模式	与服务器建立连接时，负载均衡器使用客户端 IP 地址和端口欺骗。 不需要 SNAT。
自动映射模式	负载均衡器使用接口 IP 地址和临时端口继续与最初连接到服务器已建立的侦听端口之一的客户端进行通信。 需要 SNAT。 启用端口过载，这样如果元组（源 IP、源端口、目标 IP、目标端口和 IP 协议）在执行 SNAT 过程后是唯一的，则允许对多个连接使用相同的 SNAT IP 和端口。 您还可以设置端口过载系数，以允许某个端口可同时用于多个连接的最大次数。
IP 列表模式	指定单个 IP 地址范围（例如，1.1.1.1-1.1.1.10），以便在连接到池中的任何服务器时用于 SNAT。 默认情况下，对配置的所有 SNAT IP 地址使用端口范围 4000-64000。端口范围 1000-4000 是留给从 Linux 应用程序启动的运行状况检查和连接等用途的。如果存在多个 IP 地址，则以轮循方式选择这些地址。 启用端口过载，这样如果元组（源 IP、源端口、目标 IP、目标端口和 IP 协议）在执行 SNAT 过程后是唯一的，则允许对多个连接使用相同的 SNAT IP 和端口。 您还可以设置端口过载系数，以允许某个端口可同时用于多个连接的最大次数。

8 选择服务器池成员。

服务器池由一个或多个池成员组成。每个池成员具有一个 IP 地址和一个端口。

可为每个服务器池成员配置一个权重，用于负载均衡算法。该权重表示给定池成员相对于同一池中其他成员的负载处理能力。

将池成员指定为备份成员与运行状况监控器配合使用，以提供主动/备用状态。如果活动成员未通过运行状况检查，则会将流量故障切换到备用成员。

选项	说明
静态	单击 添加 以包括一个静态池成员。 您还可以克隆现有的静态池成员。
动态	从下拉菜单中选择 NS 组。 服务器池成员资格条件在该组中定义。您可以选择定义最大组 IP 地址列表。

- 9 输入服务器池必须始终维护的最小活动成员数量。
- 10 从下拉菜单中选择服务器池的主动和被动运行状况监控器。

为服务器池设置主动和被动运行状况监控器是可选的。在选择主动运行状况监控器时，如果 Tier-1 网关连接到 Tier-O 网关，则会创建一个路由器链路端口。路由器链路端口的 IP 地址（通常采用 100.64.x.x 格式）用于为负载平衡器服务执行运行状况检查。如果 Tier-1 网关是单独的（仅具有一个集中式服务端口并且未连接到 Tier-O 网关），则使用集中式服务端口 IP 地址为负载平衡器服务执行运行状况检查。有关单独的 Tier-1 网关的信息，请参见[创建独立 Tier-1 逻辑路由器](#)。

添加一个防火墙规则，以允许 IP 地址为负载平衡器服务执行运行状况检查。

- 11 单击**完成**。

配置虚拟服务器组件

虚拟服务器中有几个组件是您可以配置的，例如，应用程序配置文件、持久配置文件和负载均衡器规则。

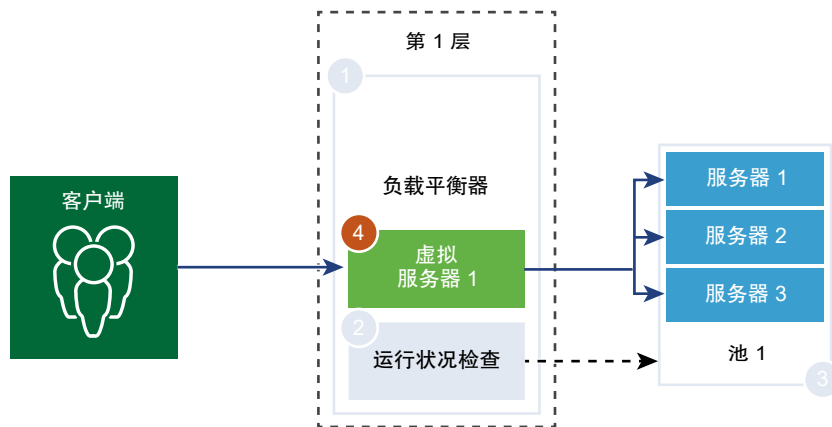
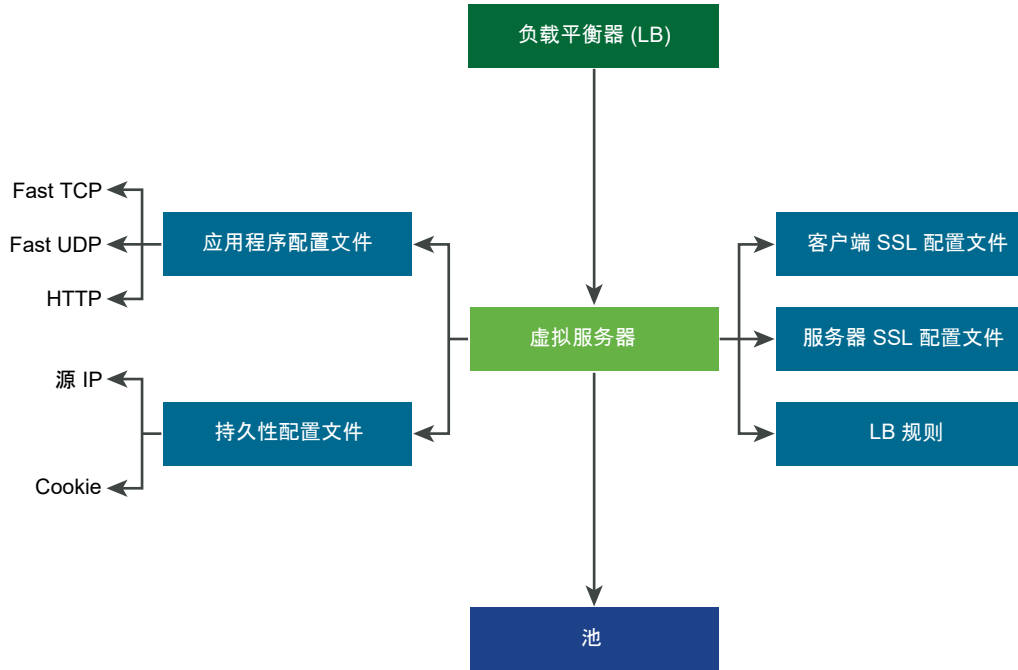


图 19-2. 虚拟服务器组件



配置应用程序配置文件

应用程序配置文件与虚拟服务器相关联，以增强负载均衡网络流量并简化流量管理任务。

应用程序配置文件定义特定网络流量类型的行为。关联的虚拟服务器会根据应用程序配置文件中指定的值处理网络流量。Fast TCP、Fast UDP 和 HTTP 应用程序配置文件是支持的配置文件类型。

默认情况下，如果没有应用程序配置文件与虚拟服务器关联，将使用 TCP 应用程序配置文件。如果应用程序基于 TCP 或 UDP 协议运行且不需要任何应用程序级负载均衡（例如，HTTP URL 负载均衡），将使用 TCP 和 UDP 应用程序配置文件。如果您只需要第 4 层负载均衡（此方法性能更高并支持连接镜像），也会使用这些配置文件。

如果负载均衡器需要根据第 7 层执行操作，例如，将所有映像请求负载均衡到某特定服务器池成员或终止 HTTPS 以从池成员卸载 SSL，则对 HTTP 和 HTTPS 应用程序使用 HTTP 应用程序配置文件。与 TCP 应用程序配置文件不同，在选择服务器池成员之前，HTTP 应用程序配置文件会终止客户端 TCP 连接。

图 19-3. 第 4 层 TCP 和 UDP 应用程序配置文件

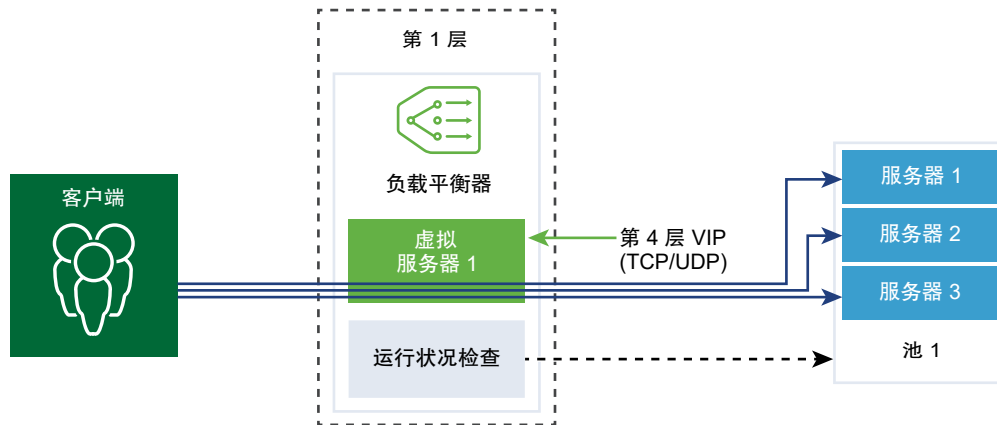
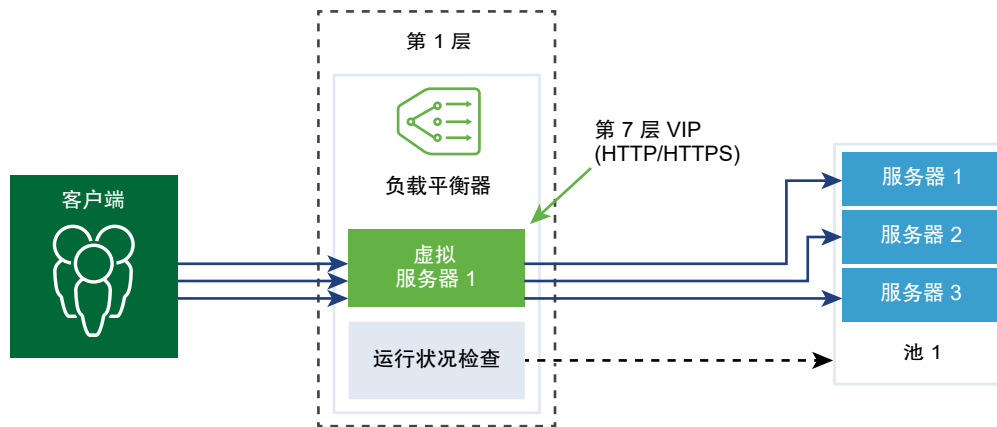


图 19-4. 第 7 层 HTTPS 应用程序配置文件



步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择高级网络和安全 > 网络 > 负载均衡器 > 配置文件 > 应用程序配置文件。
- 3 创建一个 Fast TCP 应用程序配置文件。
 - a 从下拉菜单中选择添加 > Fast TCP 配置文件。
 - b 输入 Fast TCP 应用程序配置文件的名称和描述。

- c 填写应用程序配置文件详细信息。

您也可以接受 Fast TCP 配置文件的默认设置。

选项	说明
连接闲置超时	输入在建立 TCP 连接后服务器可以保持闲置的时长（秒）。 将空闲时间设置为实际应用程序空闲时间，再加几秒，以便负载均衡器不会先于应用程序关闭其连接。
连接关闭超时	输入在关闭 TCP 连接之前 FIN 或 RST 必须为应用程序保持该连接的时间（秒）。 支持较快的连接速率可能需要短暂的关闭超时。
HA 流量镜像	切换该按钮可将发往关联虚拟服务器的所有流量镜像到 HA 备用节点。

- d 单击**确定**。

4 创建一个 Fast UDP 应用程序配置文件。

您也可以接受 UDP 配置文件的默认设置。

- 从下拉菜单中选择**添加 > Fast UDP 配置文件**。
- 输入 Fast UDP 应用程序配置文件的名称和描述。
- 填写应用程序配置文件详细信息。

选项	说明
闲置超时	输入在建立 UDP 连接后服务器可以保持闲置的时长（秒）。 UDP 是一个无连接协议。为实现负载平衡，在闲置超时期限内收到的流量签名（例如，源和目标 IP 地址或端口和 IP 协议）相同的所有 UDP 数据包均视为属于同一连接并发送到相同服务器。 如果在闲置超时期限内未收到任何数据包，则会关闭在流量签名与选定服务器之间创建关联的连接。
HA 流量镜像	切换该按钮可将发往关联虚拟服务器的所有流量镜像到 HA 备用节点。

- d 单击**确定**。

5 创建一个 HTTP 应用程序配置文件。

您也可以接受 HTTP 配置文件的默认设置。

HTTP 应用程序配置文件用于 HTTP 和 HTTPS 应用程序。

- 从下拉菜单中选择**添加 > 快速 HTTP 配置文件**。
- 输入 HTTP 应用程序配置文件的名称和描述。

c 填写应用程序配置文件详细信息。

选项	说明
重定向	<ul style="list-style-type: none"> ■ 无 - 如果网站暂时关闭，用户将收到“未找到页面”错误消息。 ■ HTTP 重定向 - 如果网站暂时关闭或已移动，该虚拟服务器的入站请求可以暂时重定向到此处指定的 URL。仅支持静态重定向。 例如，如果将“HTTP 重定向”设置为 <code>http://sitedown.abc.com/sorry.html</code>，无论实际请求如何（例如，<code>http://original_app.site.com/home.html</code> 或 <code>http://original_app.site.com/somepage.html</code>），当原始网站关闭时，入站请求都会重定向到指定 URL。 ■ HTTP 到 HTTPS 重定向 - 某些安全应用程序可能需要强制通过 SSL 进行通信，但是不拒绝非 SSL 连接，而是重定向到客户端请求以使用 SSL。通过“HTTP 到 HTTPS 重定向”，您可以保留主机和 URI 路径并重定向到客户端请求以使用 SSL。 对于 HTTP 到 HTTPS 重定向，HTTPS 虚拟服务器必须具有端口 443，并且必须在同一负载均衡器上配置相同的虚拟服务器 IP 地址。 例如，将针对 <code>http://app.com/path/page.html</code> 的客户端请求重定向到 <code>https://app.com/path/page.html</code>。如果在重定向（例如，重定向到 <code>https://secure.app.com/path/page.html</code>）时必须修改主机名或 URI，则必须使用负载均衡规则。
X-Forwarded-For (XFF)	<ul style="list-style-type: none"> ■ 插入 - 如果入站请求中不存在 XFF HTTP 标头，则负载均衡器会插入一个带有客户端 IP 地址的新 XFF 标头。如果入站请求中存在 XFF HTTP 标头，则负载均衡器会在 XFF 标头中附加客户端 IP 地址。 ■ 替换 - 如果入站请求中存在 XFF HTTP 标头，则负载均衡器会替换该标头。 Web 服务器会记录其处理的每个请求以及请求客户端 IP 地址。可使用这些日志进行调试和分析。如果部署拓扑需要在负载均衡器上进行 SNAT，则服务器会使用客户端 SNAT IP 地址，这违背了日志记录的目的。 解决办法是，可以将负载均衡器配置为插入带有原始客户端 IP 地址的 XFF HTTP 标头。可以将服务器配置为记录 XFF 标头中的 IP 地址，而不是连接的源 IP 地址。
连接闲置超时	输入 HTTP 应用程序可以保持闲置的时长（秒），而不是必须在 TCP 应用程序配置文件中配置的 TCP 套接字设置。
请求标头大小	指定用于存储 HTTP 请求标头的最大缓冲区大小（字节）。
NTLM 身份验证	<p>切换该按钮可使负载均衡器关闭 TCP 多路复用并启用 HTTP 保持活动状态。</p> <p>NTLM 身份验证协议可优先于 HTTP 使用。对于使用 NTLM 身份验证的负载均衡，必须为托管基于 NTLM 的应用程序的服务器池禁用 TCP 多路复用。否则，可能使用通过一个客户端的凭据建立的服务器端连接处理另一个客户端的请求。如果 NTLM 在配置文件中已启用并与虚拟服务器相关联，同时在服务器池启用了 TCP 多路复用，则 NTLM 优先。不会对该虚拟服务器执行 TCP 多路复用。但是，如果同一池与另一个非 NTLM 虚拟服务器相关联，则 TCP 多路复用可用于到该虚拟服务器的连接。</p> <p>如果客户端使用 HTTP/1.0，则负载均衡器将升级到 HTTP/1.1 协议并设置 HTTP 保持活动状态。基于同一客户端 TCP 连接接收的所有 HTTP 请求都通过单个 TCP 连接发送到相同服务器，以确保不需要重新授权。</p>

d 单击确定。

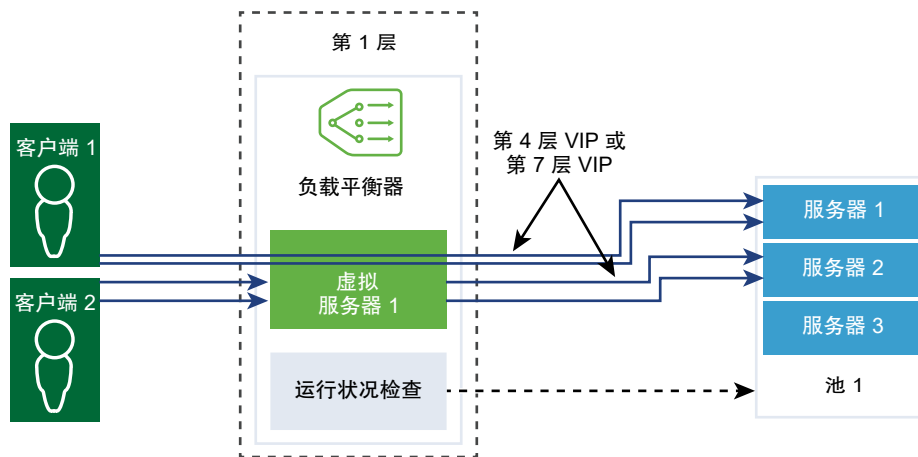
配置持久配置文件

负载均衡器可实现持久性，将所有相关连接定向到同一服务器，从而确保有状态应用程序的稳定性。为了满足不同类型的应用程序需求，支持不同类型的持久性。

某些应用程序会保持服务器状态，如购物车。此类状态可能基于客户端并由客户端 IP 地址或根据 HTTP 会话标识。在处理来自同一客户端或 HTTP 会话的后续相关连接时，应用程序可能会访问或修改此状态。

源 IP 持久性配置文件基于源 IP 地址跟踪会话。客户端请求连接到支持源地址持久性的虚拟服务器时，负载均衡器将检查该客户端之前是否曾建立连接；如果是，则将客户端返回给同一服务器。否则，可以根据池负载均衡算法选择服务器池成员。源 IP 持久性配置文件由第 4 层和第 7 层虚拟服务器使用。

Cookie 持久性配置文件将插入唯一的 Cookie，以便在客户端首次访问站点时标识会话。HTTP Cookie 在后续请求中由客户端转发，并且负载均衡器使用该信息提供 Cookie 持久性。Cookie 持久性配置文件只能由第 7 层虚拟服务器使用。请注意，不支持 Cookie 名称中存在空格。



步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择高级网络和安全 > 网络 > 负载均衡器 > 配置文件 > 持久性配置文件。
- 3 创建一个源 IP 持久性配置文件。
 - a 从下拉菜单中选择添加 > 源 IP 持久性。
 - b 输入源 IP 持久性配置文件的名称和描述。

- c 填写持久性配置文件详细信息。

您也可以接受默认源 IP 配置文件设置。

选项	说明
共享持久性	<p>切换该按钮以共享持久性，使与此配置文件关联的所有虚拟服务器均可共享持久性表。</p> <p>如果与虚拟服务器关联的源 IP 持久性配置文件中未启用持久性共享，则与配置文件关联的每个虚拟服务器都将维护一个专用持久性表。</p>
持久性条目超时	<p>输入持久性到期时间（秒）。</p> <p>负载均衡器持久性表维护用来记录客户端请求被定向到同一服务器的条目。</p> <ul style="list-style-type: none"> ■ 如果在超时期限内没有收到来自同一客户端的新连接请求，持久性条目将过期并被删除。 ■ 如果在超时期限内收到来自同一客户端的新连接请求，则会重置定时器，并将客户端请求发送到粘滞池成员。 <p>超时期限到期后，新连接请求将被发送到由负载均衡算法分配的服务器。对于 L7 负载均衡 TCP 源 IP 持久性场景，如果在一段时间内未建立新的 TCP 连接，持久性条目将超时，即使现有的连接仍处于活动状态。</p>
HA 持久性镜像	切换该按钮以将持久性条目同步到 HA 对等项。
已满时清除条目	<p>当持久性表已满时清除条目。</p> <p>如果流量很大，则较大的超时值可能会导致持久性表快速填满。当持久性表填满时，会删除最早的条目以接受最新条目。</p>

- d 单击**确定**。

4 创建一个 Cookie 持久性配置文件。

- 从下拉菜单中选择**添加 > Cookie 持久性**。
- 输入 Cookie 持久性配置文件的名称和描述。
- 切换**共享持久性**按钮以在与相同池成员关联的多个虚拟服务器之间共享持久性。

Cookie 持久性配置文件将插入格式为 **<名称>.<配置文件 ID>.<池 ID>** 的 Cookie。

如果与虚拟服务器关联的 Cookie 持久性配置文件中未启用持久性共享，则会使用每个虚拟服务器的专用 Cookie 持久性并由池成员对其进行限定。负载均衡器将插入格式为 **<名称>.<虚拟服务器 ID>.<池 ID>** 的 Cookie。

- d 单击**下一步**。

- e 填写持久性配置文件详细信息。

选项	说明
Cookie 模式	从下拉菜单中选择一个模式。 <ul style="list-style-type: none"> ■ INSERT - 添加唯一的 Cookie 以标识会话。 ■ PREFIX - 附加到现有 HTTP Cookie 信息。 ■ REWRITE - 重写现有 HTTP Cookie 信息。
Cookie 名称	输入 Cookie 名称。请注意，不支持 Cookie 名称中存在空格。
Cookie 域	输入域名。 HTTP Cookie 域只能在 INSERT 模式中配置。
Cookie 路径	输入 Cookie URL 路径。 HTTP Cookie 路径只能在 INSERT 模式中设置。
Cookie 加密	加密 Cookie 服务器 IP 地址和端口信息。 切换该按钮以禁用加密。禁用乱码时，Cookie 服务器 IP 地址和端口信息采用明文形式。
Cookie 回退	如果 Cookie 指向处于 DISABLED 或 DOWN 状态的服务器，请选择一个新的服务器来处理客户端请求。 切换该按钮，以便在 Cookie 指向处于 DISABLED 或 DOWN 状态的服务器时拒绝客户端请求。

- f 填写 Cookie 到期详细信息。

选项	说明
Cookie 时间类型	从下拉菜单中选择 Cookie 时间类型。 会话 Cookie 未存储，将在浏览器关闭后丢失。 持久性 Cookie 已由浏览器存储，将不会在浏览器关闭后丢失。
最长空闲时间	输入 Cookie 过期之前可以处于空闲状态的时间（以秒为单位）。
最长 Cookie 存在时间	仅适用于 会话 Cookie 。输入 Cookie 可以处于活动状态的最长时间（以秒为单位）。

- g 单击**完成**。

配置 SSL 配置文件

SSL 配置文件配置与应用程序无关的 SSL 属性（如密码列表）并在多个应用程序中重用这些列表。负载均衡器充当客户端和服务端时的 SSL 属性有所不同，因此支持使用单独的客户端和服务端 SSL 配置文件。

注 SSL 配置文件在 NSX-T Data Center Limited Export 版本中不受支持。

客户端 SSL 配置文件是指负载均衡器充当 SSL 服务器并终止客户端 SSL 连接。服务端 SSL 配置文件是指负载均衡器充当客户端并与服务器建立连接。

您可以在客户端和服务端 SSL 配置文件上指定密码列表。

通过 SSL 会话缓存，SSL 客户端和服务端可以重用先前商定的安全参数，避免在 SSL 握手期间发生开销很大的公钥操作。默认情况下，将在客户端和服务端禁用 SSL 会话缓存。

SSL 会话票证是另一种允许 SSL 客户端和服务端重用先前商定会话参数的机制。在 SSL 会话票证中，客户端和服务端商定是否在握手交换期间支持 SSL 会话票证。如果二者均支持，则服务器可以向客户端发送包含加密 SSL 会话参数的 SSL 票证。客户端可以在后续连接中使用该票证来重用会话。SSL 会话票证在客户端处于启用状态，但在服务器端处于禁用状态。

图 19-5. SSL 卸载

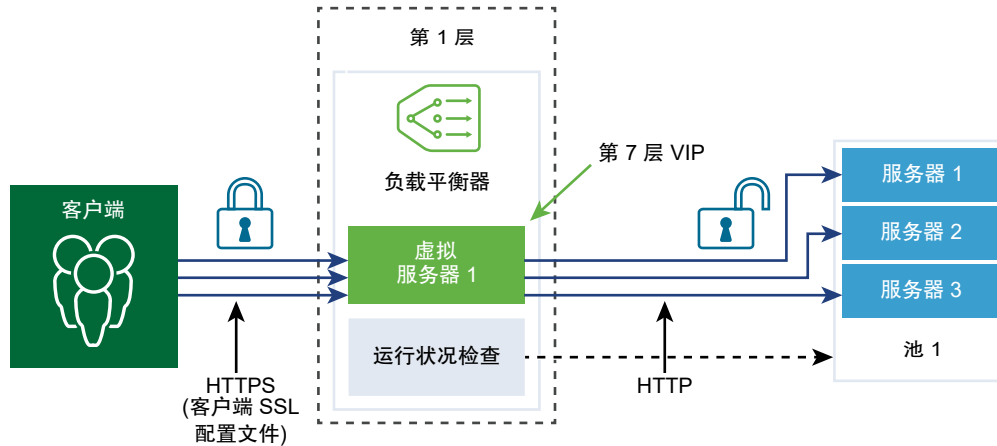
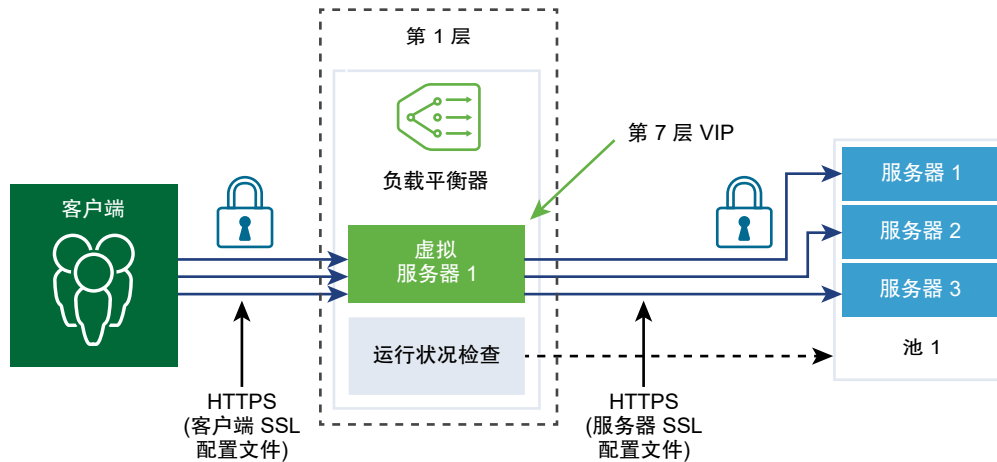


图 19-6. 端到端 SSL



步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择高级网络和安全 > 网络 > 负载均衡器 > 配置文件 > SSL 配置文件。
- 3 创建一个客户端 SSL 配置文件。
 - a 从下拉菜单中选择添加 > 客户端 SSL。
 - b 输入客户端 SSL 配置文件的名称和描述。
 - c 分配要包括在客户端 SSL 配置文件中的 SSL 密码。

此外，还可以创建自定义 SSL 密码。

- d 单击箭头将密码移至选定部分。
- e 单击**协议和会话**选项卡。
- f 选择要包括在客户端 SSL 配置文件中的 SSL 协议。

默认情况下，将启用 SSL 协议版本 TLS1.1 和 TLS1.2。TLS1.0 也受支持，但默认情况下处于禁用状态。

- g 单击箭头将协议移至选定部分。
- h 填写 SSL 协议详细信息。

您也可以接受 SSL 配置文件的默认设置。

选项	说明
会话缓存	通过 SSL 会话缓存，SSL 客户端和服务器可以重用先前商定的安全参数，避免在 SSL 握手期间发生开销很大的公钥操作。
会话缓存条目超时	输入缓存超时（秒）以指定 SSL 会话参数必须保留并可重用的时长。
首选服务器密码	切换该按钮，使服务器可以从其支持的列表中选择第一个受支持的密码。 在 SSL 握手期间，客户端向服务器发送经过排序的受支持密码列表。

- i 单击**确定**。

4 创建一个服务器 SSL 配置文件。

- a 从下拉菜单中选择**添加 > 服务器端 SSL**。
- b 输入服务器 SSL 配置文件的名称和描述。
- c 选择要包括在服务器 SSL 配置文件中的 SSL 密码。

此外，还可以创建自定义 SSL 密码。

- d 单击箭头将密码移至选定部分。
- e 单击**协议和会话**选项卡。
- f 选择要包括在服务器 SSL 配置文件中的 SSL 协议。

默认情况下，将启用 SSL 协议版本 TLS1.1 和 TLS1.2。TLS1.0 也受支持，但默认情况下处于禁用状态。

- g 单击箭头将协议移至选定部分。
- h 接受默认会话缓存设置。

通过 SSL 会话缓存，SSL 客户端和服务器可以重用先前商定的安全参数，避免在 SSL 握手期间发生开销很大的公钥操作。

- i 单击**确定**。

配置第 4 层虚拟服务器

虚拟服务器接收所有客户端连接并在服务器之间进行分发。虚拟服务器具有 IP 地址、端口和协议。对于第 4 层虚拟服务器，可以指定端口范围列表，而不是单个 TCP 或 UDP 端口，以支持具有动态端口的复杂协议。

第 4 层虚拟服务器必须与主服务器池（也称为默认池）相关联。

如果虚拟服务器状态为已禁用，则会通过发送 TCP RST（对于 TCP 连接）或 ICMP 错误消息（对于 UDP）拒绝对虚拟服务器的任何新连接尝试。即使新连接存在匹配的持久性条目，也会拒绝这些连接。活动连接将继续进行处理。如果虚拟服务器从负载均衡器中删除或与负载均衡器解除关联，则到该虚拟服务器的活动连接将失败。

前提条件

- 确认应用程序配置文件可用。请参见[配置应用程序配置文件](#)。
- 确认持久配置文件可用。请参见[配置持久配置文件](#)。
- 确认客户端和服务器的 SSL 配置文件可用。请参见[配置 SSL 配置文件](#)。
- 确认服务器池可用。请参见[添加服务器池用于负载均衡](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 选择 **高级网络和安全 > 网络 > 负载均衡器 > 虚拟服务器 > 添加**。
- 3 输入第 4 层虚拟服务器的名称和描述。
- 4 从下拉菜单中选择一个第 4 层协议。

第 4 层虚拟服务器支持 Fast TCP 或 Fast UDP 协议，而不同时支持两者。要在相同的 IP 地址和端口上支持 Fast TCP 或 Fast UDP 协议，例如 DNS，必须为每个协议创建一个虚拟服务器。

根据协议类型，将自动填充现有应用程序配置文件。

- 5 切换“访问日志”按钮以启用第 4 层虚拟服务器的日志记录。
- 6 单击**下一步**。
- 7 输入虚拟服务器 IP 地址和端口号。

您可以输入虚拟服务器的端口号或端口范围。

8 填写高级属性详细信息。

选项	说明
最大并发连接	设置允许与虚拟服务器建立的最大并发连接，这样虚拟服务器就不会耗尽托管在同一负载均衡器上的其他应用程序的资源。
最大新连接速率	设置与服务器池成员的最大新连接，这样虚拟服务器就不会耗尽资源。
默认池成员端口	如果未定义虚拟服务器的池成员端口，请输入默认池成员端口。 例如，如果虚拟服务器通过端口范围 2000-2999 定义，并且默认池成员端口范围设置为 8000-8999，则将虚拟服务器端口 2500 的入站客户端连接发送到目标端口设置为 8500 的池成员。

9 从下拉菜单中选择现有服务器池。

服务器池包含一个或多个配置类似并运行相同应用程序的服务器（也称为池成员）。

10 从下拉菜单中选择现有 Sorry Server 池。

负载均衡器无法从默认池选择后端服务器来处理请求时，Sorry Server 池将处理请求。

11 单击下一步。

12 从下拉菜单中选择现有持久性配置文件。

可以在虚拟服务器上启用持久性配置文件，从而允许将相关的客户端连接发送到相同服务器。

13 单击完成。

配置第 7 层虚拟服务器

虚拟服务器接收所有客户端连接并在服务器之间进行分发。虚拟服务器具有 IP 地址、端口和协议 TCP。

仅具有 HTTP 应用程序配置文件的第 7 层虚拟服务器支持负载均衡器规则。不同的负载均衡器服务可以使用负载均衡器规则。

每个负载均衡器规则由一个或多个匹配条件和单项或多项操作组成。如果未指定匹配条件，则负载均衡器规则始终匹配并用于定义默认规则。如果指定了多个匹配条件，则匹配策略确定必须匹配所有条件还是必须匹配任一条件，负载均衡器规则才会被视为匹配项。

每个负载均衡器规则在负载均衡处理的特定阶段实施：HTTP 请求重写、HTTP 请求转发和 HTTP 响应重写。并非所有匹配条件和操作都适用于每个阶段。

如果虚拟服务器状态为已禁用，则会通过发送 TCP RST（对于 TCP 连接）或 ICMP 错误消息（对于 UDP）拒绝对虚拟服务器的任何新连接尝试。即使新连接存在匹配的持久性条目，也会拒绝这些连接。活动连接将继续进行处理。如果虚拟服务器从负载均衡器中删除或与负载均衡器解除关联，则到该虚拟服务器的活动连接将失败。

前提条件

- 确认应用程序配置文件可用。请参见[配置应用程序配置文件](#)。
- 确认持久配置文件可用。请参见[配置持久配置文件](#)。
- 确认客户端和服务器的 SSL 配置文件可用。请参见[配置 SSL 配置文件](#)。

- 确认服务器池可用。请参见[添加服务器池用于负载均衡](#)。
- 确认 CA 和客户端证书可用。请参见[创建证书签名请求文件](#)。
- 确认证书吊销列表 (CRL) 可用。请参见[导入证书吊销列表](#)。
- **配置第 7 层虚拟服务器池和规则**
通过第 7 层虚拟服务器，您可以选择配置负载均衡器规则并使用匹配或操作规则自定义负载均衡行为。
- **配置第 7 层虚拟服务器负载均衡配置文件**
通过第 7 层虚拟服务器，您可以选择配置负载均衡器持久性配置文件、客户端 SSL 配置文件和服务器端 SSL 配置文件。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 选择**高级网络和安全 > 网络 > 负载均衡器 > 虚拟服务器 > 添加**。
- 3 输入第 7 层虚拟服务器的名称和描述。
- 4 选择“第 7 层”菜单项。
第 7 层虚拟服务器支持 HTTP 和 HTTPS 协议。
将自动填充现有 HTTP 应用程序配置文件。
- 5 （可选）单击**下一步**以配置服务器池和负载均衡配置文件。
- 6 单击**完成**。

配置第 7 层虚拟服务器池和规则

通过第 7 层虚拟服务器，您可以选择配置负载均衡器规则并使用匹配或操作规则自定义负载均衡行为。

负载均衡器规则支持 REGEX 匹配类型。支持 PCRE 样式 REGEX 模式，但高级用例存在一些限制。在匹配条件中使用 REGEX 时，支持已命名捕获组。

REGEX 限制包括：

- 不支持字符并集和交集。例如，不要使用 `[a-z[0-9]]` 和 `[a-z&&[aeiou]]`，而要相应使用 `[a-z0-9]` 和 `[aeiou]`。
- 仅支持 9 个向后引用，可以使用 `\1` 到 `\9` 来引用它们。
- 请使用 `\Odd` 格式来匹配八进制数字，而不要使用 `\ddd` 格式。
- 顶层级别不支持嵌入式标记，嵌入式标记仅在组中受支持。例如，不要使用“`Case (?i:s)ensitive`”，而要使用“`Case ((?i:s)ensitive)`”。
- 不支持预处理操作 `\l`、`\u`、`\L` 和 `\U`。其中 `\l` 是将下一字符变为小写，`\u` 是将下一字符变为大写，`\L` 将后续直至 `\E` 的字符变为小写，`\U` 则将后续直至 `\E` 的字符变为大写。
- 不支持 `(?(condition)X)`、`(? {code})`、`(??{Code})` 和 `(?#comment)`。
- 不支持预定义的 Unicode 字符类 `\X`

- 不支持对 Unicode 字符使用已命名字符构造。例如，不要使用 `\N{name}`，而要使用 `\u2018`。

在匹配条件中使用 REGEX 时，支持已命名捕获组。例如，可以使用 REGEX 匹配模式 `/news/(?<year>\d+)-(?<month>\d+)-(?<day>\d+)/(?<article>.*)` 来匹配类似于 `/news/2018-06-15/news1234.html` 的 URI。

然后按如下所示设置变量：`$year = "2018" $month = "06" $day = "15" $article = "news1234.html"`。设置变量后，可以在负载均衡器规则操作中使用这些变量。例如，可以使用匹配的变量来重写 URI，例如 `/news.py?year=$year&month=$month&day=$day&article=$article`。该 URI 随后重写为 `/news.py?year=2018&month=06&day=15&article=news1234.html`。

重写操作可以使用已命名捕获组和内置变量的组合。例如，URI 可以重写为 `/news.py?year=$year&month=$month&day=$day&article=$article&user_ip=$_remote_addr`。该示例 URI 随后重写为 `/news.py?year=2018&month=06&day=15&article=news1234.html&user_ip=1.1.1.1`。

注 对于已命名捕获组，名称不能以字符 `_` 开头。

除了已命名捕获组之外，还可以在重写操作中使用以下内置变量。所有内置变量的名称均以 `_` 开头。

- `$_args` - 请求中的参数
- `$_arg_<name>` - 请求行中的参数 `<name>`
- `$_cookie_<name>` - `<name>` Cookie 的值
- `$_upstream_cookie_<name>` - 由“Set-Cookie”响应标头字段中的上游服务器发送的具有指定名称的 Cookie
- `$_upstream_http_<name>` - 任意响应标头字段，`<name>` 是字段名称，该字段名称将转换为小写，并且其中的短划线将替换为下划线
- `$_host` - 按优先级顺序，请求行中的主机名，或者“Host”请求标头字段中的主机名或与请求匹配的服务器名称
- `$_http_<name>` - 任意请求标头字段，`<name>` 是字段名称，该字段名称将转换为小写，并且其中的短划线将替换为下划线
- `$_https` - 如果连接在 SSL 模式下工作，为 `"on"`；否则为 `""`
- `$_is_args` - 如果请求行包含参数，为 `"?"`；否则为 `""`
- `$_query_string` - 与 `$_args` 相同
- `$_remote_addr` - 客户端地址
- `$_remote_port` - 客户端端口
- `$_request_uri` - 完整的原始请求 URI（包含参数）
- `$_scheme` - 请求方案“http”或“https”
- `$_server_addr` - 接受请求的服务器的地址
- `$_server_name` - 接受请求的服务器的名称
- `$_server_port` - 接受请求的服务器的端口

- `$_server_protocol` - 请求协议，通常为“HTTP/1.0”或“HTTP/1.1”
- `$_ssl_client_cert` - 为已建立的 SSL 连接返回 PEM 格式的客户端证书，证书中除第一行以外的每一行开头均附加制表符字符
- `$_ssl_server_name` - 通过 SNI 返回请求的服务器名称
- `$_uri` - 请求中的 URI 路径
- `$_ssl_ciphers` - 返回客户端 SSL 密码
- `$_ssl_client_i_dn` - 根据 RFC 2253 返回建立的 SSL 连接的客户端证书的“颁发者 DN”字符串
- `$_ssl_client_s_dn` - 根据 RFC 2253 返回建立的 SSL 连接的客户端证书的“主体 DN”字符串
- `$_ssl_protocol` - 返回建立的 SSL 连接的协议
- `$_ssl_session_reused` - 如果重用 SSL 会话，则返回“r”，否则，返回“.”

前提条件

确认第 7 层虚拟服务器可用。请参见配置第 7 层虚拟服务器。

步骤

- 1 打开第 7 层虚拟服务器。
- 2 跳至“虚拟服务器标识符”页面。
- 3 输入虚拟服务器 IP 地址和端口号。
您可以输入虚拟服务器的端口号或端口范围。
- 4 填写高级属性详细信息。

选项	说明
最大并发连接	设置允许与虚拟服务器建立的最大并发连接，这样虚拟服务器就不会耗尽托管在同一负载均衡器上的其他应用程序的资源。
最大新连接速率	设置与服务器池成员的最大新连接，这样虚拟服务器就不会耗尽资源。
默认池成员端口	如果未定义虚拟服务器的池成员端口，请输入默认池成员端口。 例如，如果虚拟服务器的端口范围定义为 2000-2999，默认池成员端口范围设置为 8000-8999，则到虚拟服务器端口 2500 的传入客户端连接将被发送到目标端口设置为 8500 的池成员。

- 5 （可选）从下拉菜单中选择现有默认服务器池。

服务器池包含一个或多个配置类似并运行相同应用程序的服务器（称为池成员）。

6 单击**添加**以配置 HTTP 请求重写阶段的负载均衡器规则。

支持的匹配类型是 REGEX、STARTS_WITH、ENDS_WITH 等，以及逆反选项。

支持的匹配条件	说明
HTTP 请求方法	与 HTTP 请求方法匹配。 http_request.method - 要匹配的值
HTTP 请求 URI	与不带查询参数的 HTTP 请求 URI 匹配。 http_request.uri - 要匹配的值
HTTP 请求 URI 参数	与 HTTP 请求 URI 查询参数匹配。 http_request.uri_arguments - 要匹配的值
HTTP 请求版本	与 HTTP 请求版本匹配。 http_request.version - 要匹配的值
HTTP 请求标头	与任何 HTTP 请求标头匹配。 http_request.header_name - 要匹配的标头名称 http_request.header_value - 要匹配的值
HTTP 请求负载	与 HTTP 请求正文内容匹配。 http_request.body_value - 要匹配的值
TCP 标头字段	与 TCP 源或目标端口匹配。 tcp_header.source_port - 要匹配的源端口 tcp_header.destination_port - 要匹配的目标端口
IP 标头字段	与 IP 源或目标地址匹配。 ip_header.source_address - 要匹配的源地址 ip_header.destination_address - 要匹配的目标地址
操作	说明
HTTP 请求 URI 重写	修改 URI。 http_request.uri - 要写入的 URI（不含查询参数） http_request.uri_args - 要写入的 URI 查询参数
HTTP 请求标头重写	修改 HTTP 标头的值。 http_request.header_name - 标头名称 http_request.header_value - 要写入的值

7 单击**添加**以配置 HTTP 请求转发的负载均衡器规则。

所有匹配值接受正则表达式。

支持的匹配条件	说明
HTTP 请求方法	与 HTTP 请求方法匹配。 http_request.method - 要匹配的值
HTTP 请求 URI	与 HTTP 请求 URI 匹配。 http_request.uri - 要匹配的值

支持的匹配条件	说明
HTTP 请求 URI 参数	与 HTTP 请求 URI 查询参数匹配。 http_request.uri_args - 要匹配的值
HTTP 请求版本	与 HTTP 请求版本匹配。 http_request.version - 要匹配的值
HTTP 请求标头	与任何 HTTP 请求标头匹配。 http_request.header_name - 要匹配的标头名称 http_request.header_value - 要匹配的值
HTTP 请求负载	与 HTTP 请求正文内容匹配。 http_request.body_value - 要匹配的值
TCP 标头字段	与 TCP 源或目标端口匹配。 tcp_header.source_port - 要匹配的源端口 tcp_header.destination_port - 要匹配的目标端口
IP 标头字段	与 IP 源地址匹配。 ip_header.source_address - 要匹配的源地址

操作	说明
拒绝	拒绝请求，例如，通过将状态设置为 5xx。 http_forward.reply_status - 用于拒绝的 HTTP 状态代码 http_forward.reply_message - HTTP 拒绝消息
重定向	重定向请求。状态代码必须设置为 3xx。 http_forward.redirect_status - 用于重定向的 HTTP 状态代码 http_forward.redirect_url - HTTP 重定向 URL
选择池	将请求强制到特定服务器池。指定池成员的配置算法（预测器）用于在服务器池中 选择服务器。 http_forward.select_pool - 服务器池 UUID

8 单击**添加**以配置 HTTP 响应重写的负载均衡器规则。

所有匹配值接受正则表达式。

支持的匹配条件	说明
HTTP 响应标头	与任何 HTTP 响应标头匹配。 http_response.header_name - 要匹配的标头名称 http_response.header_value - 要匹配的值

操作	说明
HTTP 响应标头重写	修改 HTTP 响应标头的值。 http_response.header_name - 标头名称 http_response.header_value - 要写入的值

9 （可选）单击**下一步**以配置负载均衡配置文件。

10 单击**完成**。

配置第 7 层虚拟服务器负载均衡配置文件

通过第 7 层虚拟服务器，您可以选择配置负载均衡器持久性配置文件、客户端 SSL 配置文件和服务器端 SSL 配置文件。

注 SSL 配置文件在 NSX-T Data Center Limited Export 版本中不受支持。

如果在虚拟服务器上配置了客户端 SSL 配置文件绑定，而不是服务器端 SSL 配置文件绑定，则虚拟服务器在 SSL 终止模式下运行，该模式与客户端和服务器分别具有加密连接和明文连接。如果同时配置了客户端和服务器端 SSL 配置文件绑定，则虚拟服务器在 SSL 代理模式下运行，该模式与客户端和服务器具有加密连接。

目前不支持在不关联客户端 SSL 配置文件绑定的情况下关联服务器端 SSL 配置文件绑定。如果客户端和服务器端 SSL 配置文件绑定不与虚拟服务器相关联且应用程序基于 SSL，则虚拟服务器在 SSL 非感知模式下运行。在这种情况下，必须为第 4 层配置虚拟服务器。例如，虚拟服务器可与 Fast TCP 配置文件相关联。

前提条件

确认第 7 层虚拟服务器可用。请参见[配置第 7 层虚拟服务器](#)。

步骤

1 打开第 7 层虚拟服务器。

2 跳到“负载均衡配置文件”页面。

3 切换“持久性”按钮以启用该配置文件。

持久性配置文件允许将相关的客户端连接发送到相同服务器。

4 选择“源 IP 持久性”或“Cookie 持久性”配置文件。

5 从下拉菜单中选择现有持久性配置文件。

6 单击**下一步**。

7 切换“客户端 SSL”按钮以启用该配置文件。

客户端 SSL 配置文件绑定允许对要与同一虚拟服务器相关联的不同主机名使用多个证书。

将自动填充关联的客户端 SSL 配置文件。

8 从下拉菜单中选择一个默认证书。

如果服务器不将多个主机名托管在同一 IP 地址上或客户端不支持服务器名称指示 (SNI) 扩展，则会使用此证书。

9 选择可用的 SNI 证书，然后单击箭头将该证书移至选定部分。

10 （可选）切换“强制客户端身份验证”以启用此菜单项。

11 选择可用的 CA 证书，然后单击箭头将该证书移至选定部分。

12 设置证书链深度以验证服务器证书链深度。

- 13** 选择可用的 CRL，然后单击箭头将该证书移至选定部分。

可以将 CRL 配置为禁止已损坏的服务器证书。

- 14** 单击**下一步**。

- 15** 切换“服务器端 SSL”按钮以启用该配置文件。

将自动填充关联的服务器端 SSL 配置文件。

- 16** 从下拉菜单中选择一个客户端证书。

如果服务器不将多个主机名托管在同一 IP 地址上或客户端不支持服务器名称指示 (SNI) 扩展，则会使用客户端证书。

- 17** 选择可用的 SNI 证书，然后单击箭头将该证书移至选定部分。

- 18** （可选）切换“服务器身份验证”以启用此菜单项。

服务器端 SSL 配置文件绑定指定是否必须验证在 SSL 握手期间提供给负载均衡器的服务器证书。启用验证后，服务器证书必须由其中一个可信 CA 签名，这些 CA 的自签名证书在同一服务器端 SSL 配置文件绑定中指定。

- 19** 选择可用的 CA 证书，然后单击箭头将该证书移至选定部分。

- 20** 设置证书链深度以验证服务器证书链深度。

- 21** 选择可用的 CRL，然后单击箭头将该证书移至选定部分。

可以将 CRL 配置为禁止已损坏的服务器证书。服务器端上不支持 OCSP 和 OCSP 装订 (OCSP stapling)。

- 22** 单击**完成**。

注 如果使用**高级网络和安全**用户界面来修改策略“略界”面中创建的对象，则某些设置可能无法配置。这些只读设置的旁边有此图标：⊖。有关详细信息，请参见第 1 章 **NSX Manager 概览**。

本章讨论了以下主题：

- 在逻辑路由器中添加或删除防火墙规则
- 为逻辑交换机网桥端口配置防火墙
- 防火墙区域和防火墙规则
- 关于防火墙规则

在逻辑路由器中添加或删除防火墙规则

您可以将防火墙规则添加到 Tier-0 或 Tier-1 逻辑路由器以控制到该路由器的通信。

Edge 防火墙在上行链路路由器端口上实施，这意味着防火墙规则仅适用于流量流过 Edge 上上行链路路由器端口的情况。要将防火墙规则应用于特定的 IP 目标，必须使用 /32 网络配置组。如果提供的子网不是 /32，则防火墙规则将会应用到整个子网。

前提条件

熟悉防火墙规则的参数。请参见**添加防火墙规则**。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 选择**高级网络和安全 > 网络 > 路由器**。
- 3 如果尚未选择**路由器**选项卡，请单击该选项卡。
- 4 单击一个逻辑路由器的名称。
- 5 选择**服务 > Edge 防火墙**。
- 6 单击一个现有的区域或规则。

- 7 要添加规则，请单击菜单栏上的**添加规则**并选择**在上面添加规则**或**在下面添加规则**，或者单击规则的第一列中的菜单图标并选择**在上面添加规则**或**在下面添加规则**，然后指定规则参数。

由于该规则仅适用于逻辑路由器，因此，不会显示“应用对象”字段。

- 8 要删除规则，请选择该规则，单击菜单栏上的**删除**，或者单击第一列中的菜单图标并选择**删除**。

结果

注 如果将防火墙规则添加到 Tier-0 逻辑路由器且支持该路由器的 NSX Edge 群集在主动-主动模式下运行，则防火墙只能在无状态模式下运行。如果使用 HTTP、SSL 和 TCP 等有状态服务配置防火墙规则，防火墙规则将不按预期工作。为了避免出现此问题，请将 NSX Edge 群集配置为在活动-备用模式下运行。

为逻辑交换机网桥端口配置防火墙

可以为第 2 层网桥支持的逻辑交换机的网桥端口配置防火墙区域和防火墙规则。必须使用 NSX Edge 节点创建网桥。

前提条件

验证交换机是否已连接到网桥配置文件。请参见[创建支持网桥的第 2 层逻辑交换机](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**高级网络和安全 > 安全 > 网桥防火墙**。
- 3 选择逻辑交换机。

该交换机必须连接到网桥配置文件。
- 4 按照前几节中的相同步骤配置第 2 层或第 3 层防火墙。

防火墙区域和防火墙规则

防火墙区域用于对一组防火墙规则进行分组。

防火墙区域由一个或多个单独的防火墙规则组成。每个单独的防火墙规则包含确定是应允许还是阻止数据包的说明；允许数据包使用哪些协议；允许数据包使用哪些端口，等等。区域用于多租户，例如，用于销售和工程部门的特定规则位于单独的区域中。

可以将一个区域定义为强制实施有状态或无状态规则。无状态规则被视为传统无状态 ACL。无状态区域不支持反射 ACL。建议不要在单个逻辑交换机端口上混用无状态和有状态规则，这可能会导致未定义的行为。

可以在区域中上下移动规则。对于尝试通过防火墙的任何流量，将按照区域中显示的顺序应用规则以处理数据包信息，从顶部开始并移到底部的默认规则。与数据包匹配的第一个规则将应用它配置的操作，并执行在该规则配置的选项中指定的任何处理，而忽略所有后续规则（即使后面的规则是更好的匹配项）。因此，您应该将具体的规则放在更常规的规则上面，以确保不会忽略这些规则。默认规则（位于规则表底部）是一个总括性规则；将为与任何其他规则不匹配的数据包强制实施默认规则。

注 逻辑交换机有一个称为 **N-VDS** 模式的属性。此属性来自交换机所属的传输区域。如果 **N-VDS** 模式为 **ENS**（也称为 **Enhanced Datapath**），则无法使用交换机或其端口在 **Source**、**Destination** 或 **Applied To** 字段中创建防火墙规则或区域。

启用和禁用分布式防火墙

您可以启用或禁用分布式防火墙功能。

如果禁用该功能，则在数据层面级别不强制实施防火墙规则。重新启用时，将重新强制实施规则。

步骤

- 1 导航到 **高级网络和安全 > 安全 > 分布式防火墙**。
- 2 单击**设置**选项卡。
- 3 单击分布式防火墙**编辑**。
- 4 在对话框中，将防火墙状态切换为绿色（已启用）或灰色（已禁用）。
- 5 单击**保存**。

添加防火墙规则区域

防火墙规则区域是单独编辑和保存的，用于将单独的防火墙配置应用于租户。

步骤

- 1 选择**高级网络和安全 > 安全 > 分布式防火墙**。
- 2 对于第 3 层 (L3) 规则，请单击**常规**选项卡；对于第 2 层 (L2) 规则，请单击**以太网**选项卡。
- 3 单击一个现有的区域或规则。
- 4 单击菜单栏上的区域图标，然后选择**在上方添加区域**或**在下方添加区域**。

注 对于尝试通过防火墙的任何流量，将按照“规则”表中显示的顺序应用规则以处理数据包信息，从顶部开始并移到底部的默认规则。在某些情况下，两个或更多规则的优先级顺序在确定如何处理数据包方面可能是非常重要的。

- 5 输入区域名称。

- 6 要将防火墙设为无状态，请选择**启用无状态防火墙**。此选项仅适用于 L3。

无状态防火墙监控网络流量，并根据源和目标地址或其他静态值限制或阻止数据包。对于 TCP 和 UDP 流量，如果防火墙结果为 **ALLOW**，则在第一个数据包之后，将为任一方向的流量元组创建并维护缓存。这意味着流量不再需要通过防火墙规则进行检查，从而降低延迟。因此，在较高的流量负载下，无状态防火墙通常速度更快，性能更好。

有状态防火墙可以监控从一端到另一端的流量流。将始终针对每个数据包查询防火墙，以验证状态和序列号。有状态防火墙在识别未授权和伪造的通信方面更好。

在定义后，就不会在有状态和无状态之间进行切换。

- 7 选择一个或多个对象以应用区域。

对象类型包括逻辑端口、逻辑交换机和 NS 组。如果您选择 NS 组，则它必须包含一个或多个逻辑交换机或逻辑端口。如果 NS 组仅包含 IP 集或 MAC 集，则将被忽略。

注 区域中的**应用对象**将覆盖该区域中规则的所有**应用对象**设置。

- 8 单击**确定**。

后续步骤

将防火墙规则添加到区域。

删除防火墙规则区域

在不再使用防火墙规则区域时，可以删除该区域。

在删除防火墙规则区域时，将删除该区域中的所有规则。不能在删除某个区域后将其重新添加到防火墙表中的其他位置。要执行该操作，必须删除该区域并发布配置。然后将已删除的区域添加到防火墙表，并重新发布配置。

步骤

- 1 选择**高级网络和安全 > 安全 > 分布式防火墙**。
- 2 对于 L3 规则，请单击**常规**选项卡；对于 L2 规则，请单击**以太网**选项卡。
- 3 单击该区域的第一列中的菜单图标，然后选择**删除区域**。
也可以选择区域，然后单击菜单栏上的删除图标。

启用和禁用区域规则

您可以在防火墙规则区域中启用或禁用所有规则。

步骤

- 1 选择**高级网络和安全 > 安全 > 分布式防火墙**。
- 2 对于 L3 规则，请单击**常规**选项卡；对于 L2 规则，请单击**以太网**选项卡。
- 3 单击该区域的第一列中的菜单图标，然后选择**启用所有规则**或**禁用所有规则**。

4 单击**发布**。

启用和禁用区域日志

启用区域规则的日志将记录有关区域中的所有规则的数据包的信息。根据区域中的规则数，典型防火墙区域将生成大量日志信息，并且可能会影响性能。

日志存储在 ESXi 和 KVM 主机上的 `/var/log/dfwpktlogs.log` 文件中。

步骤

- 1 选择**高级网络和安全 > 安全 > 分布式防火墙**。
- 2 对于 L3 规则，请单击**常规**选项卡；对于 L2 规则，请单击**以太网**选项卡。
- 3 单击该区域的第一列中的菜单图标，然后选择**启用日志**或**禁用日志**。
- 4 单击**发布**。

配置防火墙排除列表

可以从防火墙规则中排除逻辑端口、逻辑交换机或 NS 组。

在创建一个具有防火墙规则的区域后，您可能希望将某个 NSX-T Data Center 设备端口从防火墙规则中排除。

注 NSX-T Data Center 会自动将 NSX Manager 和 NSX Edge 节点虚拟机添加到防火墙排除列表中。

步骤

- 1 选择**高级网络和安全 > 安全 > 分布式防火墙 > 排除列表 > 添加**。
- 2 选择一种类型和一个对象。
可用的类型包括**逻辑端口**、**逻辑交换机**和**NS 组**。
- 3 单击**确定**。
- 4 要从排除列表中移除对象，请选择该对象，然后单击菜单栏上的**删除**。

关于防火墙规则

NSX-T Data Center 使用防火墙规则指定流入和流出网络的流量处理。

防火墙提供了多组可配置的规则：第 3 层规则（“常规”选项卡）和第 2 层规则（“以太网”选项卡）。先处理第 2 层防火墙规则，然后再处理第 3 层规则。您可以配置一个排除列表，其中包含要从防火墙实施中排除的逻辑交换机、逻辑端口或组。

防火墙规则是按以下方式强制实施的：

- 规则是按从上到下的顺序处理的。
- 根据规则表中的最上面规则检查每个数据包，然后向下移到表中的后续规则。
- 强制实施表中与流量参数匹配的**第一个**规则。

无法强制实施后续规则，因为随后将停止为该数据包搜索规则。由于这种行为，始终建议将最精细的策略放在规则表顶部。这将确保在较具体的规则之前强制实施这些规则。

默认规则（位于规则表底部）是一个总括性规则；将为与任何其他规则不匹配的数据包强制实施默认规则。在执行主机准备操作后，默认规则将设置为允许操作。这可确保虚拟机到虚拟机的通信在暂存或迁移阶段不会中断。最佳做法是将该默认规则更改为阻止操作，并通过积极控制模式强制实施访问控制（即，仅允许将防火墙规则中定义的流量传输到网络上）。

注 可以在每个区域启用“TCP 严格模式”，以禁止在会话中途提取数据，并实现三向握手要求。当为某个特定的分布式防火墙区域启用“TCP 严格模式”，并使用默认的“任意-任意”阻止规则时，将丢弃此区域中不满足三向握手连接要求且与基于 TCP 的规则相匹配的数据包。“严格模式”仅适用于有状态 TCP 规则，并在分布式防火墙区域级别启用。对于符合默认的“任意-任意”允许规则的数据包，因为其没有指定任何 TCP 服务，因此不会对其强制执行“TCP 严格模式”。

表 20-1. 防火墙规则的属性

属性	说明
名称	防火墙规则的名称。
ID	系统为每个规则生成的唯一 ID。
源	规则源可以是 IP 或 MAC 地址或者 IP 地址以外的对象。如果未定义，源将与任何内容匹配。源或目标范围都支持 IPv4 和 IPv6。
目标	受规则影响的连接的目标 IP 或 MAC 地址/网络掩码。如果未定义，目标将与任何内容匹配。源或目标范围都支持 IPv4 和 IPv6。
服务	对于 L3，服务可以是预定义的端口协议组合。对于 L2，服务可以是以太网类型。对于 L2 和 L3，您可以手动定义新的服务或服务组。如果未指定，服务将与任何内容匹配。
应用对象	定义该规则的适用范围。如果未定义，范围将是所有逻辑端口。如果在某个区域中添加了“应用对象”，它将覆盖规则。
日志	可以禁用或启用日志记录。日志存储在 ESX 和 KVM 主机上的 /var/log/dfwpktlogs.log 文件中。
操作	规则应用的操作可以是 允许 、 丢弃 或 拒绝 。默认操作为 允许 。
IP 协议	选项包括 IPv4 、 IPv6 和 IPv4_IPv6 。默认选项为 IPv4_IPv6 。要访问此属性，请单击 高级设置 图标。
方向	选项包括 入站 、 出站 和 入站/出站 。默认选项为 入站/出站 。此字段指从目标对象角度来查看的流量方向。 入站 意味着只检查流入对象的流量， 出站 意味着只检查从对象流出的流量， 入站/出站 意味着检查两个方向的流量。要访问此属性，请单击 高级设置 图标。
规则标记	已添加到规则的标记。要访问此属性，请单击 高级设置 图标。
流量统计信息	这是一个只读字段，其中显示了字节数、数据包计数和会话数。要访问此属性，请单击 图形 图标。

注 如果未启用 SpoofGuard，则无法保证自动发现的地址绑定是可信的，因为恶意虚拟机可能声称具有另一个虚拟机的地址。如果启用，SpoofGuard 将验证每个发现的绑定，以便仅提供批准的绑定。

添加防火墙规则

防火墙是一个网络安全系统，它根据预定的防火墙规则监视和控制入站和出站的网络流量。

防火墙规则是在 **NSX Manager** 范围内添加的。然后，可以使用“应用对象”字段缩小要应用规则的范围。您可以在源级别和目标级别为每个规则添加多个对象，以帮助减少要添加的防火墙规则的总数。

注 默认情况下，规则与任何源、目标和服务规则元素的默认值匹配，从而与所有接口和流量方向匹配。如果要限制规则对特定接口或流量方向的影响，必须在规则中指定该限制。

前提条件

要使用一组地址，请先手动将每个虚拟机的 IP 和 MAC 地址与其逻辑交换机相关联。

步骤

- 1 选择**高级网络和安全 > 安全 > 分布式防火墙**。
- 2 对于 L3 规则，请单击**常规**选项卡；对于 L2 规则，请单击**以太网**选项卡。
- 3 单击一个现有的区域或规则。
- 4 单击规则第一列中的菜单图标，然后选择**在上面添加规则**或**在下面添加规则**。

将显示一个新行以定义防火墙规则。

注 对于尝试通过防火墙的任何流量，将按照“规则”表中显示的顺序应用规则以处理数据包信息，从顶部开始并移到底部的默认规则。在某些情况下，两个或更多规则的优先级顺序在确定如何处理数据包方面可能是非常重要的。

- 5 在**名称**列中，输入规则名称。
- 6 在**源**列中，单击编辑图标并选择规则的源。如果未定义，源将与任何内容匹配。

选项	说明
IP 地址	在以逗号分隔的列表中输入多个 IP 或 MAC 地址。该列表最多可以包含 255 个字符。支持 IPv4 和 IPv6 格式。
容器对象	可用对象为 IP 集、逻辑端口、逻辑交换机和 NS 组。选择对象，然后单击 确定 。

- 7 在**目标**列中，单击编辑图标并选择目标。如果未定义，目标将与任何内容匹配。

选项	说明
IP 地址	您可以在以逗号分隔的列表中输入多个 IP 或 MAC 地址。该列表最多可以包含 255 个字符。支持 IPv4 和 IPv6 格式。
容器对象	可用对象为 IP 集、逻辑端口、逻辑交换机和 NS 组。选择对象，然后单击 确定 。

- 8 在**服务**列中，单击编辑图标并选择服务。如果未定义，服务将与任何内容匹配。
- 9 要选择预定义的服务，请选择多个可用服务之一。

- 10 要定义新服务，请单击**原始端口协议**选项卡，然后单击**添加**。

选项	说明
服务类型	<ul style="list-style-type: none"> ■ ALG ■ ICMP ■ IGMP ■ IP ■ L4 端口集
协议	选择一个可用的协议。
源端口	输入源端口。
目标端口	选择目标端口。

- 11 在**应用对象**列中，单击编辑图标并选择对象。

- 12 在**日志**列中，设置日志记录选项。

在 ESXi 和 KVM 主机上，日志位于 `/var/log/dfwpktlogs.log` 文件中。启用日志记录功能可能会影响性能。

- 13 在**操作**列中，选择一个操作。

选项	说明
允许	允许具有指定的源、目标和协议的所有 L3 或 L2 流量通过当前防火墙上下文。与规则匹配并接受的数据包将通过系统，就好像没有防火墙一样。
丢弃	丢弃具有指定的源、目标和协议的数据包。丢弃数据包是一个静默操作，不会向源或目标系统发送通知。丢弃数据包将导致重试连接，直到达到重试阈值。
拒绝	拒绝具有指定的源、目标和协议的数据包。拒绝数据包是一种较友好的数据包阻止方式，因为将向发送方发送“无法到达目标 (destination unreachable)”消息。如果协议是 TCP，则会发送 TCP RST 消息。对于 UDP、ICMP 和其他 IP 连接，发送包含管理上被禁止的代码的 ICMP 消息。使用“拒绝”的一个好处是，在仅尝试一次后，就会向发送应用程序通知无法建立连接。

- 14 单击**高级设置**图标以指定 IP 协议、方向、规则标记和注释。

- 15 单击**发布**。

删除防火墙规则

防火墙是一个网络安全系统，它根据预定的防火墙规则监视和控制入站和出站的网络流量。可以添加和删除自定义规则。

步骤

- 1 选择**高级网络和安全 > 安全 > 分布式防火墙**。
- 2 对于 L3 规则，请单击**常规**选项卡；对于 L2 规则，请单击**以太网**选项卡。
- 3 单击规则第一列中的菜单图标，然后选择**删除规则**。
- 4 单击**发布**。

编辑默认分布式防火墙规则

您可以编辑应用于与任何用户定义的防火墙规则均不匹配的流量的默认防火墙设置。

默认防火墙规则应用于与任何用户定义的防火墙规则均不匹配的流量。默认第 3 层规则位于**常规**选项卡下面，而默认第 2 层规则位于**以太网**选项卡下面。

默认防火墙规则允许所有 L3 和 L2 流量通过基础架构中所有准备好的群集。默认规则始终位于规则表的底部，无法删除。不过，您可以将规则的操作元素从**允许**更改为**丢弃**或**拒绝**（不建议），并指示是否应记录该规则的流量。

默认第 3 层防火墙规则应用于所有流量，包括 DHCP。如果将操作更改为**丢弃**或**拒绝**，则 DHCP 流量将被阻止。您将需要创建一个规则以允许 DHCP 流量。

步骤

- 1 选择**高级网络和安全 > 安全 > 分布式防火墙**。
- 2 对于 L3 规则，请单击**常规**选项卡；对于 L2 规则，请单击**以太网**选项卡。
- 3 在**名称**列中，输入新名称。
- 4 在**操作**列中，选择一个选项。
 - 允许 - 允许具有指定的源、目标和协议的所有 L3 或 L2 流量通过当前防火墙上下文。与规则匹配并接受的数据包将通过系统，就好像没有防火墙一样。
 - 丢弃 - 丢弃具有指定的源、目标和协议的数据包。丢弃数据包是一个静默操作，不会向源或目标系统发送通知。丢弃数据包将导致重试连接，直到达到重试阈值。
 - 拒绝 - 拒绝具有指定的源、目标和协议的数据包。拒绝数据包是一种较友好的数据包阻止方式，因为将向发送方发送“无法到达目标 (destination unreachable)”消息。如果协议是 TCP，则会发送 TCP RST 消息。对于 UDP、ICMP 和其他 IP 连接，发送包含管理上被禁止的代码的 ICMP 消息。使用“拒绝”的一个好处是，在仅尝试一次后，就会向发送应用程序通知无法建立连接。

注 不建议选择**拒绝**以作为默认规则的操作。

- 5 在**日志**中，启用或禁用日志记录。
启用日志记录功能可能会影响性能。
- 6 单击**发布**。

更改防火墙规则的顺序

规则是按从上到下的顺序处理的。您可以更改列表中的规则顺序。

对于尝试通过防火墙的任何流量，将按照“规则”表中显示的顺序应用规则以处理数据包信息，从顶部开始并移到底部的默认规则。在某些情况下，两个或更多规则的优先级顺序在确定流量流方面可能是非常重要的。

自定义规则可以在表中上下移动，而默认规则始终位于表底部且无法移动。

步骤

- 1 选择**高级网络和安全 > 安全 > 分布式防火墙**。
- 2 对于 L3 规则，请单击**常规**选项卡；对于 L2 规则，请单击**以太网**选项卡。
- 3 选择规则，然后单击菜单栏上的**上移**或**下移**图标。
- 4 单击**发布**。

筛选防火墙规则

在导航到防火墙区域时，最初显示所有规则。您可以应用筛选器以控制显示的规则，以便仅查看一部分规则。这样，就可以轻松管理这些规则。

步骤

- 1 选择**高级网络和安全 > 安全 > 分布式防火墙**。
- 2 对于 L3 规则，请单击**常规**选项卡；对于 L2 规则，请单击**以太网**选项卡。
- 3 在菜单栏右侧的搜索文本字段中，选择一个对象，或者输入对象名称的开头字符以缩小待选择对象的列表。

在选择一个对象后，将应用筛选器并更新规则列表，以便仅显示在任何以下列中包含该对象的规则：

- 源
- 目标
- 应用对象
- 服务

- 4 要移除筛选器，请从文本字段中删除对象名称。

您可能需要更改安装的设备的配置，例如，添加许可证和证书以及更改密码。还应该执行一些日常维护任务，包括运行备份。此外，可以使用一些工具帮助您查找有关 **NSX-T Data Center** 基础架构和 **NSX-T Data Center** 创建的逻辑网络包含的设备的信息，其中包括远程系统日志记录、跟踪流和端口连接。

本章讨论了以下主题：

- 查看监控仪表板
- 查看各类别对象的使用情况和容量
- 检查配置更改的已实现状态
- 搜索对象
- 按对象属性筛选
- 添加计算管理器
- 添加 Active Directory
- 添加 LDAP 服务器
- 同步 Active Directory
- 管理用户帐户和基于角色的访问控制
- 备份和还原 NSX Manager
- 从 vCenter Server 中移除 NSX-T Data Center 扩展
- 管理 NSX Manager 集群
- 替换 NSX Edge 集群中的 NSX Edge 传输节点
- 在 vCenter Server 丢失且无法恢复时恢复 NSX-T
- NSX-T Data Center 的多站点部署
- 配置设备
- 添加许可证密钥并生成许可证使用情况报告
- 设置证书
- 基于合规性的配置
- 收集支持包

- 日志消息和错误代码
- 客户体验提升计划
- 将标记添加到对象
- 查找远程服务器的 SSH 指纹
- 查看有关在虚拟机上运行的应用程序的数据
- 配置外部负载均衡器

查看监控仪表板

NSX Manager 界面提供了许多可显示系统状态、网络和安全以及合规性报告相关详细信息的监控仪表板。您既可以在整个 NSX Manager 界面中显示或访问其中的单项信息，也可以在 **主页 > 监控仪表板** 页面中同时访问所有这些信息。

您可以从 NSX Manager 界面的主页中访问监控仪表板。在仪表板中，您可以单击并访问要从中提取仪表板数据的源页面。

步骤

- 1 以管理员身份登录到 NSX Manager 界面。
- 2 如果您还未进入主页，请单击**主页**。
- 3 单击“监控仪表板”，然后从下拉菜单中选择所需的仪表板类别。

该页面将显示所选类别中的仪表板。仪表板图形按颜色进行了标记，颜色代码键显示在仪表板的正上方。

- 4 要访问更深层的详细信息，请单击仪表板的标题或仪表板中的某个元素（如果已激活）。

下表介绍了默认仪表板及其数据源。

表 21-1. 系统仪表板

仪表板	源	说明
系统	系统 > 设备 > 概览	显示 NSX Manager 群集的状态和资源（CPU、内存、磁盘）消耗情况。
结构层	系统 > 结构层 > 节点 系统 > 结构层 > 传输区域 系统 > 结构层 > 计算管理器	显示 NSX-T 结构层的状态，包括主机和 Edge 传输节点、传输区域和计算管理器。
备份	系统 > 备份和还原	显示 NSX-T 备份的状态（如果已配置）。强烈建议您配置远程存储到 SFTP 站点的计划备份。
端点保护	系统 > 服务部署	显示端点保护部署的状态。

表 21-2. 网络和安全仪表板

仪表板	源	说明
安全	清单 > 组 安全 > 分布式防火墙	显示组和安全策略的状态。组是工作负载、分段、分段端口和 IP 地址的集合，其中可能会应用安全策略，包括东西向防火墙规则。
网关	网络 > Tier-0 网关 网络 > Tier-1 网关	显示 Tier-0 和 Tier-1 网关的状态。
分段	网络 > 分段	显示网络分段的状态。
负载均衡器	网络 > 负载均衡	显示负载均衡器虚拟机的状态。
VPN	网络 > VPN	显示虚拟专用网络的状态。

表 21-3. 高级网络和安全仪表板

仪表板	源	说明
负载均衡器	高级网络和安全 > 负载均衡器	显示负载均衡器服务、负载均衡器虚拟服务器和负载均衡器服务器池的状态。负载均衡器可以托管一个或多个虚拟服务器。虚拟服务器绑定到一个服务器池（包含托管应用程序的成员）。
防火墙	高级网络和安全 > 安全 > 分布式防火墙 高级网络和安全 > 安全 > 网桥防火墙 高级网络和安全 > 网络 > 路由器	指示防火墙是否已启用，并显示策略、规则和排除列表成员的数量。 注 此仪表板中显示的每个详细项目均源自所引用的源页面中的特定子选项卡。
VPN	不适用。	显示虚拟专用网络的状态以及打开的 IPSec 和 L2 VPN 会话的数量。
交换	高级网络和安全 > 交换	显示逻辑交换机和逻辑端口（包括虚拟机端口和容器端口）的状态。

表 21-4. 合规性报告仪表板

列	说明
不合规代码	显示特定的不合规代码。
说明	不合规状态的特定原因。
资源名称	不合规的 NSX-T 资源（节点、交换机和配置文件）。
资源类型	原因的资源类型。
受影响的资源	受影响的资源数。单击该数值将显示一个列表。

请参见[合规性状态报告代码](#)以获取有关每个合规性报告代码的更多信息。

查看各类别对象的使用情况和容量

您可以查看 NSX-T Data Center 环境中的各种类别的对象的使用情况和容量。您也可以设置警示，以轻松了解何时达到特定的使用情况阈值。

要查看不同类别的对象的使用情况和容量，请单击以下选项卡之一：

- **网络 > 网络概览 > 容量**
- **安全 > 安全概览 > 容量**
- **清单 > 清单概览 > 容量**
- **系统 > 系统概览 > 容量**

您也可以导航到**安全规划和故障排除 > 合并的容量**，以便在一个页面上查看所有对象类别。

在每个容量页面上，将为每个对象类别显示以下信息：

- **最大容量** - 该值基于大型设备的容量。
- **当前清单 (已实现)** - 已成功创建或配置的对象数。该数字反映了**高级网络和安全**选项卡中显示的 **NSX Manager** 对象。这些对象可能包括您在**网络、安全、清单或系统**选项卡中创建的一些对象。将显示一个颜色编码条以指示使用情况百分比。如果使用情况低于警告警示级别，则颜色为绿色。如果使用情况达到或高于警告警示级别但低于严重警示级别，则颜色为橙色。如果使用情况达到或高于严重警示级别，则颜色为红色。
- **警告警示** - 这是上述使用情况条显示橙色时的使用情况级别。您可以更改该值。
- **严重警示** - 这是上述使用情况条显示红色时的使用情况级别。您可以更改该值。

在更改警告警示或严重警示值时，您可以单击**恢复**以恢复为上次保存的值。您可以单击**重置值**以恢复所有对象类别的默认值。

网络容量页面显示以下对象类别：

- Tier-0 逻辑路由器
- Tier-1 逻辑路由器
- 前缀列表
- 系统范围的 NAT 规则
- DHCP 服务器实例
- 系统范围的 DHCP 范围和池
- 启用了 NAT 的 Tier-1 逻辑路由器
- 逻辑交换机
- 系统范围的逻辑交换机端口

安全容量页面显示以下对象类别：

- 启用了端点保护的系统范围的主机
- 启用了端点保护的系统范围的虚拟机

- Active Directory 组
- Active Directory 域
- 分布式防火墙规则
- 系统范围的防火墙规则
- 系统范围的防火墙区域
- 分布式防火墙区域

清单容量页面显示以下对象类别：

- 网络和安全组
- IP 集
- 基于 IP 集的组
- vCenter 群集
- 管理程序主机

系统容量页面显示以下对象类别：

- 系统范围的虚拟接口
- Edge 群集
- 系统范围的 Edge 节点

检查配置更改的已实现状态

进行配置更改时，NSX Manager 通常会将请求发送到另一个组件，以实施更改。对于某些第 3 层实体，如果使用 API 进行配置更改，则可以跟踪请求的状态以查看更改是否已成功实施。

您发起的配置更改称为所需状态。实施更改的结果称为已实现状态。如果 NSX Manager 成功实施更改，已实现状态将与所需状态相同。如果出现错误，已实现状态将与所需状态不同。

对于某些第 3 层实体，当调用 API 以进行配置更改时，响应将包括参数 request_id。可以使用参数 request_id 和 entity_id 进行 API 调用以查明请求的状态。

此功能支持以下实体和 API：

```
EdgeCluster
  POST /edge-clusters
  PUT /edge-clusters/<edge-cluster-id>
  DELETE /edge-clusters/<edge-cluster-id>
  POST /edge-clusters/<edge-cluster-id>?action=replace_transport_node

LogicalRouter
  POST /logical-routers
  PUT /logical-routers/<logical-router-id>
  DELETE /logical-routers/<logical-router-id>
  POST /logical-routers/<logical-router-id>?action=reprocess
  POST /logical-routers/<logical-router-id>?action=reallocate
```

```

LogicalRouterPort
  POST /logical-router-ports
  PUT /logical-router-ports/<logical-router-port-id>
  DELETE /logical-router-ports/<logical-router-port-id>

StaticRoute
  POST /logical-routers/<logical-router-id>/routing/static-routes
  PUT /logical-routers/<logical-router-id>/routing/static-routes/<static-route-id>
  DELETE /logical-routers/<logical-router-id>/routing/static-routes/<static-route-id>

BGPConfig
  PUT /logical-routers/<logical-router-id>/routing/bgp

BgpNeighbor
  POST /logical-routers/<logical-router-id>/routing/bgp/neighbors
  PUT /logical-routers/<logical-router-id>/routing/bgp/neighbors/<bgp-neighbor-id>
  DELETE /logical-routers/<logical-router-id>/routing/bgp/neighbors/<bgp-neighbor-id>
  POST /logical-routers/<logical-router-id>/routing/bgp/neighbors/<bgp-neighbor-id>

BGPCommunityList
  POST /logical-routers/<logical-router-id>/routing/bgp/community-lists
  PUT /logical-routers/<logical-router-id>/routing/bgp/community-lists/<community-list-id>
  DELETE /logical-routers/<logical-router-id>/routing/bgp/community-lists/<community-list-id>

AdvertisementConfig
  PUT /logical-routers/<logical-router-id>/routing/advertisement

AdvertiseRouteList
  PUT /logical-routers/<logical-router-id>/routing/advertisement/rules

NatRule
  POST /logical-routers/<logical-router-id>/nat/rules
  PUT /logical-routers/<logical-router-id>/nat/rules/<rule-id>
  DELETE /logical-routers/<logical-router-id>/nat/rules/<rule-id>

DhcpRelayService
  POST /dhcp/relays
  PUT /dhcp/relays/<relay-id>
  DELETE /dhcp/relays/<relay-id>

DhcpRelayProfile
  POST /dhcp/relay-profiles
  PUT /dhcp/relay-profiles/<relay-profile-id>
  DELETE /dhcp/relay-profiles/<relay-profile-id>

StaticHopBfdPeer
  POST /logical-routers/<logical-router-id>/routing/static-routes/bfd-peers
  PUT /logical-routers/<logical-router-id>/routing/static-routes/bfd-peers/<bfd-peers-id>
  DELETE /logical-routers/<logical-router-id>/routing/static-routes/bfd-peers/<bfd-peers-id>

IPPrefixList
  POST /logical-routers/<logical-router-id>/routing/ip-prefix-lists
  PUT /logical-routers/<logical-router-id>/routing/ip-prefix-lists/<ip-prefix-list-id>

```



```
DELETE /logical-routers/<logical-router-id>/routing/ip-prefix-lists/<ip-prefix-list-id>
```

RouteMap

```
POST /logical-routers/<logical-router-id>/routing/route-maps
```

```
PUT /logical-routers/<logical-router-id>/routing/route-maps/<route-map-id>
```

```
DELETE /logical-routers/<logical-router-id>/routing/route-maps/<route-map-id>
```

RedistributionConfig

```
PUT /logical-routers/<logical-router-id>/routing/redistribution
```

RedistributionRuleList

```
PUT /logical-routers/<logical-router-id>/routing/redistribution/rules
```

BfdConfig

```
PUT /logical-routers/<logical-router-id>/routing/bfd-config
```

MplsConfig

```
PUT /logical-routers/<logical-router-id>/routing/mps
```

RoutingGlobalConfig

```
PUT /logical-routers/<logical-router-id>/routing
```

IPSecVPNIKEProfile

```
POST /vpn/ipsec/ike-profiles
```

```
PUT /vpn/ipsec/ike-profiles/<ike-profile-id>
```

```
DELETE /vpn/ipsec/ike-profiles/<ike-profile-id>
```

IPSecVPNDPDProfile

```
POST /vpn/ipsec/dpd-profiles
```

```
PUT /vpn/ipsec/dpd-profiles/<dpd-profile-id>
```

```
DELETE /vpn/ipsec/dpd-profiles/<dpd-profile-id>
```

IPSecVPNTunnelProfile

```
POST /vpn/ipsec/tunnel-profiles
```

```
PUT /vpn/ipsec/tunnel-profiles/<tunnel-profile-id>
```

```
DELETE /vpn/ipsec/tunnel-profiles/<tunnel-profile-id>
```

IPSecVPNLocalEndpoint

```
POST /vpn/ipsec/local-endpoints
```

```
PUT /vpn/ipsec/local-endpoints/<local-endpoint-id>
```

```
DELETE /vpn/ipsec/local-endpoints/<local-endpoint-id>
```

IPSecVPNPeerEndpoint

```
POST /vpn/ipsec/peer-endpoints
```

```
PUT /vpn/ipsec/peer-endpoints/<peer-endpoint-id>
```

```
DELETE /vpn/ipsec/peer-endpoints/<peer-endpoint-id>
```

IPSecVPNService

```
POST /vpn/ipsec/services
```

```
PUT /vpn/ipsec/services/<service-id>
```

```
DELETE /vpn/ipsec/services/<service-id>
```

IPSecVPNSession

```
POST /vpn/ipsec/sessions
```

```
PUT /vpn/ipsec/sessions/<session-id>
```

```
DELETE /vpn/ipsec/sessions/<session-id>
```

```

DhcpServer
  POST /dhcp/servers
  PUT /dhcp/servers/<server-id>
  DELETE /dhcp/servers/<server-id>

DhcpStaticBinding
  POST /dhcp/servers/static-bindings
  PUT /dhcp/servers/<server-id>/static-bindings/<binding-id>
  DELETE /dhcp/servers/<server-id>/static-bindings/<binding-id>

DhcpIpPool
  POST /dhcp/servers/ip-pools
  PUT /dhcp/servers/<server-id>/ip-pools/<pool-id>
  DELETE /dhcp/servers/<server-id>/ip-pools/<pool-id>

DnsForwarder
  POST /dns/forwarders
  PUT /dns/forwarders/<forwarder-id>
  DELETE /dns/forwarders/<forwarder-id>

```

可以通过调用以下 API 获取已实现状态:

```

EdgeCluster
Request - GET /edge-clusters/<edge-cluster-id>/state?request_id=<request-id>
Response - An instance of EdgeClusterStateDto which will inherit ConfigurationState. If the
edge cluster is deleted then the state will be unknown and it will return the common entity
not found error.

LogicalRouter / All L3 Entities - All L3 entities can use this API to get realization state
Request - GET /logical-routers/<logical-router-id>/state?request_id=<request-id>
Response - An instance of LogicalRouterStateDto which will inherit ConfigurationState. Delete
operation of any entity other than logical router can be covered by getting the state of
logical router but if the logical router itself is deleted then the state will be unknown and
it will return the common entity not found error.

LogicalServiceRouterCluster - All L3 entities which are the part of services can use this API
to get the realization state
Request - GET /logical-routers/<logical-router-id>/service-cluster/state?request_id=<request-
id>
Response - An instance of LogicalServiceRouterClusterState which will inherit
ConfigurationState.

LogicalRouterPort / DhcpRelayService / DhcpRelayProfile
Request - GET /logical-router-ports/<logical-router-port-id>/state?request_id=<request-id>
Response - An instance of LogicalRouterPortStateDto which will inherit ConfigurationState.

IPSecVPNIKEProfile / IPSecVPNDPDProfile / IPSecVPNTunnelProfile / IPSecVPNLocalEndpoint /
IPSecVPNPeerEndpoint / IPSecVPNService / IPSecVPNSession
Request - GET /vpn/ipsec/sessions/<session-id>/state?request_id=<request-id>
Response - An instance of IPSecVPNSessionStateDto which will inherit ConfigurationState. If
the session is deleted then the state will be unknown and it will return the common entity
not found error. When IPSecVPNService is disabled, IKE itself is down and it does not
respond. It will return unknown state in such a case.

```

```

DhcpServer
Request - GET /dhcp/servers/<server-id>/state?request_id=<request-id>
Response - An instance of ConfigurationState.

DhcpStaticBinding
Request - GET /dhcp/servers/<server-id>/static-bindings/<binding-id>/state?
request_id=<request-id>
Response - An instance of ConfigurationState.

DhcpIpPool
Request - GET /dhcp/servers/<server-id>/ip-pools/<pool-id>/state?request_id=<request-id>
Response - An instance of ConfigurationState.

DnsForwarder
Request - GET /dns/forwarders/<forwarder-id>/state?request_id=<request-id>
Response - An instance of ConfigurationState.

```

有关 API 的详细信息，请参见《NSX-T Data Center API 参考》。

搜索对象

您可以使用不同的条件在整个 NSX-T Data Center 清单中搜索对象。

搜索结果是按相关性排序的，您可以根据搜索查询筛选这些结果。

注 如果搜索查询中的特殊字符还作为运算符，则必须添加前导反斜杠。作为运算符的字符包括：+、-、=、&&、||、<、>、!、(、)、{、}、[、]、^、"、~、?、:、/、\。

步骤


- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 在主页上，为对象或对象类型输入一个搜索模式。

输入搜索模式时，搜索功能会显示适用的关键字，从而为您提供帮助。

搜索	搜索查询
将 Logical 作为名称或属性的对象	Logical
精确逻辑交换机名称	display_name:LSP-301
具有特殊字符（如!）的名称	Logical\!

将列出所有相关的搜索结果并按资源类型分组在不同的选项卡中。

可以单击选项卡，查看资源类型的特定搜索结果。

- 3 （可选）在搜索栏中，单击保存图标以保存细化搜索条件。
- 4 在搜索栏中，单击  以打开高级搜索列，您可以在其中细化搜索。
- 5 指定一个或多个条件以细化搜索内容。

- 名称

- 资源类型
- 说明
- ID
- 创建者
- 修改者
- 标记
- 创建日期
- 修改日期

您还可以查看最近的搜索结果和已保存的搜索条件。

- 6 （可选）单击**全部清除**以重置高级搜索条件。

按对象属性筛选

在 NSX Manager 中查看对象时，您可以按对象的一个或多个属性对其进行筛选。例如，在查看 Tier-0 网关的详细信息时，您可以选择按**状态**进行筛选，仅查看那些**已关闭**的网关。


可以使用以下类型的筛选器：

- 预定义的筛选器 - 可应用于对象的常用筛选器列表。
- 基于文本的筛选器 - 基于您输入的属性值的筛选器。此筛选器仅适用于对象的**名称**、**标记**、**路径**和**描述**属性。
- 属性-值对 - 可用于指定要筛选的属性-值对的属性下拉菜单。

您可以使用一个对象的多个属性或单个属性的多个值来筛选对象。当您选择多个属性时，将应用 **AND** 运算符，而在指定单个属性的多个值时，将使用 **OR** 运算符。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 导航到显示要查看的对象的选项卡。
- 3 指定要用于筛选对象的属性。

- 单击 ，然后从预定义的筛选器列表中进行选择。
- 为**名称**、**标记**、**路径**或**描述**属性输入相应的值。
- 从下拉菜单中选择一个属性并指定其值。例如，**状态**：已关闭

将显示满足筛选标准的对象。

- 4 （可选）单击**清除**可重置您的筛选器。

添加计算管理器

计算管理器（如 vCenter Server）是一个管理资源（如主机和虚拟机）的应用程序。

NSX-T Data Center 会轮询计算管理器，以从 vCenter Server 中收集群集信息。

在添加 vCenter Server 计算管理器时，您必须提供 vCenter Server 用户的凭据。您可以提供 vCenter Server 管理员的凭据，或者专门为 NSX-T Data Center 创建一个角色和用户并提供该用户的凭据。该角色必须具有以下 vCenter Server 权限：

Extension.Register extension
Extension.Unregister extension
Extension.Update extension
Sessions.Message
Sessions.Validate session
Sessions.View and stop sessions
Host.Configuration.Maintenance
Host.Local Operations.Create virtual machine
Host.Local Operations.Delete virtual machine
Host.Local Operations.Reconfigure virtual machine
Tasks
Scheduled task
Global.Cancel task
Permissions.Reassign role permissions
Resource.Assign vApp to resource pool
Resource.Assign virtual machine to resource pool
Virtual Machine.Configuration
Virtual Machine.Guest Operations
Virtual Machine.Provisioning
Virtual Machine.Inventory
Network.Assign network
vApp

有关 vCenter Server 角色和权限的详细信息，请参见《vSphere 安全性》文档。

前提条件

- 确认使用支持的 vSphere 版本。请参见[支持的 vSphere 版本](#)
- 与 vCenter Server 的 IPv6 和 IPv4 通信。
- 确认使用建议数量的计算管理器。请参见 <https://configmax.vmware.com/home>。

注 NSX-T Data Center 不支持在多个 NSX Manager 中注册相同的 vCenter Server。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 选择 **系统 > 结构层 > 计算管理器 > 添加**。
- 3 填写计算管理器详细信息。

选项	说明
名称和说明	键入名称以标识 vCenter Server。 您可以选择描述任何特殊详细信息，如 vCenter Server 中的群集数。
域名/IP 地址	键入 vCenter Server 的 IP 地址。
类型	保留默认选项。
用户名和密码	键入 vCenter Server 登录凭据。
指纹	键入 vCenter Server SHA-256 指纹算法值。

如果将指纹值保留空白，将提示您接受服务器提供的指纹。

在接受该指纹后，需要几秒钟 NSX-T Data Center 才能发现并注册 vCenter Server 资源。

- 4 如果进度图标从**正在进行中**更改为**未注册**，请执行以下步骤解决错误。
 - a 选择错误消息，然后单击**解决**。一个可能的错误消息如下：

```
Extension already registered at CM <vCenter Server name> with id <extension ID>
```

- b 输入 vCenter Server 凭据，然后单击**解决**。
如果存在现有注册，则会替换它。

结果

向 vCenter Server 注册计算管理器且连接状态显示为已启动需要一些时间。

可以单击计算管理器的名称，以查看详细信息、编辑计算管理器或者管理适用于计算管理器的标记。

成功注册 vCenter Server 后，如果未先删除计算管理器，请勿关闭并删除 NSX Manager 虚拟机。否则，当部署新的 NSX Manager 时，您将无法再次注册同一个 vCenter Server。您将收到错误消息，指示已在其他 NSX Manager 中注册了 vCenter Server。

添加 Active Directory

创建基于用户的身份防火墙规则时，会使用 Active Directory。

不支持将 Windows 2008 作为 Active Directory 服务器或 RDSH 服务器操作系统。

可以向 NSX Manager 注册一个或多个 Windows 域。NSX Manager 从向其注册的每个域获取组和用户信息以及两者之间的关系。NSX Manager 还检索 Active Directory (AD) 凭据。

将 Active Directory 同步到 NSX Manager 后，您可以基于用户身份创建安全组，以及创建基于身份的防火墙规则。

注 对于身份防火墙规则实施，应为所有使用 Active Directory 的虚拟机开启 Windows 时间服务。这会确保在 Active Directory 和虚拟机之间同步日期和时间。AD 组成员资格变化（包括启用和删除用户）不会立即对登录的用户生效。要使更改生效，用户必须注销，然后重新登录。在修改组成员资格时，AD 管理员应强制注销。此行为是 Active Directory 存在的一个限制。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 导航到 **系统 > Active Directory**。
- 3 单击**添加 Active Directory**。
- 4 输入 Active Directory 的名称。
- 5 输入 **NetBios 名称**和**基本标识名**。

要检索域的 NetBIOS 名称，可在属于域或位于域控制器上的 Windows 工作站的命令窗口中输入 `nbtstat -n`。在 NetBIOS 本地名称表中，前缀为 <00> 且类型为“组”的条目是 NetBIOS 名称。

要添加 Active Directory 域，需要一个基本标识名（基本 DN）。基本 DN 是 LDAP 服务器在 Active Directory 域中搜索用户身份验证时使用的起点。例如，如果您的域名为 `corp.local`，则 Active Directory 的基本 DN 的 DN 将为“`DC=corp,DC=local`”。

- 6 如有必要，请设置**增量同步间隔**。增量同步更新上次同步事件后发生更改的本地 AD 对象
只有在执行增量同步或完全同步后，在 Active Directory 中所做的任何更改才会显示在 NSX Manager 上。
- 7 单击**保存**。

添加 LDAP 服务器

LDAP（轻型目录访问协议）服务器配置和功能仅用于身份防火墙。LDAP 提供了一个集中的位置以进行身份验证，这意味着在配置到 LDAP 服务器的连接时，用户记录将存储在外部 LDAP 服务器中。

前提条件

域帐户必须具有域树中所有对象的 AD 读权限。事件日志读取器帐户必须具有安全事件日志的读权限。

当存在 NSX Manager 集群时，所有节点都需要能够访问 LDAP 服务器。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 导航到 **系统 > Active Directory**。
- 3 选择 **LDAP 服务器**选项卡。
- 4 单击**添加 LDAP 服务器**。

- 5 输入 LDAP 服务器的主机名。
- 6 从 **连接到 (目录)** 下拉菜单中选择 LDAP 服务器要连接到的 Active Directory。
- 7 (可选) 选择**协议**: LDAP (不安全) 或 LDAPS (安全)。
- 8 如果选择了 LDAPS, 请选择 NSX Manager 建议的 SHA-256 指纹或输入一个 SHA-256 指纹。
- 9 输入 LDAP 服务器的**端口号**。
对于本地域控制器, 将在 Active Directory 同步中使用默认 LDAP 端口 389 和 LDAPS 端口 636, 不应编辑这些端口号以将其更改为非默认值。
- 10 输入至少具有 Active Directory 域的只读访问权限的 Active Directory 帐户的**用户名和密码**。
- 11 单击**保存**。
- 12 要验证是否可以连接到 LDAP 服务器, 请单击**测试连接**。

同步 Active Directory

可以使用 Active Directory 对象创建基于用户身份的安全组和基于身份的防火墙规则。

在开始完全同步后, 如果使用 API 手动将其结束, 则同步统计信息将不会正确更新。

注 IDFW 依赖于客户机操作系统的安全性和完整性。恶意本地管理员可以通过多种方法来伪造其身份以绕过防火墙规则。用户身份信息由客户机虚拟机中的客户机侦测代理提供。安全管理员必须确保每个客户机虚拟机中均已安装并正在运行 NSX 客户机侦测代理。已登录的用户不应具有移除或停止该代理的特权。

步骤

- 1 从浏览器中, 使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 导航到 **系统 > Active Directory**。
- 3 单击要同步的 Active Directory 旁边的三按钮菜单图标, 然后选择以下选项之一:

菜单项	说明
增量同步	执行增量同步, 将更新上次同步后发生更改的本地 AD 对象。
全部同步	执行完全同步, 将更新所有 AD 对象的本地状态。

- 4 单击**查看同步状态**以查看 Active Directory 的当前状态、以前的同步状态、同步状态和上次同步时间。

管理用户帐户和基于角色的访问控制

NSX-T Data Center 设备具有两个内置用户: admin 和 audit。您可以将 NSX-T Data Center 与 VMware Identity Manager (vIDM) 集成在一起, 并为 vIDM 管理的用户配置基于角色的访问控制 (Role-Based Access Control, RBAC)。

对于由 vIDM 管理的用户，应用的身份验证策略是由 vIDM 管理员配置的身份验证策略，而不是 NSX-T Data Center 的身份验证策略，后者仅适用于 **admin** 和 **audit** 用户。

管理用户密码

每个 NSX Manager 和 NSX Edge 设备都有以下三个本地帐户：**admin**、**audit** 和 **root**。您可以管理这些用户的密码，但无法添加或删除用户。

默认情况下，**audit** 用户处于非活动状态。要激活该用户，请以管理员身份登录并运行 `set user audit` 命令，然后提供一个新密码。当提示输入当前密码时，按 **Enter** 键。

默认情况下，用户密码会在 90 天后过期。您可以更改或禁用每个用户的密码过期设置。

如果 NSX Manager 上的某个本地用户的密码将在 30 天内过期，则 NSX Manager Web 界面会显示密码过期通知。如果将本地用户的密码过期时间设置为 30 天或更短，则会始终显示该通知。

从 NSX-T Data Center 2.5.1 开始，通知中将包含一个“更改密码”链接。单击该链接可从 Web 界面更改本地用户的密码。

前提条件

了解 NSX Manager 和 NSX Edge 的密码复杂性要求。请参见《NSX-T Data Center 安装指南》中的“NSX Manager 安装”和“NSX Edge 安装”。

步骤

- 1 登录到设备的 CLI。
- 2 要更改密码，请运行 `set user` 命令。例如：

```
nsx> set user admin
Current password:
New password:
Confirm new password:
nsx>
```

- 3 要获取密码过期信息，请运行 `get user <username> password-expiration` 命令。例如：

```
nsx> get user admin password-expiration
Password expires 90 days after last change
nsx>
```

- 4 要设置密码过期时间（以天为单位），请运行 `set user <username> password-expiration <number of days>` 命令。例如：

```
nsx> set user admin password-expiration 120
nsx>
```

- 5 要禁用密码过期，请运行 `clear user <username> password-expiration` 命令。例如：

```
nsx> clear user admin password-expiration
nsx>
```

重置设备密码

以下过程适用于 NSX Manager、NSX Edge 和 Cloud Service Manager 设备。

注 如果具有 NSX Manager 集群，则在一个 NSX Manager 上重置 root、admin 或 audit 用户的密码会自动重置集群中其他 NSX Manager 的密码。请注意，密码同步可能需要几分钟或更长的时间。

如果已重命名 admin 或 audit 用户，请在以下过程中使用新名称。

重新引导设备时，默认情况下不会显示 GRUB 引导菜单。以下过程要求您将 GRUB 配置为显示 GRUB 引导菜单。有关配置 GRUB 和更改 GRUB root 密码的详细信息，请参见《NSX-T Data Center 安装指南》中的“将 NSX-T Data Center 配置为在引导时显示 GRUB 菜单”。

如果运行的是 NSX-T Data Center 2.5.2 或更高版本，并且知道 root 的密码，但忘记了 admin 或 audit 的密码，您可以使用以下过程重置该密码：

- 1 以 root 身份登录到设备。
- 2 对于 NSX Edge，请运行 `/etc/init.d/nsx-edge-api-server stop` 命令。否则，运行 `/etc/init.d/nsx-mp-api-server stop` 命令。
- 3 要重置 admin 的密码，请运行 `passwd admin` 命令。
- 4 要重置 audit 的密码，请运行 `passwd audit` 命令。
- 5 运行命令 `touch /var/vmware/nsx/reset_cluster_credentials`。
- 6 对于 NSX Edge，请运行 `/etc/init.d/nsx-edge-api-server start` 命令。否则，运行 `/etc/init.d/nsx-mp-api-server start` 命令。

如果忘记了 root 用户的密码，您可以使用以下过程重置该密码。如果运行的是 NSX-T Data Center 2.5.0 或 2.5.1，并且想要重置 admin 和 audit 的密码，则也可使用以下过程。如果运行的是 NSX-T Data Center 2.5.2 或更高版本，您可以在重置 root 的密码后，再使用上述过程重置 admin 或 audit 的密码。

步骤

- 1 连接到设备的控制台。
- 2 重新引导系统。
- 3 出现 GRUB 引导菜单时，快速按左侧的 **SHIFT** 或 **ESC** 键。如果等待时间太长且引导序列未暂停，必须再次重新引导系统。
- 4 按 **e** 以编辑菜单。
输入用户名 (root) 和 root 的 GRUB 密码（与设备的用户 root 不同）。
- 5 将光标停留在 Ubuntu 选择上。
- 6 按 **e** 以编辑选定的选项。
- 7 搜索以 linux 开头的行。

8 如果运行的是 NSX-T Data Center 2.5.0 或 2.5.1，请执行以下步骤：

- a 移除 `root=UUID=<ID number>` 后面的所有选项，并在 `UUID` 后面添加 `rw single init=/bin/bash`。
- b 按 **Ctrl-X** 进行引导。
- c 日志消息停止时，按 **Enter**。
将显示提示 `root@(none) :/#`。
- d 如果要重置 `root` 的密码，则运行命令 `passwd`。
如果要重置 `admin` 或 `audit` 的密码，则运行命令 `passwd <admin or audit user ID>`。
可以多次运行 `passwd` 命令。
- e 输入新密码，然后再次输入该密码以进行确认。
- f 如果要在 `NSX Manager` 上重置密码，则运行命令 `touch /var/vmware/nsx/reset_cluster_credentials`。
- g 运行命令 `sync`。
- h 运行命令 `reboot -f`。

9 如果运行的是 NSX-T Data Center 2.5.2 或更高版本，请执行以下步骤：

- a 在行尾添加 `systemd.wants=PasswordRecovery.service`。
- b 按 **Ctrl-X** 进行引导。
- c 输入 `root` 的新密码，然后再次输入该密码以进行确认。
完成引导过程后，您可以使用新密码以 `root` 身份登录以验证密码更改。

身份验证策略设置

您可以通过 CLI 查看或更改身份验证策略设置。

您可以使用以下命令查看或设置最小密码长度：

```
get auth-policy minimum-password-length
set auth-policy minimum-password-length <password-length>
```

以下命令适用于登录到 `NSX Manager UI` 或进行 API 调用：

```
get auth-policy api lockout-period
get auth-policy api lockout-reset-period
get auth-policy api max-auth-failures
set auth-policy api lockout-period <lockout-period>
set auth-policy api lockout-reset-period <lockout-reset-period>
set auth-policy api max-auth-failures <auth-failures>
```

以下命令适用于登录到 NSX Manager 或 NSX Edge 节点上的 CLI:

```
get auth-policy cli lockout-period
get auth-policy cli max-auth-failures
set auth-policy cli lockout-period <lockout-period>
set auth-policy cli max-auth-failures <auth-failures>
```

有关 CLI 命令的详细信息, 请参阅《NSX-T 命令行界面参考》。

默认情况下, 在五次连续尝试登录到 NSX Manager UI 失败后, 管理员帐户将锁定 15 分钟。您可以使用以下命令禁用帐户锁定:

```
set auth-policy api lockout-period 0
```

同样, 您可以使用以下命令为 CLI 禁用帐户锁定:

```
set auth-policy cli lockout-period 0
```

从 vIDM 主机中获取证书指纹

在配置 vIDM 与 NSX-T 的集成之前, 您必须从 vIDM 主机中获取证书指纹。

您必须使用 OpenSSL 版本 1.x 或更高版本获取指纹。在 vIDM 主机中, 命令 `openssl` 运行较旧的 OpenSSL 版本, 因此您必须在 vIDM 主机中使用命令 `openss1`。此命令仅在 vIDM 主机中可用。

在不是 vIDM 主机的服务器中, 您可以使用运行 OpenSSL 版本 1.x 或更高版本的 `openssl` 命令。

步骤

- 1 在 vIDM 主机的控制台或以用户 **sshuser** 的身份使用 SSH 登录到 vIDM 主机, 或者登录到可以对 vIDM 主机执行 ping 操作的任何服务器。
- 2 运行以下命令以获取 vIDM 主机的指纹。
 - 如果已登录到 vIDM 主机, 请运行 `openss1` 命令来获取指纹:

```
openss1 s_client -connect <FQDN of vIDM host>:443 < /dev/null 2> /dev/null | openssl
x509 -sha256 -fingerprint -noout -in /dev/stdin
```

如果在运行命令时出错, 您可能需要使用 `sudo` 命令 (即, `sudo openss1 ...`) 运行 `openss1`。

- 如果已登录到可以对 vIDM 主机执行 ping 操作的服务器, 请运行 `openssl` 命令来获取指纹:

```
openssl s_client -connect <FQDN of vIDM host>:443 < /dev/null 2> /dev/null | openssl
x509 -sha256 -fingerprint -noout -in /dev/stdin
```

配置 VMware Identity Manager 集成

可以将 NSX-T Data Center 与 VMware Identity Manager (vIDM) 集成，vIDM 可提供身份管理服务。vIDM 部署可以是一个独立的 vIDM 主机，也可以是一个 vIDM 集群。

vIDM 主机或所有 vIDM 集群组件应具有证书颁发机构 (CA) 签名的证书。否则，使用某些浏览器（例如 Microsoft Edge 或 Internet Explorer 11）可能无法从 NSX Manager 登录到 vIDM。有关在 vIDM 上安装 CA 签名证书的信息，请参见 VMware Identity Manager 文档，网址为 <https://docs.vmware.com/cn/VMware-Identity-Manager/index.html>。

在向 vIDM 注册 NSX Manager 时，指定指向 NSX Manager 的重定向 URI。可以提供完全限定域名 (FQDN) 或 IP 地址。请务必记住使用的是 FQDN 还是 IP 地址。尝试通过 vIDM 登录到 NSX Manager 时，必须以相同的方式在 URL 中指定主机名，也就是说，如果向 vIDM 注册管理器时使用的是 FQDN，则必须在 URL 中使用 FQDN；如果向 vIDM 注册管理器时使用的是 IP 地址，则必须在 URL 中使用 IP 地址。否则，登录将失败。

如果需要 NSX-T API 访问权限，则必须具备以下某项配置：

- vIDM 具有已知的 CA 签名证书。
- vIDM 在 vIDM 服务端信任连接器 CA 证书。
- vIDM 使用出站连接器模式。

注 NSX Manager 和 vIDM 必须位于同一时区。建议的方法是使用 UTC。

如果未使用虚拟 IP 或外部负载均衡器（这意味着管理器是使用节点的物理 IP 或 FQDN 配置的），则必须将 DNS 服务器配置为具有 PTR 记录。

如果您将 vIDM 配置为与外部负载均衡器相集成，则必须在负载均衡器上启用会话持久性，以避免出现无法加载页面或用户意外注销等问题。

如果 vIDM 部署是一个 vIDM 集群，则必须配置 vIDM 负载均衡器以实现 SSL 终止和重新加密功能。

在启用 vIDM 的情况下，如果使用 URL `https://<nsx-manager-ip-address>/login.jsp?local=true`，您仍然可以使用本地用户帐户登录到 NSX Manager。

如果使用用户主体名称 (User Principal Name, UPN) 登录到 vIDM，则可能通不过 NSX-T 的身份验证。为避免出现此问题，请使用其他类型的凭据，例如，SAM 帐户名称。

如果使用 NSX Cloud，您可以使用 URL `https://<csm-ip-address>/login.jsp?local=true` 单独登录到 CSM。

前提条件

- 确认您具有来自 vIDM 主机或 vIDM 负载均衡器的证书指纹，证书指纹具体来自何处取决于 vIDM 部署的类型（独立 vIDM 主机或 vIDM 集群）。在这两种情况下，获取指纹的命令相同。请参见从 [vIDM 主机中获取证书指纹](#)。

- 确认在 vIDM 中将 NSX Manager 注册为 OAuth 客户端。在注册过程中，请记下客户端 ID 和客户端密码。有关详细信息，请参见 VMware Identity Manager 文档，网址为 <https://docs.vmware.com/cn/VMware-Workspace-ONE-Access/3.3/idm-administrator/GUID-AD4B6F91-2D68-48F2-9212-5B69D40A1FAE.html>。创建客户端时，只需执行以下操作：
 - 将访问类型设置为服务客户端令牌。
 - 指定客户端 ID。
 - 展开高级字段，然后单击生成共享密钥。
 - 单击添加。

NSX Cloud 说明 如果使用 NSX Cloud，还要确认在 vIDM 中将 CSM 注册为 OAuth 客户端。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择 **系统 > 用户**。
- 3 单击 **配置** 选项卡。
- 4 单击 **编辑**。
- 5 要启用外部负载均衡器集成，请单击 **外部负载均衡器集成** 切换按钮。

注 如果您设置了虚拟 IP (Virtual IP, VIP)（请检查 **系统 > 设备 > 虚拟 IP**），则无法使用 **外部负载均衡器集成**（即使启用了该集成也是如此）。这是因为，在配置 vIDM 时您可以具有 VIP 或外部负载均衡器，但不能同时具有两者。如果要使用外部负载均衡器，请禁用 VIP。有关详细信息，请参见 NSX-T Data Center 安装指南中的 [配置集群的虚拟 IP \(VIP\) 地址](#)。

- 6 要启用 VMware Identity Manager 集成，请单击 **VMware Identity Manager 集成** 切换按钮。
- 7 提供以下信息。

参数	说明
VMware Identity Manager 设备	vIDM 主机或 vIDM 负载均衡器的完全限定域名 (FQDN)，具体取决于 vIDM 部署的类型（独立 vIDM 主机或 vIDM 集群）。
OAuth 客户端 ID	在 vIDM 中注册 NSX Manager 时创建的 ID。
OAuth 客户端密码	在 vIDM 中注册 NSX Manager 时创建的密码。
SSL 指纹	vIDM 主机的证书指纹。
NSX 设备	NSX Manager 的 IP 地址或完全限定域名 (FQDN)。如果使用的是 NSX Manager 集群，请使用负载均衡器 FQDN 或集群 VIP FQDN 或 IP 地址。如果您指定 FQDN，则必须在 URL 中使用管理器的 FQDN 从浏览器访问 NSX Manager，如果您指定 IP 地址，则必须在 URL 中使用 IP 地址。或者，vIDM 管理员可以配置 NSX Manager 客户端，以便使用 FQDN 或 IP 地址进行连接。

- 8 单击 **保存**。
- 9 如果使用 NSX Cloud，请登录到 CSM（而不是 NSX Manager）以从 CSM 设备中重复步骤 1 至 8。

验证 VMware Identity Manager 功能

配置 VMware Identity Manager 后，请验证该功能。除非已正确配置并验证 VMware Identity Manager，否则，在尝试登录时，某些用户可能收到“未授权（错误代码 98）” (Not Authorized (Error Code 98)) 消息。

除非已正确配置并验证 VMware Identity Manager，否则，在尝试登录时，某些用户可能收到“未授权（错误代码 98）” (Not Authorized (Error Code 98)) 消息。

步骤

- 1 创建采用 base64 编码的用户名和密码。

运行以下命令以获取编码，并移除尾随“\n”字符。例如：

```
echo -n 'sfadmin@ad.node.com:password1234!' | base64 | tr -d '\n'
c2ZhZG1pbkZhZC5ub2RlLmNvbTpwYXNzd29yZDEyMzQhCg==
```

- 2 确认每个用户都可以对每个节点进行 API 调用。

使用远程授权 curl 命令：curl -k -H 'Authorization: Remote <base64 encoding string>' https://<node FQDN>/api/v1/node/aaa/auth-policy。例如：

```
curl -k -H 'Authorization: Remote c2ZhZG1pbkZhZC5ub2RlLmNvbTpwYXNzd29yZDEyMzQhCg==' /
https://tmgr1.cptroot.com/api/v1/node/aaa/auth-policy
```

这将返回授权策略设置，例如：

```
{
  "_schema": "AuthenticationPolicyProperties",
  "_self": {
    "href": "/node/aaa/auth-policy",
    "rel": "self"
  },
  "api_failed_auth_lockout_period": 900,
  "api_failed_auth_reset_period": 900,
  "api_max_auth_failures": 5,
  "cli_failed_auth_lockout_period": 900,
  "cli_max_auth_failures": 5,
  "minimum_password_length": 12
}
```

如果该命令未返回错误，则表示 VMware Identity Manager 正常工作。无需执行进一步的步骤。如果 curl 命令返回错误，则用户可能会被锁定。

注 帐户锁定策略是按节点设置和实施的。如果集群中的一个节点已锁定用户，其他节点可能未锁定该用户。

3 要在节点上重置用户锁定，请执行以下操作：

- a 使用本地 NSX Manager admin 用户检索授权策略：

```
curl -k -u 'admin:<password>' https://nsxmgr/api/v1/node/aaa/auth-policy
```

- b 将输出保存到当前工作目录中的 JSON 文件。
c 修改该文件以更改锁定时间段设置。

例如，许多默认设置会应用锁定，并将锁定时间重置为 900 秒。更改这些值以启用立即重置，例如：

```
{
  "_schema": "AuthenticationPolicyProperties",
  "_self": {
    "href": "/node/aaa/auth-policy",
    "rel": "self"
  },
  "api_failed_auth_lockout_period": 1,
  "api_failed_auth_reset_period": 1,
  "api_max_auth_failures": 5,
  "cli_failed_auth_lockout_period": 1,
  "cli_max_auth_failures": 5,
  "minimum_password_length": 12
}
```

- d 将所做更改应用到受影响的节点。

```
curl -k -u 'admin:<password>' -H 'Content-Type: application/json' -d \
@<modified_policy_setting.json> https://nsxmgr/api/v1/node/aaa/auth-policy
```

- e （可选）将授权策略设置文件恢复到以前的设置。

这应可以解决锁定问题。如果您仍可以进行远程身份验证 API 调用，但仍无法通过浏览器登录，则浏览器存储缓存或 Cookie 可能无效。请清除您的缓存和 Cookie，然后重试。

NSX Manager、vIDM 和相关组件之间的时间同步

要使身份验证能够正常进行，NSX Manager、vIDM 和其他服务提供程序（例如 Active Directory）必须进行时间同步。本节介绍如何对这些组件进行时间同步。

VMware 基础架构

按照以下知识库文章中的说明对 ESXi 主机进行同步。

- <https://kb.vmware.com/kb/1003736>
- <https://kb.vmware.com/kb/2012069>

第三方基础架构

请遵循供应商文档说明，了解如何同步虚拟机和主机。

在 vIDM 服务器上配置 NTP（不推荐）

如果您不能跨主机同步时间，则可以禁用同步到主机并在 vIDM 服务器上配置 NTP。不建议使用此方法，因为这需要在 vIDM 服务器上打开 UDP 端口 123。

- 检查 vIDM 服务器上的时钟，并确保其正确无误。

```
# hwclock
Tue May 9 12:08:43 2017 -0.739213 seconds
```

- 编辑 `/etc/ntp.conf` 并添加以下条目（如果尚不存在）。

```
server time.nist.gov
server pool.ntp.org
server time.is dynamic
restrict 192.168.100.0 netmask 255.255.255.0 nomodify notrap
```

- 打开 UDP 端口 123。

```
# iptables -A INPUT -p udp --dport 123 -j ACCEPT
```

运行以下命令检查该端口是否已打开。

```
# iptables -L -n
```

- 启动 NTP 服务。

```
/etc/init.d/ntp start
```

- 使 NTP 在重新引导后自动运行。

```
# chkconfig --add ntp
# chkconfig ntp on
```

- 检查是否可以访问 NTP 服务器。

```
# ntpq -p
```

reach 列不应显示 0。st 列应显示除 16 以外的某个数字。

基于角色的访问控制

通过使用基于角色的访问控制 (RBAC)，您可以仅允许授权的用户进行系统访问。将为用户分配角色，每个角色具有特定的权限。

共有四种类型的权限：

- 完全访问
- 执行
- 读取
- 无

完全访问为用户提供所有权限。执行权限包括读取权限。

NSX-T Data Center 具有以下内置角色。您无法添加任何新角色。

- 企业管理员
- 审核员
- 网络工程师
- 网络操作员
- 安全工程师
- 安全操作员
- 负载均衡器管理员
- 负载均衡器审核员
- VPN 管理员
- Guest Introspection 管理员
- 网络自检管理员

为 Active Directory (AD) 用户分配角色后，如果用户名在 AD 服务器上发生更改，则您需要使用新的用户名重新分配角色。

角色和权限

表 21-5. 角色和权限和表 21-6. 高级网络和安全的角色和权限显示每个角色在执行不同的操作时具有的权限。其中使用了以下缩写：

- EA - 企业管理员
- A - 审核员
- NE - 网络工程师
- NO - 网络操作员
- SE - 安全工程师
- SO - 安全操作员
- LB Adm - 负载均衡器管理员
- LB Aud - 负载均衡器审核员
- VPN Adm - VPN 管理员
- GI Adm - Guest Introspection 管理员
- NI Adm - 网络自检管理员
- FA - 完全访问
- E - 执行
- R - 读取

表 21-5. 角色和权限

操作	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Ad m	LB Au d	VPN Adm	GI Adm	NI Adm
网络 > Tier-0 网关	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
网络 > 网络接口	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
网络 > 网络静态 路由	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
网络 > 区域设置 服务	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
网络 > 静态 ARP 配 置	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
网络 > 分段	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
网络 > 分段 > 分段配置 文件	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
网络 > IP 地址 池	FA	R	FA	FA	R	R	FA	R	R	R	无	无	无
网络转发 策略	FA	R	FA	R	FA	R	FA	R	无	无	无	无	无
网络 > DNS	FA	R	FA	FA	R	R	FA	R	R	R	无	无	无
网络 > 负载均衡	FA	R	无	无	R	无	FA	R	FA	R	无	无	无
网络 > NAT	FA	R	FA	R	FA	R	FA	R	R	R	无	无	无
网络 > VPN	FA	R	FA	R	FA	R	FA	R	无	无	FA	无	无
网络 > IPv6 配 置文件													
安全 > 分布式防 火墙	FA	R	R	R	FA	R	FA	R	R	R	R	R	R

表 21-5. 角色和权限（续）

操作	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Ad m	LB Au d	VPN Adm	GI Adm	NI Adm
安全 > 网关防火 墙	FA	R	R	R	FA	R	FA	R	无	无	无	无	FA
安全 > 网络自检	FA	R	R	R	R	R	FA	R	无	无	无	无	FA
安全 > 端点保护 规则	FA	R	R	R	R	R	FA	R	无	无	无	FA	无
清单 > 上下文配 置文件	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R
清单 > 虚拟机	R	R	R	R	R	R	R	R	R	R	R	R	R
安全规划 和故障排 除 > 端 口镜像	FA	R	FA	R	R	R	FA	R	无	无	无	无	无
安全规划 和故障排 除 > 端 口镜像绑 定	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
安全规划 和故障排 除 > 监 控配置文 件绑定	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
安全规划 和故障排 除 > 防 火墙 IPFIX 配 置文件	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R
安全规划 和故障排 除 > 交 换机 IPFIX 配 置文件	FA	R	FA	R	R	R	FA	R	R	R	R	R	R
系统 > 结构层 > 节点 > 主机	FA	R	R	R	R	R	R	R	无	无	无	无	无

表 21-5. 角色和权限（续）

操作	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Ad m	LB Au d	VPN Adm	GI Adm	NI Adm
系统 > 结构层 > 节点 > 节点	FA	R	FA	R	FA	R	R	R	R	R	无	无	无
系统 > 结构层 > 节点 > Edge	FA	R	FA	R	R	R	R	R	无	无	无	无	无
系统 > 结构层 > 节点 > Edge 群 集	FA	R	FA	R	R	R	R	R	无	无	无	无	无
系统 > 结构层 > 节点 > 网桥	FA	R	FA	R	R	R	无	无	R	R	无	无	无
系统 > 结构层 > 节点 > 传输节点	FA	R	R	R	R	R	R	R	R	R	无	无	无
系统 > 结构层 > 节点 > 隧道	R	R	R	R	R	R	R	R	R	R	无	无	无
系统 > 结构层 > 配置文件 > 上行链 路配置文 件	FA	R	R	R	R	R	R	R	R	R	无	无	无
系统 > 结构层 > 配置文件 > Edge 群集配置 文件	FA	R	FA	R	R	R	R	R	R	R	无	无	无
系统 > 结构层 > 配置文件 > 配置	FA	R	无	无	无	无	R	R	无	无	无	无	无

表 21-5. 角色和权限（续）

操作	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Ad m	LB Au d	VPN Adm	GI Adm	NI Adm
系统 > 结构层 > 传输区域 > 传输区 域	FA	R	R	R	R	R	R	R	R	R	无	无	无
系统 > 结构层 > 传输区域 > 传输区 域配置文件	FA	R	R	R	R	R	R	R	无	无	无	无	无
系统 > 结构层 > 计算管理 器	FA	R	R	R	R	R	R	R	无	无	无	R	R
系统 > 证书	FA	R	无	无	FA	R	无	无	FA	R	FA	无	无
系统 > 服务部署 > 服务实 例	FA	R	R	R	FA	R	FA	R	无	无	无	FA	FA
系统 > 实用程序 > 支持包	FA	R	无	无	无	无	无	无	无	无	无	无	无
系统 > 实用程序 > 备份	FA	R	无	无	无	无	无	无	无	无	无	无	无
系统 > 实用程序 > 还原	FA	R	无	无	无	无	无	无	无	无	无	无	无
系统 > 实用程序 > 升级	FA	R	R	R	R	R	无	无	无	无	无	无	无
系统 > 用户 > 角色分配	FA	R	无	无	无	无	无	无	无	无	无	无	无
系统 > Active Director y	FA	R	FA	R	FA	FA	R	R	R	R	R	R	R
系统 > 用户 > 配置	FA	R	无	无	无	无	无	无	无	无	无	无	无

表 21-5. 角色和权限（续）

操作	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Ad m	LB Au d	VPN Adm	GI Adm	NI Adm
系统 > 许可证	FA	R	R	R	R	R	无	无	无	无	无	无	无
系统 > 系统管理	FA	R	R	R	R	R	R	R	无	无	无	无	无
自定义仪 表盘配置	FA	R	R	R	R	R	FA	R	R	R	R	R	R
系统 > 生命周期 管理 > 迁移	FA	无	无	无	无	无	无	无	无	无	无	无	无

表 21-6. 高级网络和安全的角色和权限

操作	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Ad m	LB Au d	VPN Adm	GI Adm	NI Adm
工具 > 端口连接	E	R	E	E	E	E	E	R	E	E	无	无	无
工具 > 跟踪流	E	R	E	E	E	E	E	R	E	E	无	无	无
工具 > 端口镜像	FA	R	FA	R	R	R	FA	R	无	无	无	无	无
工具 > IPFIX	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R
防火墙 > 分布式防 火墙 > 常规	FA	R	R	R	FA	R	FA	R	无	无	无	无	R
防火墙 > 分布式防 火墙 > 配置	FA	R	R	R	FA	R	FA	R	无	无	无	无	无
防火墙 > Edge 防 火墙	FA	R	R	R	FA	R	FA	R	无	无	无	无	FA
路由 > 路由器	FA	R	FA	FA	R	R	FA	R	R	R	R	无	R
路由 > NAT	FA	R	FA	R	FA	R	FA	R	R	R	无	无	无
DHCP > 服务器配 置文件	FA	R	FA	R	无	无	FA	R	无	无	无	无	无

表 21-6. 高级网络和安全的角色和权限（续）

操作	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Ad m	LB Au d	VPN Adm	GI Adm	NI Adm
DHCP > 服务器	FA	R	FA	R	无	无	FA	R	无	无	无	无	无
DHCP > 中继配置 文件	FA	R	FA	R	无	无	FA	R	无	无	无	无	无
DHCP > 中继服务	FA	R	FA	R	无	无	FA	R	无	无	无	无	无
DHCP > 元数据代 理	FA	R	FA	R	无	无	无	无	无	无	无	无	无
IPAM	FA	R	FA	FA	R	R	无	无	R	R	无	无	无
交换 > 交换机	FA	R	FA	FA	R	R	FA	R	R	R	R	无	R
交换 > 端口	FA	R	FA	FA	R	R	FA	R	R	R	R	无	R
交换 > 交换配置 文件	FA	R	FA	FA	R	R	FA	R	R	R	无	无	无
网络 > 负载均衡 器	FA	R	无	无	R	无	FA	R	FA	R	无	无	无
负载均衡 > 配置文 件 > SSL 配置文件	FA	R	无	无	FA	R	FA	R	FA	R	无	无	无
清单 > 组	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R
清单 > IP 集	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R
清单 > IP 池	FA	R	FA	R	无	无	无	无	R	R	R	R	R
清单 > MAC 集	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R
清单 > 服务	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R
清单 > 虚拟机	R	R	R	R	R	R	R	R	R	R	R	R	R
清单 > 虚拟机 > 配置标记	FA	无	无	无	无	无	无	无	无	无	无	无	无

添加角色分配或主体身份

如果 VMware Identity Manager 与 NSX-T Data Center 集成，则可以向用户或用户组分配角色。还可以向主体身份分配角色。

主体为 NSX-T Data Center 组件或第三方应用程序，例如，OpenStack 产品。通过主体身份，主体可以使用身份名称创建一个对象，并确保仅具有相同身份名称的实体可以修改或删除该对象。主体身份具有以下属性：

- 名称
- 节点 ID - 这可以是分配给主体身份的任何字母数字值
- 证书
- RBAC 角色，指明该主体的访问权限

具有企业管理员角色的用户（本地、远程或主体身份）可以修改或删除主体身份拥有的对象。不具有企业管理员角色的用户（本地、远程或主体身份）无法修改或删除主体身份拥有的受保护对象，但可以修改或删除不受保护对象。

如果主体身份用户的证书过期，您必须导入新证书，并进行 API 调用以更新主体身份用户的证书（请参见以下过程）。有关 NSX-T Data Center API 的详细信息，请访问 <https://docs.vmware.com/cn/VMware-NSX-T-Data-Center> 中的 API 资源链接。

主体身份用户的证书必须满足以下要求：

- 基于 SHA256。
- RSA/DSA 消息算法的密钥大小为 2048 位或更高。
- 不能是根证书。

您可以使用 API 删除主体身份。但是，删除主体身份不会自动删除相应的证书。您必须手动删除证书。

删除主体身份及其证书的步骤如下：

- 1 获取要删除的主体身份的详细信息，并记下响应中的 `certificate_id` 值。


```
GET /api/v1/trust-management/principal-identities/<principal-identity-id>
```
- 2 删除主体身份。


```
DELETE /api/v1/trust-management/principal-identities/<principal-identity-id>
```
- 3 使用在步骤 1 中获取的 `certificate_id` 值删除证书。


```
DELETE /api/v1/trust-management/certificates/<certificate_id>
```

前提条件

- 如果要向用户分配角色，请确认 vIDM 主机与 NSX-T 相关联。有关详细信息，请参见[配置 VMware Identity Manager 集成](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。

- 2 选择**系统 > 用户**。
- 3 要向用户分配角色，请选择**添加 > 角色分配**。
 - a 选择用户或用户组。
 - b 选择角色。
 - c 单击**保存**。
- 4 要添加主体身份，请选择**添加 > 主体身份和角色**。
 - a 输入主体身份的名称。
 - b 选择角色。
 - c 输入节点 ID。
 - d 输入 PEM 格式的证书。
 - e 单击**保存**。
- 5 （可选）如果使用 NSX Cloud，请登录到 CSM 设备而不是 NSX Manager，然后重复步骤 1 至 4。
- 6 如果主体身份的证书过期，请执行以下步骤：
 - a 导入新证书并记下证书的 ID。请参见[导入证书](#)。
 - b 调用以下 API 以获取主体身份的 ID。

```
GET https://<nsx-mgr>/api/v1/trust-management/principal-identities
```

- c 调用以下 API 以更新主体身份的证书。您必须提供导入的证书的 ID 和主体身份用户的 ID。

例如，

```
POST https://<nsx-mgr>/api/v1/trust-management/principal-identities?
action=update_certificate
{
  "principal_identity_id": "ebd3032d-728e-44d4-9914-d4f81c9972cb",
  "certificate_id" : "abd3032d-728e-44d4-9914-d4f81c9972cc"
}
```

备份和还原 NSX Manager

如果 NSX Manager 群集变得无法运行，或者如果要将环境还原到以前的状态，则可以从备份还原。NSX Manager 无法运行时，数据层面不受影响，但无法进行配置更改。

有两种备份类型：

群集备份

该备份包含虚拟网络的所需状态。

节点备份

这是 NSX Manager 节点的备份。

共有两种备份方法：

手动

可以随时手动运行备份。

自动

自动备份是根据您制订的计划运行的。强烈建议进行自动备份以确保拥有最新备份。

可以将 NSX-T Data Center 配置还原回在任何备份中捕获的状态。在还原备份时，必须还原到一个新 NSX Manager 设备，且该设备与备份的设备运行相同版本的 NSX Manager。

配置备份

必须配置备份文件服务器后，才能开始进行备份。配置备份文件服务器后，可以随时开始备份，也可以为自动备份配置计划。

前提条件

确认您具有备份文件服务器的 SSH 指纹。仅接受将 SHA256 哈希处理的 ECDSA（256 位）密钥作为指纹。请参见[查找远程服务器的 SSH 指纹](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 选择 **系统 > 备份和还原**。
- 3 单击页面右上角的**编辑**以配置备份。
- 4 输入备份文件服务器的 IP 地址或主机名。
- 5 根据需要更改默认端口。
- 6 已填写协议字段。请不要更改该值。

SFTP 是唯一支持的协议。

- 7 输入登录到备份文件服务器所需的用户名和密码。

首次配置文件服务器时，必须提供密码。以后，如果重新配置文件服务器且服务器 IP（或主机名）、端口和用户名相同，则无需重新输入密码。

8 在目标目录字段中，输入存储备份的绝对目录路径。

该目录必须已存在，且不能为 /。如果有多个 NSX-T Data Center 部署，则必须为每个部署使用不同的目录。如果备份文件服务器是 Windows 计算机，则在指定目标目录时仍需使用正斜杠。例如，如果 Windows 计算机上的备份目录为 c:\SFTP_Root\backup，请将 /SFTP_Root/backup 指定为目标目录。

注 备份过程将生成可能很长的备份文件名称。在 Windows Server 上，备份文件的完整路径名称长度可能会超过 Windows 设置的限制，从而导致备份失败。要避免出现此问题，请参见知识库文章 <https://kb.vmware.com/s/article/76528>。

9 要加密备份，请单击 **更改加密密码短语** 切换按钮，然后输入加密密码短语。

您需要使用该密码短语还原备份。如果忘记了密码短语，则无法还原任何备份。

10 输入存储备份的服务器的 SSH 指纹。

可以将其留空，并接受或拒绝服务器提供的指纹。

11 单击 **计划** 选项卡。

12 要启用自动备份，请单击 **自动备份** 切换按钮。

13 单击 **每周** 并设置备份的日期和时间，或单击 **间隔** 并设置备份之间的间隔。

14 启用 **检测到 NSX 配置更改** 后，会在检测到任何运行时更改或非配置相关更改或者任何用户配置更改时触发未计划的完整配置备份。

可以设置配置更改触发的备份之间的间隔。默认值为 5 分钟。

注 此选项可能会生成大量备份。请谨慎使用。

15 单击 **保存**。

结果

配置备份文件服务器后，可以随时单击 **立即备份** 开始备份。

移除旧备份

备份会在备份文件服务器上累积并占用大量存储。可以通过运行 NSX-T Data Center 附带的脚本自动删除旧备份。

可以在 NSX Manager 的目录 /var/vmware/nsx/file-store 下找到 Python 脚本 nsx_backup_cleaner.py。必须以 root 用户身份登录才能访问该文件。通常情况下，在备份文件服务器上调度一个作业，来定期运行此脚本以清理旧备份。以下使用信息介绍了如何运行此脚本：

```
nsx_backup_cleaner.py -d backup_dir [-k 1] [-l 5] [-h]
Or
nsx_backup_cleaner.py --dir backup_dir [--retention-period 1] [--min-count 5] [--help]

Required parameters:
  -d/--dir: Backup root directory
  -k/--retention-period: Number of days need to retain a backup file
```

Optional parameters:

```
-l/--min-count: Minimum number of backup files to be kept, default value is 100
-h/--help: Display help message
```

备份使用期限根据备份的时间戳与该脚本的运行时间之间的差值计算得出。如果该值大于保留期，则磁盘上的备份数量超过最小备份数量时，删除备份。

有关在 Linux 或 Windows 服务器上将脚本设置为定期运行的详细信息，请参见脚本开头的注释。

列出可用备份

备份文件服务器存储所有 NSX Manager 中的备份。要获取备份列表，以便可以找到要还原的备份，您必须运行 `get_backup_timestamps.sh` 脚本。

该脚本位于 NSX Manager 上。完整路径名称为 `var/vmware/nsx/file-store/`

`get_backup_timestamps.sh`。您可以在任何 Linux 计算机或 NSX-T Data Center 设备上运行此脚本。最佳做法是，安装 NSX-T Data Center 后应将此脚本复制到非 NSX Manager 的计算机，以便即使所有 NSX Manager 变得无法访问，您也可以运行此脚本。如果您需要还原备份，但无法访问此脚本，可以安装新 NSX Manager 并在那里运行此脚本。

通过以管理员身份登录到 NSX Manager 并运行 CLI 命令，可以将脚本复制到其他计算机或备份文件服务器。例如：

```
nsxmgr-1> copy file get_backup_timestamps.sh url scp://admin@10.127.1.20/tmp/
admin@10.127.1.20's password:
nsxmgr-1>
```

此脚本交互操作，将提示您提供在配置备份文件服务器时指定的信息。您可以指定要显示的备份数量。如果 NSX Manager 节点设置为发布其 FQDN 和节点 ID，则列出的每个备份将带有时间戳、NSX Manager 节点的 IP 地址或 FQDN。例如，

```
admin@host1:/home/admin# ./get_backup_timestamps.sh
Enter file server ip:
10.108.115.108
Enter port:
22
Enter directory path:
/home/nsx/backups
Enter number of latest backup or press Enter to list all backups:

root@10.108.115.108's password:
Latest backups:
[Backup timestamp; IP address/FQDN; Node id]
2019-01-22;09:00:33 10.196.196.77 35163642-6623-8f6d-7af0-52e03f16faed
2019-01-22;09:01:52 10.196.196.77 35163642-6623-8f6d-7af0-52e03f16faed
2019-01-22;09:13:30 wdc75.platformqe.com 41893642-597b-915f-5117-7da576df4ff2
2019-01-22;09:14:42 wdc75.platformqe.com 41893642-597b-915f-5117-7da576df4ff2
2019-01-22;09:16:43 wdc75.platformqe.com 41893642-597b-915f-5117-7da576df4ff2
```

还原备份

还原备份将导致还原创建备份时的网络状态。此外，还会还原由 NSX Manager 维护的配置，以及协调在创建备份后对 Fabric 进行的任何更改（如添加或删除节点）。

您必须将备份还原到新的 NSX Manager 设备。

如果在创建备份时具有 NSX Manager 集群，您还应还原到 NSX Manager 集群。还原过程先还原一个 NSX Manager 节点，然后提示您添加其他 NSX Manager 节点。

重要事项 如果 NSX Manager 集群中的任何节点仍然可用，则必须在启动还原之前关闭这些节点的电源。

前提条件

- 确认您具有备份文件服务器的登录凭据。
- 确认您具有备份文件服务器的 SSH 指纹。仅接受将 SHA256 哈希处理的 ECDSA（256 位）密钥作为指纹。请参见[查找远程服务器的 SSH 指纹](#)。
- 确认您具有备份文件的密码短语。
- 按照[列出可用备份](#)中所述的过程确定要还原的备份。记下创建备份的 NSX Manager 节点的 IP 或 FQDN。
- 如果将 NSX Manager 节点配置为发布其 FQDN，则必须为 DNS 服务器上的 NSX Manager 节点配置正向和反向查找条目。

步骤

- 1 关闭要还原的 NSX Manager 集群中的所有节点的电源。
- 2 安装一个新的 NSX Manager 节点以在其中还原备份。
 - 如果要还原的备份的备份列表包含一个 IP 地址，则必须使用该同一 IP 地址部署新的 NSX Manager 节点。请勿将 NSX Manager 节点配置为发布其 FQDN。

```
2019-01-22;09:01:52 10.196.196.77 35163642-6623-8f6d-7af0-52e03f16faed
```

- 如果要还原的备份的备份列表包含 FQDN，则必须使用此 FQDN 来配置新的 NSX Manager 节点（有关详细信息，请参见 NSX-T Data Center 安装指南 中的“NSX Manager 安装”主题中的“发布 NXS Manager 的 FQDN”部分）。此外，如果新 NSX Manager 节点的 IP 地址与原始节点不同，则必须将 NSX Manager 节点的 DNS 服务器正向和反向查找条目更新为新 IP 地址。

```
2019-01-22;09:16:43 nsxmgr.example.com 41893642-597b-915f-5117-7da576df4ff2
```

在新的 NSX Manager 节点运行且联机后，您可以继续执行还原。

- 3 从浏览器中，使用管理员特权登录到新的 NSX Manager。
- 4 选择 **系统 > 备份和还原**。
- 5 单击 **还原** 选项卡。

- 6 要配置备份文件服务器，请单击**编辑**。
- 7 输入 IP 地址或主机名。
- 8 如有必要，请更改端口号。
默认值为 22。
- 9 要登录到服务器，请输入用户名和密码。
- 10 在**目标目录**文本框中，输入存储备份的绝对目录路径。
- 11 输入用于加密备份数据的密码短语。
- 12 输入存储备份的服务器的 SSH 指纹。
- 13 单击**保存**。
- 14 选择一个备份。
- 15 单击**还原**。

将显示还原操作的状态。如果在备份后删除或添加了 Fabric 节点或传输节点，将提示您执行某些操作，例如，登录到节点并运行脚本。

如果备份包含有关 NSX Manager 集群的信息，将提示您添加 NSX Manager 节点。如果您决定不添加 NSX Manager 节点，您仍然可以进行还原。

在还原操作完成后，**还原完成**屏幕将显示还原结果、备份文件时间戳以及还原操作的开始和结束时间。

如果还原失败，该屏幕将显示失败的步骤，例如，Current Step: Restoring Cluster (DB) 或 Current Step: Restoring Node。如果集群还原或节点还原失败，该错误可能是暂时性的。在这种情况下，无需单击**重试**。您可以重新启动或重新引导管理器，然后继续进行还原。

您还可以通过查看日志文件来确定是否存在集群还原或节点还原失败情况。运行 `get log-file syslog` 以查看系统日志文件，然后搜索 Cluster restore failed 和 Node restore failed 字符串。

要重新启动管理器，请运行 `restart service manager` 命令。

要重新引导管理器，请运行 `reboot` 命令。

- 16 如果仅部署了一个节点，则在还原后的 NSX Manager 节点启动且正常运行后，您可以部署其他节点以形成一个 NSX Manager 集群。

有关说明，请参见 NSX-T Data Center 安装指南。

- 17 部署新的 NSX Manager 集群后，删除在步骤 1 中关闭其电源的原始 NSX Manager 集群虚拟机。

您还必须替换集群中第二个和第三个节点上的证书。

结果

如果在备份后添加了一个计算管理器，并且尝试在还原后再次添加该计算管理器，则会收到一条错误消息，指示注册失败。您可以单击**解决**按钮以解决错误并成功添加计算管理器。有关详细信息，请参见[添加计算管理器](#)中的步骤 4。如果要移除有关存储在 vCenter Server 中的 NSX-T Data Center 的信息，请执行[从 vCenter Server 中移除 NSX-T Data Center 扩展](#)中的步骤。

在升级过程中备份和还原

管理平面在升级过程中停止响应，为此您需要还原在进行升级的过程中创建的备份。

问题

升级协调器已升级，管理平面停止响应。您在进行升级的过程中创建了一个备份。

解决方案

- 1 使用创建备份时所使用的 IP 地址部署管理平面节点。
- 2 上载在升级过程刚开始时所使用的升级包。
- 3 对升级协调器进行升级。
- 4 还原在升级过程中创建的备份。
- 5 如有必要，请上载一个新的升级包。
- 6 继续执行升级过程。

从 vCenter Server 中移除 NSX-T Data Center 扩展

添加某个计算管理器后，NSX Manager 会将其身份作为扩展添加到 vCenter Server 中。如果移除计算管理器，将自动移除 vCenter Server 中的扩展。如果由于某种原因未移除该扩展，您可以使用以下过程手动移除该扩展。

前提条件

执行 <https://kb.vmware.com/s/article/2042554> 中的过程以允许访问 vCenter Server 受管对象浏览器 (Managed Object Browser, MOB)。

步骤

- 1 登录到 `https://<vCenter Server hostname or IP address>/mob` 中的 MOB。
- 2 单击 **content** 链接，即，“属性”表中 **content** 属性的值。
- 3 单击 **ExtensionManager** 链接，即，“属性”表中 **extensionManager** 属性的值。
- 4 单击“方法”表中的 **UnregisterExtension** 链接。
- 5 在值文本字段中输入 `com.vmware.nsx.management.nsxt`。
- 6 单击页面右侧“参数”表下方的调用方法链接。
方法结果显示 `void`，但该扩展将被移除。
- 7 要确保移除了该扩展，请单击上一页中的 **FindExtension** 方法，然后为该扩展输入相同的值以调用该方法。
结果应为 `void`。

管理 NSX Manager 集群

如果 NSX Manager 变得无法运行，可以将其重新引导。也可以更改 NSX Manager 的 IP 地址。

在生产环境中，强烈建议 NSX Manager 集群包含三个成员，以提高高可用性。如果删除一个 NSX Manager 并部署一个新的 NSX Manager，则新的 NSX Manager 可以具有相同或不同的 IP 地址。

注 主 NSX Manager 节点是您在创建管理器集群之前首先创建的节点。此节点无法删除。从主管理器节点的 UI 中部署两个新的管理器节点以形成集群后，只有第二个和第三个管理器节点具有删除选项（可通过齿轮图标找到）。有关移除和添加管理器节点的信息，请参见[更改 NSX Manager 的 IP 地址](#)。

查看 NSX Manager 集群的配置和状态

您可以从 NSX Manager UI 查看 NSX Manager 集群的配置和状态。您可以使用 CLI 获取其他信息。

步骤

1 从浏览器中，使用 admin 特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。

2 选择 **系统 > 概览**

将显示 NSX Manager 集群的状态。

3 要查看有关配置的其他信息，请运行以下 CLI 命令：

```
manager1> get cluster config
Cluster Id: 18807edd-56d1-4107-b7b7-508d766a08e3
Cluster Configuration Version: 3
Number of nodes in the cluster: 3

Node UUID: 43cd0642-275c-af1d-fe46-1f5200f9e5f9
Node Status: JOINED
  ENTITY                                UUID                                IP
ADDRESS    PORT    FQDN
  HTTPS                                5c8d01f1-f3ee-4f94-b517-a093d8fbfad3
10.160.71.225  443    ychin-nsxmanager-ob-12065118-1-F5
  CONTROLLER                                06fd0574-69c0-432e-a8af-53d140dbef8f
10.160.71.225  -    ychin-nsxmanager-ob-12065118-1-F5
  CLUSTER_BOOT_MANAGER                                da8d535e-7a0c-4dd8-8919-d88bdde006b8
10.160.71.225  -    ychin-nsxmanager-ob-12065118-1-F5
  DATASTORE                                3c9c4ec1-afef-47bd-aadb-1ed6a5536bc4
10.160.71.225  9000    ychin-nsxmanager-ob-12065118-1-F5
  MANAGER                                eb5e8922-23bd-4c3a-ae22-d13d9195a6bc
10.160.71.225  -    ychin-nsxmanager-ob-12065118-1-F5
  POLICY                                f9da1039-08ad-4a20-bacc-5b91c5d67730
10.160.71.225  -    ychin-nsxmanager-ob-12065118-1-F5

Node UUID: 8ebb0642-201e-6a5f-dd47-a1e38542e672
Node Status: JOINED
  ENTITY                                UUID                                IP
ADDRESS    PORT    FQDN
  HTTPS                                3757f155-8a5d-4b53-828f-d67041d5a210
10.160.93.240  443    ychin-nsxmanager-ob-12065118-2-F5
  CONTROLLER                                7b1c9952-8738-4900-b68b-ca862aa4f6a9
```

```

10.160.93.240 - ychin-nsxmanager-ob-12065118-2-F5
CLUSTER_BOOT_MANAGER b5e12db1-5e0d-4e33-a571-6ba258dceb2e
10.160.93.240 - ychin-nsxmanager-ob-12065118-2-F5
DATASTORE bee1f629-4e23-4ab8-8083-9e0f0bb83178
10.160.93.240 9000 ychin-nsxmanager-ob-12065118-2-F5
MANAGER 45ccd6e3-1497-4334-944c-e6bbcd5c723e
10.160.93.240 - ychin-nsxmanager-ob-12065118-2-F5
POLICY d5ba5803-b059-4fbc-897c-3aace8cf1219
10.160.93.240 - ychin-nsxmanager-ob-12065118-2-F5

Node UUID: 2e7e0642-df4a-b2ec-b9e8-633d1469f1ea
Node Status: JOINED

ENTITY                                UUID                                IP
ADDRESS    PORT    FQDN
HTTPS                                bce3cc4c-7d60-45e2-aa7b-cdc75e445a14
10.160.76.33 443    ychin-nsxmanager-ob-12065118-3-F5
CONTROLLER ced46f5c-9e52-4b31-a1cb-b3dead991c71
10.160.76.33 - ychin-nsxmanager-ob-12065118-3-F5
CLUSTER_BOOT_MANAGER 88b70d31-3428-4ccc-ab57-55859f45030c
10.160.76.33 - ychin-nsxmanager-ob-12065118-3-F5
DATASTORE fb4aec3c-cae3-4386-b5b9-c0b99b7d9048
10.160.76.33 9000 ychin-nsxmanager-ob-12065118-3-F5
MANAGER 82b07440-3ff6-4f67-a1c9-e9327d1686ad
10.160.76.33 - ychin-nsxmanager-ob-12065118-3-F5
POLICY 61f21a78-a56c-4af1-867b-3f24132d53c7
10.160.76.33 - ychin-nsxmanager-ob-12065118-3-F5

```

4 要查看有关状态的其他信息，请运行以下 CLI 命令：

```

manager1> get cluster status
Cluster Id: 18807edd-56d1-4107-b7b7-508d766a08e3
Group Type: DATASTORE
Group Status: STABLE

Members:
  UUID                                FQDN
IP      STATUS
43cd0642-275c-af1d-fe46-1f5200f9e5f9    ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225    UP
8ebb0642-201e-6a5f-dd47-a1e38542e672    ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240    UP
2e7e0642-df4a-b2ec-b9e8-633d1469f1ea    ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33    UP

Group Type: CLUSTER_BOOT_MANAGER
Group Status: STABLE

Members:
  UUID                                FQDN
IP      STATUS
43cd0642-275c-af1d-fe46-1f5200f9e5f9    ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225    UP
8ebb0642-201e-6a5f-dd47-a1e38542e672    ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240    UP
2e7e0642-df4a-b2ec-b9e8-633d1469f1ea    ychin-nsxmanager-ob-12065118-3-F5

```

```

10.160.76.33      UP

Group Type: CONTROLLER
Group Status: STABLE

Members:
    UUID                                FQDN
IP              STATUS
    7b1c9952-8738-4900-b68b-ca862aa4f6a9    ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240    UP
    ced46f5c-9e52-4b31-a1cb-b3dead991c71    ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33      UP
    06fd0574-69c0-432e-a8af-53d140dbef8f    ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225     UP

Group Type: MANAGER
Group Status: STABLE

Members:
    UUID                                FQDN
IP              STATUS
    43cd0642-275c-af1d-fe46-1f5200f9e5f9    ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225     UP
    8ebb0642-201e-6a5f-dd47-a1e38542e672    ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240     UP
    2e7e0642-df4a-b2ec-b9e8-633d1469f1ea    ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33      UP

Group Type: POLICY
Group Status: STABLE

Members:
    UUID                                FQDN
IP              STATUS
    43cd0642-275c-af1d-fe46-1f5200f9e5f9    ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225     UP
    8ebb0642-201e-6a5f-dd47-a1e38542e672    ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240     UP
    2e7e0642-df4a-b2ec-b9e8-633d1469f1ea    ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33      UP

Group Type: HTTPS
Group Status: STABLE

Members:
    UUID                                FQDN
IP              STATUS
    43cd0642-275c-af1d-fe46-1f5200f9e5f9    ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225     UP
    8ebb0642-201e-6a5f-dd47-a1e38542e672    ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240     UP
    2e7e0642-df4a-b2ec-b9e8-633d1469f1ea    ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33      UP

```

关闭 NSX Manager 集群，然后打开其电源。

如果需要关闭 NSX Manager 集群，请遵循以下过程。

步骤

- 1 要关闭 NSX Manager 集群，请一次关闭一个管理器节点。您可以用 admin 身份登录到管理器节点的命令行界面 (CLI)，然后运行命令 `shutdown`，也可以从 vCenter Server 中关闭管理器节点虚拟机。
在继续关闭下一个管理器节点之前，请确保已在 vCenter Server 中关闭虚拟机电源。
- 2 要打开 NSX Manager 集群的电源，请在 vCenter Server 中一次打开一个管理器节点虚拟机的电源。
在继续打开下一个管理器节点之前，请确保当前节点已启动并正在运行。

重新引导 NSX Manager

可以使用 CLI 命令重新引导 NSX Manager 以从严重错误中恢复。

如果需要重新引导多个 NSX Manager，则必须一次重新引导一个。等待重新引导的 NSX Manager 处于联机状态，然后再重新引导另一个。

步骤

- 1 登录到 NSX Manager 的 CLI。
- 2 运行以下命令。

```
nsx-manager> reboot
Are you sure you want to reboot (yes/no): y
```

更改 NSX Manager 的 IP 地址

您可以更改 NSX Manager 集群中的 NSX Manager 的 IP 地址。本节介绍了几种方法。

例如，如果一个集群包含 Manager A、Manager B 和 Manager C，您可以通过以下方法更改一个或多个 Manager 的 IP 地址：

- 场景 A：
 - Manager A 具有 IP 地址 172.16.1.11。
 - Manager B 具有 IP 地址 172.16.1.12。
 - Manager C 具有 IP 地址 172.16.1.13。
 - 添加具有新 IP 地址（如 192.168.55.11）的 Manager D。
 - 移除 Manager A。
 - 添加具有新 IP 地址（如 192.168.55.12）的 Manager E。
 - 移除 Manager B。
 - 添加具有新 IP 地址（如 192.168.55.13）的 Manager F。
 - 移除 Manager C。

■ 场景 B:

- Manager A 具有 IP 地址 172.16.1.11。
- Manager B 具有 IP 地址 172.16.1.12。
- Manager C 具有 IP 地址 172.16.1.13。
- 添加具有新 IP 地址（如 192.168.55.11）的 Manager D。
- 添加具有新 IP 地址（如 192.168.55.12）的 Manager E。
- 添加具有新 IP 地址（如 192.168.55.13）的 Manager F。
- 移除 Manager A、Manager B 和 Manager C。

■ 场景 C:

- Manager A 具有 IP 地址 172.16.1.11。
- Manager B 具有 IP 地址 172.16.1.12。
- Manager C 具有 IP 地址 172.16.1.13。
- 移除 Manager A。
- 添加具有新 IP 地址（如 192.168.55.11）的 Manager D。
- 移除 Manager B。
- 添加具有新 IP 地址（如 192.168.55.12）的 Manager E。
- 移除 Manager C。
- 添加具有新 IP 地址（如 192.168.55.13）的 Manager F。

在该 IP 地址更改期间，前两个场景需要为额外的 NSX Manager 提供额外的虚拟 RAM、CPU 和磁盘。

建议不要使用场景 C，因为它会暂时减少 NSX Manager 数，并在 IP 地址更改期间丢失两个活动 Manager 之一，这会对 NSX-T 运行产生影响。该方案适用于没有额外的虚拟 RAM、CPU 和磁盘并需要更改 IP 地址的情况。

注 如果使用集群 VIP 功能，您必须将相同的子网用于新 IP 地址，或者在 IP 地址更改期间禁用集群 VIP，因为集群 VIP 要求所有 NSX Manager 位于同一子网中。

前提条件

熟悉如何将 NSX Manager 部署到集群中。有关详细信息，请参见《NSX-T Data Center 安装指南》。

步骤

1 如果要移除的 NSX Manager 是手动部署的，请执行以下步骤。

- a 运行以下 CLI 命令，将 NSX Manager 从集群中分离。

```
detach node <node-id>
```

- b 删除 NSX Manager 虚拟机。

- 2 如果要删除的 NSX Manager 是通过 NSX Manager UI 自动部署的，则执行以下步骤。
 - a 从浏览器中，使用管理员权限登录到 NSX Manager (<https://nsx-manager-ip-address>)。此 NSX Manager 不得是要删除的 NSX Manager。
 - b 在系统选项卡中，单击 **NSX 管理节点**。
将显示 NSX Manager 集群的状态。
 - c 对于要删除的 NSX Manager，单击齿轮图标并选择**删除**。
- 3 部署新的 NSX Manager

调整 NSX Manager 节点的大小

您可以随时更改 NSX Manager 节点的 CPU 内核数或内存量。

请注意，在正常运作条件下，所有三个管理器节点必须具有相同数量的 CPU 内核和内存。仅当从一种大小的 NSX Manager 转换为其他大小的 NSX Manager 时，才应在 NSX 管理集群的 NSX Manager 中使用不一致的 CPU 或内存。

如果在 vCenter Server 中为 NSX Manager 虚拟机配置了资源分配预留，则可能需要调整预留。有关详细信息，请参见 vSphere 文档。

前提条件

- 确认新大小满足管理器节点的系统要求。有关详细信息，请参见《NSX-T Data Center 安装指南》中的“NSX Manager 虚拟机系统要求”。
- 熟悉如何将 NSX Manager 部署到集群中。有关详细信息，请参见《NSX-T Data Center 安装指南》。
- 有关如何从集群中移除管理器节点的信息，请参见[更改 NSX Manager 的 IP 地址](#)。

步骤

- 1 部署具有新大小的新管理器节点。
- 2 将新管理器节点添加到集群。
- 3 移除旧管理器节点。
- 4 重复步骤 1 到 3 以替换其他两个旧管理器节点。

在 vCenter Server 中添加和移除 ESXi 主机传输节点

您可以将 ESXi 主机传输节点从一个 vCenter Server (VC) 移至另一个 VC，也可以将其从一个 NSX Manager 集群移至另一个集群。

场景 1: VC1 连接到 NSX Manager 集群 1，VC2 连接到 NSX Manager 集群 2

假设 ESX1（一个 ESXi 主机传输节点）位于 VC1 中，则可以通过执行以下步骤将其移至 VC2：

- 1 从 ESX1 中卸载 NSX。

- 2 将 ESX1 移至 VC2。
- 3 将传输节点配置文件应用于 ESX1。

场景 2: VC1 和 VC2 都连接到 NSX Manager 集群

假设 ESX1（一个 ESXi 主机传输节点）位于 VC1 中，则可以通过执行以下步骤将其移至 VC2:

- 1 从 ESX1 中卸载 NSX。
- 2 将 ESX1 移至 VC2。
- 3 将传输节点配置文件应用于 ESX1。

场景 3: VC1 连接到 NSX Manager 集群 1

假设 ESX1（一个 ESXi 主机传输节点）位于 VC1 中，则可以通过执行以下步骤将其作为独立主机移至 NSX Manager 集群 2:

- 1 从 ESX1 中卸载 NSX。
- 2 将 ESX1 添加到 NSX Manager 集群 2。

替换 NSX Edge 集群中的 NSX Edge 传输节点

您可以使用 NSX Manager UI 或 API 替换 NSX Edge 集群中的 NSX Edge 传输节点。

使用 NSX Manager UI 替换 NSX Edge 传输节点

以下过程介绍了如何使用 NSX Manager UI 替换 NSX Edge 集群中的 NSX Edge 传输节点。无论 Edge 传输节点是否正在运行，您都可以替换该节点。

如果要替换的 Edge 节点未运行，新的 Edge 节点可能具有相同的管理 IP 地址和 TEP IP 地址。如果要替换的 Edge 节点正在运行，新的 Edge 节点必须具有不同的管理 IP 地址和 TEP IP 地址。

前提条件

熟悉安装 NSX Edge 节点、将 Edge 节点加入管理平面以及创建 NSX Edge 传输节点的过程。有关详细信息，请参见《NSX-T Data Center 安装指南》。

步骤

- 1 如果希望新的 Edge 传输节点具有与要替换的 Edge 传输节点相同的配置，请进行以下 API 调用以查找配置:

```
GET https://<nsx-manager-IP>/api/v1/transport-nodes/<tn-id>
```

- 2 按照《NSX-T Data Center 安装指南》中的过程安装和配置 Edge 传输节点。

如果您希望该 Edge 传输节点具有与要替换的 Edge 传输节点相同的配置，请使用在步骤 1 中获取的配置。

- 3 在 NSX Manager 中，选择**系统 > Fabric > 节点 > Edge 集群**。
- 4 单击第一列中的复选框以选择一个 Edge 集群。

5 单击 **操作 > 替换 Edge 集群成员**。

建议将要替换的传输节点置于维护模式。如果传输节点未运行，您可以安全地忽略该建议。

6 从下拉列表中选择要替换的节点。

7 从下拉列表中选择替换节点。

8 单击 **保存**。

使用 API 替换 NSX Edge 传输节点

以下过程介绍了如何使用 NSX-T API 替换 NSX Edge 集群中的 NSX Edge 传输节点。无论 Edge 传输节点是否正在运行，您都可以替换该节点。

如果要替换的 Edge 节点未运行，新的 Edge 节点可能具有相同的管理 IP 地址和 TEP IP 地址。如果要替换的 Edge 节点正在运行，新的 Edge 节点必须具有不同的管理 IP 地址和 TEP IP 地址。

前提条件

熟悉安装 NSX Edge 节点、将 Edge 节点加入管理平面以及创建 NSX Edge 传输节点的过程。有关详细信息，请参见《NSX-T Data Center 安装指南》。

步骤

1 如果希望新的 Edge 传输节点具有与要替换的 Edge 传输节点相同的配置，请进行以下 API 调用以查找配置：

```
GET https://<nsx-manager-IP>/api/v1/transport-nodes/<tn-id>
```

2 按照《NSX-T Data Center 安装指南》中的过程安装和配置 Edge 传输节点。

如果您希望该 Edge 传输节点具有与要替换的 Edge 传输节点相同的配置，请使用在步骤 1 中获取的配置。

3 进行 API 调用以获取新传输节点和要替换的传输节点的 ID。id 字段包含传输节点 ID。例如，

```
GET https://<nsx-manager-IP>/api/v1/transport-nodes
...
{
  "resource_type": "TransportNode",
  "description": "",
  "id": "73cb00c9-70d0-4808-abfe-a12a43251133",
  "display_name": "TN-edgenode-01a",
  ...
  {
    "resource_type": "TransportNode",
    "description": "",
    "id": "890f0e3c-aa81-46aa-843b-8ac25fe30bd3",
    "display_name": "TN-edgenode-03a",
```


- 4 进行 API 调用以获取 NSX Edge 集群的 ID。id 字段包含 NSX Edge 集群 ID。从 members 数组中获取 NSX Edge 集群的成员。例如，

```
GET https://<nsx-manager-IP>/api/v1/edge-clusters
....
{
  "resource_type": "EdgeCluster",
  "description": "",
  "id": "9a302df7-0833-4237-af1f-4d826c25ad78",
  "display_name": "Edge-Cluster-1",
  ...
  "members": [
    {
      "member_index": 0,
      "transport_node_id": "73cb00c9-70d0-4808-abfe-a12a43251133"
    },
    {
      "member_index": 1,
      "transport_node_id": "e5d17b14-cdeb-4e63-b798-b23a0757463b"
    }
  ],
}
```

- 5 进行 API 调用以替换 NSX Edge 集群中的传输节点。member_index 必须与要替换的传输节点的索引匹配。

例如，传输节点 TN-edgenode-01a (73cb00c9-70d0-4808-abfe-a12a43251133) 发生故障，并将其替换为 NSX Edge 集群 Edge-Cluster-1 (9a302df7-0833-4237-af1f-4d826c25ad78) 中的传输节点 TN-edgenode-03a (890f0e3c-aa81-46aa-843b-8ac25fe30bd3)。

```
POST http://<nsx-manager-IP>/api/v1/edge-clusters/9a302df7-0833-4237-af1f-4d826c25ad78?
action=replace_transport_node
{
  "member_index": 0,
  "transport_node_id" : "890f0e3c-aa81-46aa-843b-8ac25fe30bd3"
}
```

在 vCenter Server 丢失且无法恢复时恢复 NSX-T

如果 vCenter Server (VC) 丢失且无法恢复（可能是因为没有备份或备份已损坏），请在重新部署 VC 后使用以下过程恢复 NSX-T 环境。

新 VC 必须与原始 VC 具有相同的 FQDN 和 IP 地址。此外，它还必须具有包含相同主机的相同集群。在将具有已打开电源的虚拟机的主机添加到 VC 时，请务必小心。确保将这些主机添加到正确的集群，而不是 VC 数据中心。

计算管理器

在 NSX Manager 中，删除旧计算管理器。然后，将新 VC 添加为计算管理器。

主机传输节点

在 NSX Manager 中，主机将显示在正确的 VC 集群中。无需执行任何操作。

Edge 节点

您必须替换通过 NSX Manager UI 部署的 Edge 节点。

- 1 按照使用 [NSX Manager UI 替换 NSX Edge 传输节点](#)中所述的过程替换 Edge 节点。
- 2 确认已在新 Edge 虚拟机上配置网关（或逻辑路由器）和隧道。
- 3 转到**系统 > Fabric > Edge 传输节点**，以删除旧 Edge 节点。选择相应 Edge 节点，然后单击**操作 > 删除**。可以忽略诸如“关闭电源失败 (Power off failed)”之类的错误。
- 4 在 VC 中，关闭旧 Edge 虚拟机的电源并将其删除。
- 5 对每个 Edge 节点重复上述步骤。

NSX Manager

您必须替换通过 NSX Manager UI 部署的 NSX Manager。通常，第二个和第三个 NSX Manager 是通过这种方式部署的。

- 1 登录到第一个 NSX Manager 的 UI。
- 2 转到**系统 > 设备**，然后选择第三个 NSX Manager。单击**操作 > 删除**。此操作将因为无法关闭管理器虚拟机的电源而失败。此时，可以使用“强制删除”选项。选择**操作 > 强制删除**。
- 3 如果“强制删除”选项不起作用，请执行以下操作：
 - a 登录到第一个 NSX Manager 的 CLI。
 - b 运行 `get cluster status` 命令，以获取第三个 NSX Manager 的 UID。
 - c 运行 `detach node <node-uid>` 命令，以将第三个 NSX Manager 从集群中分离。
 - d 执行以下 API 调用以强制删除第三个 NSX Manager：

```
POST : https://<nsx-manager-1>/api/v1/cluster/nodes/deployments/<node-uid>?
      action=delete&force_delete=true
```

- 4 在 VC 中，关闭第三个 NSX Manager 的电源并将其删除。
- 5 部署与第三个 NSX Manager 具有相同配置的新 NSX Manager。
- 6 重复上述步骤以删除第二个 NSX Manager。
- 7 部署两个新的 NSX Manager。

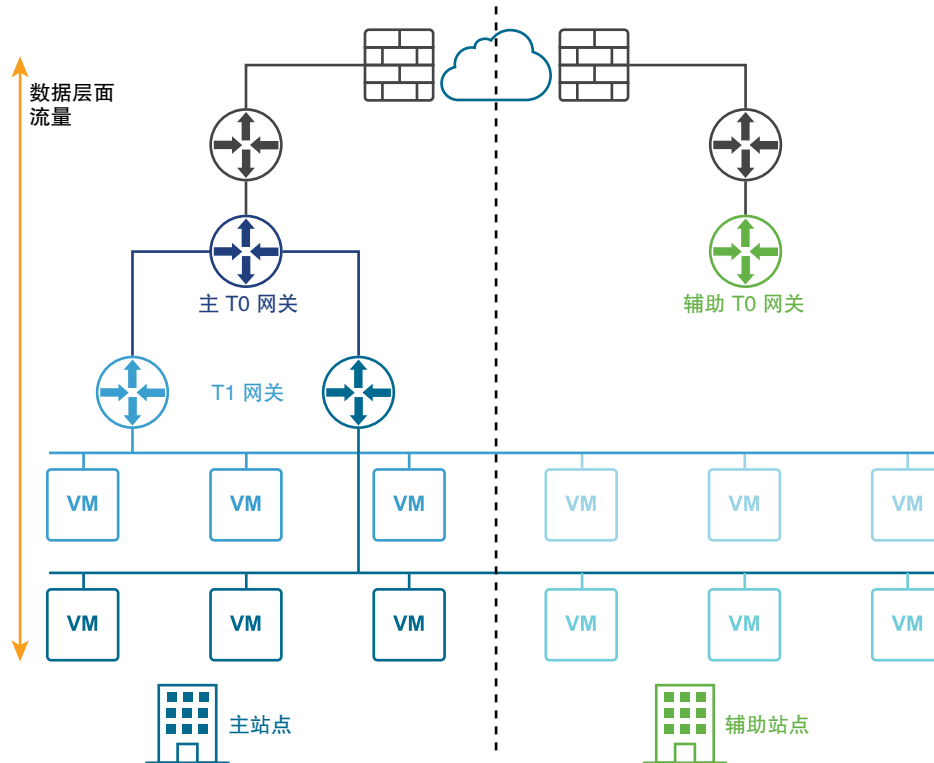
NSX-T Data Center 的多站点部署

NSX-T Data Center 支持多站点部署，您可以管理一个 NSX Manager 集群中的所有站点。

支持两种类型的多站点部署：

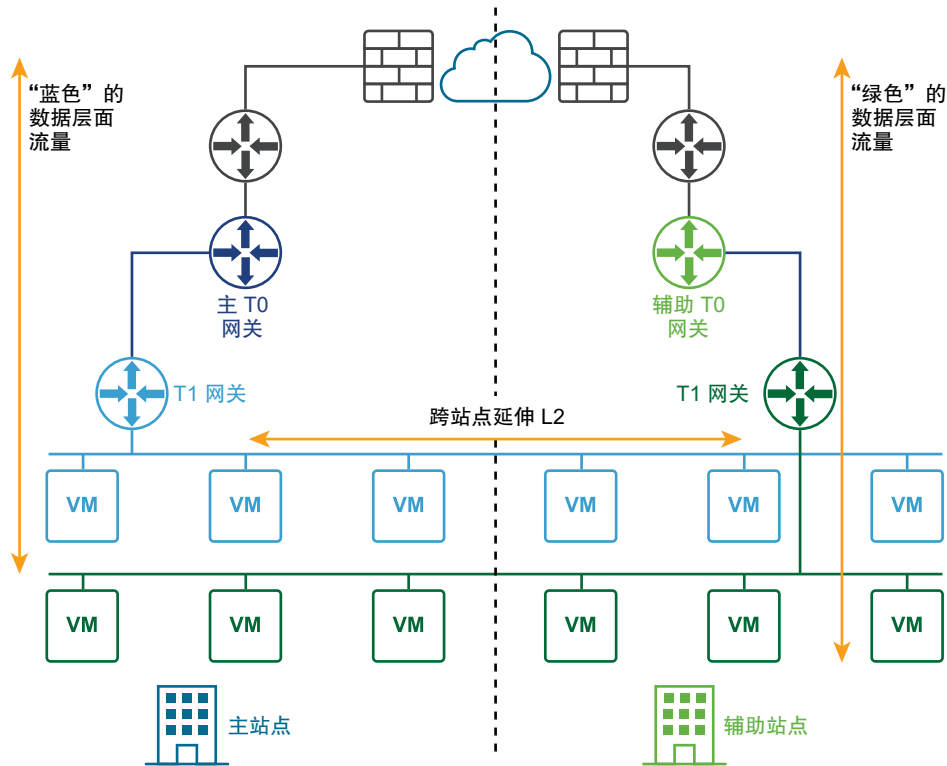
- 灾难恢复
- 活动-活动

下图显示了灾难恢复部署。



在活动-活动部署中，所有站点都处于活动状态，第 2 层流量跨越站点边界。在灾难恢复部署中，主站点的 NSX-T Data Center 处理企业网络连接。辅助站点处于待机状态，可在主站点出现灾难性故障时进行接管。

下图显示了活动-活动部署。



您可以部署两个站点，以实现管理平面和数据平面的自动或手动/脚本式恢复。

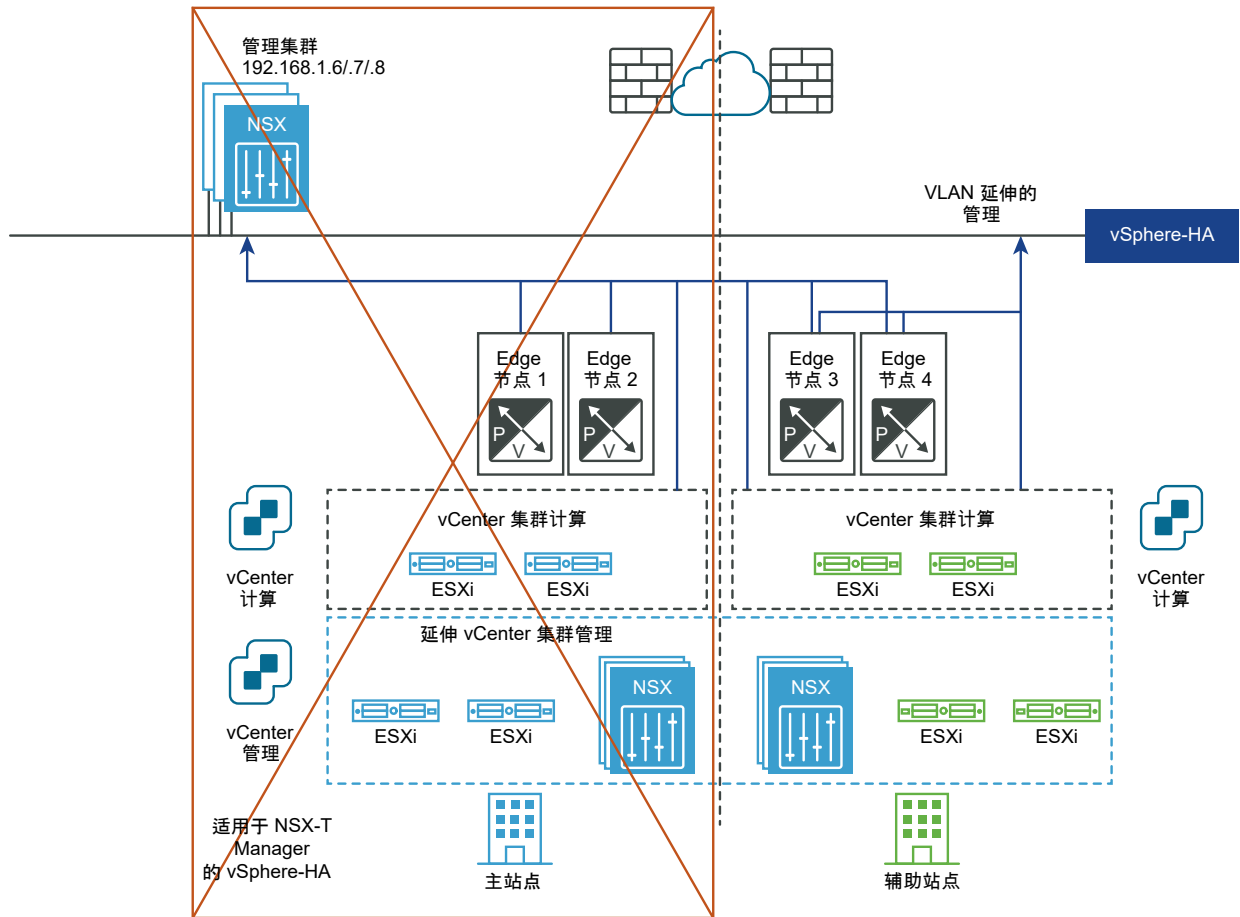
管理平面的自动恢复

要求：

- 配置了跨站点 HA 的延伸 vCenter 集群。
- 延伸的管理 VLAN。

NSX Manager 集群部署在管理 VLAN 上，其物理位置在主站点中。如果主站点出现故障，vSphere HA 将重新启动辅助站点中的 NSX Manager。所有传输节点将自动重新连接到重新启动的 NSX Manager。此过程大约需要 10 分钟。在这段时间内，管理平面不可用，但数据平面不受影响。

下图说明了管理平面的自动恢复。



数据平面的自动恢复

要求：

- Edge 节点之间的最大延迟为 10 毫秒。
- Tier-0 网关的 HA 模式必须为活动-备用，且故障切换模式必须为主动。

注意：Tier-1 网关的故障切换模式可以是主动，也可以是非主动。

配置步骤：

- 使用 API 为两个站点创建故障域，例如，FD1A-Preferred_Site1 和 FD2A-Preferred_Site1。对于主站点，将 preferred_active_edge_services 参数设置为 true；对于辅助站点，将该参数设置为 false。

```
POST /api/v1/failure-domains
{
  "display_name": "FD1A-Preferred_Site1",
  "preferred_active_edge_services": "true"
}

POST /api/v1/failure-domains
```

```
{
  "display_name": "FD2A-Preferred_Site1",
  "preferred_active_edge_services": "false"
}
```

- 使用 API 配置在两个站点之间延伸的 Edge 集群。例如，该集群在主站点中具有 Edge 节点 EdgeNode1A 和 EdgeNode1B，在辅助站点中具有 Edge 节点 EdgeNode2A 和 EdgeNode2B。活动 Tier-0 和 Tier-1 网关将在 EdgeNode1A 和 EdgeNode1B 上运行。备用 Tier-0 和 Tier-1 网关将在 EdgeNode2A 和 EdgeNode2B 上运行。
- 使用 API 将每个 Edge 节点与该站点的故障域相关联。首先调用 GET /api/v1/transport-nodes/<transport-node-id> API 以获取有关 Edge 节点的数据。使用 GET API 的结果作为 PUT /api/v1/transport-nodes/<transport-node-id> API 的输入，并正确设置附加属性 failure_domain_id。例如，

```
GET /api/v1/transport-nodes/<transport-node-id>
Response:
{
  "resource_type": "TransportNode",
  "description": "Updated NSX configured Test Transport Node",
  "id": "77816de2-39c3-436c-b891-54d31f580961",
  ...
}

PUT /api/v1/transport-nodes/<transport-node-id>
{
  "resource_type": "TransportNode",
  "description": "Updated NSX configured Test Transport Node",
  "id": "77816de2-39c3-436c-b891-54d31f580961",
  ...
  "failure_domain_id": "<UUID>",
}
```

- 使用 API 将 Edge 集群配置为根据故障域分配节点。首先调用 GET /api/v1/edge-clusters/<edge-cluster-id> API 以获取有关 Edge 集群的数据。使用 GET API 的结果作为 PUT /api/v1/edge-clusters/<edge-cluster-id> API 的输入，并正确设置附加属性 allocation_rules。例如，

```
GET /api/v1/edge-clusters/<edge-cluster-id>
Response:
{
  "_revision": 0,
  "id": "bf8d4daf-93f6-4c23-af38-63f6d372e14e",
  "resource_type": "EdgeCluster",
  ...
}

PUT /api/v1/edge-clusters/<edge-cluster-id>
{
  "_revision": 0,
  "id": "bf8d4daf-93f6-4c23-af38-63f6d372e14e",
  "resource_type": "EdgeCluster",
  ...
}
```

```

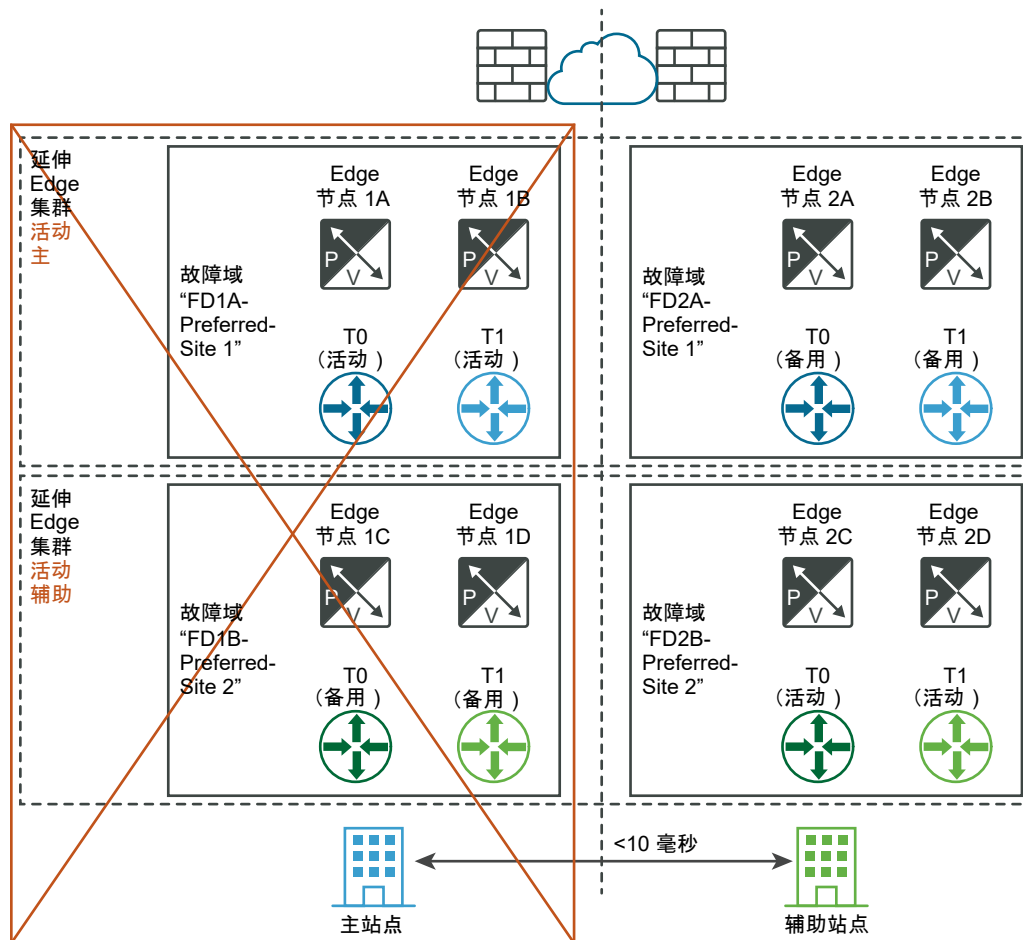
"allocation_rules": [
  {
    "action": {
      "enabled": true,
      "action_type": "AllocationBasedOnFailureDomain"
    }
  },
],
}

```

- 使用 API 或 NSX Manager UI 创建 Tier-0 和 Tier-1 网关。

当主站点中的 Edge 节点发生故障时，该节点上托管的 Tier-0 和 Tier-1 网关将迁移到辅助站点中的 Edge 节点。

下图说明了数据平面的自动恢复。



管理平面的手动/脚本式恢复

要求：

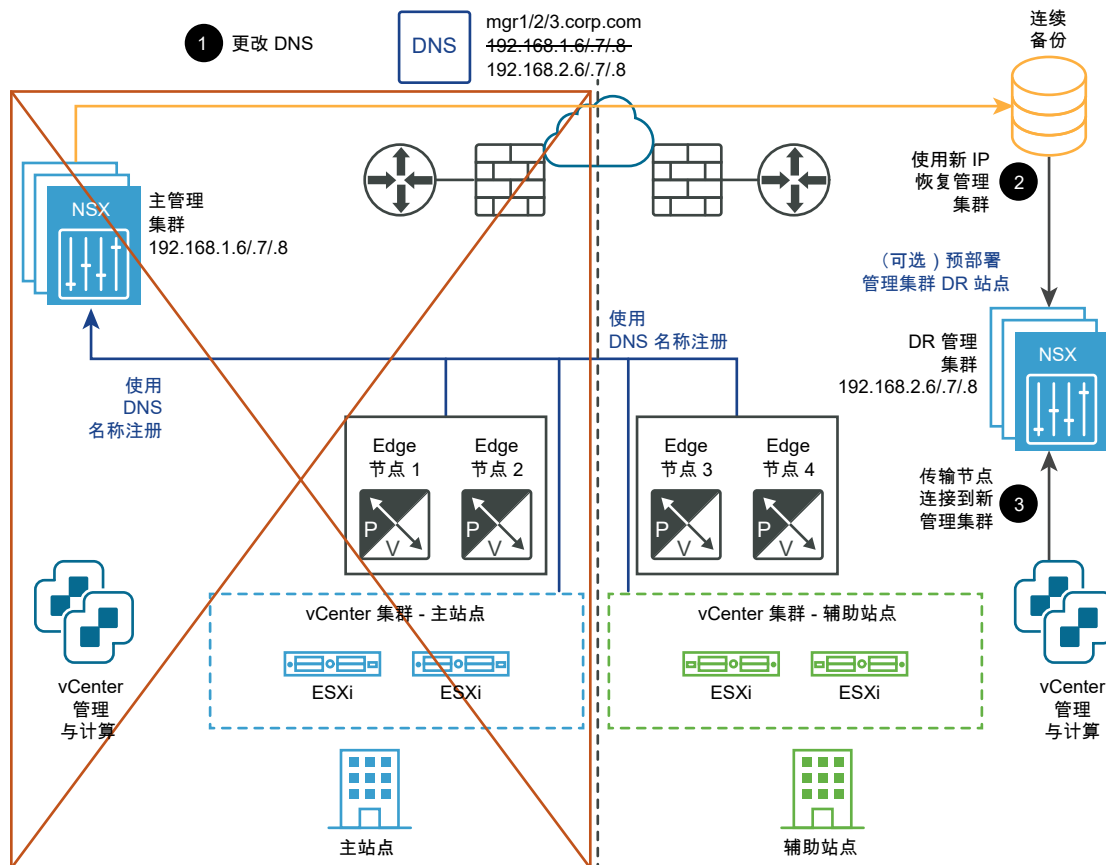
- 用于 NSX Manager 且具有短 TTL（例如，5 分钟）的 DNS。
- 连续备份。

不需要 vSphere HA 和延伸的管理 VLAN。NSX-T Manager 必须与具有短 TTL 的 DNS 名称相关联。所有传输节点（Edge 节点和管理程序）必须使用其 DNS 名称连接到 NSX Manager。为节省时间，可以选择在辅助站点中预先安装 NSX Manager 集群。

恢复步骤是：

- 1 更改 DNS 记录，以便 NSX Manager 集群具有不同 IP 地址。
- 2 从备份还原 NSX Manager 集群。
- 3 将传输节点连接到新的 NSX Manager 集群。

下图说明了管理平面的手动/脚本式恢复。



数据平面的手动/脚本式恢复

要求：

- Edge 节点之间的最大延迟为 150 毫秒。

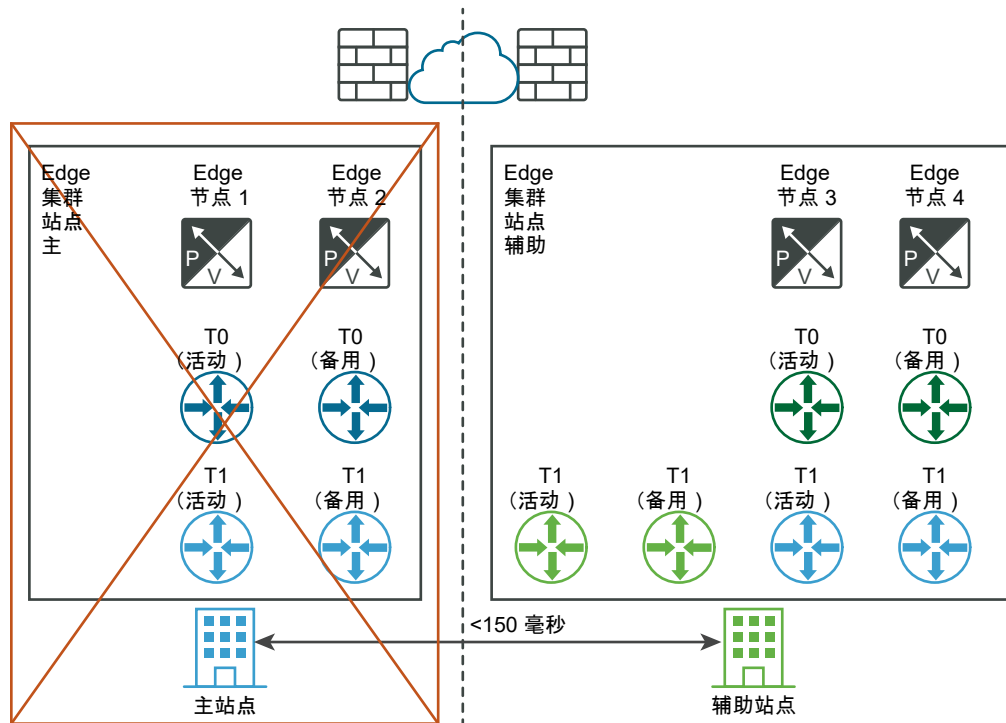
Edge 节点可以是虚拟机或裸机。Tier-0 网关可以为活动-备用或活动-活动模式。Edge 节点虚拟机可以安装在不同的 vCenter Server 中。不需要 vSphere HA。

恢复步骤是：

- 1 在灾难恢复 (Disaster Recovery, DR) 站点中的现有 Edge 集群上创建备用 Tier-0 网关。

- 2 使用 API 将连接到 Tier-0 网关的 Tier-1 网关移至 DR 站点中的 Tier-0 网关。
- 3 使用 API 将独立 Tier-1 网关移至 DR 站点。
- 4 使用 API 将第 2 层网桥移至 DR 站点。

下图说明了数据平面的手动/脚本式恢复。



Edge 集群主站点中所有 T1 (蓝色) 的脚本或手动操作：

- 传输到 Edge 集群辅助站点
- 连接到 T0 - 辅助站点 (绿色)

多站点部署的要求

站点间通信

- 带宽必须至少 1 Gbps，延迟 (RTT) 必须低于 150 毫秒。
- MTU 必须至少为 1600。建议 9000。

NSX Manager 配置

- 必须启用 NSX-T Data Center 配置更改时自动备份。
- NSX Manager 必须设置为使用 FQDN。

数据平面恢复

- 如果通过 NAT 或负载均衡器等服务显示公用 IP 地址，则必须使用同一个 Internet 提供商。
- Tier-0 网关的 HA 模式必须为活动-备用，且故障切换模式必须为主动。

云计算管理系统

- 云计算管理系统 (CMS) 必须支持一个 NSX-T Data Center 插件。在此版本中，VMware Integrated OpenStack (VIO) 和 vRealize Automation (vRA) 满足此要求。

限制

- 没有本地输出功能。所有南北向流量必须在一个站点内。
- 计算灾难恢复软件必须支持 NSX-T Data Center，例如 VMware SRM 8.1.2 或更高版本。

配置设备

必须使用命令行或 API 完成某些系统配置任务。

有关完整的命令行界面信息，请参阅《NSX-T Data Center 命令行界面参考》。有关完整的 API 信息，请参阅《NSX-T Data Center API 指南》。

表 21-7. 系统配置命令和 API 请求。

任务	命令行 (NSX Manager 和 NSX Edge)	API 请求 (仅限 NSX Manager)
设置系统时区	<code>set timezone <timezone></code>	<code>PUT https://<nsx-mgr>/api/v1/node</code>
设置 NTP 服务器	<code>set ntp-server <ntp-server></code>	<code>PUT https://<nsx-mgr>/api/v1/node/ services/ntp</code>
设置 DNS 服务器	<code>set name-servers <dns-server></code>	<code>PUT https://<nsx-mgr>/api/v1/node/ network/name-servers</code>
设置 DNS 搜索域	<code>set search-domains <domain></code>	<code>PUT https://<nsx-mgr>/api/v1/node/ network/search-domains</code>

添加许可证密钥并生成许可证使用情况报告

可以添加许可证密钥，并生成许可证使用情况报告。使用情况报告是 CSV 格式的文件。

可以使用以下非评估 NSX-T Data Center 许可证类型：

- NSX Data Center Standard
- NSX Data Center Professional
- NSX Data Center Advanced
- NSX Data Center Enterprise Plus
- NSX Data Center Remote Office Branch Office (ROBO)
- NSX Advanced（可从 NSX-T Data Center 2.5.1 中获取）
- NSX Enterprise（可从 NSX-T Data Center 2.5.1 中获取）

在安装 NSX Manager 时，预装的评估许可证将变为活动状态，有效期为 60 天。评估许可证提供了企业许可证的所有功能。您无法安装或取消分配评估许可证。存在默认评估许可证时，您可以分配新的评估许可证。新评估许可证将覆盖默认评估许可证。您也可以取消分配非默认的评估许可证。在这种情况下，将还原默认评估许可证。

您可以安装一个或多个非评估许可证，但对于每种类型，您只能安装一个密钥。在安装标准、高级或企业许可证时，评估许可证不再可用。也可以取消分配非评估许可证。如果取消分配所有非评估许可证，将会恢复评估许可证。

如果具有多个相同许可证类型的密钥并且要合并这些密钥，您必须访问 <https://my.vmware.com> 并使用合并密钥功能。NSX Manager UI 不提供该功能。

如果您的许可证将在 60 天内过期或已过期，则在您登录到 NSX Manager 后，将出现一个通知窗口，向您通知相关情况。您也可以单击窗口右上角的通知图标来查看通知。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择 **系统 > 许可证 > 添加**。
- 3 输入许可证密钥。
- 4 要生成许可证使用情况报告，请选择 **导出 > 许可证使用情况报告**。

CSV 报告列出了以下功能所使用的虚拟机、CPU、唯一并发用户以及 vCPU 和内核数：

- 交换和路由
- NSX Edge 负载均衡器
- VPN
- DFW
- 上下文感知微分段 - 应用程序识别
- 上下文感知微分段 - 远程桌面会话主机的身份防火墙
- 服务插入
- 身份防火墙
- 增强的客户机侦测

注 对于 Limited Export 发行版本，将禁用以下功能：

- IPSEC VPN
 - 基于 HTTPS 的负载均衡器
-

设置证书

您可以导入证书、创建证书签名请求 (Certificate Signing Request, CSR)、生成自签名证书，以及导入证书吊销列表 (CRL)。

安装 NSX-T Data Center 后，管理器节点和集群具有自签名证书。为了提高安全性，强烈建议您将自签名证书替换为 CA 签名证书。

导入证书

您可以导入具有私钥的证书，以便在激活后替换默认自签名证书。

请注意，仅基于 RSA 的证书受支持。

前提条件

确认具有一个证书。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 选择 **系统 > 证书**。
- 3 选择 **导入 > 导入证书**，然后输入证书详细信息。

选项	说明
名称	指定证书的名称。
证书内容	浏览到计算机上的证书文件并添加该文件。证书不得加密。如果是 CA 签名证书，请务必按以下顺序包含整个链：证书 - 中间 - 根。
私钥	浏览到计算机上的私钥文件并添加该文件。
密码短语	为此证书添加密码短语（如果加密）。在此版本中，不使用此字段，因为不支持加密证书。
说明	输入该证书中所包含内容的说明。
服务证书	要将该证书用于负载均衡器和 VPN 等服务，请设置为 是 。如果将该证书用于 NSX Manager 节点，请设置为 否 。

- 4 单击**导入**。

创建证书签名请求文件

证书签名请求 (CSR) 是包含特定信息的加密文本，例如，组织名称、公用名称、城市以及国家/地区。您可以将 CSR 文件发送到证书颁发机构 (CA) 以申请数字身份证书。

前提条件

- 收集填写 CSR 文件所需的信息。您必须知道服务器的 FQDN、组织单位、组织、城市、省/直辖市/自治区以及国家/地区。
- 确认具有公钥和私钥对。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 选择**系统 > 证书**。
- 3 单击 **CSR** 选项卡。
- 4 单击**生成 CSR**。
- 5 填写 CSR 文件详细信息。

选项	说明
名称	指定证书的名称。
公用名称	输入服务器的完全限定域名 (Fully Qualified Domain Name, FQDN)。 例如，test.vmware.com。
组织名称	输入具有相应后缀的组织名称。 例如，VMware Inc.。
组织单位	输入组织中处理该证书的部门。 例如，IT 部门。
城市	添加组织所在的城市。 例如，帕罗奥多。
州/省	添加组织所在的省/直辖市/自治区。 例如，加利福尼亚。
国家/地区	添加组织所在的国家/地区。 例如，美国 (US)。
消息算法	为证书设置加密算法。 RSA 加密 - 用于数字签名和消息加密。因此，在创建加密令牌时比 DSA 慢，但分析和验证该令牌时较快。该加密的解密速度较慢，而加密速度较快。 DSA 加密 - 用于数字签名。因此，在创建加密令牌时比 RSA 快，但分析和验证该令牌时较慢。该加密的解密速度较快，而加密速度较慢。
密钥大小	设置加密算法的密钥位大小。 使用默认值 2048 就足够了，除非您明确需要使用不同的密钥大小。很多 CA 要求最小值为 2048。较大的密钥更安全，但对性能的影响更大。
说明	输入特定的详细信息以帮助您在以后识别该证书。

- 6 单击**生成**。
自定义 CSR 将显示为一个链接。
- 7 选择该 CSR，然后单击**操作**。
- 8 从下拉菜单中选择**下载 CSR PEM**。
您可以保存 CSR PEM 文件以进行存档和提交给 CA。
- 9 使用 CSR 文件内容按照 CA 注册过程向 CA 提交证书请求。

结果

CA 根据 CSR 文件中的信息创建一个服务器证书，使用私钥对其进行签名，然后向您发送该证书。CA 还会向您发送根 CA 证书。

导入 CA 证书

您可以导入签名的 CA 证书。在导入和激活后，NSX-T Data Center 将信任该 CA 签名的其他证书。

请注意，仅基于 RSA 的证书受支持。

前提条件

确认具有一个 CA 证书。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择 **系统 > 证书**。
- 3 选择 **导入 > 导入 CA 证书**，然后输入证书详细信息。

选项	说明
名称	指定 CA 证书的名称。
证书内容	浏览到计算机上的 CA 证书文件并添加该文件。
说明	输入该 CA 证书中包含的内容的摘要。
服务证书	要将该证书用于负载均衡器和 VPN 等服务，请设置为 是 。如果将该证书用于 NSX Manager 节点，请设置为 否 。

- 4 单击**导入**。

创建自签名证书

可以创建自签名证书。但是，使用自签名证书不如使用受信任的证书安全。

在使用自签名证书时，客户端用户将收到一条警告消息，例如，无效的安全证书 (Invalid Security Certificate)。在首次连接到服务器时，客户端用户必须接受自签名证书才能继续。允许客户端用户选择该选项将提供比其他授权方法更低的安全性。

前提条件

确认具有一个 CSR。请参见[创建证书签名请求文件](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择 **系统 > 证书**。
- 3 单击 **CSR** 选项卡。
- 4 选择一个 CSR。

- 5 选择 **操作 > CSR 的自签名证书**。
- 6 输入自签名证书的有效天数。
默认值为 10 年。
- 7 单击 **添加**。

结果

自签名证书将显示在**证书**选项卡中。

替换 NSX Manager 节点或 NSX Manager 集群虚拟 IP 的证书

您可以通过进行 API 调用来替换管理器节点或管理器集群虚拟 IP (Virtual IP, VIP) 的证书。

安装 NSX-T Data Center 后，管理器节点和集群具有自签名证书。为了提高安全性，强烈建议使用 CA 签名证书替换自签名证书，并为每个节点使用不同的证书。

前提条件

确认在 NSX Manager 中具有一个证书。请参见[导入证书](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 选择 **系统 > 证书**。
- 3 在 ID 列中，单击要使用的证书的 ID，然后从弹出窗口中复制该证书 ID。

确保在导入此证书时，选项**服务证书**已设置为**否**。

- 4 要替换管理器节点的证书，请使用 `POST /api/v1/node/services/http?action=apply_certificate` API 调用。例如，

```
POST https://<nsx-mgr>/api/v1/node/services/http?
action=apply_certificate&certificate_id=e61c7537-3090-4149-b2b6-19915c20504f
```

注意：证书链必须采用“证书 - 中间 - 根”这一行业标准顺序。

有关 API 的详细信息，请参见《NSX-T Data Center API 参考》。

- 5 要替换管理器集群 VIP 的证书，请使用 `POST /api/v1/cluster/api-certificate?action=set_cluster_certificate` API 调用。例如，

```
POST https://<nsx-mgr>/api/v1/cluster/api-certificate?
action=set_cluster_certificate&certificate_id=d60c6a07-6e59-4873-8edb-339bf75711ac
```

注意：证书链必须采用“证书 - 中间 - 根”这一行业标准顺序。

有关 API 的详细信息，请参见《NSX-T Data Center API 参考》。如果未配置 VIP，则无需执行此步骤。

导入证书吊销列表

证书吊销列表 (CRL) 是订阅者及其证书状态列表。在潜在用户尝试访问服务器时，服务器将根据该特定用户的 CRL 条目拒绝访问。

该列表包含以下各项：

- 吊销的证书和吊销原因
- 证书颁发日期
- 颁发证书的实体
- 计划发行下一版本的日期

前提条件

确认具有一个 CRL。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择 **系统 > 证书**。
- 3 单击 **CRL** 选项卡。
- 4 单击 **导入并添加 CRL** 详细信息。

选项	说明
名称	指定 CRL 的名称。
证书内容	<p>复制 CRL 中的所有项目并将其粘贴到该部分中。</p> <p>示例 CRL。</p> <pre> -----BEGIN X509 CRL----- MIIBODCB4zANBgkqhkiG9w0BAQQFADBGMQswCQYDVQQGEwJBVTEMMMAoGA1 UECBMD UUxEMRkwFwYDVQQKExBNaW5jb20gUHR5LiBMdGQuMQswCQYDVQQLEwJDUz EbMBkG A1UEAxMSU1NMZW5IGRlbW8gc2VydmVyFw0wMTAxMTUxNjI2NTdaFw0wMT AyMTQx NjI2NTdaMFwiEgIBARcNOTUxMDA5MjMzMjA1WjASAgEDFw05NTEyMDEwMT AwMDBa MBMCAhI0Fw0wMTAxMTUxNjE5NDdaMBMCAhI1Fw0wMTAxMTUxNjIzNDZaMA 0GCSqG SIb3DQEBAUAUA0EABjQ3M93QOj8Ufi+jZM7Y78TfAzG4jJn/ E6MYBPFVQFY0/Gp UZexfjSVo5CIyyS0tYscz8oO7avwBxTiMpDEQg== -----END X509 CRL-- </pre>
说明	输入该 CRL 中包含的内容的摘要。

- 5 单击 **导入**。

结果

导入的 CRL 将显示为一个链接。

配置 NSX Manager 以检索证书吊销列表

通过使用 API，您可以配置 NSX Manager 以检索证书吊销列表 (CRL)。然后，您可以对 NSX Manager 进行 API 调用以检查 CRL，而不是对证书颁发机构进行调用。

该功能具有以下好处：

- 在服务器（即 NSX Manager）上缓存 CRL 可以提高效率。
- 客户端不需要创建到证书颁发机构的任何出站连接。

可以使用与证书吊销列表相关的以下 API：

```
GET /api/v1/trust-management
GET /api/v1/trust-management/crl-distribution-points
POST /api/v1/trust-management/crl-distribution-points
DELETE /api/v1/trust-management/crl-distribution-points/<crl-distribution-point-id>
GET /api/v1/trust-management/crl-distribution-points/<crl-distribution-point-id>
PUT /api/v1/trust-management/crl-distribution-points/<crl-distribution-point-id>
GET /api/v1/trust-management/crl-distribution-points/<crl-distribution-point-id>/status
POST /api/v1/trust-management/crl-distribution-points/pem-file
```

您可以管理 CRL 分发点并检索 NSX Manager 中存储的 CRL。有关详细信息，请参见《NSX-T Data Center API 参考》。

为 CSR 导入证书

您可以为 CSR 导入签名的证书。

在使用自签名证书时，客户端用户将收到一条警告消息，例如，无效的安全证书 (Invalid Security Certificate)。在首次连接到服务器时，客户端用户必须接受自签名证书才能继续。允许客户端用户选择该选项将提供比其他授权方法更低的安全性。

前提条件

确认具有一个 CSR。请参见[创建证书签名请求文件](#)。

步骤

- 1 从浏览器中，使用管理员权限登录到 `https://<nsx-manager-ip-address>` 中的 NSX Manager。
- 2 选择**系统 > 证书**。
- 3 单击 **CSR** 选项卡。
- 4 选择一个 CSR。
- 5 选择**操作 > 为 CSR 导入证书**。
- 6 浏览到计算机上的签名证书文件并添加该文件。
- 7 单击**添加**。

结果

自签名证书将显示在**证书**选项卡中。

存储公用证书和私钥

公用证书和私钥存储在 NSX Manager 上。在创建需要使用私钥的负载均衡器或 VPN 服务时，NSX Manager 将私钥副本发送到运行负载均衡器或 VPN 服务的 Edge 节点。

基于合规性的配置

可以将 NSX-T Data Center 配置为使用 FIPS 140-2 验证的加密模块来在 FIPS 合规性模式下运行。这些模块将通过 NIST 的加密模块验证计划 (Cryptographic Module Validation Program, CMVP) 来验证对 FIPS 140-2 标准的合规性。

可以使用合规性报告来检索 FIPS 合规性的所有例外情况。有关详细信息，请参见[查看合规性状态报告](#)。

NSX-T Data Center 2.5 中使用了以下验证模块：

- VMware OpenSSL FIPS 对象模块版本 2.0.9：证书 #2839
- VMware OpenSSL FIPS 对象模块版本 2.0.20-vmw：证书 #3550
- BC-FJA (Bouncy Castle FIPS Java API) 版本 1.0.1：证书 #3152
- VMware IKE 加密模块版本 1.1.0：证书 #3435
- VMware VPN 加密模块版本 1.0：证书 #3542

您可以在以下位置找到有关 VMware 根据 FIPS 140-2 标准验证的加密模块的更多信息：<https://www.vmware.com/security/certifications/fips.html>。

默认情况下，负载均衡器使用的模块已禁用 FIPS 模式。您可以为负载均衡器使用的模块启用 FIPS 模式。有关详细信息，请参见[为负载均衡器配置全局 FIPS 合规性模式](#)。

查看合规性状态报告

您可以查看 NSX-T Data Center 功能的合规性报告。您可以使用该报告配置 NSX-T Data Center 环境，以符合您的 IT 策略和行业标准。

合规性报告包含有关每个不合规配置的信息。

表 21-8. 合规性报告信息

合规性报告列	说明	示例
不合规代码	用于标识不合规类型的代码。	72301
描述	不合规类型的描述。	证书为非 CA 签名证书。
资源名称	受影响资源的名称或 ID。	nsx-manager-1
资源类型	受影响资源的类型。	CertificateComplianceReporter
受影响的资源	受影响资源的数量。如果存在不合规的配置，但未使用该功能，则该数量可能为 0。	1

您还可以使用 API `GET/policy/api/v1/compliance/status` 来检索报告。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 从主页页面中，单击**监控仪表板 > 合规性报告**。

合规性状态报告代码

您可以找到有关合规性状态报告含义的更多信息。

表 21-9. 合规性报告代码

代码	说明	合规性状态源	修复
72001	已禁用加密。	如果 VPN IPSec 配置文件配置包含 NO_ENCRYPTION、NO_ENCRYPTION_AUTH_AES_GMAC_128、NO_ENCRYPTION_AUTH_AES_GMAC_192 或 NO_ENCRYPTION_AUTH_AES_GMAC_256 encryption_algorithms，则会报告此状态。 此状态将影响使用所报告的不合规配置的 IPSec VPN 会话配置。	要修复此状态，请添加使用合规加密算法的 VPN IPSec 配置文件，并在所有 VPN 配置中使用该配置文件。请参见 添加 IPSec 配置文件 。
72011	包含邻居绕过完整性检查的 BGP 消息。未定义消息身份验证。	如果没有为 BGP 邻居配置任何密码，则会报告此状态。 此状态将影响 BGP 邻居配置。	要修复此状态，请在 BGP 邻居上配置密码，然后更新 Tier-0 网关配置以使用该密码。请参见 配置 BGP 。
72012	与 BGP 邻居的通信使用弱完整性检查。使用 MD5 进行消息身份验证。	如果将 MD5 身份验证用于 BGP 邻居密码，则会报告此状态。 此状态将影响 BGP 邻居配置。	尚无可用的修复措施，因为 NSX-T Data Center 仅支持对 BGP 进行 MD5 身份验证。
72021	使用 SSL 版本 3 建立安全套接字连接。建议运行 TLSv 1.1 或更高版本，并完全禁用具有协议漏洞的 SSLv3。	如果在负载均衡器客户端 SSL 配置文件、负载均衡器服务器 SSL 配置文件或负载均衡器 HTTPS 监控器中配置了 SSL 版本 3，则会报告此状态。 此状态将影响以下配置： <ul style="list-style-type: none"> ■ 与 HTTPS 监控器关联的负载均衡器池。 ■ 与负载均衡器客户端 SSL 配置文件或服务器 SSL 配置文件关联的负载均衡器虚拟服务器。 	要修复此状态，请将 SSL 配置文件配置为使用 TLS 1.1 或更高版本，并在所有负载均衡器配置中使用此配置文件。请参见 添加 SSL 配置文件 。

表 21-9. 合规性报告代码（续）

代码	说明	合规性状态源	修复
72022	使用 TLS 版本 1.0 建立安全套接字连接。建议运行 TLSv 1.1 或更高版本，并完全禁用具有协议漏洞的 TLSv1.0。	如果在负载均衡器客户端 SSL 配置文件、负载均衡器服务器 SSL 配置文件或负载均衡器 HTTPS 监控器中配置了 TLSv1.0，则会报告此状态。 此状态将影响以下配置： <ul style="list-style-type: none"> ■ 与 HTTPS 监控器关联的负载均衡器池。 ■ 与负载均衡器客户端 SSL 配置文件或服务器 SSL 配置文件关联的负载均衡器虚拟服务器。 	要修复此状态，请将 SSL 配置文件配置为使用 TLS 1.1 或更高版本，并在所有负载均衡器配置中使用此配置文件。请参见 添加 SSL 配置文件 。
72023	使用弱 Diffie-Hellman 组。	如果 VPN IPSec 配置文件或 VPN IKE 配置文件配置包含以下 Diffie-Hellman 组，则会报告此错误：2、5、14、15 或 16。组 2 和 5 是弱 Diffie-Hellman 组。组 14、15 和 16 不是弱组，但不符合 FIPS 标准。 此状态将影响使用所报告的不合规配置的 IPSec VPN 会话配置。	要修复该状态，请将 VPN 配置文件配置为使用 Diffie-Hellman 组 19、20 或 21。请参见 添加配置文件 。
72024	已禁用负载均衡器 FIPS 全局设置。	如果已禁用负载均衡器 FIPS 全局设置，则会报告此错误。 此状态将影响所有负载均衡器服务。	要修复此状态，请为负载均衡器启用 FIPS。请参见 为负载均衡器配置全局 FIPS 合规性模式 。
72200	可用的真实熵不足。	当使用伪随机数生成器生成熵，而不是依赖于硬件生成的熵时，会报告此状态。 没有使用硬件生成的熵，因为 NSX Manager 节点没有创建足够的真实熵所需的硬件加速支持。	要修复此状态，您可能需要使用较新的硬件来运行 NSX Manager 节点。最新的硬件支持此功能。 注 如果底层基础架构是虚拟的，那么您将无法获得真实熵。
72201	熵源未知。	当指定的节点没有可用的熵状态时，会报告此状态。	要修复此状态，请确认指定的节点正常运行。
72301	证书为非 CA 签名证书。	如果其中一个 NSX Manager 证书为非 CA 签名证书，则会报告此状态。NSX Manager 使用以下证书： <ul style="list-style-type: none"> ■ Syslog 证书。 ■ API 证书（用于各个 NSX Manager 节点）。 ■ 集群证书（用于 NSX Manager VIP）。 	要修复此状态，请安装 CA 签名证书。请参见 设置证书 。

为负载均衡器配置全局 FIPS 合规性模式

有一个全局设置，用于配置负载均衡器的 FIPS 合规性。默认情况下，将禁用该设置以提高性能。

更改负载均衡器的 FIPS 合规性全局配置会影响新的负载均衡器实例，但不会影响任何现有的负载均衡器实例。

如果将负载均衡器的 FIPS 全局设置 (lb_fips_enabled) 设为 *true*，则新的负载均衡器实例将使用符合 FIPS 140-2 的模块。现有负载均衡器实例可能使用的是不合规的模块。

要使所做的更改在现有负载均衡器上生效，必须从 tier-1 网关中分离并重新连接负载均衡器。

您可以使用 `GET /policy/api/v1/compliance/status` 检查负载均衡器的全局 FIPS 合规性状态。

```
...
{
  "non_compliance_code": 72024,
  "description": "Load balancer FIPS global setting is disabled.",
  "reported_by": {
    "target_id": "971ca477-df1a-4108-8187-7918c2f8c3ba",
    "target_display_name": "971ca477-df1a-4108-8187-7918c2f8c3ba",
    "target_type": "FipsGlobalConfig",
    "is_valid": true
  },
  "affected_resources": [
    {
      "path": "/infra/lb-services/LB_Service",
      "target_id": "/infra/lb-services/LB_Service",
      "target_display_name": "LB_1",
      "target_type": "LBService",
      "is_valid": true
    }
  ]
},
...
```

注 合规性报告将显示负载均衡器的 FIPS 合规性全局设置。任何给定的负载均衡器实例都可以具有与全局设置不同的 FIPS 合规性状态。

步骤

1 检索负载均衡器的全局 FIPS 设置。

GET `https://nsx-mgr1/policy/api/v1/infra/global-config`

响应正文示例：

```
{
  "fips": {
    "lb_fips_enabled": false
  },
  "resource_type": "GlobalConfig",
  "id": "global-config",
  "display_name": "global-config",
```

```

    "path": "/infra/global-config",
    "relative_path": "global-config",
    "marked_for_delete": false,
    "_create_user": "system",
    "_create_time": 1561225479619,
    "_last_modified_user": "admin",
    "_last_modified_time": 1561937915337,
    "_system_owned": true,
    "_protection": "NOT_PROTECTED",
    "_revision": 2
  }

```

2 更改负载均衡器的全局 FIPS 设置。

在创建新的负载均衡器实例时，将使用该全局设置。更改该设置不会影响现有的负载均衡器实例。

PUT <https://nsx-mgr1/policy/api/v1/infra/global-config>

请求正文示例：

```

{
  "fips": {
    "lb_fips_enabled": true
  },
  "resource_type": "GlobalConfig",
  "_revision": 2
}

```

响应正文示例：

```

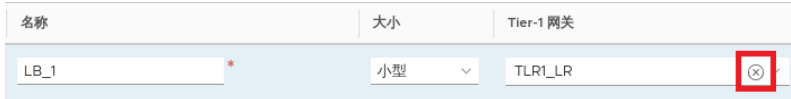
{
  "fips": {
    "lb_fips_enabled": true
  },
  "resource_type": "GlobalConfig",
  "id": "global-config",
  "display_name": "global-config",
  "path": "/infra/global-config",
  "relative_path": "global-config",
  "marked_for_delete": false,
  "_create_user": "system",
  "_create_time": 1561225479619,
  "_last_modified_user": "admin",
  "_last_modified_time": 1561937960950,
  "_system_owned": true,
  "_protection": "NOT_PROTECTED",
  "_revision": 3
}

```

- 3 如果您希望任何现有的负载均衡器实例使用此全局设置，则必须从 **tier-1** 网关中分离并重新连接负载均衡器。

小心 从 **tier-1** 网关中分离负载均衡器会导致负载均衡器实例出现流量中断。

- a 导航到 **网络 > 负载均衡**。
- b 在要分离的负载均衡器上，单击三个圆点菜单 (⋮)，然后单击**编辑**。
- c 单击 (⊗)，然后单击**保存**以从 **tier-1** 网关中分离该负载均衡器。



- d 单击三个圆点菜单 (⋮)，然后单击**编辑**。
- e 从 **Tier-1 网关**下拉菜单中选择正确的网关，然后单击**保存**以将该负载均衡器重新连接到 **tier-1** 网关。

收集支持包

您可以在注册的集群和 **Fabric** 节点上收集支持包，并将这些包下载到您的计算机或上载到文件服务器中。

如果您选择将包下载到您的计算机中，将获得一个存档文件，其中包含每个节点的清单文件和支持包。如果您选择将包上载到文件服务器中，则会将清单文件和各个包单独上载到文件服务器中。

NSX Cloud 说明 如果要收集 CSM 的支持包，请登录到 CSM，转到**系统 > 实用程序 > 支持包**，然后单击**下载**。可按照以下说明从 **NSX Manager** 获得 PCG 的支持包。PCG 的支持包还包含所有工作负载虚拟机的日志。

步骤

- 1 从浏览器中，使用管理员特权登录到 **NSX Manager**，网址为 <https://<nsx-manager-ip-address>>。
- 2 选择**系统 > 支持包**。
- 3 选择目标节点。

可用的节点类型包括**管理节点**、**Edge**、**主机**和**公有云网关**。

- 4 (可选) 指定日志期限天数以排除早于指定天数的日志。
- 5 (可选) 切换开关，选择包括或排除核心文件和审核日志。

注 核心文件和审核日志可能包含敏感信息，例如，密码或加密密钥。

- 6 (可选) 选中相应的复选框以将包上载到远程文件服务器中。
- 7 单击**开始收集支持包**以开始收集支持包。

根据存在的日志文件数，每个节点可能需要几分钟的时间。

8 监控收集过程的状态。

状态选项卡显示收集支持包的进度。

9 如果未设置将包发送到远程文件服务器的选项，请单击**下载**以下载包。

如果磁盘空间不足，管理器节点的包收集可能会失败。如果遇到错误，请检查故障节点上是否存在较旧的支持包。使用故障管理器节点的 IP 地址登录到该故障管理器节点的 NSX Manager UI，并从该节点启动包收集。当 NSX Manager 提示时，请下载旧包或将其删除。

日志消息和错误代码

NSX-T Data Center 组件将写入 /var/log 目录中的日志文件。在 NSX-T 设备和 KVM 主机上，NSX syslog 消息遵循 RFC 5424 格式规范。在 ESXi 主机上，syslog 消息遵循 RFC 3164 格式规范。

查看日志

在 NSX-T 设备上，syslog 消息位于 /var/log/syslog 中。在 KVM 主机上，syslog 消息位于 /var/log/vmware/nsx-syslog 中。

在 NSX-T 设备上，可以运行以下 NSX-T CLI 命令以查看日志：

```
get log-file <auth.log | controller | controller-error | http.log | kern.log | manager.log |
node-mgmt.log | policy.log | syslog> [follow]
```

日志文件如下：

名称	说明
auth.log	授权日志
controller	控制器日志
controller-error	控制器错误日志
http.log	HTTP 服务日志
kern.log	内核日志
manager.log	管理器服务日志
node-mgmt.log	节点管理日志
policy.log	策略服务日志
syslog	系统日志

在管理程序上，可以使用 tac、tail、grep 和 more 等 Linux 命令查看日志。

每条 syslog 消息都具有组件 (comp) 和子组件 (subcomp) 信息，可帮助标识消息的来源。

NSX-T Data Center 会生成包含程序模块 local6 的日志，该模块具有数值 22。

审核日志是 **syslog** 的一部分。可以通过 **structured-data** 字段中的字符串 **audit="true"** 来识别审核日志消息。例如：

```
<182>1 2020-05-05T00:29:02.900Z nsx-manager1 NSX 14389 - [nsx@6876 audit="true" comp="nsx-
manager" level="INFO" reqId="fe75651d-c3e7-4680-8753-9ae9d92d7f0c" subcomp="policy"
username="admin"] UserName="admin", ModuleName="AAA", Operation="GetCurrentUserInfo",
Operation status="success"
```

每个 API 调用都会生成一条审核日志消息。与 API 调用关联的审核日志具有以下信息：

- 实体 ID 参数 **entId**，用于标识 API 的对象。
- 请求 ID 参数 **req-id**，用于标识特定的 API 调用。
- 外部请求 ID 参数 **ereqId**（如果 API 调用包含标头 **X-NSX-EREQID:<string>**）。
- 外部用户参数 **euser**（如果 API 调用包含标头 **X-NSX-EUSER:<string>**）。

RFC 5424 和 RFC 3164 定义了以下严重性级别：

严重性级别	说明
0	紧急：系统无法使用
1	警报：必须立即采取措施
2	严重：严重情况
3	错误：错误情况
4	警告：警告情况
5	通知：正常但重大情况
6	信息：信息性消息
7	调试：调试级别消息

具有“紧急”、“警报”、“严重”或“错误”严重性的所有日志在日志消息的结构化数据部分中包含唯一的错误代码。错误代码由一个字符串和一个十进制数字组成。该字符串表示特定的模块。

日志消息格式

有关 RFC 5424 的详细信息，请参见 <https://tools.ietf.org/html/rfc5424>。有关 RFC 3164 的详细信息，请参见 <https://tools.ietf.org/html/rfc3164>。

RFC 5424 为日志消息定义以下格式：

```
<facility * 8 + severity> version UTC-TZ hostname APP-NAME procid MSGID [structured-data] msg
```

示例日志消息：

```
<187>1 2016-03-15T22:53:00.114Z nsx-manager NSX - SYSTEM [nsx@6876 comp="nsx-manager"
errorCode="MP4039" subcomp="manager"] Connection verification failed for broker
'10.160.108.196'. Marking broker unhealthy.
```

错误代码

有关错误代码的列表，请参见知识库文章 [71077《NSX-T Data Center 2.x 错误代码》](#)。

配置远程日志记录

您可以配置 NSX-T Data Center 设备和 Hypervisor 以将日志消息发送到远程日志服务器。

NSX Manager、NSX Edge 和 Hypervisor 支持远程日志记录。必须分别在每个节点上配置远程日志记录。

在 KVM 主机上，NSX-T Data Center 安装软件包会通过将配置文件置于 `/etc/rsyslog.d` 目录中来自自动配置 rsyslog 守护进程。

前提条件

- 请自行熟悉 CLI 命令 `set logging-server`。有关详细信息，请参见《NSX-T CLI 参考》。
- 如果在 NSX CLI 中使用 TLS 或 LI-TLS 协议来配置与日志服务器的安全连接，则服务器和客户端证书必须存储在每个 NSX-T Data Center 设备上的 `/image/vmware/nsx/file-store` 中。请注意，仅当使用 NSX CLI 配置导出程序时，才需要文件存储中的证书。如果使用 API，则无需使用文件存储。完成 syslog 导出程序配置后，必须删除此位置中的所有证书和密钥，以避免潜在的安全漏洞。
- 要配置与日志服务器的安全连接，请确认服务器配置了 CA 签名的证书。例如，如果您使用 Log Insight 服务器 `vrli.prome.local` 作为日志服务器，则可以从客户端运行以下命令以查看服务器上的证书链：

```
root@caserver:~# echo -n | openssl s_client -connect vrli.prome.local:443 | sed -ne '/
^Certificate chain/,/^---/p'
depth=2 C = US, L = California, O = GS, CN = Orange Root Certification Authority
verify error:num=19:self signed certificate in certificate chain
Certificate chain
 0 s:/C=US/ST=California/L=HTG/O=GSS/CN=vrli.prome.local
  i:/C=US/L=California/O=GS/CN=Green Intermediate Certification Authority
 1 s:/C=US/L=California/O=GS/CN=Green Intermediate Certification Authority
  i:/C=US/L=California/O=GS/CN=Orange Root Certification Authority
 2 s:/C=US/L=California/O=GS/CN=Orange Root Certification Authority
  i:/C=US/L=California/O=GS/CN=Orange Root Certification Authority
---
DONE
```

步骤

- 1 要在 NSX-T Data Center 设备上配置远程日志记录，请运行以下命令以配置日志服务器和要发送到日志服务器的消息类型。可以将多个设备或消息 ID 指定为逗号分隔列表（不含空格）。

```
set logging-server <hostname-or-ip-address[:port]> proto <proto> level <level> [facility
<facility>] [messageid <messageid>] [serverca <filename>] [clientca <filename>]
[certificate <filename>] [key <filename>] [structured-data <structured-data>]
```

您可以多次运行该命令来添加多个配置。例如：

```
nsx> set logging-server 192.168.110.60 proto udp level info facility syslog messageid
SYSTEM,FABRIC
nsx> set logging-server 192.168.110.60 proto udp level info facility auth,user
```

要仅将审核日志转发到远程服务器，请在 structured-data 参数中指定 audit="true"。例如：

```
set logging-server <server-ip> proto udp level info structured-data audit="true"
```

- 2 要使用协议 LI-TLS 配置安全远程日志记录，请指定 proto li-tls 参数。例如：

```
set logging-server vrli.prome.local proto li-tls level info messageid
SWITCHING,ROUTING,FABRIC,SYSTEM,POLICY,HEALTHCHECK,SHA,MONITORING serverca intermed-ca-
full-chain.crt
```

如果配置成功，您将收到一条不含任何文本的提示。要查看服务器证书链（中间证书后跟根证书）的内容，请以 root 的身份登录，然后运行以下命令：

```
root@nsx1:~# keytool -printcert -file /image/vmware/nsx/file-store/intermed-ca-full-
chain.crt
Certificate[1]:
Owner: CN=Green Intermediate Certification Authority, O=GS, L=California, C=US
Issuer: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Serial number: 3e726e7fbb3b0a7a6b4edd767f867fd2
Valid from: Sun Mar 15 00:00:00 UTC 2020 until: Mon Mar 17 00:00:00 UTC 2025
Certificate fingerprints:
  MD5: 94:C8:9F:92:56:60:EB:DB:ED:4B:11:17:33:27:C0:C9
  SHA1: 42:9C:3C:51:E8:8E:AC:2E:5E:62:95:82:D7:22:E0:FB:08:B8:64:29
  SHA256:
58:B8:63:3D:0C:34:35:39:FC:3D:1E:BA:AA:E3:CE:A9:C0:F3:58:53:1F:AD:89:A5:01:0D:D3:89:9E:7B:C
5:69
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3
Certificate[2]:
Owner: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Issuer: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Serial number: 3e726e7fbb3b0a7a6b4edd767f867fd1
Valid from: Mon Mar 16 07:16:07 UTC 2020 until: Fri Mar 10 07:16:07 UTC 2045
Certificate fingerprints:
  MD5: ED:AC:F1:7F:88:05:83:2A:83:C0:09:03:D5:00:CA:7B
  SHA1: DC:B5:3F:37:DF:BD:E0:5C:A4:B7:F4:4C:96:12:75:7A:16:C7:61:37
  SHA256:
```

```
F2:5B:DE:8A:F2:31:9D:E6:EF:35:F1:30:6F:DA:05:FF:92:B4:15:96:AA:82:67:E3:3C:C1:69:A3:E5:27:B
9:A5
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3
```

成功和失败情况的日志都记录在 `/var/log/loginsight-agent/liagent_2020-MM-DD-<file-num>.log` 中。如果配置成功，则可以使用以下命令来查看 Log Insight 配置：

```
root@nsx1:/image/vmware/nsx/file-store# cat /var/lib/loginsight-agent/liagent-effective.ini
; Dynamic file representing the effective configuration of VMware Log Insight Agent
(merged server-side and client-side configuration)
; DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
; Creation time: 2020-03-22T19:41:21.648800

[server]
hostname=vrli.prome.local
proto=cfapi
ssl=yes
ssl_ca_path=/config/vmware/nsx-node-api/syslog/bb466082-996f-4d77-b6e3-1fa93f4a20d4_ca.pem
ssl_accept_any_trusted=yes
port=9543
filter={filelog; nsx-syslog; pri_severity <= 6 and ( msgid == "SWITCHING" or msgid ==
"ROUTING" or msgid == "FABRIC" or msgid == "SYSTEM" or msgid == "POLICY" or msgid ==
"HEALTHCHECK" or msgid == "SHA" or msgid == "MONITORING" ) }

[filelog|nsx-syslog]
directory=/var/log
include=syslog;syslog.*
parser=nsx-syslog_parser

[parser|nsx-syslog_parser]
base_parser=syslog
extract_sd=yes

[update]
auto_update=no
```

3 要使用协议 TLS 来配置安全远程日志记录，请指定 `proto tls` 参数。例如：

```
set logging-server vrli.prome.local proto tls level info serverca Orange-CA.crt.pem
clientca Orange-CA.crt.pem certificate gc-nsxt-mgr-full.crt.pem key gc-nsxt-mgr.key.pem
```

请注意以下事项：

- 对于 `serverCA` 参数，只需提供根证书，而不是整个链。
- 如果 `clientCA` 不同于 `serverCA`，则只需提供根证书。
- 该证书应该包含 NSX Manager 的完整链（应兼容 NDcPP - EKU、BASIC 和 CDP（CDP - 可以忽略这项检查））

您可以检查每个证书的内容。例如：

```
root@gc3:~# keytool -printcert -file /image/vmware/nsx/file-store/Orange-CA.crt.pem
Owner: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Issuer: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Serial number: 3e726e7fbb3b0a7a6b4edd767f867fd1
Valid from: Mon Mar 16 07:16:07 UTC 2020 until: Fri Mar 10 07:16:07 UTC 2045
Certificate fingerprints:
    MD5: ED:AC:F1:7F:88:05:83:2A:83:C0:09:03:D5:00:CA:7B
    SHA1: DC:B5:3F:37:DF:BD:E0:5C:A4:B7:F4:4C:96:12:75:7A:16:C7:61:37
    SHA256:
F2:5B:DE:8A:F2:31:9D:E6:EF:35:F1:30:6F:DA:05:FF:92:B4:15:96:AA:82:67:E3:3C:C1:69:A3:E5:27:B
9:A5
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3
root@gc3:~#

root@gc3:/image/vmware/nsx/file-store# keytool -printcert -file gc-nsxt-mgr-full.crt.pem
Certificate[1]:
Owner: CN=gc.prome.local, O=GS, L=HTG, ST=California, C=US
Issuer: CN=Green Intermediate Certification Authority, O=GS, L=California, C=US
Serial number: bdf43ab31340b87f323b438a2895a075
Valid from: Mon Mar 16 07:26:51 UTC 2020 until: Wed Mar 16 07:26:51 UTC 2022
Certificate fingerprints:
    MD5: 36:3C:1F:57:96:07:84:C0:6D:B7:33:9A:8D:25:4D:27
    SHA1: D1:4E:F9:45:2D:0D:34:79:D2:B4:FA:65:28:E0:5C:DC:74:50:CA:3B
    SHA256:
3C:FF:A9:5D:AA:68:44:44:DD:07:2F:DD:E2:BE:9C:32:19:7A:03:D5:26:8D:5F:AD:56:CA:D2:6C:91:96:2
7:6F
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3
Certificate[2]:
Owner: CN=Green Intermediate Certification Authority, O=GS, L=California, C=US
Issuer: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Serial number: 3e726e7fbb3b0a7a6b4edd767f867fd2
Valid from: Sun Mar 15 00:00:00 UTC 2020 until: Mon Mar 17 00:00:00 UTC 2025
Certificate fingerprints:
    MD5: 94:C8:9F:92:56:60:EB:DB:ED:4B:11:17:33:27:C0:C9
    SHA1: 42:9C:3C:51:E8:8E:AC:2E:5E:62:95:82:D7:22:E0:FB:08:B8:64:29
    SHA256:
58:B8:63:3D:0C:34:35:39:FC:3D:1E:BA:AA:E3:CE:A9:C0:F3:58:53:1F:AD:89:A5:01:0D:D3:89:9E:7B:C
5:69
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3
Certificate[3]:
Owner: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Issuer: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Serial number: 3e726e7fbb3b0a7a6b4edd767f867fd1
Valid from: Mon Mar 16 07:16:07 UTC 2020 until: Fri Mar 10 07:16:07 UTC 2045
Certificate fingerprints:
    MD5: ED:AC:F1:7F:88:05:83:2A:83:C0:09:03:D5:00:CA:7B
    SHA1: DC:B5:3F:37:DF:BD:E0:5C:A4:B7:F4:4C:96:12:75:7A:16:C7:61:37
```

```

SHA256:
F2:5B:DE:8A:F2:31:9D:E6:EF:35:F1:30:6F:DA:05:FF:92:B4:15:96:AA:82:67:E3:3C:C1:69:A3:E5:27:B
9:A5
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3

```

/var/log/syslog 中成功日志记录的示例:

```

<182>1 2020-03-22T21:54:34.501Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully created CA PEM file /
config/vmwarensx-node-api/syslog/92a78d8a-acfd-4515-b05a-2927b70ae920_ca.pem for logging
server vrli.prome.local:6514
<182>1 2020-03-22T21:54:36.269Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully created client CA PEM
file /config/vmwarensx-node-api/syslog/92a78d8a-acfd-4515-b05a-2927b70ae920_client_ca.pem
for logging server vrli.prome.local:6514
<182>1 2020-03-22T21:54:36.495Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] cert issuer = /C=US/L=California/O=GS/
CN=Green IntermediateCertification Authority
<182>1 2020-03-22T21:54:36.514Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] cert subject = /C=US/ST=California/L=HTG/
O=GS/CN=gc.promelocal
<182>1 2020-03-22T21:54:36.539Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] certificate trust check succeeded.
status: 200, result: {'status': 'OK'}
<182>1 2020-03-22T21:54:36.612Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] Certificate already exists, skip import
<182>1 2020-03-22T21:54:37.322Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully created certificate PEM
file /config/vmwarensx-node-api/syslog/92a78d8a-acfd-4515-b05a-2927b70ae920_cert.pem for
logging server vrli.prome.local:6514
<182>1 2020-03-22T21:54:38.020Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully created key PEM file /
config/vmwarensx-node-api/syslog/92a78d8a-acfd-4515-b05a-2927b70ae920_key.pem for logging
server vrli.prome.local:6514

```

/var/log/syslog 中失败日志记录的示例:

```

<182>1 2020-03-22T21:33:30.424Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully created client CA PEM
file /config/vmwarensx-node-api/syslog/76332782-1ec6-483a-95d4-2adeaf2ef112_client_ca.pem
for logging server vrli.prome.local:6514
<182>1 2020-03-22T21:33:30.779Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] cert issuer = /C=US/L=California/O=GS/
CN=Green IntermediateCertification Authority
<182>1 2020-03-22T21:33:30.803Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] cert subject = /C=US/ST=California/L=HTG/
O=GS/CN=gc.promelocal
<179>1 2020-03-22T21:33:30.823Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="ERROR" errorCode="NODE10"] Certificate trust
check failed. status:200, result: {'error_message': 'Certificate
CN=gc.prome.local,O=GS,L=HTG,ST=California,C=US was not verifiably signed by
CN=gc.prome.local,O=GS,L=HTG,ST=California,C=US: certificate does not verifywith supplied

```

```
key', 'status': 'ERROR'})
<179>1 2020-03-22T21:33:30.824Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="ERROR" errorCode="NODE10"] Failed to create
certificate PEM file config/vmware/nsx-node-api/syslog/
76332782-1ec6-483a-95d4-2adeaf2ef112_cert.pem for logging server vrli.prome.local:6514
<182>1 2020-03-22T21:33:31.578Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully deleted CA PEM file /
config/vmwarensx-node-api/syslog/76332782-1ec6-483a-95d4-2adeaf2ef112_ca.pem
<182>1 2020-03-22T21:33:32.342Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully deleted client CA PEM
file /config/vmwarensx-node-api/syslog/76332782-1ec6-483a-95d4-2adeaf2ef112_ca.pem
<182>1 2020-03-22T21:33:32.346Z gc3.prome.local NSX 16698 - [nsx@6876 comp="nsx-cli"
subcomp="node-mgmt" username="admin" level="INFO" audit="true"] CMD: set logging-server
vrli.prome.local prototls level info serverca Orange-CA.crt.pem clientca Orange-CA.crt.pem
certifi
cate gc-nsxt-mgr.crt.pem key gc-nsxt-mgr.key.pem (duration: 6.365s), Operation status:
CMD_EXECUTED
```

可以使用以下命令来检查证书和私钥是否匹配。如果匹配，则输出为正在写入 RSA 密钥。任何其他输出均表示它们不匹配。例如：

```
root@caser:~/server-certs# diff <(openssl x509 -in certs/gc-nsxt-mgr.crt.pem -pubkey
-noout) <(openssl rsa -in private/gc-nsxt-mgr.key.pem -pubout)
writing RSA key
```

损坏的私钥的示例：

```
root@caser:~/server-certs# diff <(openssl x509 -in certs/gc-nsxt-mgr.crt.pem -pubkey
-noout) <(openssl rsa -in private/gc-nsxt-mgr-corrupt.key.pem -pubout)
unable to load Private Key
140404188370584:error:0D07209B:asn1 encoding routines:ASN1_get_object:too
long:asn1_lib.c:147:
140404188370584:error:0D068066:asn1 encoding routines:ASN1_CHECK_TLEN:bad object
header:tasn_dec.c:1205:
140404188370584:error:0D07803A:asn1 encoding routines:ASN1_ITEM_EX_D2I:nested asn1
error:tasn_dec.c:386:Type=RSA
140404188370584:error:04093004:rsa routines:OLD_RSA_PRIV_DECODE:RSA lib:rsa_ameth.c:119:
140404188370584:error:0D07209B:asn1 encoding routines:ASN1_get_object:too
long:asn1_lib.c:147:
140404188370584:error:0D068066:asn1 encoding routines:ASN1_CHECK_TLEN:bad object
header:tasn_dec.c:1205:
140404188370584:error:0D07803A:asn1 encoding routines:ASN1_ITEM_EX_D2I:nested asn1
error:tasn_dec.c:386:Type=PKCS8_PRIV_KEY_INFO
140404188370584:error:0907B00D:PEM routines:PEM_READ_BIO_PRIVATEKEY:ASN1
lib:pem_pkey.c:141:
1,14d0
< -----BEGIN PUBLIC KEY-----
< MIICIJANBgkqhkiG9w0BAQEFAAOCAg8AMIICGgKCAgEAv3yH7pZidfkLrEP3zVa9
< EcOKXlFFjkThZRZMfguenlm8s6QHYVvuUX8IRB48Li3/DUfOj0bzaPWktpv+Q2P0
< N/j4LoX2RzjV/DPxYfLP6GMNMc21L3s9ruBeWUthtUP8khCwd2d2rZ09cUZVl0P9
< kIYBb5RMFC7Z1OUtH3bKdepEf+sXz3DaKZ/WySzYq9x86QDaA3ABO3Q0i7txBscI
< FvXuMDOMQaC3pPp9FWO6IPRAWB57wahLJv6K5qGIfwubSBFg53grT4snf1lDZAHz
< 9hz5JgGr80GVyWyb7rgigpl9iUWAZx8U9De9XoxmvBN5iEGTIuKGaEgICL176crb
< RMkhjnCqNHI+z6sQvpYJ7U0zZc72eBIWoHUKcWWk3eU6Oy4OiyW6jYuXG7hZy1ly
```

```
< nSkme3mZUWJKvcoX05+3zeCP623/HzE7X2sNyWFjzeF3XEvauZrIbsJh/xp2ShDa
< uKKEY0gUGhLtCa3TpV9l8d6tFWVy8XjVjdjoVt4s7MfUo/airVmRykfsWrKyNUOQ
< qRZvSbqjt8pm+3bSvKdXX4ul7ptPG2GF20ETWHPwk2JwQpGhR9zK8fsKzvm6hXi
< kq76zI4FefuVps3e1r39+0F+p6d6i2oUoo24sC1iSePTDhU74efVp6iv8HmnDgYX
< Ylm6Kusr0JT5TJFDfASmrj8CAwEAAQ==
< -----END PUBLIC KEY-----
```

彼此不配对但有效的私钥和证书的示例：

```
root@caserver:~/server-certs# diff <(openssl x509 -in certs/gc-nsxt-mgr.crt.pem -pubkey
-noout) <(openssl rsa -in private/vrli.key.pem -pubout)
writing RSA key
2,13c2,13
< MIICijANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA3yH7pZidfkLrEP3zVa9
< EcOKXlFFjkThZRMfguenlm8s6QHfVvuUX8IRB48Li3/DUfOj0bzaPWktpv+Q2P0
< N/j4LoX2RzjV/DPxYfLP6GMNMc21L3s9ruBeWUtthtUP8khCWd2d2rZ09cUZVl0P9
< kIYBb5RMFC7Zl0UtH3bkdepEf+sXz3DaKZ/WySzYq9x86QDaA3ABO3Q0i7txBscI
< FvXuMDOMQaC3pPp9FWO6IPRAWB57wahLJv6K5qGIfwubSBFg53grT4snf11DZAhZ
< 9hz5JgGr80GvYWyb7rgigpl9iUWAZx8U9De9XoxmvBN5iEGTIuKGaEgICLl76crb
< RMkhjnCqNHI+z6sQvpYJ7U0zZc72eBIWoHUKcWWk3eU6Oy4OiyW6jYuXG7hZYlly
< nSkme3mZUWJKvcoX05+3zeCP623/HzE7X2sNyWFjzeF3XEvauZrIbsJh/xp2ShDa
< uKKEY0gUGhLtCa3TpV9l8d6tFWVy8XjVjdjoVt4s7MfUo/airVmRykfsWrKyNUOQ
< qRZvSbqjt8pm+3bSvKdXX4ul7ptPG2GF20ETWHPwk2JwQpGhR9zK8fsKzvm6hXi
< kq76zI4FefuVps3e1r39+0F+p6d6i2oUoo24sC1iSePTDhU74efVp6iv8HmnDgYX
< Ylm6Kusr0JT5TJFDfASmrj8CAwEAAQ==
---
> MIICijANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAqvsjay7+o7gCW7szT3ho
> bc34XX2l6u5Jl4/X/pUDI/YHmIf06bsZlr/14bTL4Q7BM6+9MI6UYEE7DxUoINGO
> o4FEEQE32KWVFe3gw3homHU39q4pQjsJsxTcTE3oDMLIY0nWJ0PRUst3DffYUH1L
> W0NUN9ydn+fAl2Uf02liuDqVy9V8AH3ON6fu+QCA8nt7lzkzeTxSA0ldpl2NA17F
> rD8rm05wxnV7WtuV7V8PstISiClzhHgZRMl+B0r300itnyAzEGLaRT3//PKfe0Oe
> HCdxGMLrUtMqxIItJahEsqvMufyqNYecVscYXLHPelizKCsQfy8c08LnznG8VAdc
> YILSn3uYGZap6aF1SgVxsvZicwvYnssmgE13Af0nScmfM96k9h5joHVEkWK608v
> oT5DGG1kVL2Qly97x0b6EnzUorzivv5zJMKvFcOektR8HdMHQit5uvmMRY3S5zow
> FtvfSDfWxxKyTy6GBRpp+8F+Jq9lyGy/qa9lhKBzT2lg+rJp7T8k7/Nm9Tjyx7jL
> EggEKZEL4chxpo8ucF98hbvXWRuaFHC2iDzGuUmuS1FfjVvHTuIbEMQfjapLZrHx
> 8jHfOP/PL+6kPbvNZ2rTpczuEoGTQFFW9vX48GzIEyMeR6QWpPR0F7r4xak68P5
> 2PJmMveinDhU35IqWEXHAWcCAwEAAQ==
```

- 4 要查看日志记录配置，请运行 `get logging-server` 命令。例如，

```
nsx> get logging-servers
192.168.110.60 proto udp level info facility syslog messageid SYSTEM,FABRIC
192.168.110.60 proto udp level info facility auth,user
```

- 5 要清除远程日志记录配置，请运行以下命令：

```
nsx> clear logging-servers
```


6 要在 ESXi 主机上配置远程日志记录，请执行以下操作：

a 运行以下命令以配置 syslog 并发送测试消息：

```
esxcli network firewall ruleset set -r syslog -e true
esxcli system syslog config set --loghost=udp://<log server IP>:<port>
esxcli system syslog reload
esxcli system syslog mark -s "This is a test message"
```

b 可以运行以下命令以显示配置：

```
esxcli system syslog config get
```

7 要在 KVM 主机上配置远程日志记录，请执行以下操作：

a 针对您的环境编辑文件 /etc/rsyslog.d/10-vmware-remote-logging.conf。

b 将以下行添加到该文件中：

```
*.* @<ip>:514;RFC5424fmt
```

c 运行以下命令：

```
service rsyslog restart
```

日志消息 ID

在日志消息中，消息 ID 字段标识消息的类型。您可以在 `set logging-server` 命令中使用 `messageid` 参数筛选将哪些日志消息发送到日志记录服务器。

表 21-10. 日志消息 ID

消息 ID	示例
FABRIC	主机节点 主机准备 Edge 节点 传输区域 传输节点 上行链路配置文件 集群配置文件 Edge 集群
SWITCHING	逻辑交换机 逻辑交换机端口 交换配置文件 交换机安全功能
ROUTING	逻辑路由器 逻辑路由器端口 静态路由 动态路由 NAT

表 21-10. 日志消息 ID （续）

消息 ID	示例
FIREWALL	防火墙规则 防火墙规则区域
FIREWALL-PKTLOG	防火墙连接日志 防火墙数据包日志
GROUPING	IP 集 Mac 集 NS 组 NS 服务 NS 服务组 VNI 池 IP 池
DHCP	DHCP 中继
SYSTEM	设备管理（远程 syslog、ntp 等） 集群管理 信任管理 许可 用户和角色 任务管理 安装 升级（NSX Manager、NSX Edge 和主机软件包升级） 实现 标记
MONITORING	SNMP 端口连接 流跟踪
-	所有其他日志消息。

对 Syslog 问题进行故障排除

如果远程日志服务器不接收日志，请执行以下步骤。

- 验证远程日志服务器的 IP 地址。
- 验证 level 参数是否正确配置。
- 验证 facility 参数是否正确配置。
- 如果协议为 TLS，请将协议设置为 UDP，以查看是否存在证书不匹配问题。
- 如果协议为 TLS，请验证端口 6514 是否在两端都已打开。
- 移除消息 ID 筛选器，并查看服务器是否接收日志。
- 使用命令 `restart service rsyslogd` 重新启动 rsyslog 服务。

在设备虚拟机上配置串行日志记录

您可以在设备虚拟机上配置串行日志记录，以便在虚拟机崩溃时捕获日志消息。

步骤

- 1 以 root 身份登录到虚拟机。
- 2 编辑 /etc/default/grub。
- 3 找到 GRUB_CMDLINE_LINUX_DEFAULT 参数并附加 console=ttyS0 console=tty0。
- 4 运行命令 update-grub2。
- 5 确认 /boot/grub/grub.cfg 文件具有在步骤 3 中所做的更改。
- 6 关闭虚拟机电源。
- 7 编辑虚拟机的配置 (.vmx) 文件，并添加以下行：

```
serial0.present = "TRUE"
serial0.fileType = "file"
serial0.fileName = "serial.out"
serial0.yieldOnMsrRead = "TRUE"
answer.msg.serial.file.open = "Append"
```

- 8 打开虚拟机电源。

结果

如果在虚拟机中发生内核崩溃，您可以在与 .vmx 文件相同的位置中找到包含日志消息的 serial.out 文件。

客户体验提升计划

NSX-T Data Center 参与 VMware 客户体验提升计划 (CEIP)。

信任与保证中心 (<https://www.vmware.com/solutions/trustvmware/ceip.html>) 详细阐述了通过 CEIP 收集的数据以及 VMware 将该数据用于何种用途。

要加入或退出 NSX-T Data Center CEIP 或者编辑计划设置，请参见[编辑客户体验提升计划配置](#)。

编辑客户体验提升计划配置

安装或升级 NSX Manager 时，您可以决定是否加入 CEIP 并配置数据收集设置。

此外，还可以编辑现有 CEIP 配置以加入或退出 CEIP 计划，定义信息收集的频率和天数以及代理服务器配置。

前提条件

- 验证 NSX Manager 是否已连接并可以与 Hypervisor 同步。
- 验证 NSX-T Data Center 是否已连接到公共网络以上载数据。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**系统 > 客户计划**。
- 3 在“客户体验提升计划”部分中，单击**编辑**。
- 4 在“编辑客户体验提升计划”对话框中，选中**加入 VMware 客户体验提升计划**复选框。
- 5 切换**计划**开关以禁用或启用数据收集。
默认情况下启用计划。
- 6 （可选）配置数据收集设置和上载重复周期设置。
- 7 单击**保存**。

将标记添加到对象

您可以为对象添加标记以简化搜索过程。在指定标记时，您还可以指定范围。

NSX Cloud 说明 如果使用 NSX Cloud，请参见 [NSX Cloud 支持的 NSX-T Data Center 功能](#)以查看自动生成的逻辑实体、支持的功能以及 NSX Cloud 所需的配置的列表。

大多数对象最多可以有 30 个标记。但对于以下对象，由于有些标记是在内部创建和使用的，因此所拥有的最大标记数将低于 30。

表 21-11. 使用“高级网络和安全”选项卡为对象创建的最大标记数

对象	最大标记数
虚拟机	25
逻辑端口	29

表 21-12. 使用“网络”、“安全”或“清单”选项卡为对象创建的最大标记数

对象	最大标记数
组	29
分段	27
分段端口	29
逻辑路由器端口	30 - 标签数
NAT 规则	27
IPSec VPN 会话	29

表 21-13. Cloud Service Manager 对象的最大标记数

对象	最大标记数
BFD 运行状况监控配置文件、传输区域、上行链路主机交换机配置文件、传输节点、Edge 群集	23

表 21-14. Public Cloud Manager 对象的最大标记数

对象	最大标记数
BFD 运行状况监控配置文件、传输区域、逻辑交换机、节点、传输节点、Edge 群集、逻辑路由器、逻辑路由器上行链路端口、静态路由、DHCP 配置文件、NS 组、防火墙区域规则列表	23
NAT 规则	20
IP 集、NS 组	22

步骤

1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。

2 编辑对象。

例如，转到**分段**选项卡，然后编辑分段。

3 转到**标记**字段，然后添加标记。

每个标记都有一个必填的标记值和一个可选填的范围值。标记的最大长度为 256 个字符。范围的最大长度为 128 个字符。

4 单击**保存**。

查找远程服务器的 SSH 指纹

涉及与远程服务器之间复制文件的某些 API 请求要求在请求正文中提供远程服务器的 SSH 指纹。SSH 指纹是从远程服务器上的主机密钥中获取的。

要通过 SSH 进行连接，NSX Manager 和远程服务器必须具有相同的主机密钥类型。如果具有多个相同的主机密钥类型，将根据 NSX Manager 上的 HostKeyAlgorithm 配置确定首选的类型。

具有远程服务器的指纹可以帮助您确认连接到正确的服务器，从而防止受到中间人攻击。您可以询问远程服务器管理员他们是否可以提供服务器的 SSH 指纹。或者，您可以连接到远程服务器以查找指纹。通过控制台连接到服务器比通过网络更安全。

下表按从首选到非首选顺序列出 NSX Manager 支持的主机密钥。

表 21-15. 按优先顺序排列的 NSX Manager 主机密钥

NSX Manager 支持的主机密钥类型	默认密钥位置
ECDSA (256 位)	/etc/ssh/ssh_host_ecdsa_key.pub
ED25519	/etc/ssh/ssh_host_ed25519_key.pub

步骤

- 1 以 root 身份登录到远程服务器。

使用控制台登录比通过网络更安全。

- 2 列出 /etc/ssh 目录中的公钥文件。

```
$ ls -al /etc/ssh/*pub
-rw-r--r-- 1 root root 601 Apr  8 18:10 ssh_host_dsa_key.pub
-rw-r--r-- 1 root root  93 Apr  8 18:10 ssh_host_ed25519_key.pub
-rw-r--r-- 1 root root 393 Apr  8 18:10 ssh_host_rsa_key.pub
```

- 3 将可用的密钥与 NSX Manager 支持的密钥进行比较。

在该示例中，ED25519 是唯一可接受的密钥。

- 4 获取密钥的指纹。

```
# awk '{print $2}' /etc/ssh/ssh_host_ed25519_key.pub | base64 -d | sha256sum -b | sed
's/ .*$/' | xxd -r -p | base64 | sed 's/./44g' | awk '{print "SHA256:"$1}'
SHA256:KemgftCfsd/hn7EEflhJ4m1698rRhMmNN2IW8y9iq2A
```

查看有关在虚拟机上运行的应用程序的数据

您可以查看有关在作为 NS 组成员的虚拟机上运行的应用程序的信息。这是一个技术预览版功能。

步骤

- 1 从浏览器中，使用管理员权限登录到 <https://<nsx-manager-ip-address>> 中的 NSX Manager。
- 2 选择**高级网络和安全 > 清单 > 组**。
- 3 单击 NS 组的名称。
- 4 单击**应用程序**选项卡。
- 5 单击**收集应用程序数据**。

该过程可能需要几分钟的时间。在该过程完成后，将显示以下信息：

- 总进程数。
- 表示各种层的圆，例如，Web 层、数据库层和应用程序层。还会显示每个层中的进程数。

- 6 单击某个圆以查看有关该层中的进程的详细信息。

配置外部负载均衡器

您可以配置外部负载均衡器，以便将流量分发到管理器集群中的 NSX Manager。

NSX Manager 集群不需要外部负载均衡器。在 Manager 节点出现故障时，可使用 NSX Manager 虚拟 IP (VIP) 进行恢复，但存在以下限制：

- VIP 不会跨 NSX Manager 执行负载均衡。

- VIP 要求所有 NSX Manager 都位于同一子网中。
- 在 Manager 节点出现故障时，VIP 恢复大约需要 1-3 分钟。

外部负载均衡器具有以下优势：

- 可跨 NSX Manager 进行负载均衡。
- NSX Manager 可以位于不同的子网中。
- 可在 Manager 节点出现故障时快速恢复。

请注意，外部负载均衡器无法与 NSX Manager VIP 同时使用。如果使用外部负载均衡器，则请勿配置 NSX Manager VIP。

通过外部负载均衡器从浏览器访问 NSX Manager 时，必须在负载均衡器上启用会话持久性。

通过外部负载均衡器从 API 客户端访问 NSX Manager 时，可以使用四种身份验证方法（有关更多信息，请参见《NSX-T Data Center API 指南》）：

- HTTP 基本身份验证 - 不需要在负载均衡器上启用会话持久性。
- 客户端证书身份验证 - 不需要在负载均衡器上启用会话持久性。
- 向 vIDM 进行身份验证 - 不需要在负载均衡器上启用会话持久性。
- 基于会话的身份验证 - 需要在负载均衡器上启用会话持久性。

建议：

- 在外部负载均衡器上配置一个同时用于浏览器访问和 API 访问的 IP。必须为负载均衡器启用会话持久性。

通过 NSX Cloud，您能够使用 NSX-T Data Center 管理和保护公有云清单。

有关 NSX Cloud 部署工作流，请参见 NSX-T Data Center 安装指南中的[安装 NSX Cloud 组件](#)。

另请参见：[公有云](#)。

本章讨论了以下主题：

- [Cloud Service Manager 快速概览](#)
- [使用 NSX Cloud 隔离策略的威胁检测](#)
- [NSX 实施模式](#)
- [云原生实施模式](#)
- [NSX Cloud 支持的 NSX-T Data Center 功能](#)
- [常见问题解答 \(FAQ\)](#)

Cloud Service Manager 快速概览

Cloud Service Manager (CSM) 为公有云清单提供了单一窗口管理端点。

CSM 界面分为以下几类：

- **搜索：**可以使用搜索文本框查找公有云帐户或相关构造。
- **云：**通过此类别下的各个部分管理公有云清单。
- **系统：**可以从此类别访问 Cloud Service Manager 的 **设置**、**实用程序**和**用户**。

可以通过转到 CSM 的**云**子部分来执行所有公有云操作。

要执行基于系统的操作（例如，备份、还原、升级和用户管理），请转到**系统**子部分。

云

云下包含以下部分：

云 > 概览

可以通过单击**云**来访问您的公有云帐户。

概览：此屏幕上的每个图标显示您的公有云帐户以及该帐户包含的帐户、区域、VPC 或 VNet 以及实例（工作负载虚拟机）的数量。

您可以执行以下任务：

添加公有云帐户或订阅	您可以添加一个或多个公有云帐户或订阅。这样，您能够在 CSM 中查看公有云清单，并指示由 NSX-T Data Center 管理的虚拟机的数量及其状态。 有关详细说明，请参见 NSX-T Data Center 安装指南中的 添加公有云帐户 。
部署/取消部署 NSX Public Cloud Gateway	您可以部署或取消部署一个或两个（用于高可用性）PCG。您可以从 CSM 取消部署 PCG。 有关详细说明，请参见 NSX-T Data Center 安装指南中的 部署 PCG 或 取消部署 PCG 。
启用或禁用隔离策略	您可以启用或禁用隔离策略。请参见 使用 NSX Cloud 隔离策略的威胁检测 以了解详细信息。
网格和卡片视图之间切换	卡片会显示清单的概览。网格则显示更多详细信息。单击图标可在这两个视图类型之间切换。

CSM 以不同方式呈现公有云清单，因此您能够全面了解与 NSX Cloud 连接的所有公有云帐户：

- 您可以查看正在操作的区域的数量。
- 您可以查看每个区域的 VPC/VNet 的数量。
- 您可以查看每个 VPC/VNet 的工作负载虚拟机的数量。

云下有四个选项卡。

云 > {Your Public Cloud} > 帐户

CSM 的“帐户”部分提供有关已添加的公有云帐户的信息。

每个卡代表您从“云”中选择的云提供商的一个公有云帐户。

您可以从此部分执行以下操作：

- 添加帐户
- 编辑帐户
- 删除帐户
- 重新同步帐户

云 > {Your Public Cloud} > 区域

“区域”部分显示所选区域的清单。

可以按公有云帐户筛选“区域”。每个区域都具有 VPC/VNet 以及实例。如果您部署了任何 PCG，则它们会在此处显示为**网关**且带有 PCG 运行状况的指示信息。

云 > {Your Public Cloud} > VPC 或 VNet

“VPC 或 VNet”部分将显示公有云清单。

可以按帐户和区域筛选清单。

- 每个卡代表一个 VPC/VNet。

- 可以在转换 VPC/VNet 上部署一个或两个（实现 HA）PCG。
- 可以将计算 VPC/VNet 链接到转换 VPC/VNet。
- 通过切换到网格视图，可以查看每个 VPC 或 VNet 的更多详细信息。

注 在网格视图中，可以看到三个选项卡：**概览**、**实例**和**分段**。

- **概览**列出了“操作”下的选项，如下一步中所述。
 - **实例**显示了 VPC/VNet 中的实例列表。
 - **分段**显示了 NSX-T 中的覆盖网络分段。NSX Cloud 的当前版本不支持此功能。请勿在 AWS 或 Microsoft Azure 中使用此屏幕上显示的标记来标记工作负载虚拟机。
-
- 单击**操作**可访问以下选项：
 - **编辑配置**（仅适用于转换 VPC/VNet）：
 - 如果在 NSX 实施模式下，请启用或禁用隔离策略。
 - 使用 NSX 实施模式时，请提供 VPC/VNet 从 NSX Cloud 中退出时所需的回退安全组。请参见**禁用隔离策略时的影响**。
 - 更改代理服务器选择。
 - **链接到转换 VPC/VNet**：此选项仅适用于未部署任何 PCG 的 VPC/VNet。单击可选择要链接到的转换 VPC/VNet。
 - **部署 NSX Cloud 网关**：此选项仅适用于未部署 PCG 的 VPC/VNet。单击此选项可开始在此 VPC/VNet 上部署 PCG 并使其成为转换或自我管理 VPC/VNet。有关详细说明，请参见 NSX-T Data Center 安装指南中的**部署或链接 NSX 公有云网关**。

云 > {Your Public Cloud} > 实例

“实例”部分显示 VPC 或 VNet 中的实例的详细信息。

可以按帐户、区域以及 VPC 或 VNet 筛选实例清单。

每个卡代表一个实例（工作负载虚拟机）并显示摘要。

有关实例的详细信息，请单击相应的卡或切换到网格视图。

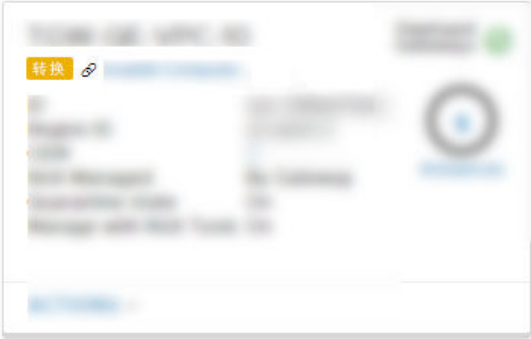
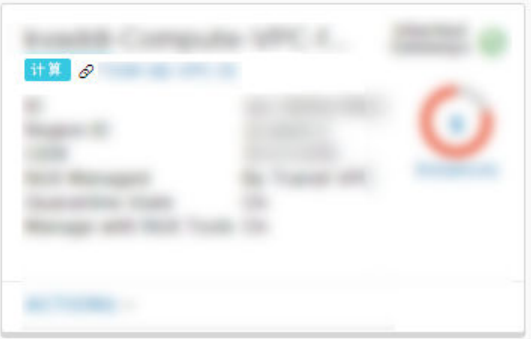
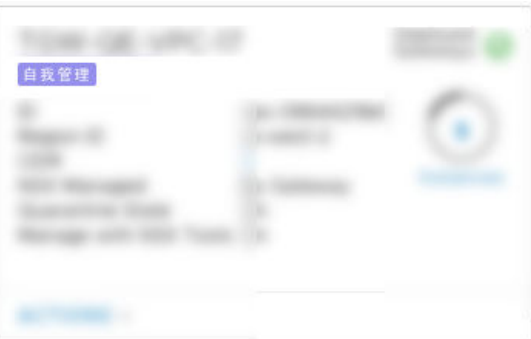
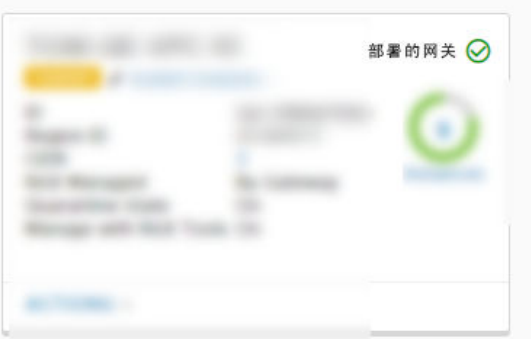
您可以在 CSM 白名单中添加或移除实例。有关详细信息，请参见**将虚拟机添加到白名单**。


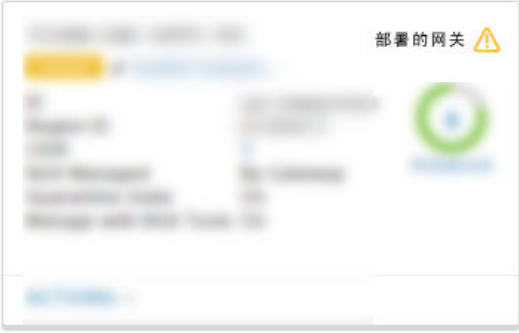
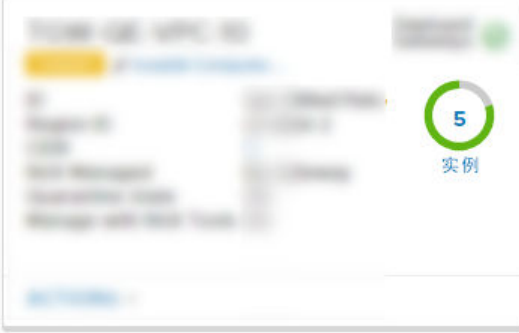
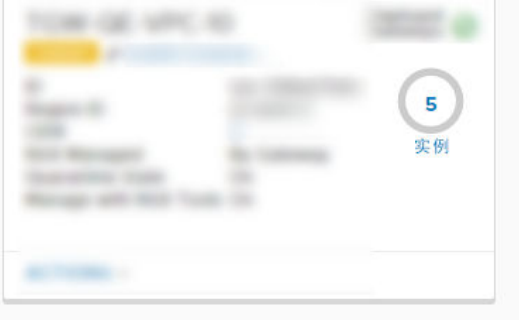
CSM 图标

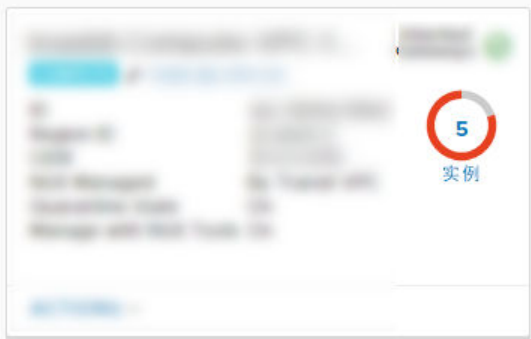
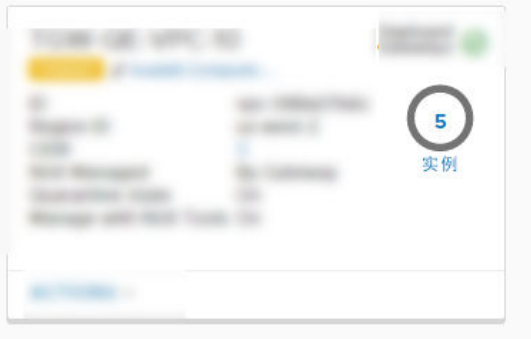


CSM 使用描述性图标来显示公有云构造的状态和运行状况。

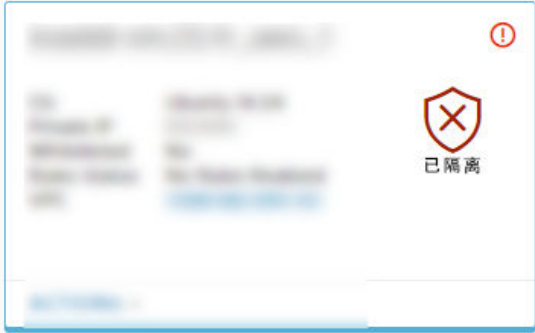

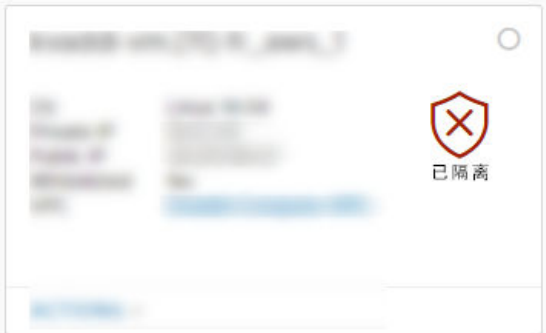
注 在云原生实施模式下：隔离策略始终处于启用状态，且所有虚拟机始终都受 NSX 管理。此模式仅适用于已为 NSX 管理的虚拟机启用隔离策略的情况。

在 NSX 实施模式下：可以禁用隔离策略，且 VPC/VNet 中可以具有非受管虚拟机。此模式适用于所有相关情况。

CSM 区域和图标	说明
VPC/VNet	
	转换 VPC/VNet
	计算 VPC/VNet
	自我管理 VPC/VNet
	显示处于正常运行状态的 PCG 的 VPC/VNet

CSM 区域和图标	说明
	显示处于错误状态的 PCG 的 VPC/VNet
	显示一个处于错误状态和一个处于正常状态的 PCG 的 VPC/VNet。
	显示 NSX 管理的虚拟机的 VPC/VNet。
	显示非受管虚拟机的 VPC/VNet。

CSM 区域和图标	说明
	显示出现错误的虚拟机的 VPC/VNet。
	显示已关闭电源的虚拟机的 VPC/VNet。
实例	
	未出现错误的 NSX 管理的虚拟机。
	出现了错误且已禁用隔离策略的 NSX 管理的虚拟机。

CSM 区域和图标	说明
	出现了错误且已启用隔离策略的 NSX 管理的虚拟机。
	已列入白名单的未受管虚拟机。
	已隔离的非受管虚拟机。

系统

系统下包含以下部分：

系统 > 设置

安装 CSM 时，首先配置这些设置。以后可以对其进行编辑。

将 CSM 与 NSX Manager 相连接

必须将 CSM 设备与 NSX Manager 连接，以允许这些组件互相通信。

前提条件

- 必须安装 NSX Manager 且您必须具有 admin 帐户的用户名和密码才能登录到 NSX Manager

- 必须安装 CSM，并且您必须具有 CSM 中分配的企业管理员角色。

步骤

- 1 从浏览器中，登录到 CSM。
- 2 设置向导中出现提示时，单击**开始设置**。
- 3 在“NSX Manager 凭据”屏幕中输入以下详细信息：

选项	说明
NSX Manager 主机名	输入 NSX Manager 的完全限定域名 (FQDN)（如果可用）。您还可以输入 NSX Manager 的 IP 地址。
管理员凭据	为 NSX Manager 输入企业管理员用户名和密码。
Manager 指纹	（可选）输入 NSX Manager 的指纹值。如果将此字段留空，则系统将识别指纹并在下一个屏幕中显示它。

- 4 （可选）如果未提供 NSX Manager 的指纹值，或者值不正确，则将显示**验证指纹**屏幕。选中复选框以接受系统发现的指纹。
- 5 单击**连接**。

注 如果在设置向导中错过此设置，或者要更改关联的 NSX Manager，则登录到 CSM，单击**系统 > 设置**，然后在标题为**关联的 NSX 节点**的面板上单击**配置**。

CSM 将验证 NSX Manager 指纹并建立连接。

- 6 （可选）设置代理服务器。请参见（可选）[配置代理服务器](#)中的说明。

（可选）配置代理服务器

如果要通过可靠的 HTTP 代理路由并监控 Internet 绑定的所有 HTTP/HTTPS 流量，则可以在 CSM 中配置最多五个代理服务器。

来自 PCG 和 CSM 的所有公有云通信都通过选定的代理服务器进行路由。

PCG 的代理设置独立于 CSM 的代理设置。可以选择不为 PCG 使用代理服务器或者使用不同的代理服务器。

可以选择以下级别的身份验证：

- 基于凭据的身份验证。
- 用于 HTTPS 拦截的基于证书的身份验证。
- 无身份验证。

步骤

- 1 单击**系统 > 设置**。然后在标题为**代理服务器**的面板上单击**配置**。

注 使用首次安装 CSM 时可用的 CSM 设置向导，也可以提供这些详细信息。

2 在“配置代理服务器”屏幕中，输入以下详细信息：

选项	说明
默认	使用此单选按钮指示默认代理服务器。
配置文件名称	提供代理服务器的配置文件名称。这是必填的。
代理服务器	输入代理服务器的 IP 地址。这是必填的。
端口	输入代理服务器的端口。这是必填的。
身份验证	可选。如果要设置其他身份验证，则选中此复选框并提供有效的用户名和密码。
用户名	如果选中“身份验证”复选框，则为必填项。
密码	如果选中“身份验证”复选框，则为必填项。
证书	可选。如果要为 HTTPS 拦截提供身份验证证书，则选中此复选框，并在出现的文本框中复制并粘贴该证书。
无代理	如果不希望使用已配置的任何代理服务器，则选中此选项。

系统 > 实用程序

可以使用以下实用程序。

备份和还原

请按照备份和还原 NSX Manager 时的相同说明，备份和还原 CSM。请参见[备份和还原 NSX Manager](#) 以了解详细信息。

支持包

单击[下载](#)以检索 CSM 的支持包。这用于故障排除。有关详细信息，请参见 NSX-T Data Center 故障排除指南。

系统 > 用户

使用基于角色的访问控制 (RBAC) 管理用户。

请参见[管理用户帐户和基于角色的访问控制](#)以了解详细信息。

使用 NSX Cloud 隔离策略的威胁检测

NSX Cloud 中的隔离策略功能为 NSX 管理的工作负载虚拟机提供了一种威胁检测机制。

两种虚拟机管理模式下的隔离策略实施方式有所不同。

表 22-1. NSX 实施模式和云原生实施模式下的隔离策略实施

与隔离策略相关的配置	在 NSX 实施模式下	在云原生实施模式下
默认状态	使用 NSX Tools 部署 PCG 时处于禁用状态。您可以从 PCG 部署屏幕或以后启用它。请参见 如何启用或禁用隔离策略 。	始终启用。无法禁用。
自动创建的每种模式专用的安全组	所有正常运行的 NSX 管理的虚拟机均分配了 vm-underlay-sg 安全组。	为与 NSX Manager 中分布式防火墙策略匹配的 NSX 管理的工作负载虚拟机创建并应用 nsx-<NSX GUID> 安全组
自动创建的两种模式通用的公有云安全组：	<p>gw 安全组应用于 AWS 和 Microsoft Azure 中相应的 PCG 接口。</p> <ul style="list-style-type: none"> ■ gw-mgmt-sg ■ gw-uplink-sg ■ gw-vtep-sg <p>虚拟机安全组根据其当前状态以及启用还是禁用隔离策略，应用于 NSX 管理的虚拟机：</p> <ul style="list-style-type: none"> ■ vm-quarantine-sg（在 Microsoft Azure 中）和 default（在 AWS 中）。 <p>注 在 AWS 中，default 安全组已存在。它不是由 NSX Cloud 创建的。</p>	

适用于 NSX 实施模式的常规建议：

对于**棕地 (Brownfield)** 部署，开始时为禁用：默认情况下禁用隔离策略。已在公有云环境中设置虚拟机时，对隔离策略使用禁用模式，直到载入工作负载虚拟机。这样可以确保您现有的虚拟机不会被自动隔离。

对于**绿地 (Greenfield)** 部署，开始时为启用：对于绿地部署，建议您启用隔离策略，以允许对由 NSX Cloud 管理的虚拟机执行威胁检测。

NSX 实施模式下的隔离策略

在 NSX 实施模式下，启用隔离策略为可选操作。

如何启用或禁用隔离策略

在 NSX 实施模式下，您可以选择通过两种方式启用隔离策略。

启用隔离策略的第一种情况为在转换 VPC/VNet 上部署 PCG 或将计算 VPC/VNet 链接到转换时。将**关联的 VPC/VNet 上的隔离策略**的滑块从默认的**已禁用**状态移动到**已启用**状态。请参见 NSX-T Data Center 安装指南中的**部署 PCG**。

您也可以稍后按照以下步骤启用隔离策略。

前提条件

如果在部署或链接到 PCG 后启用隔离策略，则您必须具有一个或多个在 NSX 实施模式下载入的转换或计算 VPC/VNet，也就是说，您选择了使用 NSX Tools 管理工作负载虚拟机。

步骤

1 登录到 CSM 并转到公有云：

- a 如果使用的是 AWS，请转到云 > **AWS** > **VPC**。单击“转换 VPC”或“计算 VPC”。
- b 如果使用的是 Microsoft Azure，请转到云 > **Azure** > **VNet**。单击“转换 VNet”或“计算 VNet”。

2 使用以下任一方法启用此选项：

- 在图标视图中，单击**操作** > **编辑配置**。
- 如果位于网格视图中，请选择 VPC 或 VNet 旁边的复选框，然后单击**操作** > **编辑配置**。

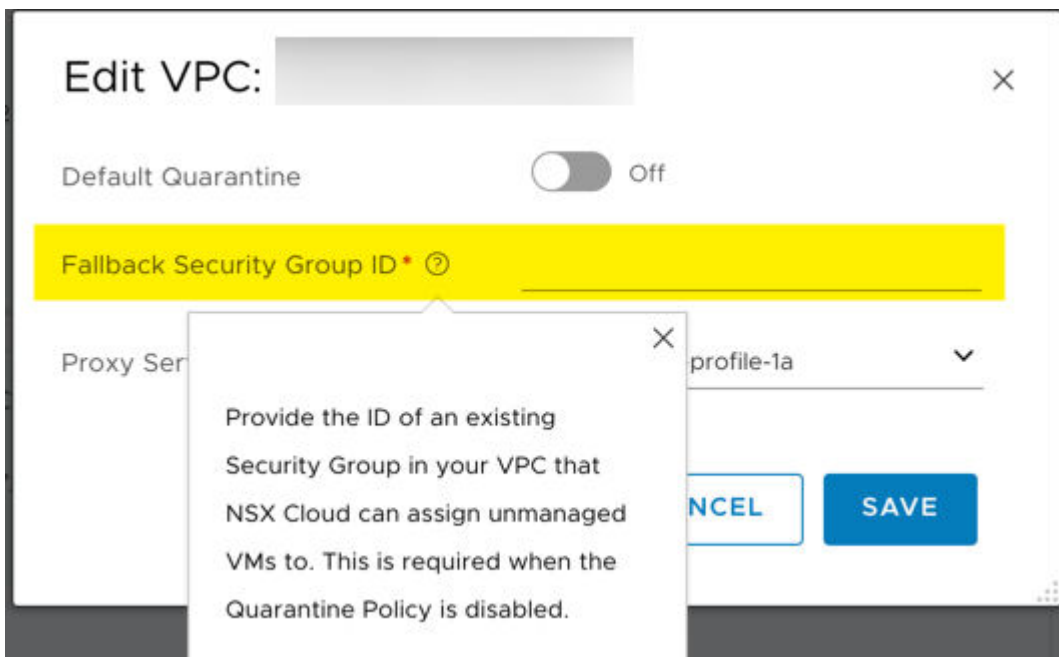


- ◆ 如果位于 VPC 或 VNet 的页面中，请单击“操作”图标以转到**编辑配置**。

3 打开或关闭**默认隔离**以将其启用或禁用。

4 如果禁用隔离策略，则必须提供回退安全组。

注 回退安全组必须是公有云中用户定义的现有安全组。不能使用任何 NSX Cloud 安全组作为回退安全组。



- 禁用隔离策略后，此 VPC 或 VNet 中的所有非受管虚拟机都会分配有该回退安全组。
- 所有受管虚拟机保留 NSX Cloud 分配的安全组。首次在禁用隔离策略后取消标记此类虚拟机并变为非受管虚拟机时，这些虚拟机也会分配有该回退安全组。

5 单击保存。

禁用隔离策略时的影响

禁用隔离策略时，NSX Cloud 不会管理未标记的虚拟机的公有云安全组。

但是，对于公有云中带 `nsx.network=default` 标记的虚拟机，NSX Cloud 会根据虚拟机的状态分配相应的安全组。此行为与启用隔离策略时的行为类似，但隔离安全组 `vm-quarantine-sg`（在 Microsoft Azure 中）和 `default`（在 AWS 中）中的规则并不具有较强的限制性。对已标记虚拟机的安全组进行的任何手动更改将在两分钟内恢复为 NSX Cloud 分配的安全组。

注 如果您不希望 NSX Cloud 将安全组分配给 NSX 管理的（已标记）虚拟机，请在 CSM 中将其列入白名单。请参见[将虚拟机添加到白名单](#)。

下表显示了在禁用隔离策略的情况下，NSX Cloud 如何管理工作负载虚拟机的公有云安全组。

表 22-2. 禁用隔离策略时 NSX Cloud 对公有云安全组的分配

虚拟机在公有云中是否标记有 <code>nsx.network=default</code> ?	虚拟机是否已列入白名单?	禁用隔离策略时虚拟机的公有云安全组以及相关说明
已标记	未列入白名单	<ul style="list-style-type: none"> 如果虚拟机不存在威胁：<code>vm-underlay-sg</code> 如果虚拟机存在潜在威胁（请参见注释）：<code>vm-quarantine-sg</code>（在 Microsoft Azure 中）；<code>default</code>（在 AWS 中） <p>注 在将 <code>nsx.network=default</code> 标记应用于工作负载虚拟机的 90 秒内，将会触发公有云安全组分配。您仍需要安装 NSX Tools 以将虚拟机交由 NSX 管理。在安装 NSX Tools 之前，标记的工作负载虚拟机会一直处于隔离状态。</p>
未标记	未列入白名单	保留现有公有云安全组，因为 NSX Cloud 不会对未标记的虚拟机执行操作。
已标记	已列入白名单	保留现有公有云安全组，因为 NSX Cloud 不会对已列入白名单的虚拟机执行任何操作。
未标记		

下表显示了如果之前已启用了隔离策略，而现在使用为处理此 VPC/VNet 的安全组分配而配置的回退安全组禁用了该隔离策略，则 NSX Cloud 如何管理虚拟机的公有云安全组。

表 22-3. 先启用然后禁用隔离策略时 NSX Cloud 对公有云安全组的分配

虚拟机在公有云中是否标记有 <i>nsx.network=default</i> ?	虚拟机是否已列入白名单?	启用隔离策略时虚拟机的现有公有云安全组	禁用隔离策略后虚拟机的公有云安全组以及提供的回退安全组
未标记	未列入白名单	vm-quarantine-sg (Microsoft Azure) 或 default (AWS)	在禁用隔离策略时，此虚拟机会分配给提供的回退安全组，因为该安全组未进行标记，不会未视为受 NSX 管理，因此 NSX Cloud 会在禁用隔离策略时恢复已分配该虚拟机的安全组。
已标记	未列入白名单	vm-underlay-sg 或 vm-quarantine-sg (Microsoft Azure) 或者 default (AWS)	保留 NSX Cloud 分配的安全组，因为已标记虚拟机的安全组在启用或禁用隔离模式下是一致的。
已标记	已列入白名单	任何现有公有云安全组	保留现有公有云安全组，因为 NSX Cloud 不会对已列入白名单的虚拟机执行任何操作。
未标记			注 如果任何 NSX Cloud 分配的安全组中有已列入白名单的虚拟机，必须手动将其移动到指定的回退安全组。

启用隔离策略时的影响

在启用隔离策略时，NSX Cloud 会管理此 VPC/VNet 中所有工作负载虚拟机的公有云安全组。

对安全组进行的任何手动更改将在两分钟内恢复为 NSX Cloud 分配的安全组。如果您不希望 NSX Cloud 将安全组分配给虚拟机，请在 CSM 中将它们列入白名单。请参见[将虚拟机添加到白名单](#)。

注 从白名单中移除虚拟机会使虚拟机恢复为 NSX Cloud 分配的安全组。

表 22-4. 启用隔离策略时 NSX Cloud 对公有云安全组的分配

虚拟机在公有云中是否标记有 <i>nsx.network=default</i> ?	虚拟机是否已列入白名单?	启用隔离策略时虚拟机的公有云安全组以及相关说明
已标记	未列入白名单	<ul style="list-style-type: none"> 如果虚拟机不存在威胁: <code>vm-underlay-sg</code> 如果虚拟机存在潜在威胁 (请参见注释): <code>vm-quarantine-sg</code> (在 Microsoft Azure 中); <code>default</code> (在 AWS 中) <p>注 在将 <code>nsx.network=default</code> 标记应用于工作负载虚拟机的 90 秒内, 将会触发公有云安全组分配。您仍需要安装 NSX Tools 以将虚拟机交由 NSX 管理。在安装 NSX Tools 之前, 标记的工作负载虚拟机会一直处于隔离状态。</p>
未标记	未列入白名单	<code>vm-quarantine-sg</code> (在 Microsoft Azure 中); <code>default</code> (在 AWS 中)。未标记的虚拟机被视为未受管, 因此会被 NSX Cloud 隔离。
已标记	已列入白名单	保留现有公有云安全组, 因为 NSX Cloud 不会对已列入白名单的虚拟机执行操作。
未标记		

下表列出了隔离策略先禁用然后再启用时对安全组分配产生的影响:

表 22-5. 先禁用然后启用隔离策略时 NSX Cloud 对公有云安全组的分配

虚拟机在公有云中是否标记有 <i>nsx.network=default</i> ?	虚拟机是否已列入白名单?	禁用隔离策略时虚拟机的现有公有云安全组	启用隔离策略后虚拟机的公有云安全组
未标记	未列入白名单	任何现有公有云安全组	<code>vm-quarantine-sg</code> (Microsoft Azure) 或 <code>default</code> (AWS)
已标记	未列入白名单	<code>vm-underlay-sg</code> 或 <code>vm-quarantine-sg</code> (Microsoft Azure) 或者 <code>default</code> (AWS)	保留 NSX Cloud 分配的安全组, 已标记虚拟机的安全组在启用或禁用隔离模式下是一致的。
已标记	已列入白名单	任何现有公有云安全组。	保留现有公有云安全组, 因为 NSX Cloud 不会对已列入白名单的虚拟机执行任何操作。
未标记			

云原生实施模式下的隔离策略

在云原生实施模式下将始终启用隔离策略。

表 22-6. 云原生实施模式下公有云安全组的分配

虚拟机是否属于有效的 NSX-T 安全策略？	虚拟机是否已列入白名单？	虚拟机的公有云安全组及相关说明
是，虚拟机与有效的 NSX-T 安全策略匹配	未列入白名单	NSX Cloud 创建的公有云安全组，其名称类似于 <code>nsx-{NSX-GUID}</code> ，它是 NSX-T 安全策略的对应公有云安全组。
否，虚拟机没有有效的 NSX-T 防火墙策略	未列入白名单	Microsoft Azure 中的 <code>vm-quarantine-sg</code> 或 AWS 中的 <code>default</code> ，因为这是 NSX Cloud 的威胁检测行为。在云原生实施模式下，NSX Cloud 在 Microsoft Azure 中创建的安全组 <code>vm-quarantine-sg</code> 或在 AWS 中创建的安全组 <code>default</code> 模仿默认公有云安全策略。 注 在 CSM 中，虚拟机显示错误状态。
是，虚拟机具有有效的 NSX-T 安全策略	已列入白名单	保留现有公有云安全组，因为 NSX Cloud 不会对已列入白名单的虚拟机执行任何操作。
否，虚拟机没有有效的 NSX-T 安全策略		

将虚拟机添加到白名单

白名单是 CSM 中提供的一个选项，适用于公有云清单中的所有工作负载虚拟机。

白名单可在以下两种虚拟机管理模式下工作：NSX 实施模式和云原生实施模式。

为什么要将虚拟机添加到白名单？

- 在 NSX 实施模式下：如果启用了隔离策略，并且需要在虚拟机上使用现有应用程序验证任何特定的 DFW 策略，则在使用 NSX Cloud 将虚拟机载入之前，可将此虚拟机添加到白名单。
- 在 NSX 实施模式或云原生实施模式下：
 - 如果虚拟机出错，您希望访问这些虚拟机来解决这些错误，则可将这些虚拟机添加到白名单中，以便您可以将它们移出隔离状态并根据需要使用调试工具。
 - 将公有云清单中您不希望受 NSX-T 管理的虚拟机添加到白名单，例如 DNS 转发器、代理服务器等。

如何在白名单中添加或移除虚拟机

按照以下说明在白名单中添加或移除虚拟机。

前提条件

您必须将一个或多个公有云帐户添加到 CSM。

步骤

- 1 使用企业管理员帐户登录到 CSM 并转到公有云帐户。
 - a 如果使用的是 AWS，请转到云 > **AWS** > **VPC** > 实例。
 - b 如果使用的是 Microsoft Azure，请转到云 > **Azure** > **VNet** > 实例。
- 2 如果处于“图标”模式，请单击“实例”视图右上角的模式选择器切换到“网格”模式。
- 3 选择要在白名单中添加或移除的虚拟机（实例）。
- 4 单击**操作**，然后选择**添加到白名单**或**从白名单中移除**。
- 5 返回到“帐户”选项卡，选择帐户图标，然后单击**操作** > **重新同步帐户**。

结果

添加到白名单的每个虚拟机都将保留在添加到白名单之前分配的安全组中。现在，您可以根据需要将任何其他安全组应用到虚拟机。无论隔离策略的状态如何，NSX Cloud 都将忽略已列入白名单的虚拟机。

如果在云原生实施模式下从白名单中移除虚拟机，或在 NSX 实施模式下从白名单中移除 NSX 管理的虚拟机，则 NSX Cloud 将根据该虚拟机的状态为其分配安全组。

NSX 实施模式

在 NSX 实施模式（即通过使用 NSX Tools）下，您必须先通过将虚拟机标记为公有云并为它们安装 NSX Tools 来载入这些虚拟机，然后再开始使用 NSX-T Data Center 管理这些虚拟机。

工作负载虚拟机当前支持的操作系统

下表列出了 NSX 实施模式下 NSX Cloud 当前针对工作负载虚拟机支持的操作系统。

目前支持以下操作系统：

注 有关异常情况，请参见《NSX-T Data Center 发行说明》中的“NSX Cloud 已知问题”部分。对于受支持的操作系统，假定您使用的是标准 Linux 内核版本。不支持使用自定义内核的公有云商城映像，例如，具有修改了源的上游 Linux 内核。

- Red Hat Enterprise Linux (RHEL) 7.2、7.3、7.4、7.5、7.6

- CentOS 7.2、7.3、7.4、7.5、7.6

注 不支持 RHEL 和 CentOS 中的 RHEL 扩展更新支持 (Extended Update Support, EUS) 内核。

注 NSX Cloud 只支持发行版与预期的次要内核版本匹配的 CentOS marketplace 映像。例如，发行版及其相应的内核版本应如下所示：

RHEL 版本	内核版本
RHEL 7.6	3.10.0-957
RHEL 7.5	3.10.0-862
RHEL 7.4	3.10.0-693
RHEL 7.3	3.10.0-514
RHEL 7.2	3.10.0-327

- Ubuntu 14.04、16.04、18.04
- Microsoft Windows Server 2016 - 基于服务的版本、桌面体验（1709、1803、1809）
- Microsoft Windows Server 2019 Datacenter
- Microsoft Windows Server 2012 R2
- Microsoft Windows 10 版本 1809、1803、1709（仅在当前 NSX Cloud 版本中的 Microsoft Azure 中受支持）

在 NSX 实施模式下载入虚拟机

请参阅以下工作流，大概了解在 NSX 实施模式下从公有云载入和管理工作负载虚拟机时涉及的步骤。

表 22-7. 将工作负载虚拟机载入到 NSX Cloud 的第 N 天工作流

任务	说明
<input type="checkbox"/> 使用键-值 <code>nsx.network=default</code> 标记工作负载虚拟机。	按照公有云文档中的说明标记工作负载虚拟机。
<input type="checkbox"/> 在 Windows 或 Linux 工作负载虚拟机上安装 NSX Tools。	请参见 安装 NSX Tools
注 如果在 CSM 中为 Microsoft Azure VNet 启用了 自动安装 NSX Tools ，则将自动安装 NSX Tools。	
<input type="checkbox"/> （可选）在 CSM 中，从白名单中移除希望由 NSX 管理的所有虚拟机。	请参见 如何在白名单中添加或移除虚拟机 。
注 在 CSM 中添加公有云清单后，建议在初始工作流中手动执行列入白名单步骤。如果未向白名单中添加任何虚拟机，则无需从白名单中移除虚拟机。	

在公有云中标记虚拟机

将 `nsx.network=default` 标记应用到要使用 NSX-T Data Center 管理的虚拟机。

步骤

- 1 登录公有云帐户，然后转到具有要由 NSX-T Data Center 管理的工作负载虚拟机的 VPC 或 VNet。
- 2 选择要使用 NSX-T Data Center 管理的虚拟机。
- 3 为虚拟机添加以下标记详细信息并保存所做的更改。

```
Key: nsx.network  
Value: default
```

注 在虚拟机级别应用此标记。

结果

您可能已经载入了已将 `nsx.network=default` 标记应用于工作负载虚拟机的 VPC/VNet。您还可以在应用标记后载入这些 VPC/VNet。成功载入 VPC/VNet 后，这些工作负载虚拟机会被视为受 NSX 管理。

后续步骤

在这些虚拟机上安装 NSX Tools。请参见[安装 NSX Tools](#)。

如果使用 Microsoft Azure，则可以选择在标记的虚拟机上自动安装 NSX Tools。请参见[自动安装 NSX Tools](#) 以了解详细信息。

安装 NSX Tools

在工作负载虚拟机上安装 NSX Tools

可通过多种选项来安装 NSX Tools：

- 在各个工作负载虚拟机中下载并安装 NSX Tools。Linux 和 Windows 虚拟机存在一些差异。
- 借助您的公有云支持的方法（例如，在 AWS 中创建 AMI，或在 Microsoft Azure 中创建受管映像），使用安装了 NSX Tools 的可复制映像。
- 仅限 AWS：启动虚拟机后，在[用户数据](#)中提供 NSX Tools 下载位置和安装命令。

- 仅限 Microsoft Azure：在 Microsoft Azure VNet 中部署 PCG 或链接到转换 VNet 时，或者通过编辑转换/计算 VNet 的配置，启用 NSX Tools 的自动安装。

注 如果要在添加到白名单的工作负载虚拟机上安装 NSX Tools，请确保已在分配给此类虚拟机的安全组中打开以下端口：

- 入站 UDP 6081：用于覆盖网络数据包。应允许（活动/备用）PCG 的 VTEP IP 地址使用该端口（eth1 接口）。
- 出站 TCP 5555：用于控制数据包。应允许（活动/备用）PCG 的管理 IP 地址使用该端口（eth0 接口）。
- TCP 8080：用于 PCG 的管理 IP 地址上的安装/升级。
- TCP 80：用于在安装 NSX Tools 时下载任何第三方依赖项。
- UDP 67、68：用于 DHCP 数据包。
- UDP 53：用于 DNS 解析。

在 Linux 虚拟机上安装 NSX Tools

要在 Linux 工作负载虚拟机上安装 NSX Tools，请按照以下说明进行操作。

请参见[工作负载虚拟机当前支持的操作系统](#)获取当前支持的 Linux 发行版列表。

注 要确认此脚本的校验和，请转到 **Vmware 下载 > 驱动程序和工具 > NSX Cloud 脚本**。

前提条件

您需要使用以下命令运行 NSX Tools 安装脚本：

- `wget`
- `nslookup`
- `dmidecode`

步骤

1 登录到 CSM 并转到公有云：

- 如果使用的是 AWS，请转到云 > **AWS** > **VPC**。单击一个转换或计算 VPC。
- 如果使用的是 Microsoft Azure，请转到云 > **Azure** > **VNet**。单击已在其中部署并正在运行一个或一对 PCG 的 VNet。

注意：转换 VPC/VNet 是部署和运行一个或一对 PCG 的位置。计算 VPC/VNet 链接到转换 VPC/VNet，并且可以使用在其中部署的 PCG 实例。

2 在屏幕的 **NSX Tools 下载与安装**部分，记下 **Linux** 下的**下载位置**和**安装命令**。

注 对于 VNet，安装命令中的 DNS 后缀是动态生成的，与您在部署 PCG 时选择的 DNS 设置相匹配。对于转换 VNet，`-dnsServer <dns-server-ip>` 参数是可选的。对于计算 VNet，必须提供 DNS 转发器 IP 地址才能完成此命令。

- 3 使用超级用户特权登录到 Linux 工作负载虚拟机。
- 4 在 Linux 虚拟机上使用 `wget` 或等效命令从在 CSM 中记录的[下载位置](#)下载安装脚本。安装脚本下载到运行 `wget` 命令的目录中。

注 要确认此脚本的校验和，请转到 **Vmware 下载 > 驱动程序和工具 > NSX Cloud 脚本**。

- 5 如有必要，更改安装脚本的权限以使其可以执行，然后运行该脚本：

```
$ chmod +x install_nsx_vm_agent.sh && sudo ./install_nsx_vm_agent.sh
```

注意：在 Red Hat Enterprise Linux 及其衍生产品上，不支持 SELinux。要安装 NSX Tools，请禁用 SELinux。

- 6 在开始安装 NSX Tools 后，将断开与 Linux 虚拟机的连接。屏幕上显示内容如下的消息：
Installation completed!!! Starting NSX Agent service. SSH connection will now be lost.. 要完成载入过程，请再次登录到您的虚拟机。

结果

在工作负载虚拟机上安装了 NSX Tools。

注

- 在成功安装 NSX Tools 后，端口 8888 在工作负载虚拟机上显示为打开的端口，但为处于底层模式的虚拟机阻止该端口，并且只能在需要时使用该端口进行高级故障排除。如果跳转主机也位于与要访问的工作负载虚拟机相同的 VPC 中，您可以使用跳转主机通过端口 8888 访问工作负载虚拟机。
- 该脚本使用 `eth0` 作为默认接口。

后续步骤

在 [NSX 实施模式下管理虚拟机](#)

在 Windows 虚拟机上安装 NSX Tools

请按照以下说明在 Windows 工作负载虚拟机上安装 NSX Tools。

请参见[工作负载虚拟机当前支持的操作系统](#)，获取当前支持的 Microsoft Windows 版本列表。

注 要确认此脚本的校验和，请转到 **Vmware 下载 > 驱动程序和工具 > NSX Cloud 脚本**。

步骤

- 1 登录到 CSM 并转到公有云：
 - a 如果使用的是 AWS，请转到云 > **AWS** > **VPC**。单击转换 VPC 或计算 VPC。
 - b 如果使用的是 Microsoft Azure，请转到云 > **Azure** > **VNet**。单击部署并运行一个或一对 PCG 的 VNet。

注意：转换 VPC/VNet 是部署和运行一个或一对 PCG 的位置。计算 VPC/VNet 链接到转换 VPC/VNet，并可以使用在那里部署的 PCG。

- 2 在屏幕的 **NSX Tools 下载与安装** 部分，记下 **Windows** 下的**下载位置**和**安装命令**。

注 对于 VNet，安装命令中的 DNS 后缀是动态生成的，与您部署 PCG 时选择的 DNS 设置相匹配。对于转换 VNet，`-dnsServer <dns-server-ip>` 参数是可选的。对于计算 VNet，必须提供 DNS 转发器 IP 地址才能完成此命令。

- 3 以管理员身份连接到 Windows 工作负载虚拟机。
- 4 在 Windows 虚拟机上从在 CSM 中记录的**下载位置**下载安装脚本。您可以使用任意浏览器（如 Internet Explorer）下载脚本。脚本将下载到浏览器的默认下载目录中，例如，C:\Downloads。

注 要确认此脚本的校验和，请转到 **VMware 下载 > 驱动程序和工具 > NSX Cloud 脚本**

注意：

- 5 打开 PowerShell 提示符并转到包含已下载脚本的目录。
- 6 使用在 CSM 中记录的**安装命令**运行下载脚本。

例如：

```
c:\> powershell -file 'nsx_install.ps1' -operation install -dnsSuffix <>
```

注 文件参数需要完整路径，除非您就在该目录中或 PowerShell 脚本已在该路径中。例如，如果将脚本下载到 C:\Downloads，但您目前不在该目录中，那么脚本必须包含位置：`powershell -file 'C:\Downloads\nsx_install.ps1' ...`

- 7 运行脚本，且完成时，将显示一条消息，指示 NSX Tools 安装是否成功。

注 该脚本会将主网络接口视为默认设置。

后续步骤

在 [NSX 实施模式下管理虚拟机](#)

生成可复制映像

对于装有 NSX 代理的虚拟机，可以在 AWS 中生成 AMI，在 Microsoft Azure 中生成受管映像。

利用此功能，可以启动多个配置并运行代理的虚拟机。

可以采用两种方法为装有 NSX 代理的虚拟机生成 AMI/受管映像（本主题其余部分将介绍此映像）：

- **在未配置 NSX 代理的情况下生成映像：**可以从已安装但未使用 `-noStart` 选项进行配置的 NSX 代理的虚拟机生成映像。此选项允许获取并安装 NSX 代理软件包，但不启动 NSX Services。此外，也不执行生成证书等 NSX 配置。
- **移除现有 NSX 代理配置后生成映像：**可以从 NSX 管理的现有虚拟机中移除配置并将其用于生成映像。

在未配置 NSX 代理的情况下生成 AMI

可以为装有 NSX 代理但未进行配置的虚拟机生成 AMI。

要使用 **noStart** 选项从装有 NSX 代理的虚拟机生成映像，请执行以下操作：

步骤

- 1 从 CSM 复制粘贴 NSX 代理安装命令。有关说明，请参见[安装 NSX Tools](#)

- a 对于 Windows，编辑如下命令：

```
c:\> powershell -file 'nsx_install.ps1' -operation install -dnsSuffix <> -noStart true
```

- b 对于 Linux，编辑如下命令：

```
$ chmod +x install_nsx_vm_agent.sh && sudo ./install_nsx_vm_agent.sh --no-start
```

- 2 转到公有云中的这个虚拟机并创建映像。

移除现有 NSX 代理配置后生成映像

可以为已配置 NSX 代理的虚拟机生成映像。

要从 NSX 管理的现有虚拟机中移除配置并将其用于生成映像，请执行以下操作：

步骤

- 1 从 Windows 或 Linux 虚拟机中移除 NSX 代理配置：

- a 最好使用跳转主机登录到工作负载虚拟机。
- b 打开 NSX-T CLI：

```
sudo nsxcli
```

- c 输入下列命令：

```
hostname> set debug
hostname> clear nsx-vm-agent state
```

- 2 在公有云中找到此虚拟机并创建映像。

自动安装 NSX Tools

目前，仅 Microsoft Azure 支持自动安装。

在 Microsoft Azure 中，满足以下条件时，会自动安装 NSX Tools：

- 在 VNet 中的虚拟机上安装的 Azure 虚拟机扩展已添加到 NSX Cloud。有关更多详细信息，请参见[有关虚拟机扩展的 Microsoft Azure 文档](#)。
- 应用于 Microsoft Azure 中的虚拟机的安全组必须允许访问才能安装 NSX Tools。如果启用了隔离策略，则可以在安装之前在 CSM 中将虚拟机添加到白名单，然后在安装后将其从白名单中移除。
- 已使用键 `nsx.network` 和值 `default` 标记虚拟机。

要启用此功能，请执行以下操作：

- 1 转到云 > Azure > VNet。
- 2 选择要自动安装 CSM 的虚拟机所在的 VNet。
- 3 使用以下任一方法启用此选项：

- 在图标视图中，单击操作 > 编辑配置。



- 如果位于网格视图中，请选择 VNet 旁边的复选框，然后单击操作 > 编辑配置。



- 如果位于 VNet 选项卡中，请单击“操作”图标以转到编辑配置。



- 4 将自动安装 NSX Tools 旁边的滑块移动到“开启”位置。

注 如果 NSX Tools 安装失败，请执行以下操作：

- 1 登录到 Microsoft Azure 门户并导航到 NSX Tools 安装失败的虚拟机。
- 2 转到虚拟机的“扩展”，然后卸载名为 VMwareNsxAgentInstallCustomScriptExtension 的扩展。
- 3 从该虚拟机中移除 nsx.network=default 标记。
- 4 重新在该虚拟机上添加 nsx.network=default 标记。

在大约三分钟内，NSX Tools 将安装到该虚拟机上。

在 AWS 中使用用户数据安装 NSX Tools

在 AWS VPC 中启动新的工作负载虚拟机时，您可以通过在“用户数据”字段中提供 NSX Tools 下载和安装说明来安装 NSX Tools。

在启动新的工作负载虚拟机时，从 CSM 中复制 NSX Tools 的下载和安装说明，并将其粘贴到用户数据中。

步骤

- 1 登录到 AWS 控制台并开始启动新工作负载虚拟机的过程。

2 在另一个浏览器窗口中，登录到 CSM。

a 转到云 > **AWS > VPC**

注 转换 VPC/VNet 是部署和运行一个或一对 PCG 的位置。计算 VPC/VNet 链接到转换 VPC/VNet，并可以使用在那里部署的 PCG。

b 单击转换 VPC 或计算 VPC。

c 在屏幕的 **NSX Tools 下载与安装**部分，根据用于工作负载虚拟机的操作系统，复制 **Linux** 或 **Windows** 下的**下载位置**和**安装命令**。

3 在 AWS 的启动新工作负载虚拟机实例步骤中，将下载位置和安装命令作为**文本**粘贴到“高级详细信息”部分的“用户数据”中。

结果

工作负载虚拟机已启动，并且已自动安装 NSX Tools。

卸载 NSX Tools

使用这些操作系统特定的命令卸载 NSX Tools。

从 Windows 虚拟机中卸载 NSX Tools

注 要查看安装脚本可用的其他选项，请使用 `-help`。

- 1 使用 RDP 远程登录到虚拟机。
- 2 使用 `uninstall` 选项运行安装脚本：

```
\nsx_install.ps1 -operation uninstall
```

从 Linux 虚拟机中卸载 NSX Tools

注 要查看安装脚本可用的其他选项，请使用 `--help`。

- 1 使用 SSH 远程登录到虚拟机。
- 2 使用 `uninstall` 选项运行安装脚本：

```
sudo ./install_nsx_vm_agent.sh --uninstall
```

才 NSX 实施模式载入后的安全组

将自动执行以下安全组配置：

如果隔离策略已启用：

- 正常运行的 NSX 管理的虚拟机将移至公有云中的 `vm-underlay-sg`。
- 未受管的虚拟机或存在错误的 NSX 管理的虚拟机将移动到 AWS 的 `default` 安全组和 Microsoft Azure 的 `vm-quarantine-sg` 网络安全组。

- 列入白名单的虚拟机不受影响。

如果隔离策略已禁用：

- 正常运行的 NSX 管理的虚拟机将移至公有云中的 `vm-underlay-sg`。
- 存在错误的 NSX 管理的虚拟机将移动到 AWS 的 `default` 安全组和 Microsoft Azure 的 `vm-quarantine-sg` 网络安全组。
- 未受管的虚拟机和列入白名单的虚拟机不受影响。

在 NSX 实施模式下管理虚拟机

请按照以下步骤开始在 NSX 实施模式下管理成功载入的虚拟机。

表 22-8. NSX 实施模式 下 NSX 管理的工作负载虚拟机的微分段 workflow

任务	说明
 要允许入站访问工作负载虚拟机，请根据需要创建分布式防火墙 (DFW) 规则。	请参见 NSX 实施模式下 NSX 管理的工作负载虚拟机的默认连接策略 。
 使用公有云标记或 NSX-T Data Center 标记分组工作负载虚拟机，并设置微分段。	请参见在 NSX 实施模式下为工作负载虚拟机设置微分段 。 另请参见：使用 NSX-T Data Center 和公有云标记对虚拟机分组

NSX 实施模式下 NSX 管理的工作负载虚拟机的默认连接策略

当您在转换 VPC/VNet 上部署 PCG 时或将计算 VPC/VNet 链接到转换 VPC/VNet 时，NSX Cloud 会在相应位置为 NSX 管理的工作负载虚拟机创建默认安全策略和 DFW 规则。

两个无状态规则用于 DHCP 访问且不会影响对工作负载虚拟机的访问。

两个有状态规则如下所示：

NSX Cloud 在策略下创建的 DFW 规则：cloud-stateful-cloud-<VPC/VNet ID>	属性
cloud-<VPC/VNet ID>-managed	允许访问同一 VPC/VNet 内的虚拟机。
cloud-<VPC/VNet ID>-inbound	阻止从 VPC/VNet 外部的任何位置访问 NSX 管理的虚拟机。

注 请勿编辑任何默认规则。

可以创建现有入站规则的副本，调整源和目标，并设置为允许。将允许规则放置在默认拒绝规则的上方。还可以添加新策略和规则。有关说明，请参见[添加分布式防火墙](#)。

在 NSX 实施模式下为工作负载虚拟机设置微分段

可以为受管工作负载虚拟机设置微分段。

执行以下操作将分布式防火墙规则应用于 NSX 管理的工作负载虚拟机：

- 1 使用虚拟机名称、标记或者其他成员资格条件为 **web**、**应用程序**、**数据库** 层等创建组。有关说明，请参阅 [添加组](#)。

注 您可以使用以下任意标记作为成员资格条件。请参见 [使用 NSX-T Data Center 和公有云标记对虚拟机分组](#) 以了解详细信息。

- 系统定义的标记
- NSX Cloud 在 VPC 或 VNet 中发现的标记
- 或自定义标记

注 DFW 规则取决于分配给虚拟机的标记。由于这些标记可由拥有相应公有云权限的任何人进行修改，因此 NSX-T Data Center 假定此类用户是可信的，并且将由公有云网络管理员负责确保和审核虚拟机始终进行了正确标记。

- 2 创建一个东西向分布式防火墙策略和规则，并应用于您创建的组。请参见 [添加分布式防火墙](#)。

此微分段在从 CSM 手动重新同步清单时生效或在所做的更改从公有云进入 CSM 后的大约三分钟内生效。

云原生实施模式

在云原生实施模式下，所有工作负载虚拟机都自动由 NSX 管理。按照此处所述的工作流开始使用 NSX-T Data Center 管理这些虚拟机。

注 在云原生实施模式下，工作负载虚拟机支持所有操作系统。

在 云原生实施模式下管理虚拟机

在云原生实施模式下，NSX Cloud 利用 NSX-T Data Center 组和分布式防火墙规则在 Microsoft Azure 中创建相应的应用程序安全组和网络安全组，以及在 AWS 中创建安全组。

云原生实施模式下载入的 VPC/VNet 中的所有工作负载虚拟机均由 NSX 管理。

请遵循以下工作流：

表 22-9. 云原生实施模式下的工作负载虚拟机的微分段工作流

任务	说明
<input type="checkbox"/> 在 NSX Manager 中创建一个或多个组，以包含公有云中的工作负载虚拟机。	请参见在 云原生实施模式下为工作负载虚拟机设置微分段 另请参见： 使用 NSX-T Data Center 和公有云标记对虚拟机分组
<input type="checkbox"/> 在 NSX Manager 中创建一个或多个安全策略以应用于您为公有云工作负载虚拟机创建的组。	
<input type="checkbox"/> 如果您希望由 NSX-T 安全策略管理工作负载虚拟机，请将其从 CSM 的白名单中移除。	

表 22-9. 云原生实施模式下的工作负载虚拟机的微分段工作流（续）

任务	说明
 在 CSM 中重新同步公有云帐户。	
 在 VPC/VNet 中，切换到 CSM 中的详细信息视图，以便在出现任何错误时对安全策略进行故障排除。	请参见 当前限制和常见错误

在云原生实施模式下为工作负载虚拟机设置微分段

请参考此工作流，了解如何在云原生实施模式（即在工作负载虚拟机上不安装 NSX Tools）下在 NSX Manager 中为工作负载虚拟机配置安全策略。

前提条件

您的转换或计算 VPC/VNet 必须处于云原生实施模式。

步骤

- 1 在 NSX Manager 中，编辑或创建工作负载虚拟机的组，例如，以 web、app、db 开头的虚拟机名称可以分别表示三个不同的组。有关说明，请参见[添加组](#)。另请参见[使用 NSX-T Data Center 和公有云标记对虚拟机分组](#)，以了解有关使用公有云标记为工作负载虚拟机创建组的信息。

将匹配条件的工作负载虚拟机添加到组中。将与任何分组条件都不匹配的虚拟机放置到 AWS 中的 default 安全组和 Microsoft Azure 中的 vm-quarantine-sg 网络安全组中。

注 您不能使用由 NSX Cloud 自动创建的组。

注 DFW 规则取决于分配给虚拟机的标记。由于这些标记可由拥有相应公有云权限的任何人进行修改，因此 NSX-T Data Center 假定此类用户是可信的，并且将由公有云网络管理员负责确保和审核虚拟机始终进行了正确标记。

- 2 在 NSX Manager 中，使用源、目标或应用对象字段中的组创建分布式防火墙 (DFW) 规则。有关说明，请参见[添加分布式防火墙](#)。

注 公有云工作负载虚拟机仅支持有状态策略。无状态策略可以在 NSX Manager 中创建，但不会与包含公有云工作负载虚拟机的任何组进行匹配。

- 3 在 CSM 中，从要受 NSX 管理的白名单中移除这些虚拟机。有关说明，请参见[如何在白名单中添加或移除虚拟机](#)。

注 在 CSM 中添加公有云清单后，强烈建议在初始工作流中手动执行列入白名单步骤。如果未将任何虚拟机列入白名单，则无需将其从白名单中移除。

4 对于在公有云中找到匹配项的组和 DFW 规则，将自动执行以下操作：

- a 在 AWS 中，NSX Cloud 会创建一个新安全组，其名称类似于 `nsx-<NSX GUID>`。
- b 在 Microsoft Azure 中，NSX Cloud 会创建一个应用程序安全组 (Application Security Group, ASG)（对应于在 NSX Manager 中创建的组）和一个网络安全组 (Network Security Group, NSG)（对应于与分组工作负载虚拟机匹配的 DFW 规则）。

注 NSX Cloud 将每 30 秒同步一次 NSX Manager、公有云组和 DFW 规则。

5 在 CSM 中重新同步公有云帐户：

- a 登录到 CSM 并转到公有云帐户。
- b 从公有云帐户中，单击**操作 > 重新同步帐户**。等待重新同步完成。
- c 转到 VPC/VNet，然后单击红色的“错误”指示信息。这将转到“实例”视图。
- d 如果当前位于“网格”视图，则将该视图切换到“详细信息”，然后在“规则实现”列中单击**失败**以查看错误（如果有）。

后续步骤

请参见[当前限制和常见错误](#)。

当前限制和常见错误

请参考以下已知的限制和常见错误，以便对在云原生实施模式中管理公有云工作负载虚拟机进行故障排除。

注 通过公有云可设置以下限制：

- 可应用于工作负载虚拟机的安全组数。
- 可为工作负载虚拟机实现的规则数。
- 每个安全组可以实现的规则数。
- 安全组分配的范围，例如，Microsoft Azure 中的网络安全组 (NSG) 的范围仅限于该区域，而 AWS 中安全组 (SG) 的范围仅限于该 VPC。

有关这些限制的详细信息，请参阅公有云文档。

当前限制

当前版本对于工作负载虚拟机的 DFW 规则具有以下限制：

- 不支持嵌套组。
- 不支持没有虚拟机和/或 IP 地址作为成员的组，例如，不支持基于分段或逻辑端口的条件。
- 不支持将源和目标设为基于 IP 地址或 CIDR 的组。
- 不支持将源和目标设为“任意”。
- **应用对象**组只能是源或目标或者“源 + 目标”组。其他选项均不受支持。

- 仅支持本地 VPC/VNet 规则实施。您可以在 NSX Manager 中创建跨 VPC/Vnet 的组。但是，此类规则仅会在 VPC/VNet 中实现。不会实现跨 VPC/VNet 的 DFW 规则。
- 仅支持 TCP 和 UDP。

注 仅在 AWS 中：

不会在 AWS 上实现为 AWS VPC 中的工作负载虚拟机创建的拒绝规则，因为在 AWS 中，默认情况下所有虚拟机均被列入黑名单中。这会导致 NSX-T Data Center 中出现以下结果：

- 如果在虚拟机 1 和虚拟机 2 之间创建了拒绝规则，则不允许虚拟机 1 和虚拟机 2 之间的流量，这是由于默认的 AWS 行为所致，而不是因为拒绝规则。拒绝规则不会在 AWS 中实现。
- 假设在 NSX Manager 中为同一个虚拟机创建了两个规则，其中规则 1 的优先级高于规则 2：
 - a 虚拟机 1 到虚拟机 2 拒绝 SSH
 - b 虚拟机 1 到虚拟机 2 允许 SSH

拒绝规则会被忽略，因为它不会在 AWS 中实现，因此会实现“允许 SSH”规则。这与预期相反，这是由于默认的 AWS 行为所产生的限制所致。

常见错误及其解决方法

错误：未对虚拟机应用任何 NSX 策略。

如果您看到此错误，则表示没有对特定虚拟机应用任何 DFW 规则。在 NSX Manager 中编辑规则或的组以包含此虚拟机。

错误：不支持无状态 NSX 规则。

如果您看到此错误，则表示您已在无状态安全策略中为公有云工作负载虚拟机添加了 DFW 规则。这种情况不受支持。在“有状态”模式下创建新安全策略或使用现有安全策略。

NSX Cloud 支持的 NSX-T Data Center 功能

NSX Cloud 通过在 NSX-T Data Center 中生成逻辑网络实体来为公有云 VPC 或 VNet 创建网络拓扑。

以下列表介绍了自动生成的实体，以及 NSX-T Data Center 功能应用于公有云时应使用这些功能的方式，供您参考。

NSX Manager 配置

有关在成功部署 PCG 后创建的逻辑实体的详细信息，请参见 NSX-T Data Center 安装指南中的“自动创建的 NSX-T 逻辑实体”。

重要事项 请勿编辑或删除所有这些自动创建的实体。

注 如果无法访问 Windows 工作负载虚拟机上的某些功能，请确保已正确配置 Windows 防火墙设置。

表 22-10.

NSX-T Data Center 功能	详细信息	NSX Cloud 备注
分段或逻辑交换机	请参见第 4 章 分段	将为受管虚拟机连接到的每个公有云子网创建一个分段。这是一个混合分段。
网关或逻辑路由器	请参见第 2 章 Tier-0 网关和第 3 章 Tier-1 网关。	在转换 VPC 或 VNet 上部署 PCG 时，NSX Cloud 将自动创建 Tier-0 逻辑路由器。将每个计算 VPC/VNet 链接到转换 VPC/VNet 时，将为其创建 Tier-1 路由器
IPFIX	请参见配置 IPFIX。	<ul style="list-style-type: none"> ■ 在 NSX Cloud 中，仅 UDP 端口 4739 支持 IPFIX。 ■ 交换机和 DFW IPFIX: 如果收集器与应用 IPFIX 配置文件的 Windows 虚拟机位于同一子网，则 Windows 虚拟机需要收集器的静态 ARP 条目，因为 Windows 找不到 ARP 条目时会静默丢弃 UDP 数据包。
端口镜像	请参见监控端口镜像会话。	<p>在当前版本中，仅 AWS 支持端口镜像。</p> <ul style="list-style-type: none"> ■ 对于 NSX Cloud，请从工具 > 端口镜像会话配置端口镜像。 ■ 仅支持 L3SPAN 端口镜像。 ■ 收集器必须与源工作负载虚拟机位于同一个 VPC。
网关防火墙	请参见配置网关防火墙。	仅在 Tier-0 网关上受支持。

使用 NSX-T Data Center 和公有云标记对虚拟机分组

NSX Cloud 允许您使用分配给工作负载虚拟机的公有云标记。

NSX Manager 使用标记对虚拟机进行分组，就像公有云一样。因此，为便于对虚拟机分组，只要应用于工作负载虚拟机的公有云标记满足预定义大小和保留字条件，NSX Cloud 就会将这些标记拉入 NSX Manager。

注 DFW 规则取决于分配给虚拟机的标记。由于这些标记可由拥有相应公有云权限的任何人进行修改，因此 NSX-T Data Center 假定此类用户是可信的，并且将由公有云网络管理员负责确保和审核虚拟机始终进行了正确标记。

标记术语

NSX Manager 中的**标记**在公有云环境中称为**值**。公有云标记的**键**在 NSX Manager 中称为**范围**。

标记的组件	
(NSX Manager 中)	公有云中的等效标记组件
范围	键
标记	值

标记类型和限制

NSX Cloud 允许对 NSX 管理的公有云虚拟机使用三种类型的标记。

- **系统标记：** 这些标记是系统定义的，无法添加、编辑或删除。NSX Cloud 使用以下系统标记：
 - azure:subscription_id
 - azure:region
 - azure:vm_rg
 - azure:vnet_name
 - azure:vnet_rg
 - azure:transit_vnet_name
 - azure:transit_vnet_rg
 - aws:account
 - aws:availabilityzone
 - aws:region
 - aws:vpc
 - aws:subnet
 - aws:transit_vpc
- **发现的标记：** 您添加到公有云虚拟机中的标记，NSX Cloud 会自动发现此类标记并针对 NSX Manager 清单中的工作负载虚拟机进行显示。在 NSX Manager 中无法编辑这些标记。发现的标记没有数量限制。这些标记带有 `dis:azure:` 前缀，表示它们是从 Microsoft Azure 中发现的；带有 `dis:aws` 前缀，表示它们是从 AWS 中发现的。

在公有云中对标记进行任何更改时，所做的更改三分钟内即反映在 NSX Manager 中。

默认情况下，将启用该功能。可以在添加 Microsoft Azure 订阅或 AWS 帐户时启用或禁用 Microsoft Azure 或 AWS 标记的发现。

- **用户标记：** 您最多可以创建 25 个用户标记。您可以添加、编辑和删除用户标记。有关管理用户标记的信息，请参见[管理虚拟机的标记](#)。

表 22-11. 标记类型和限制摘要

标记类型	标记范围或预定的前缀	限制	企业管理员特权	审核员特权
系统定义	完整的系统标记： <ul style="list-style-type: none"> ■ azure:subscription_id ■ azure:region ■ azure:vm_rg ■ azure:vnet_name ■ azure:vnet_rg ■ aws:vpc ■ aws:availability zone 	范围（键）：20 个字符 标记（值）：65 个字符 可能的最大数：5 个	只读	只读
发现	从 VNet 导入的 Microsoft Azure 标记的前缀： dis:azure: 从 VPC 导入的 AWS 标记的前缀： dis:aws:	范围（键）：20 个字符 标记（值）：65 个字符 允许的最大数：无限制 注 字符数限制不包括前缀 dis:<公有云名称> 。超出这些限制的标记不会反映在 NSX Manager 中。 将忽略具有前缀 nsx 的标记。	只读	只读
用户	用户标记可以包含允许字符数内的任何范围（键）和值，除了： <ul style="list-style-type: none"> ■ 范围（键）前缀 dis:azure: 或 dis:aws: ■ 与系统标记相同的范围（键） 	范围（键）：30 个字符 标记（值）：65 个字符 允许的最大数：25 个	添加/编辑/删除	只读

发现的标记示例

注 标记在公有云中的格式为 **key=value**，在 NSX Manager 中的格式为 **scope=tag**。

表 22-12.

工作负载虚拟机的公有云标记	由 NSX Cloud 发现?	工作负载虚拟机的等效 NSX Manager 标记
Name=Developer	是	dis:azure:Name=Developer
ValidDisTagKeyLength=ValidDisTagValue	是	dis:azure:ValidDisTagKeyLength=ValidDisTagValue
Abcdefghijklmnopqrstuvwxyz=value2	否 (键超过 20 个字符)	无
tag3=AbcdefghijklmnopqrstuvwxyzAb23690hgjguytreswqacvbcdefghijklmnopqrstuvwxyz	否 (值超过 65 个字符)	无
nsx.name=Tester	否 (键具有前缀 nsx)	无

标记在 NSX Manager 中的用途

- 请参见[管理虚拟机的标记](#)。
- 请参见[搜索对象](#)。
- 请参见[添加组](#)。
- 请参见在 [NSX 实施模式](#) 下为工作负载虚拟机设置微分段。

使用云原生服务

以下云原生服务支持与 NSX Manager 中的公有云工作负载虚拟机配合使用。

部署 PCG 时，会在 NSX Manager 中为每个受支持的云原生服务创建一个组。

为当前支持的公有云服务创建以下组：

- aws-dynamo-db-service-endpoint
- aws-elb-service-endpoint
- aws-rds-service-endpoint
- aws-s3-service-endpoint
- azure-cosmos-db-service-endpoint
- azure-load-balancer-service-endpoint
- azure-sql-service-endpoint
- azure-storage-service-endpoint

要使用这些云原生服务，请根据需要创建 DFW 策略以包含规则的“源”或“目标”字段中的云原生服务组。

DFW 规则是针对虚拟机实施的，而不是针对非云原生服务实施。

注 在 NSX 实施模式下（即使用 NSX Tools 管理工作负载），当前不支持 Microsoft Azure 的云原生服务。

当前限制

端点			服务作为“目标”的 DFW 规则		服务作为“源”的 DFW 规则	
公有云	服务	范围	对虚拟机实施?	对服务实施?	对服务实施?	对虚拟机实施?
Microsoft Azure	BLOB 存储	全局	是	否	否	是
	Cosmos DB					
	SQL					
	负载均衡器					
AWS	S3	VPC 本地	是	否	否	是
	Dynamo DB					
	RDS					
	ELB					

在公有云中使用服务插入

NSX Cloud 支持在公有云中对 NSX 管理的工作负载虚拟机使用第三方服务。

要将服务插入用于公有云工作负载虚拟机，必须在公有云（而不是在 NSX-T Data Center）中托管服务设备。建议在转换 VPC/VNet 中托管服务设备。

必须在转换 VPC 或 VNet 中部署 PCG，才能启用服务插入。

下面提供了允许对 NSX 管理的工作负载虚拟机使用服务插入的一次性配置概览。

表 22-13. 在公有云中对 NSX 管理的工作负载虚拟机使用服务插入时所需的配置概览

配置频率	任务	说明
初始设置时一次性配置	在公有云中设置服务设备，最好在转换 VPC 或 VNet（已部署 PCG）中设置。	请参见特定于第三方服务设备和公有云的说明。
	在 NSX-T Data Center 中注册第三方服务。	请参见 创建服务定义和相应的虚拟端点
	使用服务设备要仅用于服务插入的 /32 服务虚拟 IP 地址 (VSIP) 创建服务的虚拟实例端点。VSIP 不应与 VPC 或 VNet 的 CIDR 范围冲突。此 VSIP 通过 BGP 通告到 PCG。	请参见 创建服务定义和相应的虚拟端点
	在服务设备和 PCG 之间创建 IPSec VPN 隧道。	请参见 设置 IPSec VPN 会话

表 22-13. 在公有云中对 NSX 管理的工作负载虚拟机使用服务插入时所需的配置概览（续）

配置频率	任务	说明
	在 PCG 和服务设备之间配置 BGP，并从服务设备通告 VSIP，从 PCG 通告默认路由 (0.0.0.0/0)。 注 在当前版本中，仅南北向流量支持服务插入。	请参见配置 BGP 和路由重新分发
按需随时配置	一次性配置完成后，设置重定向规则以将来自 NSX 管理的工作负载虚拟机的选择性流量重新路由到 VSIP。这些规则将应用于 PCG 的上行链路端口。	请参见设置重定向规则。

步骤

1 创建服务定义和相应的虚拟端点

必须使用 NSX Manager API 为公有云中的服务设备创建服务定义和虚拟端点。

2 设置 IPsec VPN 会话

在 PCG 和服务设备之间设置 IPsec VPN 会话。

3 配置 BGP 和路由重新分发

通过 IPsec VPN 隧道在 PCG 和服务设备之间配置 BGP。

4 设置重定向规则

可以根据您的要求调整重定向规则。

创建服务定义和相应的虚拟端点

必须使用 NSX Manager API 为公有云中的服务设备创建服务定义和虚拟端点。

前提条件

挑选一个预留的 /32 IP 地址作为公有云中服务设备的虚拟端点，例如，100.100.100.100/32。这称为虚拟服务 IP (VSIP)。

注 如果成对部署服务设备以实现高可用性，不要创建另一个服务定义，而是在 BGP 配置期间将其通告到 PCG 时使用相同的 VSIP。

步骤

1 要为服务设备创建服务定义，请使用授权的 NSX Manager 凭据运行以下 API 调用：

```
POST https://{NSX Manager-IP}/policy/api/v1/enforcement-points/default/service-definitions
```

示例请求：

```
{
  "resource_type": "ServiceDefinition",
  "description": "NS-Service",
  "display_name": "Service_Appliance1",
  "attachment_point": [
    "TIER0_LR"
  ]
}
```

```

    ],
    "transports": [
        "L3_ROUTED"
    ],
    "functionalities": [
        "NG_FW", "BYOD"
    ],
    "on_failure_policy": "ALLOW",
    "implementations": [
        "NORTH_SOUTH"
    ],
    "vendor_id" : "Vendor1"
}

```

示例响应:

```

{
    "resource_type": "ServiceDefinition",
    "description": "NS-Service",
    "id": "33890153-6eea-4c9d-8e34-7b6532b9d65c",
    "display_name": "Service_Appliance1",
    "attachment_point": [
        "TIER0_LR"
    ],
    "transports": [
        "L3_ROUTED"
    ],
    "functionalities": [
        "NG_FW", "BYOD"
    ],
    "vendor_id": "Vendor1",
    "on_failure_policy": "ALLOW",
    "implementations": [
        "NORTH_SOUTH"
    ],
    "_create_time": 1540424262137,
    "_last_modified_user": "nsx_policy",
    "_system_owned": false,
    "_protection": "REQUIRE_OVERRIDE",
    "_last_modified_time": 1540424262137,
    "_create_user": "nsx_policy",
    "_revision": 0
}

```

2 要为服务设备创建虚拟端点，请使用授权的 NSX Manager 凭据运行以下 API 调用:

```
PATCH https://{NSX Manager-IP}/policy/api/v1/infra/tier-0s/<tier-0 router ID>/locale-
services/cloud/endpoints/virtual-endpoints/Service_Appliance1_Endpoint
```

示例请求：

```
{
  "resource_type": "VirtualEndpoint",
  "display_name": "Service_Appliance1_Endpoint",
  "target_ips": [
    {
      "ip_addresses": [
        "100.100.100.100"
      ],
      "prefix_length": 32
    }
  ],
  "service_names": [
    "Service_Appliance1"
  ]
}
```

示例响应：

```
200 OK
```

注 步骤 1 中的 `display_name` 必须与步骤 2 中的 `service_names` 一致。

后续步骤

设置 IPsec VPN 会话

设置 IPsec VPN 会话

在 PCG 和服务设备之间设置 IPsec VPN 会话。

前提条件

- 必须在转换 VPC/VNet 中部署一个或一对（实现 HA）PCG。
- 必须在公有云中设置服务设备，最好在转换 VPC/VNet 中进行设置。

步骤

- 1 导航到 **网络 > VPN**
- 2 添加类型为 IPsec 的 **VPN 服务**并注意以下特定于 NSX Cloud 的配置选项。有关其他详细信息，请参见 [添加 IPsec VPN 服务](#)。

选项	说明
名称	此 VPN 服务的名称用于设置本地端点和 IPsec VPN 会话。请将其记录下来。
服务类型	确认此值设置为 IPsec。
Tier-0 网关	选择为转换 VPC/VNet 自动创建的 Tier-0 网关。其名称包含 VPC/VNet ID，例如，cloud-t0-vpc-6bcd2c13。

- 3 为 PCG 添加**本地端点**。本地端点的 IP 地址为在转换 VPC/VNet 中部署的 PCG 的标记 `nsx:local_endpoint_ip` 的值。登录到转换 VPC/VNet，查看此值。请注意以下特定于 NSX Cloud 的配置。有关其他详细信息，请参见[添加本地端点](#)。

选项	说明
名称	本地端点名称用于设置 IPSec VPN 会话。请将其记录下来。
VPN 服务	选择在步骤 2 中添加的 VPN 服务。
IP 地址	登录到 AWS 控制台或 Microsoft Azure 门户可查找此值。它是应用于 PCG 的上行链路接口的标记 <code>nsx:local_endpoint_ip</code> 的值。

- 4 在 PCG 和公有云中的服务设备（最好是在转换 VPC/VNet 中托管的服务设备）之间创建**基于路由的 IPSec 会话**。

选项	说明
类型	确认此值设置为 基于路由 。
VPN 服务	选择在步骤 2 中添加的 VPN 服务。
本地端点	选择在步骤 3 中创建的本地端点。
远程 IP	输入服务设备的专用 IP 地址。 注 如果可使用公共 IP 地址访问服务设备，则将本地端点 IP 的公共 IP 地址（也称为辅助 IP）分配给 PCG 的上行链路接口。
隧道接口	此子网必须与 VPN 隧道的服务设备子网一致。输入在服务设备中为 VPN 隧道设置的子网值，或记下在此处输入的值并确保在服务设备中设置 VPN 隧道时使用同一子网。 注 在此隧道接口上配置 BGP。请参见 配置 BGP 和路由重新分发 。
远程 ID	输入公有云中服务设备的专用 IP 地址。
IKE 配置文件	IPSec VPN 会话必须与 IKE 配置文件相关联。如果创建了配置文件，请从下拉菜单中选择该配置文件。也可以使用默认配置文件。

后续步骤

配置 BGP 和路由重新分发

配置 BGP 和路由重新分发

通过 IPSec VPN 隧道在 PCG 和服务设备之间配置 BGP。

在 PCG 和服务设备之间建立的 IPSec VPN 隧道接口上设置 BGP 邻居。有关更多详细信息，请参见[配置 BGP](#)。

需要在服务设备上以类似的方式配置 BGP。有关详细信息，请参见公有云中的特定服务所对应的文档。

接下来，设置路由重新分发，如下所示：

- PCG 将其默认路由 (0.0.0.0/0) 通告到服务设备。

- 服务设备将 VSIP 通告到 PCG。这是注册服务时使用的同一 IP 地址。请参见[创建服务定义和相应的虚拟端点](#)。

注 如果成对部署服务设备以实现高可用性，则从这两个服务设备通告相同的 VSIP。

步骤

- 1 导航到**网络 > Tier-0 网关**。
- 2 为转换 VPC/VNet 选择自动创建的 Tier-0 网关，其名称类似于 cloud-t0-vpc-6bcd2c13，然后单击**编辑**。
- 3 单击 **BGP** 区域下 **BGP 邻居** 旁边的编号或图标。
- 4 请注意以下配置：

选项	描述
IP 地址	使用在服务设备隧道接口上为 PCG 和服务设备之间的 VPN 配置的 IP 地址。
远程 AS 编号	此编号必须与公有云中服务设备的 AS 编号一致。
路由筛选器	设置出站筛选器，以将 PCG 中的默认路由 (0.0.0.0/0) 通告到服务设备。

- 5 从路由重新分发部分中，启用 Tier-0 网关上的静态路由。

设置路由重新分发



后续步骤

[设置重定向规则](#)

设置重定向规则

可以根据您的要求调整重定向规则。

完成初始设置后，可以根据需要创建和编辑重定向规则，以便重新路由 NSX 管理的工作负载虚拟机的不同类型的流量，使其通过服务设备。

前提条件

必须完成所有服务插入设置才能创建重定向规则。

步骤

- 1 导航到 **安全性 > 南北向防火墙 > 网络侦测 (南北向)**
- 2 单击**添加策略**。

选项	说明
名称:	提供策略的描述性名称，例如 Azure 虚拟机的南北向服务插入 。
重定向至:	选择注册服务时为此服务设备创建的虚拟端点的名称。请参见 创建服务定义和相应的虚拟端点 。
应用对象:	选择 PCG 的 Tier-0 网关。

- 3 选择新的策略，然后单击**添加规则**。请注意以下特定于服务插入的值：

选项	说明
源	选择必须重定向其流量的一组子网，例如，一组 NSX 管理工作负载虚拟机。
目标	选择要路由以通过服务设备的目标 IP 地址或服务列表，例如， Google 。
应用对象	选择主动和备用 PCG 的上行链路端口。
操作	选择 重定向 。

在 NSX 管理的虚拟机上启用 NAT

NSX Cloud 支持在 NSX 管理的虚拟机上启用 NAT。

可以使用公有云标记在 NSX 管理的虚拟机中启用南北向流量。

在要为其启用 NAT 的 NSX 管理的虚拟机上，应用以下标记：

表 22-14.

键	值
nsx.publicip	来自公有云的公共 IP 地址，例如，50.1.2.3

注 您在此处提供的公共 IP 地址必须可用，并且不能分配给任何虚拟机，甚至要为其启用 NAT 的工作负载虚拟机。如果分配以前与任何其他实例或专用 IP 地址关联的公共 IP 地址，则 NAT 将不起作用。在这种情况下，请取消分配公共 IP 地址。

应用此标记后，工作负载虚拟机可以访问 Internet 流量。

启用 Syslog 转发

NSX Cloud 支持 syslog 转发。

您可以为受管虚拟机上的分布式防火墙 (DFW) 数据包启用 syslog 转发。有关更多详细信息，请参见《NSX-T Data Center 故障排除指南》中的[配置远程日志记录](#)。

执行以下操作：

步骤

- 1 使用跳转主机登录到 PCG。
- 2 键入 **nsxcli** 以打开 NSX-T Data Center CLI。
- 3 键入以下命令以启用 DFW 日志转发：

```
nsx-public-cloud-gateway> set gw-controller vm-log-forwarding enabled
nsx-public-cloud-gateway> set logging-server <server-IP-address> proto udp level info
messageid FIREWALL-PKTLOG
```

进行此设置后，可从 PCG 的 `/var/logs/syslog` 下获取 NSX 代理 DFW 数据包日志。

- 4 要每个虚拟机启用日志转发，请输入以下命令：

```
nsx-public-cloud-gateway> set gw-controller vm-log-forwarding enabled <vm-id>
```

在 NSX 实施模式下设置 VPN

您可以使用在内部部署的 NSX-T Data Center 部署中显示为自动创建的 Tier-0 网关的 PCG 来设置 VPN。这些说明特定于在 NSX 实施模式下管理的工作负载虚拟机。

按照此处所述的其他步骤使用 PCG（与在 NSX Manager 中使用 Tier-0 网关一样）来设置 VPN。您可以在同一公有云或不同公有云中部署的 PCG 之间创建 VPN 隧道，或者在使用内部部署网关或路由器部署的 PCG 之间创建 VPN 隧道。有关 NSX-T Data Center 中 VPN 支持的详细信息，请参见第 5 章 [虚拟专用网络 \(VPN\)](#)。

前提条件

- 确认已在 VPC/VNet 中部署一个 PCG 或一个 PCG HA 对。
- 确认远程对等项支持基于路由的 VPN 和 BGP。

步骤

- 1 在公有云中，找到 PCG 的由 NSX 分配的本地端点，并根据需要为其分配公共 IP 地址：
 - a 转到公有云中的 PCG 实例，然后导航到“标记”。
 - b 记下 `nsx.local_endpoint_ip` 标记的值字段中的 IP 地址。

- c （可选）如果您的 VPN 隧道需要公共 IP，例如，如果要将 VPN 设置为另一个公有云或内部部署的 NSX-T Data Center 部署，请执行以下操作：
 - 1 导航到 PCG 实例的上行链路接口。
 - 2 将公共 IP 地址附加到您在步骤 **b** 中记录的 `nsx.local_endpoint_ip` IP 地址。
- d （可选）如果您具有 PCG 实例的 HA 对，请重复执行步骤 **a** 和 **b**，并根据需要附加公共 IP 地址（如步骤 **c** 中所述）。

- 2 在 NSX Manager 中，为显示为 Tier-0 网关（名称类似于 `cloud-t0-vpc/vnet-<vpc/vnet-id>`）的 PCG 启用 IPsec VPN，并在此 Tier-0 网关的端点与所需 VPN 对等项的远程 IP 地址之间创建基于路由的 IPsec 会话。有关其他详细信息，请参见[添加 IPsec VPN 服务](#)。

- a 转到**网络 > VPN > VPN 服务 > 添加服务 > IPsec**。提供以下详细信息：

选项	描述
名称	输入 VPN 服务的描述性名称，例如 <code><VPC-ID>-AWS_VPN</code> 或 <code><VNet-ID>-AZURE_VPN</code> 。
Tier-0/Tier-1 网关	在公有云中选择 PCG 的 Tier-0 网关。

- b 转到**网络 > VPN > 本地端点 > 添加本地端点**。提供以下信息，并查看[添加本地端点](#)以了解其他详细信息：

注 如果您具有 PCG 实例的 HA 对，请在公有云中使用已附加到每个实例的相应本地端点 IP 地址为每个实例创建一个本地端点。

选项	描述
名称	输入本地端点的描述性名称，例如 <code><VPC-ID>-PCG-preferred-LE</code> 或 <code><VNET-ID>-PCG-preferred-LE</code> 。
VPN 服务	选择您在步骤 2a 中创建的 PCG Tier-0 网关的 VPN 服务。
IP 地址	输入您在步骤 1b 中记录的 PCG 本地端点 IP 地址的值。

- c 转到**网络 > VPN > IPsec 会话 > 添加 IPsec 会话 > 基于路由**。提供以下信息，并查看[添加基于路由的 IPsec 会话](#)以了解其他详细信息：

注 如果要在 VPC 中部署的 PCG 与 VNet 中部署的 PCG 之间创建 VPN 隧道，则必须为 VPC 中每个 PCG 的本地端点和 VNet 中 PCG 的远程 IP 地址创建一个隧道，相反，从 VNet 中的 PCG 到 VPC 中 PCG 的远程 IP 地址亦是如此。您必须为活动 PCG 和备用 PCG 创建单独的隧道。这将在两个公有云之间生成全网状 IPsec 会话。

选项	描述
名称	输入 IPsec 会话的描述性名称，例如 <code><VPC-ID>-PCG1-to-remote_edge</code> 。
VPN 服务	选择在步骤 2a 中创建的 VPN 服务。
本地端点	选择在步骤 2b 中创建的本地端点。
远程 IP	输入要与其创建 VPN 隧道的远程对等项的公共 IP 地址。 注 远程 IP 可以是专用 IP 地址，前提是您能够访问该专用 IP 地址，例如使用 DirectConnect 或 ExpressRoute 进行访问。
隧道接口	以 CIDR 格式输入隧道接口。必须对远程对等方使用同一子网才能建立 IPsec 会话。

步骤 2a.

VPN 服务 IPSEC 会话 L2 VPN 会话 本地端点 配置文件

添加服务

名称	服务类型	Tier-0/Tier-1 网关	会话	状态
<VPC-ID>-AWS_VPN	IPSec	cloud-to-vpc-073617880a9622d93	1	成功
描述	VPN service on AWS Transit VPC vpc-073617880a9622d93	管理状态	已启用	
IKE 日志级别	信息	标记	0	
会话同步	已启用			
全局概览规则				

步骤 2b.

VPN 服务 IPSEC 会话 L2 VPN 会话 本地端点 配置文件

添加本地端点

名称	VPN 服务	IP 地址	站点证书	会话	状态
<VPC-ID>-PCG-preferred-LE	<VPC-ID>-AWS_VPN	10.99.3.35	未设置	1	成功
描述	未设置	本地 ID	10.99.3.35		
受信任的 CA 证书	未设置	证书吊销列表	未设置		
标记	0				

步骤 2c.

VPN 服务 IPSEC 会话 L2 VPN 会话 本地端点 配置文件

添加 IPSEC 会话

名称	类型	VPN 服务	本地端点	远程 IP	状态	警报
<VPC-ID>-PCG-to-remote_edge	基于路由	<VPC-ID>-AWS_VPN	<VPC-ID>-PCG-preferred-LE	3.213.92.220	已关闭	0
描述	未设置	管理状态	已启用			
合规性套件	无	隧道接口	192.168.50.10/24			
身份验证模式	PSK	远程 ID	172.0.3.145			
预共享密钥	*****					
高级属性						
IKE 配置文件	nsx-default-13vpn-ike-profile	连接启动模式	启动器			
IPSec 配置文件	nsx-default-13vpn-tunnel-profile	TCP MSS 限制	已禁用			

VPN 对等方的 IP 地址

查看统计信息 下载配置

刷新

第 1-1 项, 共 1 项 IPSEC 会话

3 在您在步骤 2 中建立的 IPsec VPN 隧道接口上设置 BGP 邻居。有关更多详细信息，请参见[配置 BGP](#)。

- a 导航到**网络 > Tier-0 网关**
- b 选择为其创建 IPsec 会话的自动创建的 Tier-0 网关，然后单击**编辑**。
- c 单击 **BGP** 部分下 **BGP 邻居** 旁边的编号或图标，并提供以下详细信息：

选项	描述
IP 地址	使用在 IPsec 会话中的隧道接口上为 VPN 对等项配置的远程 VTI 的 IP 地址。
远程 AS 编号	此编号必须与远程对等项的 AS 编号相匹配。

Tier-0 网关

添加网关

全部展开 按名称

	Tier-0 网关名称	HA 模式	已链接 Tier-1 网关	链接分段
>	多播			
▼	BGP			
	本地 AS	1000	服务路由期间 iBGP	● 开启
	BGP	● 开启	ECMP	● 开启
	平滑重启	仅帮助程序	多路径负载均衡	● 开启
	平滑重启定时器	180 秒	平滑重启失效定时器	600 秒
	路由聚合	0	BGP 邻居	

BGP 邻居

Tier-0 网关 cloud-t0-415...

#邻居 1

	IP 地址	BFD	远程 AS 编号
⋮ ▼	192.168.50.11	已禁用	1000
	源地址	未设置	
	最大跃点限制	1	

步骤 3.

- 4 使用重新分发配置文件通告要用于 VPN 的前缀。在 NSX 实施模式下，连接重新分发配置文件中启用了 Tier-1 的路由。

Tier-0 网关

添加网关 ▾ 全部展开 按名称、路径和其他

Tier-0 网关名称	HA 模式	已链接 Tier-1 网关	链接分段	状态 ⓘ
<div> <div>> BGP</div> <div> <div>▼ 路由重新分发</div> <div>路由重新分发</div> </div> </div>				
2 步骤 4	路由重新分发状态	● 开启		
<div> <div>⋮ > 🔍</div> <div>VRF TOrvf</div> </div>	主动-主动	0	0	● 成功

刷新

路由重新分发

Tier-0 网关 cloud-t0-vpc... #选定源 ⓘ

Tier-0 子网

已通告的 Tier-1 子网

- 已连接接口和分段
- 服务接口子网
- 已连接分段

常见问题解答 (FAQ)

本主题列出了一些常见问题及其解答。

我如何验证 NSX Cloud 组件是否已安装并正在运行？

- 1 要验证工作负载虚拟机上的 NSX Tools 是否已连接到 PCG，请执行以下操作：

- 键入 `nsxcli` 命令以打开 NSX CLI。
- 键入以下命令以获取网关连接状态，例如：

```
get gateway connection status
Public Cloud Gateway : nsx-gw.vmware.com:5555 Connection Status : ESTABLISHED
```

- 2 工作负载虚拟机必须具有正确的标记才能连接到 PCG：

- 登录到 AWS 控制台或 Microsoft Azure 门户。
- 验证虚拟机的 `eth0` 或接口标记。

`nsx.network` 键的值必须为 `default`。

我的通过使用云初始化脚本启动的虚拟机被隔离，且不允许安装第三方工具。我该怎么办？

启用隔离策略后，使用具有以下规范的云初始化脚本启动虚拟机时，则虚拟机将在启动时被隔离，并且您将无法在这些虚拟机上安装自定义应用程序或工具：

- 标记有 `nsx.network=default`
- 在虚拟机打开电源时自动安装或引导自定义服务

解决方案：

更新 `default` (AWS) 或 `default-vnet-<vnet-ID>-sg` (Microsoft Azure) 安全组，以添加安装自定义或第三方应用程序所需的入站/出站端口。

我已正确标记我的虚拟机并安装了 NSX Tools，但我的虚拟机被隔离。我该怎么办？

如果您遇到此问题，请尝试执行以下操作：

- 检查 NSX Cloud 标记 `nsx.network` 及其值 `default` 是否正确键入。应区分大小写。
- 从 CSM 重新同步 AWS 或 Microsoft Azure 帐户：
 - 登录到 CSM。
 - 转到云 > **AWS/Azure** > 帐户。
 - 从公有云帐户屏幕单击**操作**，然后单击**重新同步帐户**。

如果我无法访问我的工作负载虚拟机，该怎么办？

从公有云（AWS 或 Microsoft Azure）中：

- 1 确保虚拟机上的所有端口（包括由 NSX Cloud 管理的端口）、操作系统防火墙（Microsoft Windows 或 IPTables）和 NSX-T Data Center 正确配置为允许流量。

例如，要允许 ping 通虚拟机，需要正确进行以下配置：

- AWS 或 Microsoft Azure 上的安全组。有关详细信息，请参见使用 [NSX Cloud 隔离策略的威胁检测](#)。
 - NSX-T Data Center DFW 规则。请参见 [NSX 实施模式下 NSX 管理的工作负载虚拟机的默认连接策略](#)以了解详细信息。
 - Linux 上的 Windows 防火墙或 IPTables。
- 2 尝试使用 SSH 或其他方法（例如，Microsoft Azure 中的串行控制台）登录到虚拟机以解决该问题。
 - 3 可以重新引导锁定的虚拟机。
 - 4 如果仍无法访问该虚拟机，则将辅助网卡连接到要从中访问该工作负载虚拟机的工作负载虚拟机。

是否即使在云原生实施模式下仍需要使用 PCG？

是。

在 CSM 中载入我的公有云帐户后，是否可以更改 PCG 的 IAM 角色？

是。您可以重新运行适用于公有云的 NSX Cloud 脚本以重新生成 PCG 角色。在重新生成 PCG 角色后，在 CSM 中编辑您的公有云帐户以使用新的角色名称。在您的公有云帐户中部署的任何新 PCG 实例将使用新角色。

请注意，现有 PCG 实例继续使用旧 PCG 角色。如果要更新现有 PCG 实例的 IAM 角色，请转到公有云，然后手动更改该 PCG 实例的角色。

是否可以对 NSX Cloud 使用 NSX-T Data Center 内部部署许可证？

可以，但前提是您的 ELA 中具有相关条款。

VMware NSX® Intelligence™ 提供内部部署 NSX-T Data Center 环境的安全状态的可视化。该可视化基于特定时间段内汇总的网络流量流。此外，NSX Intelligence 还会根据安全策略实施分析提出建议，进而帮助您进行微分段规划。

重要事项 您必须具有企业管理员角色才能有权安装、配置和使用 NSX Intelligence。

您必须先安装并配置 NSX Intelligence 设备，然后才能开始使用 NSX Intelligence 功能。请参见 NSX-T Data Center 安装指南中的“安装和配置 NSX Intelligence 设备”。

本章讨论了以下主题：

- [NSX Intelligence 入门指南](#)
- [了解 NSX Intelligence 视图和流量](#)
- [使用 NSX Intelligence 建议](#)
- [备份和还原 NSX Intelligence](#)
- [解决 NSX Intelligence 问题](#)

NSX Intelligence 入门指南

要开始使用 NSX Intelligence 功能，请熟悉 NSX Intelligence 图形用户界面。

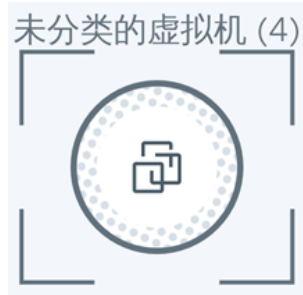
安装并配置 NSX Intelligence 设备后，在 NSX Manager UI 的**安全规划和故障排除**选项卡中启用 NSX Intelligence 功能。在**检测和安全规划**部分中，您可以使用**发现并执行操作**直观地显示 NSX-T Data Center 实体，并使用**建议**获取微分段规划建议。

NSX Intelligence 主页概览

要访问 NSX Intelligence 主页，请在 NSX Manager 用户界面中单击**安全规划和故障排除 > 发现并执行操作**。

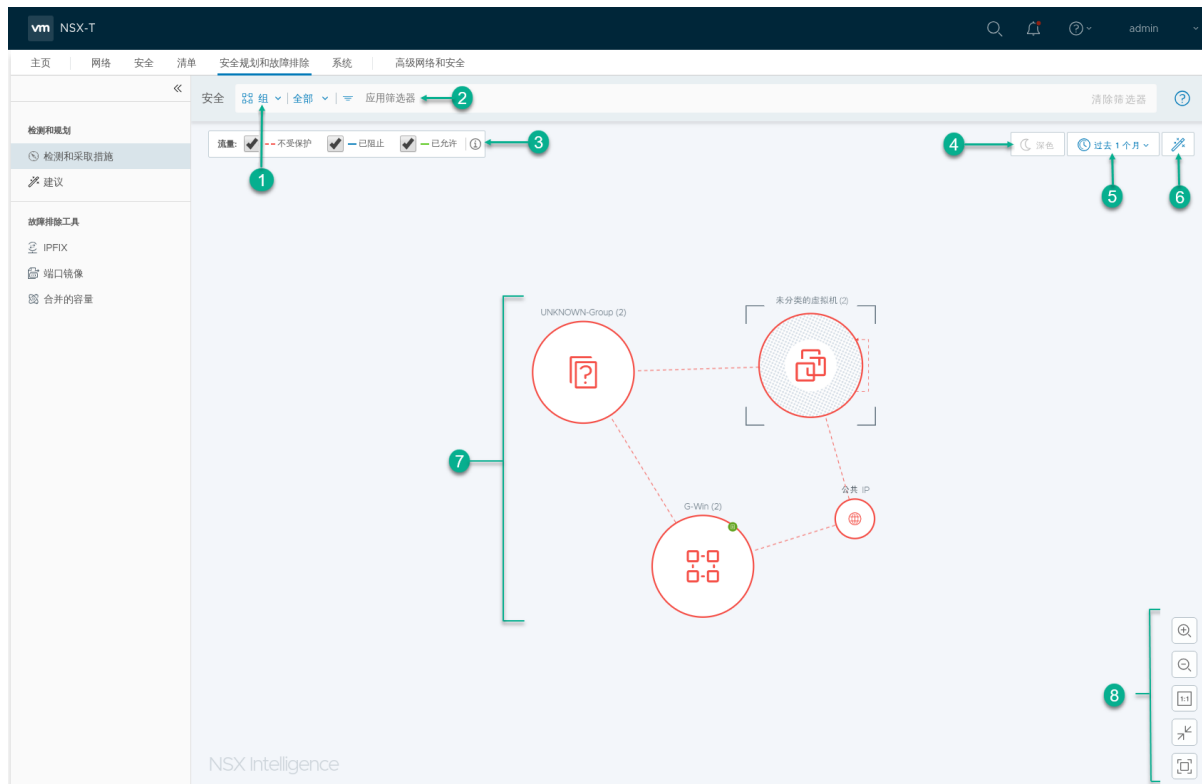
首次安装并配置 NSX Intelligence 后，在单击**发现并执行操作**时，您可能会看到找不到数据。您可能需要修改上面的筛选器 (No data found. You might need to modify your filters above) 消息。显示该消息是因为，NSX Intelligence 尚未收到用于创建可视化的网络流量数据。从 NSX Manager 收到一些网络流量数据后，NSX Intelligence 便可以开始呈现一些可视化。

默认情况下，在单击**发现并执行操作**时，您会看到内部部署 NSX-T Data Center 中的所有以下组的安全状态可视化：其虚拟机成员之间在过去 24 小时内发生不受保护的流量流。不受保护的流量流是指，未实施任何微分段的虚拟机之间的流。如果尚未定义组，则不会显示任何组。如果具有虚拟机，但它们不属于任何组，则会看到“未分类的虚拟机”组的以下图标。



如果已定义组，并且捕获了流量数据，则可能会看到类似于以下屏幕截图的可视化。后面的表格介绍了屏幕截图中的编号区域。

注 NSX Intelligence 将属于以下任一 CIDR 表示法的 IP 地址分类为专用 IP 地址：192.168.0.0/16、172.16.0.0/12 和 10.0.0.0/8。不属于其中任一 CIDR 表示法的任何 IP 地址均分类为公共 IP 地址。如果您的虚拟机的 IP 地址不属于其中任一 CIDR 表示法，请考虑使用《NSX-T Data Center API 指南》中的 PATCH /api/v1/intelligence/host-config API 添加 CIDR 表示法。



区域	说明
1	<p>“安全”视图选择区域是选择要显示的安全可视化类型的位置。共有两种类型的“安全”视图：组和虚拟机。在单击发现并执行操作时，显示的默认“安全”视图是 NSX-T Data Center 中在过去 24 小时内发生不受保护的流量流的组对象的“组”视图。</p> <ul style="list-style-type: none"> ■ 要选择“虚拟机”视图，请单击组旁边的向下箭头，然后选择虚拟机。 ■ 要选择在视图中包含的特定组或虚拟机，请单击全部旁边的向下箭头，然后从列表中进行选择。 ■ 要清除选择筛选器，请单击屏幕右上角的清除筛选器。在“虚拟机”视图中单击清除筛选器时，将清除选择筛选器并置于“组”视图中。 <p>有关如何使用这两种视图类型的更多信息，请参见使用“组”视图和使用“虚拟机”视图。</p>
2	<p>通过使用应用筛选器，您可以细化用于可视化的条件。从下拉列表中，您可以选择用于可视化的条件。您可以选择虚拟机成员、标记、流量类型、源 IP、目标 IP、规则 ID 或名称。您可以通过再次单击应用筛选器来定义多个要应用的筛选器。</p>
3	<p>在该流量区域中，您可以选择可视化在选定时间段内包含的流量流类型。此区域还显示了可视化中用于各种流量类型的颜色。</p> <ul style="list-style-type: none"> ■ 不受保护的流量用红色虚线表示 ■ 已阻止的流量用蓝色实线表示 ■ 已允许的流量用绿色实线表示 <p>默认情况下，将为当前 NSX Intelligence 可视化选择不受保护流量流类型。有关详细信息，请参见使用流量流。</p>
4	<p>显示模式区域定义要用于可视化的主题。默认使用“浅色”主题模式。</p> <ul style="list-style-type: none"> ■ 要使用深色主题模式，请单击深色图标。只有在以全屏模式查看可视化时，才能使用深色主题。 ■ 要进入全屏模式，请在查看控件区域中单击 。
5	<p>在该区域中，您可以选择相应的时间段，以用来确定使用哪些网络流数据生成所需的可视化和建议。您的选择将决定“组”或“虚拟机”视图中使用的历史数据。时间段是指相对于当前时间的过去某个时间段。</p> <p>默认使用“过去 24 小时”时间范围。要更改选择的时间段，请单击当前选择的时间段，然后选择过去 1 小时、过去 12 小时、过去 24 小时、过去 1 周或过去 1 个月。</p>
6	<p>在单击该建议魔法棒  图标时，“建议”对话框将显示当前视图的清单摘要。如果您位于“虚拟机”视图中，可通过单击启动新的建议来生成 NSX Intelligence 建议。请参见使用 NSX Intelligence 建议。</p>
7	<p>此区域是内部部署 NSX-T Data Center 中的组或虚拟机的安全状态的可视化。它还包括在选定时间段内出现的网络流量流的可视化。在此区域中，您可以指向某个特定节点或流量箭头以获取有关该特定实体的详细信息。</p> <p>有关更多信息，请参见熟悉 NSX Intelligence 图形元素和了解 NSX Intelligence 视图和流量。</p>
8	<p>该区域包含放大、缩小、应用 1:1 纵横比、调整大小以适合视图、进入或退出全屏查看模式的查看控件。您还可以使用键盘热键来管理查看控件。要显示“键盘快捷方式帮助”窗口，请按 Shift+/?。</p> <p>要导航到之前查看的可视化，请使用 Web 浏览器的“返回”按钮。处于全屏模式时，单击返回（位于屏幕左上角）可执行相同的返回导航操作。</p>

熟悉 NSX Intelligence 图形元素

NSX Intelligence 用户界面提供了多个图形元素，这些元素有助于直观显示 NSX-T Data Center 环境中的数据中心实体、流量流和特定活动。

下表列出了您可能在 NSX Intelligence 可视化中看到的各个 NSX-T Data Center 图形元素。

图形元素	说明
	该图标表示一个组，它是一组可以应用安全策略（包括东西向防火墙规则）的虚拟机。请参见 使用“组”视图 。
	该图标表示属于 NSX-T Data Center 的虚拟机 (VM)。一个虚拟机可以属于多个组。请参见 使用“虚拟机”视图 。
	该图标表示 Internet 中的公共 IP。如果您的 NSX-T Data Center 环境中的至少一个虚拟机在选定时间段内与一个公共 IP 进行通信，则在当前可视化中包含该流量流。
	在选定时间段内参与网络流量活动的 IP 地址，如单播、广播或多播 IP。
未分类的虚拟机 (4) 	该图标用于不属于任何组的一组虚拟机。
	箭头表示在选定时间段内两个虚拟机之间发生的网络流量流。共有三种不同类型的箭头：红色虚线箭头表示不受保护的流，蓝色箭头表示阻止的流，绿色箭头表示允许的流。请参见 使用流量流 。
	被选作当前主节点的节点将使用虚线圆圈圈起来。在显示选择模式和当前视图期间，该节点为固定节点。
	如果在选定时间段内将一个组添加到 NSX-T Data Center 清单中，则在该组节点的边框上显示该图标。如果 NSX-T Data Center 在选定时间段内发现一个虚拟机，则在该虚拟机节点的边框上显示该图标。
	如果在选定时间段内删除了组，但未删除虚拟机成员，则会在组节点的边框上显示该图标。在虚拟机节点的边框上，该图标表示在选定时间段内删除了虚拟机。尽管已删除某个虚拟机或组，但它仍会出现在当前可视化中，以指示在选定时间段内移除了该虚拟机或组。
	只要同时看到组和虚拟机，就会显示该图标。例如，在深入探讨组视图或组的相关虚拟机中。 在以下情况下，在虚拟机节点的边框上显示该图标。 <ul style="list-style-type: none"> ■ 如果在选定时间段内将虚拟机从当前查看的组中移出 ■ 如果虚拟机在选定时间段的某个时间点属于您当前查看的组，但它现在不再是该相同组的成员

了解 NSX Intelligence 视图和流量

NSX Intelligence 可视化包含组或虚拟机，以及这些组或虚拟机在选定时间段内发生的网络流量。

重要事项 显示的特定时间段的可视化表示该时间段内您的 NSX-T Data Center 中所发生的所有网络流量和活动，例如添加、删除或移动虚拟机和组。一个虚拟机可能会多次出现在可视化中。例如，如果一个虚拟机连接到最初未管理的 ESXi 主机，而该主机在选定时间段内改由 VMware vCenter Server™ 管理，该虚拟机将在“虚拟机”视图中出现两次。同样地，如果 ESXi 主机在同一选定时间段内断开连接然后重新添加到 vCenter Server，则连接到该主机的虚拟机在该选定时间段内将同时显示为“已删除”和“新建”。在“组”视图中，如果虚拟机在同一选定时间段内属于“未分类”组并添加到另一个组中，该虚拟机将同时显示在“未分类”组和新的组中。

NSX Intelligence 仅支持具有虚拟机成员类型的组。如果组具有任何其他类型的成员，“组”视图可能会显示具有虚拟机成员类型的组之间的关联流，而不是安全规则中的实际组。

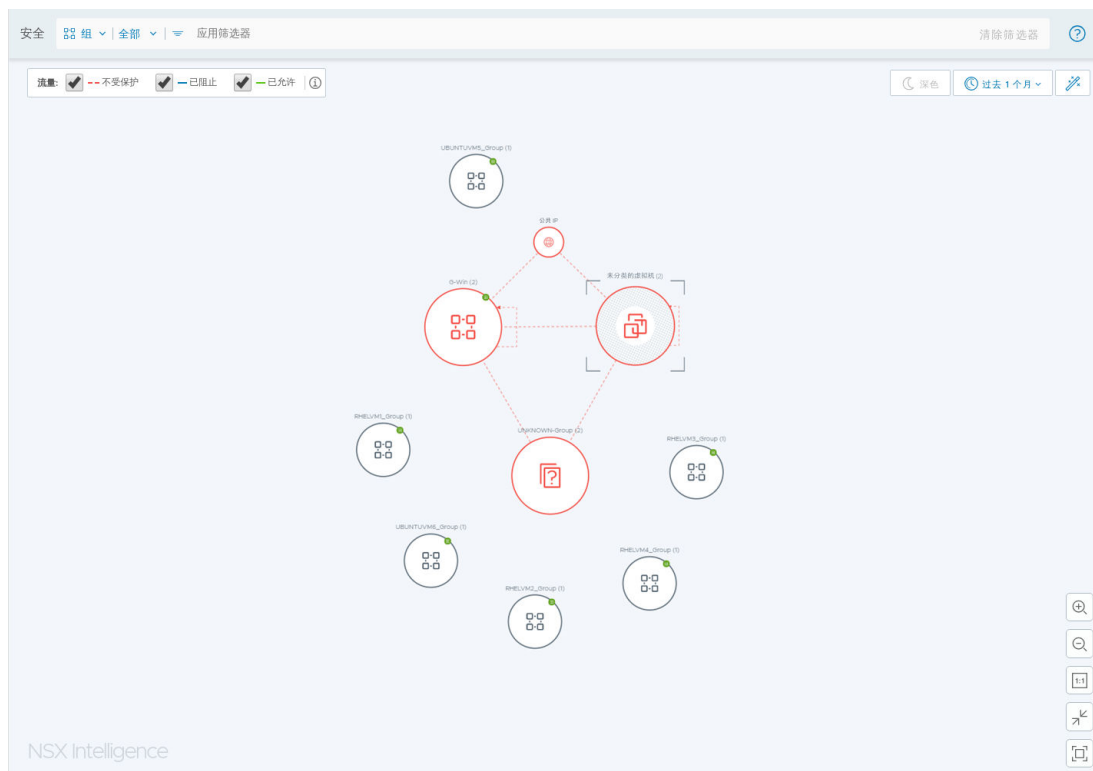
阅读本节内容，可了解有关如何使用“组”视图、“虚拟机”视图和不同流量类型的更多信息。

使用“组”视图





NSX Intelligence 主页中显示的默认视图是“组”视图。此“组”视图经过筛选，显示过去 24 小时内具有未受保护的流量流的所有组。

“组”视图中的节点和箭头

“组”视图中的节点表示您的 NSX-T Data Center 环境中的 NSX 对象，如虚拟机和 IP 集等。以下屏幕截图是一个“组”视图示例。



下表列出了您可能在“组”视图中看到的组节点类型。

组节点类型	图标	说明
常规组		NSX Intelligence 中的常规组节点表示您的 NSX-T Data Center 环境中的任何 NSX 对象集合。对于此版本，这些 NSX 对象仅为虚拟机，因此 NSX Intelligence 支持仅具有虚拟机成员类型的常规组。一个 NSX 对象可以属于多个组，因此，一个虚拟机可能会出现在多个组节点中。
未分类的组		未分类的组节点表示一组不属于任何组的虚拟机。
未知组		未知组节点表示在您的 NSX-T Data Center 清单中未找到的一组其他对象。但是，这些对象正在与您的 NSX-T Data Center 环境中的一个或多个 NSX 对象进行通信。
公共 IP 组		公共 IP 组节点表示与 NSX-T Data Center 中的 NSX 对象通信的一组公共 IP 地址（IPv4 或 IPv6）。

“组”视图中的节点大小基于属于该组的 NSX 对象（如虚拟机）数量。例如，组的节点越大，属于该组的虚拟机就越多。组的名称及其拥有的成员虚拟机数显示在节点上方。

组节点之间的箭头表示在选定时间段内这些相关联的组节点中的虚拟机之间所发生的流量流。组节点上的自引用箭头表示至少一个虚拟机以前与该相同组中的另一个虚拟机进行通信。有关详细信息，请参见[使用流量流](#)。

具有红色边框的节点表示与组中的一个虚拟机之间发生至少一个不受保护的流，而无论在选定时间段内检测到多少个阻止或允许的流。节点上的蓝色边框表示未检测到不受保护的流量流，但检测到至少一个阻止的流，而无论在选定时间段内检测到多少个允许的流量。具有绿色边框的节点表示在选定时间段内没有检测到不受保护或阻止的流，但检测到至少一个允许的流。具有灰色边框的节点表示在选定时间段内没有为属于该组的虚拟机检测到任何流量流。

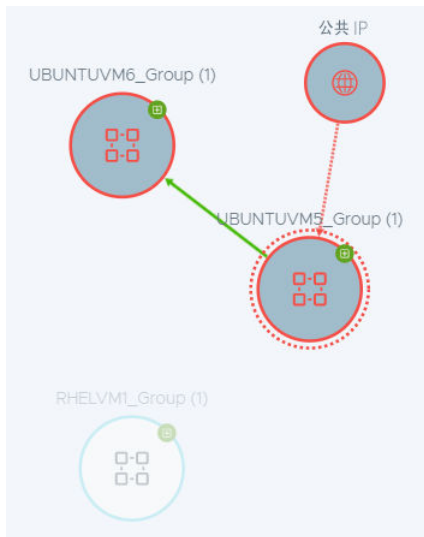
如果未看到“组”视图，请单击“安全”视图选择区域中的**虚拟机**旁边的向下箭头，然后选择**组**。在显示的选择下拉列表中，您可以从列表中选择**所有组**或特定组，然后单击**应用**。使用**搜索**文本框筛选选择列表。如果单击以离开选择下拉列表而未选择任何内容，或者在下拉列表中选择**所有组**，则会将**所有组**选项应用于“组”视图。

“组”视图中的节点选择

在指向某个组的节点时，将显示有关该组的信息，如以下示例中的 **G-Win** 组所示。还会列出在选定时间段内检测到的流数量和类型。如果组是在选定时间段内添加的，还会显示“新建”标志图标以及何时创建组的详细信息。



在单击某个组的节点时，将使用虚线圆圈将所选节点标记为固定的组节点。还会在视图中突出显示连接到选定组节点的其他组。所有其他节点将变灰。例如，在以下屏幕截图中，选择了 **UBUNTUVM5_Group** 节点，并且还突出显示在选定时间段内与 **UBUNTUVM5_Group** 共享流量流的其他组。未与 **UBUNTUVM5_Group** 通信的所有其他组将在视图中变灰。



要清除选择的固定节点，请单击“组”视图的任意空白区域。

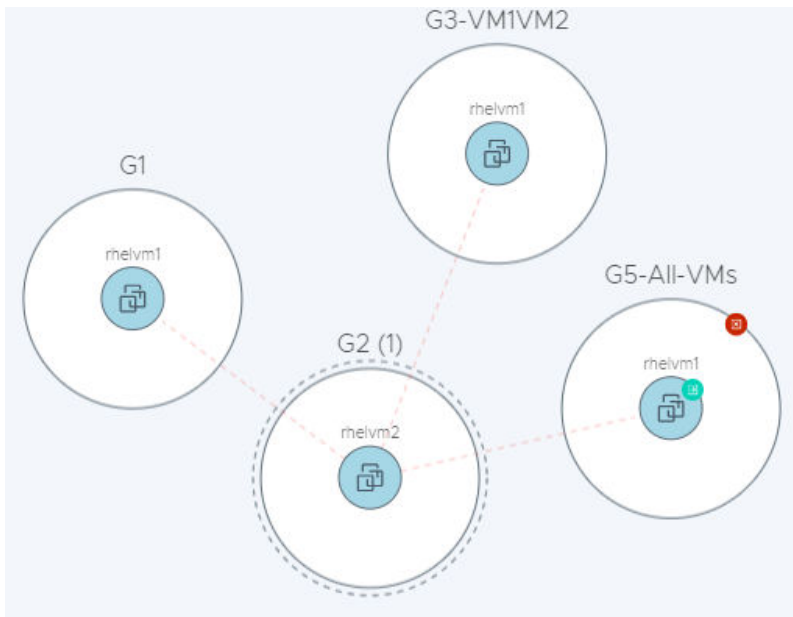
如果缩小“组”视图，并且节点上的详细信息不再可见，请指向节点的任意可见部分，即可显示其详细信息。

“组”视图中的可用操作

在右键单击组的节点时，将显示可用操作的上下文菜单，如下图中所示。



- 在选择**深入探讨: *Group_Name***时，将使用虚线圆圈圈住选定组的节点以将其标记为固定组节点或当前主节点。属于该组的虚拟机将显示在该组的节点中。在选定时间段内与固定组中的虚拟机之间发生流量流的所有组也会放在“组”视图中。在以下示例中，G2 组是固定组，并在视图中包含其他组，因为它们的虚拟机成员在选定时间段内与 G2 组中的 rhelvm2 之间发生流量流。



- 在选择**筛选方式**时，当前组将添加到用于当前“组”视图的可视化筛选器中。
- 在选择**虚拟机**时，将显示一个表，其中包含在选定时间段内属于当前组的所有虚拟机。从该“查看虚拟机”表中，您可以查看属于选定组的虚拟机以及每个虚拟机还属于的其他组的详细信息。要将虚拟机添加到当前可视化筛选器中，请单击筛选器图标。
- 在选择**流量详细信息**时，将显示当前选择的组的“流量详细信息”表，如以下屏幕截图中所示。它显示有关在选定时间段内与属于当前组的虚拟机之间已发生和当前正在发生的流的详细信息。详细信息包括流类型、流的源和目标组、流的开始和结束时间以及使用的服务。您可以单击某些详细信息以获取更多信息。有关详细信息，请参见[使用流量流](#)。

流量详细信息
过去 24 小时

显示 未分类的虚拟机 的流量详细信息

完成的流量
活动流

搜索

源	源组	目标	目标组	服务	结束时间	最新流量
ubuntu12.04.1-2G-LA...	G5	ubuntu12.04-pa...	UNCATEGORIZED	SSH... + 另外 2 项	2019/11/6 下午4:05	● 不受保护
ubuntu12.04.1-2G-LA...	G1	ubuntu12.04-pa...	UNCATEGORIZED	SSH... + 另外 2 项	2019/11/6 下午4:05	● 不受保护

刷新

1 - 2 of 2 流量

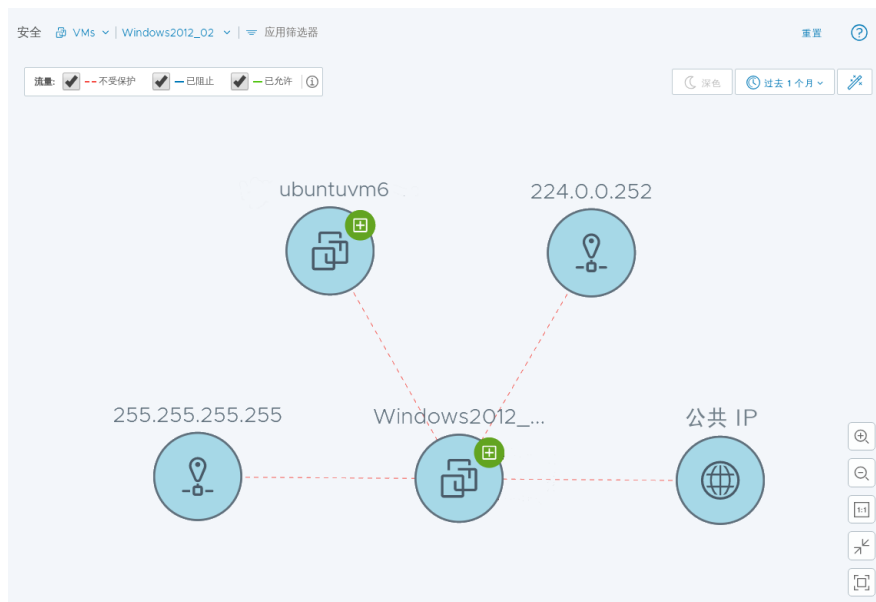
关闭

使用“虚拟机”视图

“虚拟机”视图中的节点表示您的内部部署 NSX-T Data Center 环境中的虚拟机 (VM)。

“虚拟机”视图中的节点和箭头

位于“虚拟机”视图中时，组边界不可见。如果任何节点与您的 NSX-T Data Center 环境中的某个虚拟机通信，但未被标识为 NSX-T Data Center 清单的一部分，则也会在“虚拟机”视图中显示该节点。以图展示了一个简单的“虚拟机”视图。



下表列出了您可能在“虚拟机”视图中看到的虚拟机节点类型。

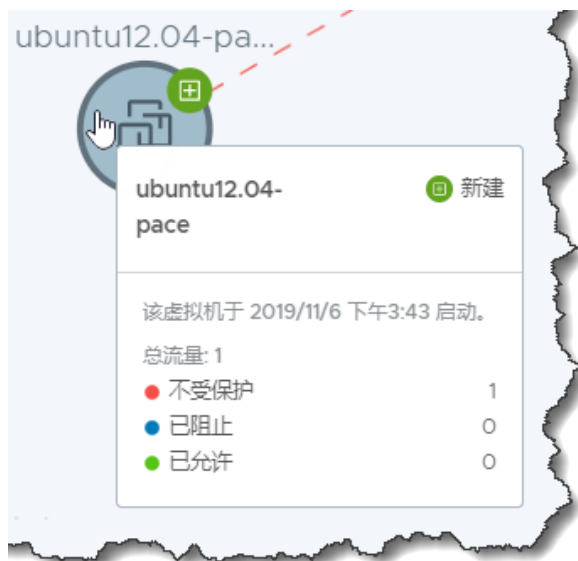
虚拟机节点类型	图标	说明
常规虚拟机		常规虚拟机节点表示属于您的 NSX-T Data Center 环境的虚拟机 (VM)。一个虚拟机可以属于多个组。
公共 IP		公共 IP 节点表示与您的 NSX-T Data Center 环境之间通信的公共 IP 地址 (IPv4 或 IPv6)。
IP		IP 节点表示在选定时间段内参与网络流量活动的 IP 地址。IP 地址可以是单播、广播或多播 IP。

如果未看到“虚拟机”视图，请单击“安全”视图选择区域中的**组**旁边的向下箭头，然后选择**虚拟机**。在显示的选择下拉列表中，您可以从列表中选择**所有虚拟机**或特定虚拟机，然后单击**应用**。使用**搜索**文本框筛选选择列表。如果单击以离开下拉列表而未选择任何内容，或者在下拉列表中选择**所有虚拟机**，则会将**所有虚拟机**选项应用于“虚拟机”视图。

虚拟机节点之间的箭头表示虚拟机之间在选定时间段内发生的流量流。有关详细信息，请参见[使用流量流](#)。

“虚拟机”视图中的节点选择

在指向某个虚拟机节点时，将显示有关该节点的信息，如下示例中所示。还会列出在选定时间段内检测到与虚拟机之间发生的流数量和类型。如果虚拟机是在选定时间段内添加的，还会显示“新建”标志图标以及何时添加虚拟机的详细信息。



单击某个虚拟机的节点时，会用虚线圆圈将选定节点标记为固定的虚拟机节点。“虚拟机”视图中还会突出显示与该固定虚拟机节点发生流量往来的其他虚拟机节点。所有其他节点将变灰，以使其不可见。要清除选择的固定节点，请单击“虚拟机”视图中的任意空白区域。

如果缩小“虚拟机”视图，并且虚拟机节点中的详细信息不再可见，请指向虚拟机节点的任意可见部分，即可显示其详细信息。

“虚拟机”视图中的可用操作

右键单击某个虚拟机的节点时，会显示可用操作的上下文菜单，如下图所示。



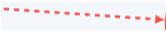


选择内容	说明
筛选方式	虚拟机将添加到用于当前“虚拟机”视图的可视化筛选器中。
虚拟机信息	显示在选定时间段内的虚拟机详细信息。
相关组	“组”表并包含有关虚拟机在选定时间段内所属的组的信息。
流量详细信息	<p>显示有关在选定时间段内与虚拟机之间已发生和当前正在发生的流的详细信息。这些详细信息包括以下各项。</p> <ul style="list-style-type: none">■ 流量类型■ 流量的源组和目标组■ 流量的开始时间和结束时间■ 使用的服务 <p>您可以单击某些详细信息以获取更多信息。有关详细信息，请参见使用流量流。</p>
启动建议	显示“启动新的建议”向导。有关更多详细信息，请参见 使用 NSX Intelligence 建议 。

使用流量流

组或虚拟机节点之间的箭头表示在选定时间段内虚拟机之间发生的网络流量流。

网络流量流基于采用的 L3 分布式防火墙 (DFW) 规则以及在选定时间段内发生的流量流。将在可视化和流详细信息中包含与使用 IPv4 或 IPv6 以及 TCP、UDP、GRE、ESP 和 SCTP 协议的有状态 L3 DFW 规则匹配的所有网络流量流。TCP 和 UDP 流具有 IP 和端口级别详细信息，而其他流仅具有 IP 级别详细信息。

流量流分为以下类型。

流量类型	图形	说明
不受保护		红色虚线箭头表示系统检测到流量流符合一个规则（源：任意 目标：任意 操作：允许、拒绝或丢弃），并需要使用更精细的安全策略。该规则可能是默认规则，也可能位于东西向分布式防火墙中的任意位置。
已阻止		蓝色实线箭头表示系统检测到流量流符合“拒绝”或“丢弃”规则，该规则比“不受保护”流定义中提到的规则更精细。
已允许		绿色实线箭头表示系统检测到流量流符合“允许”规则，该规则比“不受保护”流定义中提到的规则更精细。

要仅关注具有某些类型的流量流的对象，请使用“安全”视图选择区域选择视图类型，并使用“流量类型”筛选器属性缩小选择范围。

如果取消选择某种流类型，则会从显示的图形中隐藏该流类型的流线。除非生效的筛选器排除某些对象，否则，所有组或虚拟机对象都会保持显示状态，而无论这些对象在选定时间段内发生何种类型的流量流。例如，如果取消选择“已允许”流类型，则在图形中隐藏所有“已允许”流线。但仍会显示所有对象，甚至是在选定时间段内仅具有“已允许”流量流的对象。

流量箭头的方向表示检测到的流量流的源和目标。在位于“组”视图时，组节点上的自引用箭头表示至少一个虚拟机以前与该相同组中的另一个虚拟机进行通信。在“虚拟机”视图中，自引用箭头表示虚拟机中的 NSX 对象与同一虚拟机中的另一个 NSX 对象进行通信。

当您指向某个流量箭头时，将显示与涉及组或虚拟机的流量有关的信息，如以下示例中组 G2 所示。



在单击流箭头时，将显示“流量详细信息”对话框。该对话框中显示与选定时间段内已完成流量和活动流量相关的详细信息。要获取有关流的源、目标、服务类型以及流类型的更多信息，请单击表中的链接以查看更多信息。

使用 NSX Intelligence 建议

NSX Intelligence 可以提供微分段建议，这些建议基于选定时间段内 NSX-T Data Center 环境中虚拟机之间发生的流量模式。

了解 NSX Intelligence 建议

NSX Intelligence 生成的建议包括应用程序的安全策略、策略安全组和服务。

这些建议基于由 vCenter Server 管理的 ESXi 主机上虚拟机工作负载之间的网络通信流量模式。这些建议可以通过关联您 NSX-T Data Center 环境中已发生的通信流量模式，来帮助您实施更动态的安全策略。

安全策略建议是应用程序类别的东西向分布式防火墙安全策略。安全组建议由一组在指定时间段和虚拟机边界内出现在所分析网络流量中的虚拟机组成。服务建议是由指定虚拟机中应用程序在某些端口中使用的服务对象，但这些服务尚未在 NSX-T Data Center 清单中定义。

请求建议的方法有多种，但最简单的方法是使用**安全规划和故障排除 > 建议**选项卡，然后单击**启动新的建议**。您需要提供构成应用程序边界的虚拟机 (VM)，以及分析这些特定虚拟机的网络流量时要采用的时间范围。建议分析完成后，您可以查看建议的详细信息，并根据需要在建议发布之前对其进行修改。有关详细信息，请参见生成新的 **NSX Intelligence 建议**。

生成新的 NSX Intelligence 建议

NSX Intelligence 建议功能可为您提供建议，帮助您对应用程序进行微分段。

生成 NSX Intelligence 建议涉及应用程序的安全策略建议、策略安全组建议和服务建议。建议基于 NSX-T Data Center 中虚拟机之间的通信流量模式。使用 NSX Intelligence UI 生成建议的方法有多种。以下过程介绍了三种可使用的方法。

前提条件

安装 NSX Intelligence。请参见 NSX-T Data Center 安装指南中的“安装和配置 NSX Intelligence”。

步骤

- 1 从浏览器中，使用企业管理员权限登录到 NSX Manager (<https://<nsx-manager-ip-address>>)。
- 2 启动新建议的生成过程。

通过下表可确定要使用三种可用方法中的哪一种。

方法	步骤
选择 安全规划和故障排除 > 建议 。	单击 启动新的建议 。
在“虚拟机”视图中，选择一个虚拟机，然后单击鼠标右键。	从上下文菜单中，选择 启动新的建议 。
选择 安全规划和故障排除 > 发现并执行操作 。	<ol style="list-style-type: none"> 1 在“安全状态”筛选器中，单击向下箭头，然后选择虚拟机。 2 选择构成应用程序边界的虚拟机，然后单击应用。 3 单击建议魔法棒图标 。 4 在“建议”对话框中，单击启动新的建议。

- 3 在“启动新的建议”向导中，可以选择更改**建议名称**的默认值。
- 4 定义或修改将用作安全策略建议边界的虚拟机。
 - a 单击**选择虚拟机**或**选定的虚拟机**数量。
 - b 在“选择虚拟机”对话框中，选择要用作分析边界的虚拟机，然后取消选择不希望包含在内的虚拟机。
 您最多可以选择 100 个要用于建议边界的虚拟机。您还可以开始在选择栏中输入名称，以筛选要选择的虚拟机。
 - c 单击**保存**。
 选定的虚拟机数量将显示在“发现新建议”对话框中。
- 5 展开**更多选项**，以更改用于建议分析的**描述**和**时间范围**的默认值。默认**时间范围**值为“过去 1 个月”，这意味着在建议分析期间使用上个月在选定虚拟机之间发生的网络流量流。

6 单击启动发现。

建议是按顺序处理的。平均来说，完成每个建议可能需要 3 到 4 分钟，具体取决于是否还有其他待处理的建议。如果必须分析在虚拟机之间发生的很多流量流，建议的生成时间可能需要 10-15 分钟。可以从[建议](#)选项卡跟踪状态。状态从正在等待变为正在分析，并最后变为准备发布。以下屏幕截图显示了所生成建议的三种不同状态。

	名称	状态	虚拟机	创建时间	上次修改时间
>	REC 20191107 10:09:19	无可用建议	6	2019/11/7 上午2:09	2019/11/7 上午2:09
>	REC 20191106 16:39:30	无可用建议	1	2019/11/6 上午8:39	2019/11/6 上午8:39
>	REC 20191106 16:15:53	无可用建议	1	2019/11/6 上午8:16	2019/11/6 上午8:16

建议在成功发布之后，状态将变为“已发布”。

后续步骤

查看生成的建议并确定是否发布该建议。请参见[查看并发布生成的建议](#)。

查看并发布生成的建议

生成的 NSX Intelligence 建议达到“准备发布”状态后，您可以查看建议，根据需要进行修改，并决定是否发布该建议。

前提条件

生成新的建议。请参见[生成新的 NSX Intelligence 建议](#)。

步骤

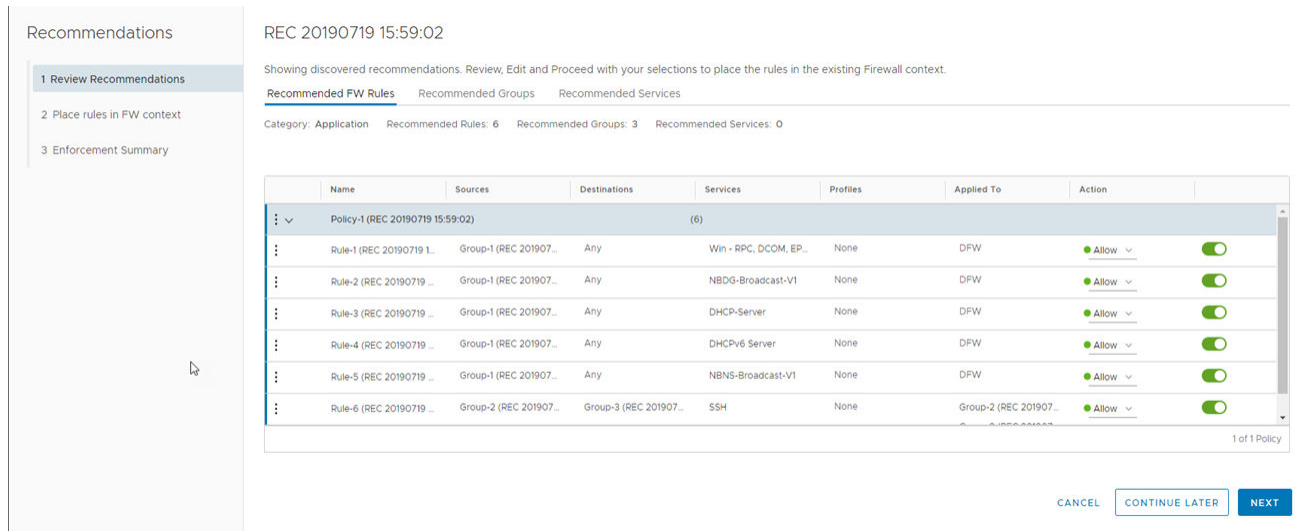
- 1 从浏览器中，使用企业管理员权限登录到 NSX Manager (<https://<nsx-manager-ip-address>>)。
- 2 单击[安全规划和故障排除 > 建议](#)。
- 3 要帮助缩小显示的建议列表，请单击屏幕右上角的[按名称、路径或其他内容筛选](#)，然后指定要使用的筛选条件。
- 4 如果决定不使用建议，请单击三点菜单图标，然后选择[删除](#)。
- 5 要查看建议的摘要，请单击建议名称旁边的箭头以展开该行。

将会看到生成的规则数以及受影响的组数。

6 查看并管理建议的详细信息。

a 单击建议的名称。

将显示类似于下图的**建议**向导。



b 在**建议的防火墙规则**选项卡中，查看防火墙规则详细信息。要修改任何详细信息，请单击相应列中的值，然后选择编辑（铅笔）图标。

c 要定义数据包的处理方式，请在**操作**列中选择**允许**、**丢弃**或**拒绝**。

d 切换右侧的按钮以启用或禁用该规则。默认情况下，生成的规则设置为发布时启用，如上一步中的图像所示。

e 单击**建议的组**。

f 单击**成员**列中的链接，以查看有关为组建议设置的虚拟机和 IP 的详细信息。

g 单击组名称旁边的菜单图标（三个点），然后选择**编辑**以修改组建议。

h 单击**建议的服务**并查看详细信息。

i 单击服务名称旁边的菜单图标（三个点），然后选择**编辑**以修改名称或说明。在删除某个服务之前，请确保没有使用该服务的规则。

j 单击**下一步**。

7 在**将规则放置在防火墙上下文中**窗格中，您可以更改将规则建议应用于现有防火墙规则的顺序。拖动突出显示的部分，或单击三个点菜单图标，然后选择**移到选定区域上方**或**移到选定区域下方**。

8 单击**发布**。

9 在**发布建议**对话框中，单击**是**。

10 在“实施摘要”页面中，确认安全策略已成功发布，然后单击**关闭**。

建议表中该建议的“状态”列已更改为“已发布”。

结果

安全策略建议成功发布后，它们在[安全规划和故障排除 > 建议](#)选项卡中将处于只读模式。要查看和管理已发布的规则建议，请转到[安全 > 分布式防火墙](#)。

重要事项 在发布规则建议后，可视化继续将虚拟机之间的受影响的流显示为橙色箭头（不受保护的流），直到在受影响的虚拟机之间生成新的流。可视化仅根据在主机上发生的时间报告流量流，而不反映在这些流量流发生后发布的规则集。在发布规则集并生成新的流量流后，新流将显示为绿色箭头（允许的流）。

备份和还原 NSX Intelligence

如果您当前的 NSX Intelligence 配置变得无法运行，或者如果要将其还原到以前的状态，则可以从备份还原您的配置。只能通过 NSX Intelligence CLI 来支持备份和还原工作流。

执行备份时，NSX Intelligence 只备份由包含 NSX Intelligence 设备的所有服务使用的配置文件。备份中不包含可视化数据。

如果 NSX Intelligence 中发生数据丢失或损坏，相关流量和建议的所有现有数据也将丢失。重新安装 NSX Intelligence 将重新开始收集网络流量数据，并从该点开始可以对收集的数据进行可视化。

完成备份配置后，您可以随时在 NSX Intelligence 设备上手动运行备份命令。备份将进行加密和压缩，并存储在备份配置过程中定义的远程服务器上。创建备份时，执行备份的日期和时间将附加到备份文件名中，以便每个备份文件都是唯一的。例如，config-backup-2019-06-21T21_06_07UTC.tar.gz。

在还原 NSX Intelligence 备份时，会还原捕获备份时的配置状态。要将备份还原到某个 NSX Intelligence 设备，该设备运行的 NSX Intelligence 设备版本必须与创建备份文件时所用的设备版本相同。您可以还原到现有的 NSX Intelligence 设备，也可以还原到全新安装的 NSX Intelligence 设备，但这些设备的版本必须与您备份的 NSX Intelligence 设备相同。

配置 NSX Intelligence 备份

您必须先配置备份文件服务器，然后才能对 NSX Intelligence 配置进行备份。配置备份文件服务器后，您可以随时对 NSX Intelligence 进行备份。

前提条件

- 确认您具有 NSX Intelligence CLI 的 CLI 管理员凭据。
- 确保您具有远程服务器的用户名和密码。
- 获取备份文件在远程服务器中的存储位置的文件路径。

步骤

- 1 从命令行提示符中，使用管理员特权登录到 NSX Intelligence CLI 主机。

```
$ ssh admin@cli-ip-address
admin@cli-ip-address's password:
```


2 配置备份文件服务器。

命令语法为

```
set backup remote-host remote_host_address remote-path remote_folder_path remote-host-username remote_host_username remote-host-password remote_host_password passphrase pass_phrase
```

其中, `remote_host_address` 是备份文件服务器的远程主机 IP 或 FQDN 地址, 并且 `remote_host_username` 帐户必须具有在 `remote_folder_path` 中创建备份文件所必需的特权。您必须为 `passphrase` 参数提供一个强值。该值的长度必须至少为八个字符, 且至少包含一个大写字母、一个小写字母和一个特殊字符。例如,

```
set backup remote-host 10.11.22.33 remote-path /root remote-host-username root remote-host-password MyRemotePassword passphrase MyPassPhra$e
```

3 确认配置。

```
get configuration
```

从输出中, 确认包含 `set backup` 的行正确无误。如果使用上一步中的示例, 输出必须包含以下行。

```
set backup remote-host 10.11.22.33 remote-path /root remote-host-username root
```

备份 NSX Intelligence

您可以使用 CLI 命令备份您的 NSX Intelligence 设备配置文件。

前提条件

- 确保您拥有对 NSX Intelligence CLI 的管理员访问权限。
- 配置备份文件服务器。请参见[配置 NSX Intelligence 备份](#)。

步骤

- 1 使用管理员特权登录到 NSX Intelligence CLI。
- 2 创建备份。

```
backup intelligence configuration
```

如果备份成功, 您将看到类似以下内容的消息。

```
Backup Complete. Archived at: backup_file_server-IP_address:/root/backup_archives/intelligence-config-backup-2019-07-18T07_00_26UTC.tar.gz
```

- 3 您可以使用另一个 CLI 会话来查看备份进度。
 - a 登录到另一个 NSX Intelligence CLI 会话。
 - b 输入以下命令。

```
get log-file node-mgmt.log follow
```

还原 NSX Intelligence 备份

还原备份时，将还原 NSX Intelligence 配置在进行备份时的状态。您可以使用 CLI 命令还原 NSX Intelligence 备份。

要在某个安装的 NSX Intelligence 设备上还原备份，该设备的版本必须与要还原的备份相同。默认情况下，所还原的备份文件是最近生成的备份。如果要将备份还原到新安装的 NSX Intelligence 设备，请在还原备份之前设置存档名称。

前提条件

- 确认您具有备份文件服务器的管理员登录凭据和主机信息。
- 确保您拥有对 NSX Intelligence CLI 的管理员访问权限。

步骤

- 1 使用管理员特权登录到新的 NSX Intelligence CLI 服务器。
- 2 配置备份所在的远程服务器。

命令语法为

```
set restore remote-host backup_server_IP_address remote-path remote_folder_path remote-
host-username remote_host_username remote-host-password remote_host_password passphrase
pass_phrase
```

其中，backup_server_IP_address 是备份文件服务器的远程主机 IP 或 FQDN 地址，remote_host_username 帐户必须具有在 remote_folder_path 中访问备份文件所需的特权。例如，

```
set restore remote-host 10.11.22.33 remote-path /root remote-host-username root remote-
host-password MyRemotePassword passphrase MyPassPhra$e
```

- 3 确认还原配置。

```
get configuration
```

从输出中，确认包含 set restore 的行正确无误。如果使用上一步中的示例，输出必须包含以下行。

```
set restore remote-host 10.11.22.33 remote-path /root remote-host-username root
```

4 使用以下命令还原备份。

```
restore intelligence configuration
```

如果还原成功，您将看到类似以下内容的消息。

```
NSX Intelligence Restore Complete.
```

5 您可以使用另一个 CLI 会话来查看备份还原进度。

- a 登录到另一个 NSX Intelligence CLI 会话。
- b 输入以下命令。

```
get log-file node-mgmt.log follow
```

解决 NSX Intelligence 问题

如果 NSX Intelligence 设备停止响应，或者您需要了解在使用设备时收到的错误消息的更多详细信息，您可以运行特定的命令以获取 NSX Intelligence 服务的状态。

您还可以收集支持包，以帮助您和 VMware 支持人员调试您可能遇到的问题。

检查 NSX Intelligence 设备的状态

如果 NSX Intelligence 设备停止响应，请检查 NSX Intelligence 服务的状态。

问题

NSX Intelligence 设备已停止响应，或者您收到一条错误消息，指示设备无法正常工作。

原因

一个或多个底层 NSX Intelligence 服务可能已停止或未处于正常运行状态。

解决方案

- 1 使用具有企业管理员角色的帐户登录到 NSX Intelligence 设备 CLI 主机。
- 2 使用 `get services` 命令检查 NSX Intelligence 服务的状态。

如果所有 NSX Intelligence 服务正常工作，则会看到类似于以下示例的输出。

```
my_nsx-intel> get services
Service name:          druid
Service state:         running
Coordinator health:    good
Broker health:         good
Historical health:     good
Overlord health:       good
MiddleManager health:  good

Service name:          http
Service state:         running
```

```

Session timeout:          1800
Connection timeout:       30
Redirect host:            (not configured)
Client API rate limit:    100 requests/sec
Client API concurrency limit: 40
Global API concurrency limit: 199

Service name:             kafka
Service state:            running
Service health:           good

Service name:             liagent
Service state:            stopped

Service name:             mgmt-plane-bus
Service state:            stopped

Service name:             node-mgmt
Service state:            running

Service name:             nsx-config
Service state:            running

Service name:             nsx-message-bus
Service state:            stopped

Service name:             nsx-upgrade-agent
Service state:            running

Service name:             ntp
Service state:            running
Start on boot:            True

Service name:             pace-server
Service state:            running

Service name:             postgres
Service state:            running
Service health:           good

Service name:             processing
Service state:            running

Service name:             snmp
Service state:            stopped
Start on boot:            False

Service name:             spark
Service state:            running
Service health:           good

Service name:             spark-job-scheduler
Service state:            running

Service name:             ssh

```

```

Service state:          running
Start on boot:         True

Service name:          syslog
Service state:         running

Service name:          ui-service
Service state:         running

Service name:          zookeeper
Service state:         running
Service health:        good

my_nsx-intel>

```

服务状态可能是 running 或 stopped。服务运行状况可能是 good 或 degraded。

- 您还可以查看 syslog 文件，并搜索将 NSX Intelligence 服务运行状况记录到 syslog 文件的 pace-monitor.sh 运行状况检查脚本的输出。

如果所有服务正常工作，在运行 `get log-file syslog | find pace-monitor` 命令后，看到的输出类似于以下示例输出。

```

my_nsx-intel> get log-file syslog | find pace-monitor
<13>1 2019-08-30T03:19:20.409899+00:00 my_nsx-intel pace-monitor.sh - - - "_self": {
<13>1 2019-08-30T03:19:20.410253+00:00 my_nsx-intel pace-monitor.sh - - -   "href": "/"
node/pace/appliance-health",
<13>1 2019-08-30T03:19:20.410623+00:00 my_nsx-intel pace-monitor.sh - - -   "rel":
"self"
<13>1 2019-08-30T03:19:20.410908+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.411162+00:00 my_nsx-intel pace-monitor.sh - - - "appliance-
health": {
<13>1 2019-08-30T03:19:20.411416+00:00 my_nsx-intel pace-monitor.sh - - -   "status":
"Following NSX Intelligence first boot services are either PENDING or FAILED - Token-
Registration",
<13>1 2019-08-30T03:19:20.411668+00:00 my_nsx-intel pace-monitor.sh - - -   "sub-system-
status": {
<13>1 2019-08-30T03:19:20.411923+00:00 my_nsx-intel pace-monitor.sh - - -     "app-
services": {
<13>1 2019-08-30T03:19:20.412280+00:00 my_nsx-intel pace-monitor.sh - - -     "services": [],
<13>1 2019-08-30T03:19:20.412528+00:00 my_nsx-intel pace-monitor.sh - - -     "status": ""
<13>1 2019-08-30T03:19:20.412807+00:00 my_nsx-intel pace-monitor.sh - - -   },
<13>1 2019-08-30T03:19:20.413075+00:00 my_nsx-intel pace-monitor.sh - - -   "base-
infra-services": {
<13>1 2019-08-30T03:19:20.413303+00:00 my_nsx-intel pace-monitor.sh - - -     "services": [
<13>1 2019-08-30T03:19:20.413613+00:00 my_nsx-intel pace-monitor.sh - - -       {
<13>1 2019-08-30T03:19:20.413848+00:00 my_nsx-intel pace-monitor.sh - - -     "druid-health": {
<13>1 2019-08-30T03:19:20.414146+00:00 my_nsx-intel pace-monitor.sh - - -     "broker": "good",
<13>1 2019-08-30T03:19:20.414473+00:00 my_nsx-intel pace-monitor.sh - - -

```

```

"coordinator": "good",
<13>1 2019-08-30T03:19:20.414717+00:00 my_nsx-intel pace-monitor.sh - - -
"historical": "good",
<13>1 2019-08-30T03:19:20.414979+00:00 my_nsx-intel pace-monitor.sh - - -
"middlemanager": "good",
<13>1 2019-08-30T03:19:20.415295+00:00 my_nsx-intel pace-monitor.sh - - -
"overlord": "good"
<13>1 2019-08-30T03:19:20.415533+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.415762+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "druid"
<13>1 2019-08-30T03:19:20.415982+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.416269+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.416539+00:00 my_nsx-intel pace-monitor.sh - - -
"health": "good",
<13>1 2019-08-30T03:19:20.416772+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "kafka"
<13>1 2019-08-30T03:19:20.416991+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.417204+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.417510+00:00 my_nsx-intel pace-monitor.sh - - -
"health": "good",
<13>1 2019-08-30T03:19:20.417745+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "postgres"
<13>1 2019-08-30T03:19:20.418133+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.418389+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.418626+00:00 my_nsx-intel pace-monitor.sh - - -
"health": "good",
<13>1 2019-08-30T03:19:20.418855+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "spark"
<13>1 2019-08-30T03:19:20.419157+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.419435+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.419684+00:00 my_nsx-intel pace-monitor.sh - - -
"health": "good",
<13>1 2019-08-30T03:19:20.419928+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "zookeeper"
<13>1 2019-08-30T03:19:20.420165+00:00 my_nsx-intel pace-monitor.sh - - - }
<13>1 2019-08-30T03:19:20.420496+00:00 my_nsx-intel pace-monitor.sh - - - ],
<13>1 2019-08-30T03:19:20.420786+00:00 my_nsx-intel pace-monitor.sh - - -
"status": ""
<13>1 2019-08-30T03:19:20.421022+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.421255+00:00 my_nsx-intel pace-monitor.sh - - - "first-
boot-services": {
<13>1 2019-08-30T03:19:20.421539+00:00 my_nsx-intel pace-monitor.sh - - -
"services": [
<13>1 2019-08-30T03:19:20.421777+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.422010+00:00 my_nsx-intel pace-monitor.sh - - -
"health": "degraded",
<13>1 2019-08-30T03:19:20.422277+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "token-registration"
<13>1 2019-08-30T03:19:20.422512+00:00 my_nsx-intel pace-monitor.sh - - - }
<13>1 2019-08-30T03:19:20.422770+00:00 my_nsx-intel pace-monitor.sh - - - ],
<13>1 2019-08-30T03:19:20.423012+00:00 my_nsx-intel pace-monitor.sh - - -
"status": "Following NSX Intelligence first boot, services are either PENDING or FAILED -
Token-Registration"
<13>1 2019-08-30T03:19:20.423354+00:00 my_nsx-intel pace-monitor.sh - - - }
<13>1 2019-08-30T03:19:20.423601+00:00 my_nsx-intel pace-monitor.sh - - - }

```

```
<13>1 2019-08-30T03:19:20.423882+00:00 my_nsx-intel pace-monitor.sh - - - }
<13>1 2019-08-30T03:19:20.424339+00:00 my_nsx-intel pace-monitor.sh - - - }
<13>1 2019-08-30T03:19:20.972629+00:00 my_nsx-intel pace-monitor.sh - - - NSX
Intelligence health OK.
<30>1 2019-08-30T03:19:20.973076+00:00 my_nsx-intel pace-monitor 20804 - - <13>Aug 30
03:19:19 pace-monitor.sh: NSX Intelligence health OK.
<182>1 2019-08-30T03:23:23.857Z my_nsx-intel NSX 21752 - [nsx@6876 comp="nsx-cli"
subcomp="node-mgmt" username="admin" level="INFO"] CMD: get log-file syslog | find pace-
monitor
```

如果其中的一个服务出现问题，则可能会在运行 `get log-file syslog | grep pace-monitor` 时看到以下行。

```
NSX Intelligence health DEGRADED. Return code not HTTP OK.
```

4 如果遇到以下输出之一，请使用 `restart service service-name` 命令重新启动该服务。

- 在运行 `get services` 命令后，其中的一个服务显示 `Service state: stopped` 或 `Service health: degraded`。
- 在运行 `get log-file syslog | grep pace-monitor` 命令后，输出将显示类似于 `PACE health DEGRADED.Return code not HTTP OK.` 的消息。

例如，如果 `postgres` 服务的状态显示为 `stopped`，或者其状态为 `running` 但服务运行状况为 `degraded`，请运行以下命令。

```
restart service postgres
```

重要事项 您必须使用 `restart service service-name` 命令重新启动 **NSX Intelligence** 服务。如果您决定同时使用 `stop service service-name` 和 `start service service-name` 命令，则还必须手动重新启动依赖于 *service-name* 的每项服务。以下列表显示了重新启动 **NSX Intelligence** 服务时必须遵循的依赖关系顺序。

```
zookeeper > druid > kafka > spark > spark-job-scheduler > nsx-config > processing > pace-
server
```

例如，如果在 `nsx-config` 服务停止后又使用 `stop|start service service-name` 命令将其启动，则还必须使用 `restart service service-name` 命令重新启动 `processing` 和 `pace-server` 服务。

此外，如果使用 `restart service service-name` 命令重新启动依赖关系顺序列表中在 `spark-job-scheduler` 服务之前显示的任何服务，则还必须使用 `restart service spark-job-scheduler` 命令手动重新启动 `spark-job-scheduler` 服务。如果不这样做，则会导致 `spark-job-scheduler` 服务进入错误状态。

收集 NSX Intelligence 支持包

您可以使用 NSX Intelligence CLI 收集支持包。

支持包文件内容不包含数据。它包含以下目录中的文件。

- /opt/vmware/*
- /var/log/*
- /etc/*
- 使用 journalctl 和 systemctl 的系统状态

前提条件

确保您拥有对 NSX Intelligence CLI 的企业管理员访问权限。

步骤

- 1 使用具有企业管理员角色特权的帐户登录到 NSX Intelligence CLI。
- 2 生成支持包。

命令语法如下所示，您需为其中的 support_filename.tgz 提供相应的值。

```
get support-bundle file support_filename.tgz
```

例如，

```
get support-bundle file support_bundle123.tgz
```

在成功创建包文件后，您会收到类似于以下示例的消息。

```
support_bundle123.tgz created, use the following command to transfer the file: copy file
support_bundle123.tgz url <url> After transferring support_bundle123.tgz, extract it
using:tar xvf support_bundle123.tgz
```

- 3 使用以下命令验证支持包是否存在。

```
get files
```

您会收到类似于以下内容的输出。

```
Directory of filestore:/
-rw- 21377586 June 29 05:29:12 UTC support_bundle123.tgz
```